

Е. Е. ТЫРТЫШНИКОВ

ОСНОВЫ АЛГЕБРЫ

$$a_{ijk} = \sum_{\alpha=1}^R u_{i\alpha} v_{j\alpha} w_{k\alpha}$$

$$\bar{S}_k \neq S_k$$

Е. Е. ТЫРТЫШНИКОВ

ОСНОВЫ АЛГЕБРЫ

*Допущено НМС по математике Минобрнауки РФ
в качестве учебника для студентов
высших учебных заведений, обучающихся
по направлениям подготовки
010100 «Математика»,
010400 «Прикладная математика и информатика»*



МОСКВА
ФИЗМАТЛИТ®
2017

УДК 512
ББК 22.14
Т 93

Тыртышников Е.Е. **Основы алгебры.** — М.: ФИЗМАТЛИТ, 2017. — 464 с. — ISBN 978-5-9221-1728-9.

В учебнике систематически излагаются основные понятия алгебры — от элементарных, с которых начинается ее изучение, до не очень простых, включающих теорию полиномиальных уравнений, которая необходима, в частности, для понимания свойств тензорных разложений многомерной матрицы. Каких-либо специальных знаний, кроме школьной программы, от читателя не требуется.

Книга будет интересна широкому кругу студентов, изучающих математику и ее приложения, а также аспирантам и специалистам, желающим углубить свои знания.

Рецензенты:

д.ф.-м.н., профессор механико-математического факультета
МГУ им. М.В. Ломоносова *А. Э. Гутерман*;

д.ф.-м.н., профессор факультета вычислительной математики
и кибернетики МГУ им. М.В. Ломоносова *Х. Д. Икрамов*;

д.ф.-м.н., профессор физического факультета
МГУ им. М.В. Ломоносова *А. Г. Ягола*

ОГЛАВЛЕНИЕ

Предисловие	8
Глава 1. Введение	11
1.1. Предмет алгебры	11
1.2. Арифметические векторы	12
1.3. Линейная зависимость и независимость	16
1.4. Подстановки и перестановки	19
1.5. Определитель и формулы Крамера	22
1.6. Теорема Лапласа	28
1.7. Операции с матрицами	31
1.8. Обратная матрица	37
1.9. Формула Бине–Коши	40
1.10. Ранг матрицы	43
1.11. Однородные системы	48
1.12. Скалярное и векторное произведения	49
1.13. Кривые второго порядка	56
1.14. Ступенчатые матрицы и треугольные разложения	64
1.15. Алгоритмы и оценки сложности вычислений	68
1.16. Комплексные числа и комплексные матрицы	73
Глава 2. Что нужно знать о группах	79
2.1. Определение группы	79
2.2. Избыточность в определении группы	84
2.3. Аддитивные и мультипликативные группы	85
2.4. Изоморфизмы групп	87
2.5. Группа корней n -й степени из единицы	89
2.6. Группы и подгруппы	91
2.7. Смежные классы и нормальные подгруппы	93
2.8. Циклические группы	96
2.9. Действие группы на множестве	98

2.10. Группа движений	101
2.11. Группа дробно-линейных преобразований комплексной плоскости	102
2.12. Гомоморфизмы групп	103
2.13. Теорема Кэли о конечных группах	106
2.14. Конечно порожденные абелевы группы	107
 Глава 3. Кольца, поля, многочлены	111
3.1. Определения кольца и поля	111
3.2. Поле вычетов	116
3.3. Кольцо многочленов	118
3.4. Деление с остатком и алгоритм Евклида	120
3.5. Разложение на неприводимые множители	124
3.6. Многочлены с целыми коэффициентами	126
3.7. Круговые многочлены	129
3.8. Поле частных	130
3.9. Многочлены от нескольких переменных	132
3.10. Матрица Сильвестра и результат	136
3.11. Симметрические многочлены	139
 Глава 4. Линейные пространства, поля и их расширения	144
4.1. Линейные пространства и подпространства	144
4.2. Базисы и размерность	148
4.3. Конечные и алгебраические расширения полей	153
4.4. Присоединение корня	156
4.5. Поле разложения	159
4.6. Производная многочлена и кратные корни	162
4.7. Неприводимость круговых многочленов	164
4.8. Малая теорема Веддерберна	165
4.9. Конечные поля	166
4.10. Мультипликативная группа конечного поля	168
4.11. Расширения полей в геометрии	170
4.12. Основная теорема алгебры	171
 Глава 5. Линейные операторы	177
5.1. Определение линейного оператора	177
5.2. Операторы и матрицы	180

5.3. Характеристический многочлен	184
5.4. Матричные многочлены и подобие	189
5.5. Собственные значения и собственные векторы	193
5.6. Теорема Шура и нормальные матрицы	196
5.7. Сингулярное разложение	200
5.8. Инвариантные пространства и прямая сумма операторов	206
5.9. Нильпотентные операторы и корневое разложение	210
5.10. Пространства Крылова и максимальное расщепление	213
5.11. Жорданова форма	219
5.12. Блочная жорданова форма вещественной матрицы	221
5.13. Вычисление минимального многочлена	224
5.14. Резольвенты Лагранжа	228
Глава 6. Нормы и неравенства	236
6.1. Расстояния, нормы, длины	236
6.2. Сходимость, полнота, пополнение	240
6.3. Ограниченность, замкнутость, компактность	244
6.4. Нормы линейных операторов	250
6.5. Выпуклые множества и выпуклые функции	253
6.6. Неравенства Гёльдера и Минковского	259
6.7. Наилучшие приближения на выпуклых множествах	261
6.8. Разделяющие и опорные гиперплоскости	263
6.9. Продолжение линейных функционалов	266
6.10. Системы линейных неравенств	269
6.11. Грани полиэдра и выпуклые многогранники	273
6.12. Сопряженный оператор и нормальные операторы	276
6.13. Собственные значения эрмитовых матриц	280
6.14. Конгруэнтность и закон инерции	286
6.15. Мажоризация и двоякостochasticеские матрицы	289
6.16. Унитарно инвариантные нормы	294
Глава 7. Группы, поля, уравнения	299
7.1. Линейная независимость автоморфизмов поля	299
7.2. Неподвижные поля и группы автоморфизмов	301
7.3. Группы Галуа и поля разложения	304
7.4. Вычисление группы Галуа	309
7.5. Теория Галуа	313

7.6. Прimitивные расширения	315
7.7. Циклические и радикальные расширения	317
7.8. Полициклические расширения	319
7.9. Теорема Абеля–Галуа	322
7.10. Казус Руффини	327
7.11. Концептуальный вывод основной теоремы алгебры	330
7.12. Теорема Силова	332
 Глава 8. Кольца и идеалы	336
8.1. Идеалы и вычеты	336
8.2. Идеалы и модули	339
8.3. Радикалы и нильпотенты	341
8.4. Простые и примарные идеалы	342
8.5. Кольца частных, расширения и сужения идеалов	347
8.6. Максимальные идеалы и локальные кольца	350
8.7. Упорядоченные множества	353
8.8. Неконструктивные построения	357
8.9. Алгебраическое замыкание поля	360
8.10. Алгебраическая зависимость и независимость	362
8.11. Целая алгебраическая зависимость	366
8.12. Дифференцирования в кольцах и полях	372
8.13. Теорема Гильберта о базисе	375
8.14. Деление с остатком и базисы Грёбнера	377
8.15. Критерий Бухбергера	381
 Глава 9. Алгебраические многообразия	386
9.1. Множества нулей и аннуляторы	386
9.2. Условие совместности	389
9.3. Теорема Нётер о нормализации	391
9.4. Теорема Гильберта о нулях	394
9.5. Неприводимые многообразия	397
9.6. Координатные кольца и полиномиальные отображения	399
9.7. Рациональные отображения	403
9.8. Проекции многообразия	405
9.9. Конструктивные множества	411
9.10. Размерность и степень	413
9.11. Размерность собственного подмногообразия	421

9.12. Размерность многообразия и ранг матрицы Якоби	422
9.13. Размерность пересечения многообразий	425
9.14. Комплексные многообразия	431
9.15. Подготовительная теорема Вейерштрасса	435
9.16. Применение теорем о неявной функции	439
9.17. Главные тензорные ранги трехмерных матриц	446
Список литературы	449
Предметный указатель	451

ПРЕДИСЛОВИЕ

Эту книгу я посвящаю тем, кто любит алгебру, и особенно тем, кто начинает изучать ее в университете, обычно на первом курсе. Читать им лекции — особое удовольствие! Оттого что видишь, как каждый из них искренне тянется к знанию и как зажигаются чудесные огоньки в глазах, когда возникает понимание. Уже через пару лет с горечью замечаешь, что у многих тяга к знанию ослабла и огоньков совсем мало. Наверное, мы как-то не так учим? Я далек от того, чтобы преувеличивать значение дидактики. Но согласитесь, трудный путь к пониманию очень часто освещается вдруг всего лишь одним верным словом. Мне хотелось найти это слово.

Мои слушатели — студенты Московского университета им. М. В. Ломоносова, поступившие на факультет вычислительной математики и кибернетики. Здесь с самого начала сложился хороший, сильный курс линейной алгебры, включающий также элементы геометрии. Мы должны с благодарностью вспомнить того, кто фактически его создал — Валентина Васильевича Воеводина, моего учителя и наставника.

По понятным причинам алгебра изучается в основном линейная. Но курс включает, конечно, и все основные ее понятия. Более того, в последние годы все больше ощущается потребность в углублении именно этой части. В какой-то момент, после нескольких лет чтения лекций я понял, что стиль изложения основных понятий алгебры, когда о них бегло сообщается среди другого материала, не очень удачен. Все говорило о том, что для большей части слушателей они стремительно ускользают в область непознанного. Тогда я решил, что группы, кольца, поля и т. д. должны получить отдельное, систематическое изложение — конечно, после введения, которое включает понятия арифметического и геометрического вектора, операции с матрицами и теорию определителей. Прочитав первую лекцию собственно о группах, я случайно услышал, как один из студентов ска-

зал соседу: «Какая замечательная лекция, мне наконец удалось понять!» Можно и не говорить, как это было приятно и как воодушевило, чтобы начать книгу.

Книга содержит девять глав, первые шесть адресованы непосредственно первокурсникам. В последних трех сложность изрядно возрастает. Но и там я очень старался писать честно и просто. В каком-то смысле все включенное в книгу есть некий теоретический минимум и навеяно вопросами, которые вроде бы должны, на первый взгляд, решаться известными средствами теории матриц и линейной алгебры. Но не решаются.

Вот один из вопросов. Имеется пространство $n \times n$ -матриц с комплексными элементами и в нем берется произвольное подпространство размерности $(n - 1)^2 + 1$. Попробуйте доказать, что в этом подпространстве обязательно найдется матрица ранга 1.

Другой вопрос связан с *трехмерными матрицами* — так называются таблицы с элементами $a(i, j, k)$, где индексы i, j, k изменяются, скажем, от 1 до n . Трехмерная матрица ранга 1 — это, по определению, таблица с элементами вида $u(i)v(j)w(k)$ с хотя бы одним ненулевым элементом. Любую трехмерную матрицу можно записать в виде суммы трехмерных матриц ранга 1 и наименьшее возможное число слагаемых называется *тензорным рангом* заданной трехмерной матрицы. Будем рассматривать таблицы с комплексными элементами. Можно ли вычислить тензорный ранг за конечное число арифметических операций?

Кроме того, мы знаем, что в любой сколь угодно малой окрестности комплексной $n \times n$ -матрицы есть матрица ранга n . По аналогии можно предположить, что в любой окрестности комплексной трехмерной матрицы размера $n \times n \times n$ имеется трехмерная матрица ранга r , где r зависит от n . Почему это так? Какой вид имеет функция $r = r(n)$?

Какую алгебру необходимо знать, чтобы изучать эти вопросы? В восьмой и девятой главах почти все — необходимый минимум для ответов. Как видим, знать требуется весьма немало и все это совершенно необходимо! Знания сосредоточены нередко в середине или в конце пятисотстраничных монографий или учебников. Извлечение нужного минимума может оказаться нелегким делом. Поэтому у меня есть надежда, что эта книга, возможно, встретит благодарного читателя.

Разных и хороших книг по алгебре, впрочем и к счастью, много. Что бы я ни говорил в оправдание, книга возникла из какой-то непостижимой внутренней потребности и странной

уверенности в том, что именно она будет полезна изучающим алгебру. Получилось или нет — судить читателю.

Искреннюю благодарность выражаю всем, кто нашел время познакомиться с рукописью книги и высказать свои замечания и предложения. Особо признателен Х. Д. Икрамову и А. Э. Гутерману, сделавшим самое большое число замечаний, улучшивших книгу, и Н. Е. Тиртышниковой за помощь в составлении предметного указателя.

Данную книгу можно рассматривать как теоретический минимум для тех, кто намерен профессионально заниматься исследованиями алгебраических методов представления и аппроксимации многомерных данных и связанных с ними вопросов оптимизации, и я считаю приятным долгом отметить поддержку этих исследований Российским научным фондом (проект 14-11-00806).

Е. Е. Тиртышников

Глава 1

ВВЕДЕНИЕ

1.1. Предмет алгебры

Если судить по первым впечатлениям об алгебре в школе, то это прежде всего *наука о вычислениях с буквами*. Из букв a, b, c, d можно составлять выражения типа

$$0, \quad 0 + 0 \cdot a, \quad 1 + 2a + 4a^2, \\ (a^2 - b^2)(c + d) + (a + b)^2(c^3 - d^3) \quad \text{и т. п.}$$

Если деление не используется, то получаются *многочлены* от букв a, b, c, d . Первый пример показывает, что в выражении букв может и не быть. Числа в выражении называются *коэффициентами* многочлена. Если после приведения подобных членов все они равны нулю, то многочлен называется *нулевым*.

Число букв в каждом выражении должно быть конечным, но может выбираться из бесконечно большого запаса букв. Тогда, очевидно, придется какие-то буквы снабжать индексами, например a_1, a_2 и т. п. Если помимо сложения, вычитания, умножения используется также и деление, то получаются *рациональные функции* — формальные дроби, где в числителе и знаменателе стоят многочлены и при этом многочлен в знаменателе не должен быть нулевым. Вот пример рациональной функции:

$$\frac{a}{b + \frac{c}{d}} = \frac{ad}{bd + c}.$$

Одно из излюбленных упражнений в школе — упростить выражение. Как выясняется, для этого есть некоторый набор правил — можно утверждать, что в общих и достаточно абстрактных ситуациях подобные правила изучаются в разных разделах алгебры. Еще один тип упражнений — найти значение выражения, когда буквам придаются какие-то числовые значения. В общей

ситуации значения берутся из некоторых *множеств*, для элементов которых определены *операции*. Важнейшей частью алгебры является *изучение абстрактных операций и их свойств*.

Использование букв стремительно упрощает решение многих задач, которые без них требуют иногда немалого напряжения — это серьезная демонстрация силы алгебры для тех, кто знакомится с ней в школе. Условия задачи записываются в виде уравнений, содержащих буквы. Затем нужно находить решения уравнений. Таким образом, алгебра — это также *наука о решении уравнений*. В том числе и о возможности их решения с помощью последовательности действий из заранее определенного запаса. Например, было много попыток искать корни многочленов с помощью арифметических операций над коэффициентами и получения *радикалов*, т.е. решений специальных уравнений вида $x^n = a$. Развитие алгебры пресекло эти попытки, так как было доказано, что для многочленов степени 5 и выше этого сделать нельзя — эти вопросы требуют уже солидной алгебраической подготовки. Минимальный объем знаний соответствует первым пяти главам этой книги, вопрос о решении уравнений в радикалах мы сможем разобрать детально только в гл. 7.

Другой, более простой пример — вопросы о геометрических построениях с помощью циркуля и линейки, в том числе невозможность построения правильного 7-угольника и одно из первых открытий Гаусса — то, что правильный 17-угольник построить можно. К решению этих вопросов мы будем готовы уже в гл. 4.

Более трудная задача — понять, как устроено множество решений системы полиномиальных уравнений. Этим вопросам посвящены главы 8 и 9.

Теперь мы, пожалуй, оставим не очень благодарное дело описания предмета алгебры. Самое разумное (и малополезное) определение предмета — сказать, что это ровно то, что мы будем изучать.

1.2. Арифметические векторы

Начнем с простой системы уравнений, например такой:

$$x + 2y = 3,$$

$$3x + y = 4.$$

Наша цель совсем не в том, чтобы найти решение (в данном случае $x = y = 1$). Как *записать* подобную систему общего вида, когда у нас n неизвестных?

Неизвестные обозначим через $x_1, \dots, x_n$. А для известных коэффициентов при них используем букву с двумя индексами, скажем a_{ij} , — пусть индекс i указывает на номер уравнения, а j на неизвестную x_j . Заметим, что идею о двойной индексации для записи уравнений Лейбниц считал большим открытием. В 17 веке эта идея казалась потрясающе новой! Теперь мы воспринимаем ее как нечто само собой разумеющееся. Итак, рассмотрим систему вида

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2, \\ &\dots \quad \dots \quad \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= b_m. \end{aligned} \quad (*)$$

По определению, это *система линейных алгебраических уравнений* относительно неизвестных $x_1, \dots, x_n$ с коэффициентами a_{ij} и элементами $b_1, \dots, b_m$ правой части.

Коэффициенты системы (*) удобно записывать в виде прямоугольной таблицы

$$\begin{bmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{bmatrix}.$$

В 19 веке такие таблицы стали называть *матрицами*. Оставив только часть строк и столбцов, можно получать *подматрицы* данной матрицы. Если в таблице m строк и n столбцов, то говорят, что это *матрица размера $m \times n$* или *$m \times n$ -матрица*. Множество всех $m \times n$ -матриц с элементами a_{ij} из множества M обозначается $M^{m \times n}$. Если $m = n$, то матрица называется *квадратной*. Ее размер определяется одним числом, которое называется *порядком матрицы*.

Если система (*) совместна, то как описать множество всех ее решений? Пусть $x_i \in \mathbb{R}$, где $\mathbb{R}$ — стандартное обозначение для множества всех вещественных чисел. Конечно же, нас интересует отображение $i \rightarrow x_i$, которое полностью задается упорядоченной числовой последовательностью

$$x = (x_1, x_2, \dots, x_n), \quad x_1, \dots, x_n \in \mathbb{R}.$$

Будем говорить, что x — это вещественный *арифметический вектор* с n координатами. Если все координаты равны нулю, то вектор называется *нулевым* и обозначается так же, как число 0. Множество всех вещественных арифметических векторов с n координатами обозначим через $V_n = V_n(\mathbb{R})$.

Для функций с числовыми значениями естественным образом определяются операция сложения и операция умножения функции на число. Эти же операции мы будем выполнять с арифметическими векторами. По определению,

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) := (x_1 + y_1, \dots, x_n + y_n),$$

$$\alpha(x_1, \dots, x_n) := (\alpha x_1, \dots, \alpha x_n), \quad \alpha \in \mathbb{R}.$$

Рассмотрим произвольное непустое подмножество $V \subseteq V_n$ такое, что для любых векторов из V их сумма принадлежит V и при умножении на любое число вектор из V остается в множестве V . В таких случаях будем называть V *подпространством арифметического пространства V_n* или *векторным пространством*. Обратим внимание на то, что векторное пространство $V \subseteq V_n$ является арифметическим пространством только в том случае, когда $V = V_n$. Векторное пространство называется *нулевым*, если оно состоит из одного лишь нулевого вектора.

Система (*) с нулевой правой частью $b_1 = \dots = b_m = 0$ называется *однородной*. Вот первое вполне содержательное наблюдение.

Утверждение 1.2.1. *Однородная система линейных алгебраических уравнений всегда совместна и ее множество решений представляет собой векторное пространство. Если система (*) совместна, $x^{(0)}$ — ее частное решение и V — множество всех решений соответствующей однородной системы, то множество всех решений системы (*) имеет вид*

$$x^{(0)} + V := \{x^{(0)} + y: y \in V\}.$$

Доказательство. Нулевой вектор является решением любой однородной системы и если $(x_1, \dots, x_n)$, $(y_1, \dots, y_n)$ — два решения и α — число, то векторы $(x_1 + y_1, \dots, x_n + y_n)$ и $(\alpha x_1, \dots, \alpha x_n)$ будут решениями той же однородной системы. Далее, разность любых двух решений системы (*) будет решением соответствующей однородной системы, и если к фиксированному частному решению системы (*) прибавить произвольное

решение однородной системы, то, очевидно, получится решение системы (*). $\square$

Как видим, векторные пространства можно задавать как множества решений однородных систем. Еще один способ их получения — строить всевозможные векторы вида

$$a = \alpha_1 a_1 + \dots + \alpha_k a_k,$$

где $a_1, \dots, a_k \in V_n$ — фиксированные арифметические векторы, а $\alpha_1, \dots, \alpha_k$ — произвольные числа. Вектор a называется *линейной комбинацией* векторов $a_1, \dots, a_k$, а числа $\alpha_1, \dots, \alpha_k$ — коэффициентами этой линейной комбинации. Если все коэффициенты равны нулю, то линейная комбинация называется *тривиальной*. Множество всевозможных линейных комбинаций заданных векторов называется их *линейной оболочкой*.

Утверждение 1.2.2. *Линейная оболочка арифметических векторов $a_1, \dots, a_k \in V_n$ является векторным пространством.*

Утверждение 1.2.3. *Для системы линейных алгебраических уравнений вида (*) введем арифметические векторы*

$$a_1 := (a_{11}, a_{21}, \dots, a_{m1}), \dots, a_n := (a_{1n}, a_{2n}, \dots, a_{mn}),$$

$$b := (b_1, \dots, b_m).$$

Тогда система будет совместной в том и только том случае, когда вектор b является линейной комбинацией векторов $a_1, \dots, a_n$ с коэффициентами $x_1, \dots, x_n$.

Проверка утверждений тривиальна и предоставляется читателю.

Арифметические векторы имеют очевидную связь с *геометрическими векторами*. Упорядоченная пара точек A, B в геометрическом пространстве определяет *направленный отрезок $\overline{AB}$* , все направленные отрезки одинаковой длины и одного и того же направления *отождествляются* и называются геометрическим вектором или просто *вектором*.

Сделаем общее замечание в связи с отождествлением формально разных объектов. В совершенно абстрактной форме оно означает, что среди множества объектов $\mathcal{M}$ выделены какие-то упорядоченные пары (a, b) , которые определяют *бинарное отношение* между объектом a и объектом b . Пусть запись $a \sim b$ означает, что пара (a, b) является выделенной. Тогда в случае

отождествления объектов a и b от бинарного отношения требуется выполнение трех свойств:

- $a \sim a \quad \forall a \in M$ (рефлексивность);
- $a \sim b \Rightarrow b \sim a$ (симметричность);
- $a \sim b, b \sim c \Rightarrow a \sim c$ (транзитивность).

Бинарное отношение с такими свойствами называется *отношением эквивалентности*. При этом множество M разбивается на непересекающиеся подмножества, которые называются *классами эквивалентности*. Каждый класс состоит из элементов, эквивалентных между собой и неэквивалентных никакому элементу другого класса. Таким образом, каждому геометрическому вектору соответствует класс эквивалентных направленных отрезков.

Ясно, что любой геометрический вектор можно задать *радиус-вектором* — направленным отрезком с выделенной общей начальной точкой. При выборе системы координат с началом в этой точке вектор однозначно задается своими координатами, т.е. некоторым арифметическим вектором. Заметим, кстати, что линейная оболочка пары линейно независимых геометрических векторов с общей точкой — это не что иное, как плоскость, параллельная этим векторам и проходящая через общую точку.

Задача 1. Докажите, что линейная оболочка любой конечной системы арифметических векторов может быть задана как множество всех решений некоторой однородной системы линейных алгебраических уравнений.

1.3. Линейная зависимость и независимость

Система арифметических векторов $a_1, \dots, a_k$ называется *линейно зависимой*, если нулевой вектор можно представить в виде нетривиальной линейной комбинации этих векторов, т.е. $\alpha_1 a_1 + \dots + \alpha_k a_k = 0$, и хотя бы один из коэффициентов отличен от нуля. Система, не являющаяся линейно зависимой, называется *линейно независимой*.

Утверждение 1.3.1. Любая часть (подсистема) линейно независимой системы является также линейно независимой. Любая система, в которой есть линейно зависимая подсистема, является линейно зависимой.

Утверждение 1.3.2. Пусть система содержит более одного вектора. Тогда для ее линейной зависимости необходимо

и достаточно, чтобы какой-то вектор был линейной комбинацией остальных векторов.

Доказательство. Пусть система $a_1, \dots, a_k$ линейно зависима. Тогда существуют не равные одновременно нулю числа $\alpha_1, \dots, \alpha_k$, такие что $\alpha_1 a_1 + \dots + \alpha_k a_k = 0$. Пусть $\alpha_j \neq 0$. Тогда, очевидно,

$$a_j = \sum_{1 \leq i \leq k, i \neq j} \left(-\frac{\alpha_i}{\alpha_j} \right) a_i.$$

Необходимость доказана. Достаточность:

$$a_j = \sum_{1 \leq i \leq k, i \neq j} \alpha_i a_i \Rightarrow (-1) \cdot a_j + \sum_{1 \leq i \leq k, i \neq j} \alpha_i a_i = 0. \quad \square$$

Утверждение 1.3.3. Пусть система $a_1, \dots, a_k$ содержит более одного вектора и при этом $a_1 \neq 0$. Тогда для ее линейной зависимости необходимо и достаточно, чтобы некоторый вектор a_j при $2 \leq j \leq k$ был линейной комбинацией предыдущих векторов $a_1, \dots, a_{j-1}$.

Доказательство. Рассмотрим нетривиальную линейную комбинацию

$$\alpha_1 a_1 + \dots + \alpha_k a_k = 0.$$

Если $\alpha_k \neq 0$, то вектор a_k является линейной комбинацией предыдущих векторов $a_1, \dots, a_{k-1}$. В общем случае пусть $\alpha_l \neq 0$ и $\alpha_{l+1} = \dots = \alpha_k = 0$. Тогда $l \neq 1$, иначе $\alpha_1 a_1 = 0 \Rightarrow a_1 = 0$ — нарушено условие $a_1 \neq 0$. Итак, $l \geq 2$ и вектор a_l является линейной комбинацией предыдущих векторов $a_1, \dots, a_{l-1}$. $\square$

Лемма 1.3.1. Пусть система векторов $a_1, \dots, a_k$ линейно независима и каждый из векторов a_i есть линейная комбинация векторов $b_1, \dots, b_m$. Тогда $k \leq m$.

Доказательство. Система $a_1, b_1, \dots, b_m$, очевидно, линейно зависима. Поэтому какой-то из этих векторов есть линейная комбинация предыдущих векторов. Не ограничивая общности, предположим, что это вектор b_m . Тогда каждый из векторов $a_2, \dots, a_k$ есть линейная комбинация векторов $a_1, b_1, \dots, b_{m-1}$.

Поэтому система $a_2, a_1, b_1, \dots, b_{m-1}$ линейно зависима, и значит, какой-то ее вектор линейно выражается через предыдущие. Пусть это будет b_{m-1} . Тогда каждый из векторов $a_3, \dots, a_k$ есть линейная комбинация векторов $a_2, a_1, b_1, \dots, b_{m-2}$. Если $m < k$, то после m повторений описанной процедуры мы увидим,

что вектор a_{m+1} является линейной комбинацией векторов $a_1, \dots, a_m$, что противоречит условию леммы. $\square$

Максимальное число линейно независимых векторов в векторном пространстве V называется его *размерностью*. Обозначение: $\dim V$. Равенство $k = \dim V$ означает, что в V можно найти k линейно независимых векторов и любая система, в которой более чем k векторов, является линейно зависимой. Система векторов $a_1, \dots, a_k \in V$ называется *базисом* векторного пространства V , если любой вектор из V представляется линейной комбинацией ее векторов, а сама система линейно независима.

Пример. Пусть $V \subseteq V_n$ — множество решений уравнения $x_1 + \dots + x_n = 0$. Очевидно, векторы

$$a_1 = (-1, 1, 0, \dots, 0), \quad a_2 = (-1, 0, 1, 0, \dots, 0), \quad \dots \\ \dots, \quad a_{n-1} = (-1, 0, \dots, 0, 1)$$

являются решениями. Они линейно независимы:

$$\alpha_1 a_1 + \dots + \alpha_{n-1} a_{n-1} = \left(-\sum_{i=1}^{n-1} \alpha_i, \alpha_1, \dots, \alpha_{n-1} \right) = 0 \Rightarrow \\ \Rightarrow \alpha_1 = \dots = \alpha_{n-1} = 0.$$

Если $x = (x_1, \dots, x_n)$ — произвольное решение, то равенство $\alpha_1 a_1 + \dots + \alpha_{n-1} a_{n-1} = x$ равносильно системе уравнений

$$-\sum_{i=1}^{n-1} \alpha_i = x_1, \quad \alpha_1 = x_2, \quad \dots, \quad \alpha_{n-1} = x_n,$$

которая решается без труда. Таким образом, система $a_1, \dots, a_{n-1}$ образует базис векторного пространства V .

Теорема 1.3.1. *Любое ненулевое векторное пространство обладает базисом, и число векторов в любом его базисе равно его размерности.*

Доказательство. Возьмем произвольный ненулевой вектор $a_1 \in V \subseteq V_n$ и рассмотрим всевозможные системы вида a_1, a , где $a \in V$. Пусть все такие системы линейно зависимы. Тогда любой вектор a линейно выражается через a_1 . В этом случае получаем базис из одного вектора a_1 . Если же имеется линейно независимая система вида a_1, a_2 , то будем рассматривать

всевозможные системы вида a_1, a_2, a , где $a \in V$. Если все они линейно зависимы, то система a_1, a_2 образует базис. В противном случае имеется линейно независимая система a_1, a_2, a_3 . Продолжая в том же духе, на некотором шаге мы получим линейно независимую систему, через которую линейно выражается любой вектор из V . Это произойдет потому, что каждый вектор из $V \subseteq V_n$ является линейной комбинацией векторов $e_1 = (1, 0, \dots, 0)$, $e_2 = (0, 1, 0, \dots, 0)$, $\dots$, $e_n = (0, \dots, 0, 1)$ и, в силу леммы 1.3.1, число линейно независимых векторов, принадлежащих пространству $V \subseteq V_n$, не может быть больше n . То, что любые два базиса имеют одно и то же число векторов, также следует из леммы 1.3.1. $\square$

Следствие 1.3.1. $\dim V_n = n$.

Следствие 1.3.2. Любую линейно независимую систему векторов из векторного пространства V можно достроить до базиса.

Следствие 1.3.3. В линейной оболочке векторов $a_1, \dots, a_k$ существует базис, составленный из них или какой-то их части.

Задача 2. Для векторного пространства решений уравнения $x_1 + \dots + x_n = 0$ найдите базис с максимально возможным общим числом нулевых координат.

1.4. Подстановки и перестановки

В дальнейшем нам будут нужны некоторые свойства взаимно однозначных отображений конечного множества на себя. Такие отображения называются *подстановками*. Название объясняется такой интерпретацией отображения: каждый элемент остается на месте либо вместо него подставляется другой элемент того же множества. Множество всех подстановок n -элементного множества $\{a_1, \dots, a_n\}$ обозначается $S_n = S_n(a_1, \dots, a_n)$. Если в множестве n элементов, то их можно снабдить номерами от 1 до n и считать, что $a_1 = 1, \dots, a_n = n$. Отображение $\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ полностью определяется таблицей

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix},$$

которую мы также будем обозначать через σ . Числа $\sigma(1), \dots, \sigma(n)$ образуют *перестановку* номеров $1, \dots, n$. То же отображение задается, очевидно, любой таблицей с переставленными столбцами:

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ \sigma(i_1) & \sigma(i_2) & \dots & \sigma(i_n) \end{pmatrix}, \quad \{i_1, \dots, i_n\} = \{1, \dots, n\}.$$

Понятно, что композиция (последовательное выполнение) взаимно однозначных отображений будет также взаимно однозначным отображением. Композиция подстановок f и g — это новая подстановка σ , которая определяется правилом

$$\sigma(i) := f(g(i)), \quad i \in \{1, \dots, n\}.$$

Назовем σ *произведением* подстановок f и g и будем писать $\sigma = fg$. Таким образом, на множестве $S_n = S_n(1, \dots, n)$ у нас есть *операция умножения подстановок*. Обратим внимание на то, что умножение подстановок, в отличие от умножения вещественных чисел, в общем случае *некоммутативно*, например:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq \\ \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Подстановка

$$e := \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

реализует тождественное отображение и называется *единичной*. Ее роль аналогична роли числа 1 при умножении чисел: подстановка не меняется при умножении ее на единичную подстановку e справа или слева. Для любой подстановки $\sigma: i \rightarrow \sigma(i)$ можно определить подстановку $\sigma(i) \rightarrow i$, представляющую собой обратное отображение. Такая подстановка называется *обратной* и обозначается σ^{-1} . Ясно, что обратная подстановка задается таблицей

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}$$

и всегда выполняются равенства

$$\sigma\sigma^{-1} = \sigma^{-1}\sigma = e.$$

Пусть $i_1, \dots, i_k \in \{1, \dots, n\}$ — какие-то разные номера. Подстановка σ называется *циклом длины k* , если $\sigma(i) = i \forall i \notin \{i_1, \dots, i_k\}$, а действие на выделенных номерах циклическое:

$$\sigma: i_1 \rightarrow i_2 \rightarrow \dots \rightarrow i_{k-1} \rightarrow i_k \rightarrow i_1.$$

Цикл σ принято записывать следующим образом: $\sigma = (i_1, \dots, i_k)$. В этой записи нет информации об общем числе номеров n множества $\{1, \dots, n\}$, но действие на любом таком множестве определяется однозначно. Циклы $(i_1, \dots, i_k)$ и $(j_1, \dots, j_l)$ называются *независимыми*, если $\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_l\} = \emptyset$. Цикл длины 2 называется также *транспозицией*.

Утверждение 1.4.1. *Любая подстановка является произведением независимых циклов.*

Доказательство. Сначала строим цикл, в котором есть номер 1. Затем строим цикл, в котором есть номер, не входящий в первый цикл. И так далее. $\square$

Утверждение 1.4.2. *Любой цикл есть произведение транспозиций.*

Доказательство. $(i_1, i_2, \dots, i_k) = (i_1, i_2)(i_2, i_3) \dots$
 $\dots (i_{k-2}, i_{k-1})(i_{k-1}, i_k)$. $\square$

Теорема 1.4.1. *Любая подстановка записывается в виде произведения транспозиций и четность числа транспозиций в произведении не зависит от способа его получения.*

Доказательство. Отмеченные выше утверждения доказывают первую часть теоремы: любая подстановка разложима в произведение транспозиций. Чтобы доказать нетривиальную вторую часть о четности числа транспозиций, введем понятие *инверсии* для подстановки σ — так называется пара номеров (i, j) , таких что $i < j$, но $\sigma(i) > \sigma(j)$. Общее число инверсий для подстановки σ обозначим через $\delta(\sigma)$.

Будем считать, что $i < j$, и рассмотрим произвольную транспозицию $\tau = (i, j)$. Докажем, что при умножении произвольной подстановки σ на τ четность числа инверсий меняется, т. е. число $\delta(\sigma\tau) - \delta(\sigma)$ является нечетным. Если $j = i + 1$, то утверждение очевидно: если пара (i, j) была инверсией для σ , то она перестает быть инверсией для $\sigma\tau$, и наоборот. В общем случае находим

$$\begin{aligned} \sigma\tau &= \sigma \cdot \underbrace{(j, j-1) \cdot (j-1, j-2) \cdot \dots \cdot (i+2, i+1)}_{=f} \times \\ &\quad \times \underbrace{(i, i+1) \cdot (i+1, i+2) \cdot \dots \cdot (j-1, j)}_{=g}. \end{aligned}$$

Подстановка g перемещает j -й элемент на i -е место с помощью транспозиций соседних элементов. Для этого нужно $j - i$ транспозиций. Далее, подстановка f перемещает $(i + 1)$ -й элемент

на j -е место — опять с помощью транспозиций соседних элементов. Теперь нужно $j - i - 1$ таких транспозиций. В итоге $\sigma\tau$ получается из σ с помощью последовательных умножений на транспозиции соседних элементов и число таких транспозиций равно $2(j - i) - 1$. $\square$

Подстановка с четным числом транспозиций называется *четной*, а с нечетным числом транспозиций — *нечетной*.

Задача 3. Найдите минимальное число транспозиций в разложении подстановки, которая является произведением двух независимых циклов длины k и l соответственно.

1.5. Определитель и формулы Крамера

Рассмотрим систему линейных алгебраических уравнений (*) в случае, когда число уравнений совпадает с числом неизвестных. Нетрудно понять, что каждая из неизвестных должна быть рациональной функцией (отношением двух многочленов) от букв a_{ij} и b_i . Это, конечно, не означает совместности при любых числовых значениях, приданных этим буквам, — ведь знаменатели могут обратиться в нуль!

Вид упомянутых рациональных функций был обнаружен Г. Крамером в 1750 г. По предложению К. Ф. Гаусса полученные Крамером многочлены в числителях и знаменателях этих рациональных функций через 50 лет после их открытия были названы *определителями*.

Чтобы понять, как выглядят эти многочлены, полезно начать с частных случаев. Пусть $m = n = 2$. Тогда мы имеем систему

$$a_{11}x_1 + a_{12}x_2 = b_1,$$

$$a_{21}x_1 + a_{22}x_2 = b_2.$$

Чтобы получить x_1 , сложим уравнения, предварительно умножив первое из них на a_{22} и второе на $-a_{12}$. Формула для x_2 получается аналогично. Вот результат:

$$x_1 = \frac{b_1 a_{22} - b_2 a_{12}}{a_{11} a_{22} - a_{21} a_{12}}, \quad x_2 = \frac{a_{11} b_2 - a_{21} b_1}{a_{11} a_{22} - a_{21} a_{12}}.$$

Числители и знаменатели можно рассматривать как функции арифметических векторов $a_1 := (a_{11}, a_{21})$, $a_2 := (a_{12}, a_{22})$, $b := (b_1, b_2)$. Пусть знаменатель определяется функцией $f(a_1, a_2) :=$

$:= a_{11}a_{22} - a_{12}a_{21}$. Тогда можно заметить, что числители имеют вид $f(b, a_2)$ и $f(a_1, b)$. Таким образом,

$$x_1 = \frac{f(b, a_2)}{f(a_1, a_2)}, \quad x_2 = \frac{f(a_1, b)}{f(a_1, a_2)}.$$

В случае произвольной системы, в которой число уравнений и неизвестных равно n , мы можем ввести арифметические векторы

$$a_1 = (a_{11}, \dots, a_{n1}), \quad \dots, \quad a_n = (a_{1n}, \dots, a_{nn}), \quad b = (b_1, \dots, b_n)$$

и сформулировать *гипотезу* о том, что выражения для неизвестных имеют вид

$$x_i = \frac{f(a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_n)}{f(a_1, a_2, \dots, a_n)}, \quad i = 1, 2, \dots, n,$$

где $f(a_1, a_2, \dots, a_n)$ — некоторая функция. Если эта гипотеза верна, то функция f должна обладать определенными свойствами.

Во-первых, пусть правая часть имеет вид $b = \alpha_1 b^{(1)} + \alpha_2 b^{(2)}$. Тогда очевидно, что решение должно иметь вид $x = \alpha_1 x^{(1)} + \alpha_2 x^{(2)}$, где $x^{(1)}$ и $x^{(2)}$ — решения для правых частей $b^{(1)}$ и $b^{(2)}$ соответственно. Таким образом, естественно предположить, что

$$\begin{aligned} f(a_1, \dots, a_{i-1}, \alpha_1 b^{(1)} + \alpha_2 b^{(2)}, a_{i+1}, \dots, a_n) = \\ = \alpha_1 f(a_1, \dots, a_{i-1}, b^{(1)}, a_{i+1}, \dots, a_n) + \\ + \alpha_2 f(a_1, \dots, a_{i-1}, b^{(2)}, a_{i+1}, \dots, a_n) \\ \forall \alpha_1, \alpha_2 \in \mathbb{R}, \quad \forall b^{(1)}, b^{(2)} \in V_n. \end{aligned}$$

В таких случаях говорят, что функция f *линейна по i -му аргументу*. Функция от n аргументов, линейная по каждому из них, называется *полилинейной* (также *мультилинейной* или *n -линейной*). В рамках нашей гипотезы естественно предположить, что функция f является полилинейной.

Во-вторых, если $a_j = b$, то мы имеем решение, в котором $x_j = 1$ и $x_i = 0$ при $i \neq j$. Поэтому можно предположить, что f принимает нулевое значение при совпадении i -го и j -го аргументов, конечно при условии $i \neq j$.

В-третьих, в рамках нашей гипотезы f можно смело умножать на произвольный ненулевой множитель — значения неизвестных не изменятся. Значит, без ограничения общности мы

можем ввести какое-то условие нормировки. Например, мы можем считать, что $f(e_1, \dots, e_n) = 1$ на векторах

$$e_1 = (1, 0, \dots, 0), \quad e_2 = (0, 1, 0, \dots, 0), \quad \dots, \quad e_n = (0, \dots, 0, 1).$$

Такие векторы принято называть *естественным базисом* пространства V_n .

Возможно, это покажется удивительным, но три условия определяют функцию f однозначно!

Теорема 1.5.1. *Существует только одна числовая функция $f(a_1, \dots, a_n)$ от арифметических векторов $a_1, \dots, a_n \in V_n$, которая является полилинейной, обнуляется при совпадении значений разных аргументов и равна 1 на векторах естественного базиса пространства V_n .*

Доказательство. Предположим, что функция f с указанными тремя свойствами существует, и докажем ее единственность. Прежде всего заметим, что такая функция обязана менять знак при перестановке любых двух аргументов. Пусть $i < j$. Тогда

$$\begin{aligned} 0 &= f(a_1, \dots, a_{i-1}, a_i + a_j, a_{i+1}, \dots, a_{j-1}, a_i + a_j, a_{j+1}, \dots, a_n) = \\ &= \underbrace{f(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_{j-1}, a_i, a_{j+1}, \dots, a_n)}_{=0} + \\ &+ \underbrace{f(a_1, \dots, a_{i-1}, a_j, a_{i+1}, \dots, a_{j-1}, a_j, a_{j+1}, \dots, a_n)}_{=0} + \\ &+ f(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_{j-1}, a_j, a_{j+1}, \dots, a_n) + \\ &+ f(a_1, \dots, a_{i-1}, a_j, a_{i+1}, \dots, a_{j-1}, a_i, a_{j+1}, \dots, a_n). \end{aligned}$$

Функция, меняющая знак при перестановке любых двух аргументов, называется *знакопеременной* или *кососимметрической*.

Теперь рассмотрим разложения $a_k = \sum_{i_k=1}^n a_{i_k,k} e_{i_k}$, $k = 1, 2, \dots, n$, воспользуемся полилинейностью, исключим из суммы заведомо нулевые члены и примем во внимание знакопеременность:

$$\begin{aligned} f\left(\sum_{i_1=1}^n a_{i_1,1} e_{i_1}, \dots, \sum_{i_n=1}^n a_{i_n,n} e_{i_n}\right) = \\ = \sum_{i_1=1}^n \dots \sum_{i_n=1}^n a_{i_1,1} \dots a_{i_n,n} f(e_{i_1}, \dots, e_{i_n}) = \end{aligned}$$

$$\begin{aligned}
&= \sum_{\sigma \in S_n} a_{\sigma(1),1} \dots a_{\sigma(n),n} f(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = \\
&= \sum_{\sigma \in S_n} a_{\sigma(1),1} \dots a_{\sigma(n),n} (-1)^{\delta(\sigma)}.
\end{aligned}$$

Напомним, что $\delta(\sigma)$ обозначает число инверсий в подстановке σ . Здесь нам очень пригодилась теорема 1.4.1 о разложении подстановки в произведение транспозиций. В силу свойства знакопеременности, каждая транспозиция аргументов меняет знак функции f . Если нужно μ транспозиций, чтобы перейти от системы $e_1, \dots, e_n$ к системе $e_{\sigma(1)}, \dots, e_{\sigma(n)}$, то находим

$$f(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = (-1)^\mu f(e_1, \dots, e_n).$$

Согласно теореме 1.4.1, четность числа μ не зависит от способа перехода $\Rightarrow$

$$(-1)^\mu = (-1)^{\delta(\sigma)}.$$

Таким образом, если функция f с указанными тремя свойствами существует, то она обязана иметь следующий вид:

$$f(a_1, \dots, a_n) = \sum_{\sigma \in S_n} a_{\sigma(1),1} \dots a_{\sigma(n),n} (-1)^{\delta(\sigma)}. \quad (\Delta)$$

Следующий шаг — доказать существование такой функции. Для этого используем правую часть формулы (Δ) как *определение* функции f . Полилинейность проверяется непосредственно:

$$\begin{aligned}
&f(a_1, \dots, a_{j-1}, \alpha_1 b^{(1)} + \alpha_2 b^{(2)}, a_{j+1}, \dots, a_n) = \\
&= \sum_{\sigma \in S_n} a_{\sigma(1),1} \dots a_{\sigma(j-1),j-1} (\alpha_1 b_{\sigma(j)}^{(1)} + \alpha_2 b_{\sigma(j)}^{(2)}) a_{\sigma(n),n} (-1)^{\delta(\sigma)} = \\
&= \alpha_1 \sum_{\sigma \in S_n} a_{\sigma(1),1} \dots a_{\sigma(j-1),j-1} b_{\sigma(j)}^{(1)} a_{\sigma(n),n} (-1)^{\delta(\sigma)} + \\
&+ \alpha_2 \sum_{\sigma \in S_n} a_{\sigma(1),1} \dots a_{\sigma(j-1),j-1} b_{\sigma(j)}^{(2)} a_{\sigma(n),n} (-1)^{\delta(\sigma)} = \\
&= \alpha_1 f(a_1, \dots, a_{j-1}, b^{(1)}, a_{j+1}, \dots, a_n) + \\
&+ \alpha_2 f(a_1, \dots, a_{j-1}, b^{(2)}, a_{j+1}, \dots, a_n).
\end{aligned}$$

Далее, пусть $i < j$ и $a_i = a_j = b$. Обозначим через $A_n \subset S_n$ множество всех четных подстановок, зафиксируем транспозицию $\tau := (i, j)$ и заметим, что

$$S_n \setminus A_n = \{\sigma\tau : \sigma \in A_n\}.$$

Тогда

$$\begin{aligned} f(a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_{j-1}, b, a_{j+1}, \dots, a_n) &= \\ &= \sum_{\sigma \in S_n} a_{\sigma(1),1} \dots a_{\sigma(i-1),i-1} \underline{b_{\sigma(i)}} a_{\sigma(i+1),i+1} \dots \\ &\dots a_{\sigma(j-1),j-1} \underline{b_{\sigma(j)}} a_{\sigma(j+1),j+1} \dots a_{\sigma(n),n} (-1)^{\delta(\sigma)} = \\ &= \sum_{\sigma \in A_n} + \sum_{\sigma \in S_n \setminus A_n} = 0. \end{aligned}$$

Две последние суммы содержат члены с противоположными знаками, так как разность $\delta(\sigma\tau) - \delta(\sigma)$ является числом нечетным.

Равенство $f(e_1, \dots, e_n) = 1$ проверяется непосредственно: в правой части формулы (Δ) для любой подстановки, отличной от единичной, соответствующий член суммы равен нулю, так как $e_{\sigma(i),i} = 0$, если $\sigma(i) \neq i$. $\square$

Построенная нами функция $f(a_1, \dots, a_n)$ называется *определителем* матрицы

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{bmatrix},$$

столбцы которой задаются векторами $a_1, \dots, a_n$. Обозначения:

$$\det A = |A| = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} := \sum_{\sigma \in S_n} a_{\sigma(1),1} \dots a_{\sigma(n),n} (-1)^{\delta(\sigma)}.$$

Наиболее существенные свойства определителя квадратной матрицы — это, конечно, его полилинейность как функции столбцов матрицы, обнуление в случае пары одинаковых столбцов, изменение знака при перестановке двух столбцов и значение единица на столбцах естественного базиса. Для практического вычисления определителя наиболее ценным дополнением можно считать следующее утверждение.

Утверждение 1.5.1. *Определитель не меняется, если к произвольному столбцу прибавить линейную комбинацию остальных столбцов.*

Доказательство. Это прямое следствие полилинейности и обнуления при совпадении столбцов. $\square$

Теперь можно вспомнить о поиске рациональных функций для представления решений системы линейных алгебраических уравнений и о той гипотезе, которая привела нас к определителю.

Утверждение 1.5.2. *Пусть A — матрица коэффициентов системы*

$$a_{11}x_1 + \dots + a_{1n}x_n = b_1,$$

$$\dots \quad \dots \quad \dots$$

$$a_{n1}x_1 + \dots + a_{nn}x_n = b_n.$$

Если система совместна, то имеют место формулы Крамера

$$x_i |A| = |A_i|, \quad 1 \leq i \leq n,$$

$$A_i = \begin{bmatrix} a_{11} & \dots & a_{1,i-1} & b_1 & a_{1,i+1} & \dots & a_{1n} \\ a_{21} & \dots & a_{2,i-1} & b_2 & a_{2,i+1} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n-1,1} & \dots & a_{n-1,i-1} & b_{n-1} & a_{n-1,i+1} & \dots & a_{n-1,n} \\ a_{n1} & \dots & a_{n,i-1} & b_n & a_{n,i+1} & \dots & a_{nn} \end{bmatrix}.$$

Доказательство. В силу совместности $b = \sum_{i=1}^n x_i a_i$, где $a_1, \dots$

$\dots, a_n$ — столбцы матрицы коэффициентов. Далее используем полилинейность и то, что определитель равен нулю при совпадении столбцов:

$$|A_i| = f(a_1, \dots, a_i, b, a_{i+1}, \dots, a_n) =$$

$$= \sum_{j=1}^n x_j f(a_1, \dots, a_{i-1}, a_j, a_{i+1}, \dots, a_n) =$$

$$= x_i f(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n). \quad \square$$

Определитель матрицы появился у нас как функция столбцов этой матрицы. Его можно рассматривать также как функцию строк, используя ту же формулу. Мы сейчас докажем, что результат будет таким же. Пусть A — матрица размера $m \times n$ с элементами a_{ij} . Матрица B размера $n \times m$ с элементами

$b_{ji} := a_{ij}$ называется *транспонированной* к матрице A . Обозначение: $B = A^\top$.

Теорема 1.5.2. Пусть A — произвольная квадратная матрица. Тогда $|A^\top| = |A|$.

Доказательство. Согласно определению

$$\begin{aligned} |A^\top| &= \sum_{\sigma \in S_n} a_{1,\sigma(1)} \dots a_{n,\sigma(n)} (-1)^{\delta(\sigma)} = \\ &= \sum_{\sigma \in S_n} a_{\sigma^{-1}(1),1} \dots a_{\sigma^{-1}(n),n} (-1)^{\delta(\sigma^{-1})} = |A|. \end{aligned}$$

Следствие 1.5.1. Определитель является полилинейной функцией строк, меняет знак при перестановке строк, равен нулю при совпадении строк и не меняется, если к произвольной строке прибавить произвольную линейную комбинацию остальных строк.

Задача 4. Докажите, что для матрицы порядка 4 с элементами ± 1 максимально возможное значение определителя равно 16.

Задача 5. В матрице A порядка n обнаружена состоящая из нулей подматрица размера $p \times q$, причем $p + q = n + 1$. Докажите, что $|A| = 0$.

1.6. Теорема Лапласа

Пусть A — матрица размера $m \times n$. Выберем строки и столбцы с номерами

$$1 \leq i_1 < \dots < i_k \leq m, \quad 1 \leq j_1 < \dots < j_k \leq n$$

соответственно и рассмотрим матрицу B , которая получается на пересечении данных строк и столбцов. Матрица B называется *квадратной подматрицей* и обозначается следующим образом:

$$B = A \begin{pmatrix} i_1, \dots, i_k \\ j_1, \dots, j_k \end{pmatrix}.$$

Ее определитель называется *минором*.

Теорема 1.6.1 (ТЕОРЕМА ЛАПЛАСА). Пусть A — матрица порядка n . Пусть выбраны строки с номерами $1 \leq i_1 < \dots < i_k \leq n$, а остальные строки имеют номера $1 \leq i_{k+1} < \dots < i_n \leq n$. Аналогично, в случае выбора столбцов с номерами

$1 \leq j_1 < \dots < j_k \leq n$ через $1 \leq j_{k+1} < \dots < j_n \leq n$ обозначаются номера остальных столбцов. Тогда

$$|A| = \sum_{1 \leq j_1 < \dots < j_k \leq n} \left| A \begin{pmatrix} i_1, \dots, i_k \\ j_1, \dots, j_k \end{pmatrix} \right| \left| A \begin{pmatrix} i_{k+1}, \dots, i_n \\ j_{k+1}, \dots, j_n \end{pmatrix} \right| \times \\ \times (-1)^{i_1 + \dots + i_k + j_1 + \dots + j_k}.$$

Доказательство. Согласно определению

$$\left| A \begin{pmatrix} i_1, \dots, i_k \\ j_1, \dots, j_k \end{pmatrix} \right| = \sum_{\alpha \in S_n(i_1, \dots, i_k)} a_{\alpha(i_1), j_1} \dots a_{\alpha(i_k), j_k} (-1)^{\delta(\alpha)},$$

$$\left| A \begin{pmatrix} i_{k+1}, \dots, i_n \\ j_{k+1}, \dots, j_n \end{pmatrix} \right| = \sum_{\beta \in S_n(i_{k+1}, \dots, i_n)} a_{\beta(i_{k+1}), j_{k+1}} \dots a_{\beta(i_n), j_n} (-1)^{\delta(\beta)}.$$

Произведение

$$p(j_1, \dots, j_k) := \left| A \begin{pmatrix} i_1, \dots, i_k \\ j_1, \dots, j_k \end{pmatrix} \right| \left| A \begin{pmatrix} i_{k+1}, \dots, i_n \\ j_{k+1}, \dots, j_n \end{pmatrix} \right| = \\ = \sum_{\alpha \in S_n(i_1, \dots, i_k)} \sum_{\beta \in S_n(i_{k+1}, \dots, i_n)} a_{\alpha(i_1), j_1} \dots a_{\alpha(i_k), j_k} a_{\beta(i_{k+1}), j_{k+1}} \dots \\ \dots a_{\beta(i_n), j_n} (-1)^{\delta(\alpha)} (-1)^{\delta(\beta)} \quad (!)$$

представляется суммой, содержащей $k!(n-k)!$ членов, которые совпадают с соответствующими членами определителя $|A|$ с точностью до знака. Знак члена в формуле для определителя задается четностью числа инверсий подстановки

$$\begin{pmatrix} \alpha(i_1) & \dots & \alpha(i_k) & \beta(i_{k+1}) & \dots & \beta(i_n) \\ j_1 & \dots & j_k & j_{k+1} & \dots & j_n \end{pmatrix}.$$

Искомая четность совпадает с четностью суммы чисел инверсий в подстановках вида

$$f = \begin{pmatrix} 1 & \dots & k & k+1 & \dots & n \\ \alpha(i_1) & \dots & \alpha(i_k) & \beta(i_{k+1}) & \dots & \beta(i_n) \end{pmatrix}$$

и

$$g = \begin{pmatrix} 1 & \dots & k & k+1 & \dots & n \\ j_1 & \dots & j_k & j_{k+1} & \dots & j_n \end{pmatrix}.$$

Для подстановки g инверсии могут быть только среди пар вида (i, j) , где $i \in \{1, \dots, k\}$ и $j \in \{k+1, \dots, n\}$. Среди пар вида $(1, j)$ инверсий в точности $j_1 - 1$, среди пар $(2, j)$ будет $j_2 - 2$

инверсий, так как пара $(1, 2)$ не является инверсией. И так далее. В итоге

$$\delta(g) = (j_1 - 1) + (j_2 - 2) + \dots + (j_k - k).$$

Для f число инверсий среди пар вида (i, j) , где $i \in \{1, \dots, k\}$ и $j \in \{k+1, \dots, n\}$, подсчитывается аналогичным образом, а общее число инверсий имеет вид

$$\delta(f) = \delta(\alpha) + \delta(\beta) + (i_1 - 1) + (i_2 - 2) + \dots + (i_k - k).$$

Таким образом, каждый член суммы (!) отличается от соответствующего члена определителя $|A|$ множителем $(-1)^{i_1+\dots+i_k+j_1+\dots+j_k}$. Следовательно,

$$|A| = \sum_{1 \leq j_1 < \dots < j_k \leq n} p(j_1, \dots, j_k) (-1)^{i_1+\dots+i_k+j_1+\dots+j_k},$$

так как правая часть содержит $\frac{n!}{k!(n-k)!}$ слагаемых, каждое из которых есть сумма $k!(n-k)!$ разных членов исходного определителя, и поэтому мы получаем здесь в точности сумму всех $n!$ членов определителя $|A|$. $\square$

Минор $\left| A \begin{pmatrix} i_{k+1}, \dots, i_n \\ j_{k+1}, \dots, j_n \end{pmatrix} \right|$ называется *дополнительным* по отношению к минору $\left| A \begin{pmatrix} i_1, \dots, i_k \\ j_1, \dots, j_k \end{pmatrix} \right|$, а величина

$$\left| A \begin{pmatrix} i_{k+1}, \dots, i_n \\ j_{k+1}, \dots, j_n \end{pmatrix} \right| (-1)^{i_1+\dots+i_k+j_1+\dots+j_k}$$

называется *алгебраическим дополнением* минора $\left| A \begin{pmatrix} i_1, \dots, i_k \\ j_1, \dots, j_k \end{pmatrix} \right|$. В этих терминах теорема Лапласа утверждает, что *при фиксированных строках определитель есть сумма произведений всевозможных миноров, расположенных на этих строках, на соответствующие им алгебраические дополнения*. В силу теоремы 1.5.2 *при фиксированных столбцах определитель есть сумма произведений всевозможных миноров на этих столбцах на их алгебраические дополнения*.

Пример. Матрица Вандермонда имеет вид

$$V(x_1, \dots, x_n) := \begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-2} & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-2} & x_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & x_{n-1} & x_{n-1}^2 & \dots & x_{n-1}^{n-2} & x_{n-1}^{n-1} \\ 1 & x_n & x_n^2 & \dots & x_n^{n-2} & x_n^{n-1} \end{bmatrix}.$$

Чтобы вычислить *определитель Вандермонда* $|V(x_1, \dots, x_n)|$, вычтем из последнего столбца предпоследний, умноженный на x_1 . Далее, двигаясь справа налево, из каждого столбца, кроме первого, будем вычитать предыдущий, умноженный на x_1 . Первый столбец останется без изменений, а первая строка получит вид $[1, 0, \dots, 0]$. Разложение Лапласа по ней сводит определитель к минору, который получается после вычеркивания первой строки и первого столбца. Нужно заметить, что в каждой строке этого минора есть общий множитель вида $x_i - x_1$, который можно вынести за знак определителя. В результате возникает рекуррентное соотношение

$$\begin{aligned} |V(x_1, \dots, x_n)| &= \prod_{j=2}^n (x_j - x_1) |V(x_2, \dots, x_n)| \Rightarrow \\ &\Rightarrow |V(x_1, \dots, x_n)| = \prod_{1 \leq j < i \leq n} (x_i - x_j). \end{aligned}$$

Задача 6. В матрице порядка n имеется единственный минор порядка $r < n$, отличный от нуля. Докажите, что все миноры порядка $k \geq r + 1$ равны нулю.

Задача 7. Докажите, что в случае $0 < x_1 < \dots < x_n$ все миноры матрицы Вандермонда $V(x_1, \dots, x_n)$ положительны.

1.7. Операции с матрицами

Напомним, что $\mathbb{R}^{m \times n}$ — это множество всех вещественных матриц размера $m \times n$. Матрица A определяется своими элементами a_{ij} и, очевидно, с ней можно ассоциировать функцию $(i, j) \rightarrow a_{ij}$, заданную на множестве пар

$$\{(i, j) : i, j = 1, \dots, n\} = \{1, \dots, n\} \times \{1, \dots, n\}.$$

В общем случае множество пар $\{(a, b) : a \in \mathcal{A}, b \in \mathcal{B}\}$ называется *декартовым произведением* множеств $\mathcal{A}$ и $\mathcal{B}$ и обозначается $\mathcal{A} \times \mathcal{B}$.

Функции можно складывать и умножать на числа — это делается поточечно. Таким образом естественно возникают операции сложения матриц и умножения матрицы на число. Вот формальные определения: *суммой матриц* $A = [a_{ij}]$ и $B = [b_{ij}]$ одного размера называется матрица $C = [c_{ij}]$ такого же размера с элементами $c_{ij} := a_{ij} + b_{ij}$, результат *умножения матрицы* $A = [a_{ij}]$ *на число* α — это матрица $D = [d_{ij}]$ такого же размера с элементами $d_{ij} := \alpha a_{ij}$. Обозначения: $C = A + B$, $D = \alpha A$.

Матрицу размера $m \times n$ можно рассматривать также как арифметический вектор, имеющий mn координат. Конечно, для получения вектора имеется много способов нумерации элементов матрицы. Естественно выбрать и зафиксировать какой-то один способ нумерации. Тогда результаты операций сложения и умножения на число над матрицами будут, очевидно, те же, что и при выполнении таких же операций над соответствующими арифметическими векторами. Для матриц мы можем использовать понятия, введенные для арифметических векторов — такие как линейная зависимость и независимость, линейная оболочка, размерность и базис.

Нетривиальной новой операцией для матриц является *умножение матриц*. Один из поводов к ее введению — короткая запись связи величин a_{ij} , x_j и b_i в системе линейных алгебраических уравнений. Пусть заданы следующие матрицы:

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{bmatrix} \in \mathbb{R}^{m \times n},$$

$$x = \begin{bmatrix} x_1 \\ \dots \\ x_n \end{bmatrix} \in \mathbb{R}^{n \times 1}, \quad b = \begin{bmatrix} b_1 \\ \dots \\ b_m \end{bmatrix} \in \mathbb{R}^{m \times 1}.$$

Будем писать $b = Ax$ и говорить, что матрица b есть произведение матриц A и x , если

$$b_1 := a_{11}x_1 + \dots + a_{1n}x_n$$

$$\dots \quad \dots \quad \dots$$

$$b_m := a_{m1}x_1 + \dots + a_{mn}x_n.$$

Таким образом, запись системы линейных алгебраических уравнений приобретает вид

$$Ax = b.$$

Теперь предположим, что у нас имеются l систем с одной и той же матрицей A . Положим

$$b^{(1)} := Ax^{(1)}, \quad \dots \quad b^{(l)} := Ax^{(l)}.$$

В этом случае составим матрицы

$$X := [x^{(1)}, \dots, x^{(l)}] \in \mathbb{R}^{n \times l}, \quad B := [b^{(1)}, \dots, b^{(l)}] \in \mathbb{R}^{m \times l},$$

и будем писать $B = AX$ и говорить, что матрица B размера $m \times l$ есть *произведение матрицы A размера $m \times n$ и матрицы X размера $n \times l$* .

Теперь дадим эквивалентное формальное определение: *матрица B размера $m \times l$ с элементами b_{ik} называется произведением матрицы A размера $m \times n$ с элементами a_{ij} и матрицы X размера $n \times l$ с элементами x_{jk} , если*

$$b_{ik} := \sum_{j=1}^n a_{ij}x_{jk}, \quad 1 \leq i \leq m, \quad 1 \leq k \leq l.$$

Элемент произведения на пересечении i -й строки и k -го столбца есть сумма произведений элементов i -й строки левого множителя на элементы k -го столбца правого множителя. Поэтому часто говорят, что матрицы перемножаются по правилу «*строка на столбец*».

Сразу обратим внимание на то, что при умножении матриц A и X их размеры должны быть согласованы: число столбцов левого множителя A должно совпадать с числом строк правого множителя X . Поэтому *произведение существует не для любых матриц*. Кроме того, если существует произведение AX , то совсем не обязательно существует XA . Но даже если оба произведения существуют, то, скорее всего, $AX \neq XA$. В общем случае умножение матриц *некоммутативно*. Вот пример:

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Приятным и важным свойством операции умножения матриц является ее *частичная ассоциативность*. Что это такое — записано в следующем утверждении.

Утверждение 1.7.1. Пусть заданы матрицы A, B, C , для которых существуют произведения AB и BC . Тогда существуют также произведения $(AB)C$ и $A(BC)$ и эти произведения равны, т.е.

$$(AB)C = A(BC).$$

Доказательство. Пусть $A = [a_{i_1 i_2}]$, $B = [b_{i_2 i_3}]$, $C = [c_{i_3 i_4}]$ имеют соответственно размеры $n_1 \times n_2$, $n_2 \times n_3$ и $n_3 \times n_4$. Произведение $(AB)C$ существует, так как число столбцов матрицы AB равно числу строк матрицы C . По той же причине существует произведение $A(BC)$. Далее,

$$\begin{aligned} ((AB)C)_{i_1 i_4} &= \sum_{i_3=1}^{n_3} (AB)_{i_1 i_3} c_{i_3 i_4} = \sum_{i_3=1}^{n_3} \left(\sum_{i_2=1}^{n_2} a_{i_1 i_2} b_{i_2 i_3} \right) c_{i_3 i_4} = \\ &= \sum_{i_3=1}^{n_3} \sum_{i_2=1}^{n_2} a_{i_1 i_2} b_{i_2 i_3} c_{i_3 i_4}, \\ (A(BC))_{i_1 i_4} &= \sum_{i_2=1}^{n_2} a_{i_1 i_2} (BC)_{i_2 i_4} = \sum_{i_2=1}^{n_2} a_{i_1 i_2} \left(\sum_{i_3=1}^{n_3} b_{i_2 i_3} c_{i_3 i_4} \right) = \\ &= \sum_{i_2=1}^{n_2} \sum_{i_3=1}^{n_3} a_{i_1 i_2} b_{i_2 i_3} c_{i_3 i_4}. \end{aligned}$$

Как видим, $((AB)C)_{i_1 i_4} = (A(BC))_{i_1 i_4}$ при всех $1 \leq i_1 \leq n_1$, $1 \leq i_4 \leq n_4 \Rightarrow (AB)C = A(BC)$. $\square$

Смысл утверждения в том, что от расстановки скобок, определяющих пары перемножаемых матриц, результат не зависит. Таким образом, можно писать ABC без скобок. Этот результат распространяется на произвольное число перемножаемых матриц.

Теорема 1.7.1. Пусть заданы матрицы $A_1, \dots, A_N$, для которых существуют произведения $A_1 A_2, A_2 A_3, \dots, A_{N-1} A_N$. Тогда произведение $A_1 A_2 \dots A_N$ может быть определено какой-то расстановкой скобок, определяющих пары перемножаемых матриц, и от расстановки скобок результат не зависит.

Доказательство. Проведем индукцию по N . Пусть $k < l$ и имеются два произведения следующего вида:

$$B := (A_1 \dots A_k)(A_{k+1} \dots A_N), \quad D := (A_1 \dots A_l)(A_{l+1} \dots A_N).$$

Тогда, в силу уже доказанной частичной ассоциативности,

$$\begin{aligned} B &= (A_1 \dots A_k)((A_{k+1} \dots A_l)(A_{l+1} \dots A_N)) = \\ &= ((A_1 \dots A_k)(A_{k+1} \dots A_l))(A_{l+1} \dots A_N) = D. \quad \square \end{aligned}$$

Матрица, в которой все элементы равны нулю, называется *нулевой* и обозначается так же, как число 0. Чтобы указать размер нулевой матрицы, иногда пишут $0_{m \times n}$ или 0_n в случае квадратной матрицы порядка n .

Довольно часто матрицы состояются из *подматриц* или *блоков*. Пусть фиксированы натуральные числа $s_1, \dots, s_m, t_1, \dots, t_n, r_1, \dots, r_l$ и рассматриваются матрицы вида

$$A = \begin{bmatrix} A_{11} & \dots & A_{1n} \\ \dots & \dots & \dots \\ A_{m1} & \dots & A_{mn} \end{bmatrix}, \quad B = \begin{bmatrix} B_{11} & \dots & B_{1l} \\ \dots & \dots & \dots \\ B_{n1} & \dots & B_{nl} \end{bmatrix},$$

где блоки A_{ij} и B_{jk} имеют соответственно размеры $s_i \times t_j$ и $t_j \times r_l$. Такие матрицы называются *блочными*. В данном случае размеры блоков согласованы и поэтому существует произведение AB , которое также имеет блочный вид:

$$AB = \begin{bmatrix} C_{11} & \dots & C_{1l} \\ \dots & \dots & \dots \\ C_{m1} & \dots & C_{ml} \end{bmatrix}, \quad C_{ik} = \sum_{j=1}^n A_{ij} B_{jk}, \quad 1 \leq i \leq m, \quad 1 \leq k \leq l.$$

Данное свойство проверяется непосредственно на основе определения операции умножения матриц. Его смысл очень прост: блочные матрицы перемножаются по правилу «*блочная строка на блочный столбец*».

Для заданных матриц A и B иногда рассматривают еще две операции, которые также называют умножением. Первая из них — поэлементное умножение. Здесь $A = [a_{ij}]$ и $B = [b_{ij}]$ должны иметь один и тот же размер, матрица C с элементами $a_{ij}b_{ij}$ называется *адамаровым произведением* матриц A и B . Обозначение: $C = A \circ B$. Вторая операция применима к матрицам разных размеров. Если A имеет элементы a_{ij} , то строится блочная матрица D с блоками вида $a_{ij}B$. Такая матрица D называется *кронекеровым произведением* матриц A и B и обозначается $D = A \otimes B$. Если A и B имеют размеры $m_A \times n_A$ и $m_B \times n_B$, то матрица $A \otimes B$ имеет размер $(m_A m_B) \times (n_A n_B)$.

Постоянно приходится рассматривать те или иные матрицы *специального вида*. Квадратная матрица вида

$$D = \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{bmatrix}$$

называется *диагональной*. Числа $d_1, \dots, d_n$ расположены на так называемой *главной диагонали* матрицы D , все остальные элементы равны нулю. Если $d_1 = \dots = d_n = d$, то диагональная матрица называется *скалярной*. В случае $d = 1$ скалярная матрица называется *единичной* и обозначается буквой I . Чтобы указать порядок единичной матрицы, иногда пишут I_n .

Пусть матрица A имеет элементы a_{ij} . Матрица A называется

- *матрицей перестановки*, если

$$a_{ij} = \begin{cases} 1, & i = \sigma(j), \\ 0, & i \neq \sigma(j), \end{cases} \quad \sigma \in S_n,$$

предполагается, что A — квадратная матрица порядка n ; заметим, что для любых подстановок $\sigma, \tau \in S_n$ выполняется равенство $P_\sigma P_\tau = P_{\sigma\tau}$;

- *верхней треугольной*, если $a_{ij} = 0$ при $i > j$;
- *нижней треугольной*, если $a_{ij} = 0$ при $i < j$;
- *верхней почти треугольной*, если $a_{ij} = 0$ при $i > j + 1$;
- *нижней почти треугольной*, если $a_{ij} = 0$ при $i + 1 < j$;
- *ленточной*, если равенство $a_{ij} = 0$ имеет место как при $i > j + l$, так и при $i + u < j$, где l и u — натуральные числа, характеризующие *ширину ленты* в нижней и верхней треугольной части матрицы A ;
- $(2d + 1)$ -*диагональной*, если $a_{ij} = 0$ при $|i - j| > d$, в частности, *трехдиагональной* в случае $d = 1$.

Замечательно, что многие классы матриц специального вида *замкнуты относительно операции умножения матриц* — замкнутость означает, что произведение принадлежит тому же классу, что и множители. Такими являются, в частности, классы матриц перестановки, нижних треугольных и верхних треугольных матриц. Класс трехдиагональных матриц незамкнут, но произведение таких матриц «достаточно близко» к трехдиагональной матрице — оно всегда будет пятидиагональной матрицей.

Задача 8. Пусть u и v — матрицы-столбцы размера $n \times 1$. Докажите, что

$$|I_n + uv^\top| = 1 + v^\top u.$$

Задача 9. Пусть A и B — матрицы порядка n . Докажите, что $|A \otimes B| = |A|^n |B|^n$.

Задача 10. Докажите, что любую квадратную матрицу можно представить в виде произведения нескольких трехдиагональных матриц.

1.8. Обратная матрица

Матрица A порядка n называется *обратимой*, если существует матрица B порядка n , такая что имеют место равенства

$$AB = BA = I_n.$$

Такая матрица B определяется однозначно: пусть также $AB_1 = B_1A = I_n \Rightarrow$

$$B = I_n B = (B_1 A) B = B_1 (AB) = B_1 I_n = B_1.$$

Матрица B называется *обратной* к матрице A и обозначается A^{-1} .

Легко видеть, что матрица A^{-1} также обратима и $(A^{-1})^{-1} = A$. Кроме того, если A и B — обратимые матрицы одного и того же порядка, то их произведение AB обратимо и $(AB)^{-1} = B^{-1}A^{-1}$.

Утверждение 1.8.1. Если матрица A системы линейных алгебраических уравнений $Ax = b$ является обратимой, то решение системы существует и единственно.

Доказательство. Положим $x := A^{-1}b$. Тогда, очевидно,

$$Ax = A(A^{-1}b) = (AA^{-1})b = Ib = b.$$

Если x — решение, то выполняется равенство $Ax = b$. Умножая обе части слева на матрицу A^{-1} , находим: $x = A^{-1}b$. $\square$

Пусть матрица A имеет порядок n и обратима. Тогда столбцы $x^{(1)}, \dots, x^{(n)}$ матрицы A^{-1} являются решениями систем линейных алгебраических уравнений вида

$$Ax^{(i)} = e^{(i)}, \quad 1 \leq i \leq n,$$

где $e^{(1)}, \dots, e^{(n)}$ — столбцы единичной матрицы порядка n .

Согласно формулам Крамера,

$$|A| x_j^{(i)} = \begin{vmatrix} a_{11} & \dots & a_{1,j-1} & 0 & a_{1,j+1} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \dots & a_{i-1,n} \\ a_{i1} & \dots & a_{i,j-1} & 1 & a_{i,j+1} & \dots & a_{in} \\ a_{i+1,1} & \dots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{n,j-1} & 0 & a_{n,j+1} & \dots & a_{nn} \end{vmatrix}.$$

В правой части мы видим алгебраическое дополнение элемента a_{ij} матрицы A (как минора порядка 1), обозначим его через A_{ij} . Согласно определению, A_{ij} — это умноженный на $(-1)^{i+j}$ минор порядка $n-1$, получаемый после вычеркивания i -й строки и j -го столбца.

Матрица $\hat{A}$ с элементами $\hat{a}_{ji} := A_{ij}$ называется *присоединенной* к матрице A . Ее основное свойство вытекает из формул Крамера: $A\hat{A} = |\hat{A}| I$.

Сейчас мы дадим еще одно доказательство этого свойства, которое не опирается на формулы Крамера и не использует обратимость матрицы A .

Теорема 1.8.1. Пусть $A = [a_{ij}]$ — матрица порядка n и $\hat{A}$ — ее присоединенная матрица. Тогда

$$A\hat{A} = \hat{A}A = |A| I_n.$$

Доказательство. Обозначим через A_{ij} алгебраическое дополнение элемента a_{ij} . Согласно определению в позиции (j, i) матрицы $\hat{A}$ находится элемент $\hat{a}_{ji} = A_{ij}$. Применяя теорему Лапласа для i -й строки матрицы A , находим

$$\sum_{j=1}^n a_{ij} A_{ij} = |A|.$$

Теперь возьмем $k \neq i$ и рассмотрим матрицу M , которая получается из A заменой k -й строки на i -ю. В матрице M есть одинаковые строки, поэтому ее определитель равен 0. Записав для M разложение Лапласа по k -й строке, находим

$$\sum_{j=1}^n a_{ij} A_{kj} = |M| = 0, \quad k \neq i.$$

Таким образом,

$$\sum_{j=1}^n a_{ij} c_{jk} = \sum_{j=1}^n a_{ij} A_{kj} = \begin{cases} |A|, & i = k, \\ 0, & i \neq k. \end{cases} \Rightarrow A\hat{A} = |A| I_n.$$

Равенство $\hat{A}A = |A| I_n$ получается аналогично с помощью разложений Лапласа по столбцам. $\square$

Квадратная матрица называется *невырожденной*, если ее определитель отличен от нуля.

Следствие 1.8.1. Если матрица A невырождена, то она обратима и обратная к ней матрица имеет вид

$$A^{-1} = \frac{1}{|A|} \hat{A},$$

где $\hat{A}$ — присоединенная матрица, составленная из алгебраических дополнений элементов матрицы A .

Следствие 1.8.2. Если матрица A невырождена, то система линейных алгебраических уравнений $Ax = b$ совместна и имеет единственное решение, которое может быть получено по формулам Крамера.

Верно и то, что обратимая матрица должна быть невырожденной. Но это мы докажем в следующем разделе.

Задача 11. Докажите, что любую невырожденную матрицу можно сделать вырожденной, изменив лишь один из ее элементов.

Задача 12. Невырожденная матрица и обратная к ней разбиты на блоки одинаковых размеров:

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}, \quad B = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}.$$

Докажите, что блок A_{11} невырожден тогда и только тогда, когда невырожден блок B_{22} .

Задача 13. Даны числа a и b , такие что $1 - ab \neq 0$. Докажите, что матрица

$$A = \begin{bmatrix} 1 & a & a^2 & \dots & a^n \\ b & 1 & a & \dots & a^{n-1} \\ b^2 & b & 1 & \dots & a^{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ b^n & b^{n-1} & b^{n-2} & \dots & 1 \end{bmatrix}$$

обратима и обратная матрица имеет трехдиагональный вид.

Задача 14. Пусть A и B — матрицы размеров $m \times n$ и $n \times m$ соответственно. Докажите, что обратимость блочной матрицы $\begin{bmatrix} I_m & A \\ B & I_n \end{bmatrix}$ равносильна обратимости каждой из матриц $I_m - AB$ и $I_n - BA$.

Задача 15. Пусть матрица A имеет порядок n и $\hat{A}$ — ее присоединенная матрица. Докажите, что

$$\left| \hat{A} \begin{pmatrix} 1 & \dots & k \\ 1 & \dots & k \end{pmatrix} \right| = |A|^{k-1} \left| A \begin{pmatrix} k+1 & \dots & n \\ k+1 & \dots & n \end{pmatrix} \right|, \quad 1 \leq k \leq n-1.$$

Задача 16. Матрица $A = A_1 A_2 \dots A_n$ задана как произведение $n \times n$ -матриц,

$$A_k = \begin{bmatrix} I_{k-1} & & \\ & C_k & \\ & & I_{n-k-1} \end{bmatrix}, \quad C_k = \begin{bmatrix} a_k & 1 \\ 1 & 0 \end{bmatrix} \text{ при } 1 \leq k \leq n-1,$$

$$A_n = \begin{bmatrix} I_{n-1} & \\ & a_n \end{bmatrix}.$$

Докажите, что

$$A_1 A_2 \dots A_n = \begin{bmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ 1 & 0 & & & \\ & \ddots & \ddots & & \\ & & 1 & 0 & \\ & & & 1 & 0 \end{bmatrix}.$$

Докажите также, что для любой перестановки $i_1, \dots, i_n$ номеров $1, \dots, n$ матрица $B := A_{i_1} A_{i_2} \dots A_{i_n}$ связана с A соотношением $B = P A P^{-1}$, где P — некоторая зависящая от перестановки обратимая матрица.

1.9. Формула Бине–Коши

Теорема 1.9.1 (БИНЕ–КОШИ). Пусть $n \leq m$ и даны матрицы A и B размеров $n \times m$ и $m \times n$ соответственно. Тогда

$$|AB| = \sum_{1 \leq j_1 < \dots < j_n \leq m} \left| A \begin{pmatrix} 1 & \dots & n \\ j_1 & \dots & j_n \end{pmatrix} \right| \left| B \begin{pmatrix} j_1 & \dots & j_n \\ 1 & \dots & n \end{pmatrix} \right|.$$

Доказательство. Пусть матрицы A и $C = AB$ имеют соответственно столбцы $a_1, \dots, a_m$ и $c_1, \dots, c_n$. Тогда

$$c_k = \sum_{j_k=1}^m b_{j_k, k} a_{j_k},$$

где $b_{j_k, k}$ — элементы матрицы B . Используем то, что определитель является полилинейной функцией столбцов и обнуляется при совпадении разных столбцов:

$$\begin{aligned} |AB| &= f(c_1, \dots, c_n) = \sum_{j_1=1}^m \dots \sum_{j_n=1}^m b_{j_1, 1} \dots b_{j_n, n} f(a_{j_1}, \dots, a_{j_n}) = \\ &= \sum_{1 \leq j_1 < \dots < j_n \leq m} \sum_{\sigma \in S_n(j_1, \dots, j_n)} b_{\sigma(j_1), 1} \dots b_{\sigma(j_n), n} f(a_{\sigma(j_1)}, \dots, a_{\sigma(j_n)}) = \\ &= \sum_{1 \leq j_1 < \dots < j_n \leq m} f(a_{j_1}, \dots, a_{j_n}) \times \\ &\times \sum_{\sigma \in S_n(j_1, \dots, j_n)} b_{\sigma(j_1), 1} \dots b_{\sigma(j_n), n} (-1)^{\delta(\sigma)} = \\ &= \sum_{1 \leq j_1 < \dots < j_n \leq m} \left| A \begin{pmatrix} 1 & \dots & n \\ j_1 & \dots & j_n \end{pmatrix} \right| \left| B \begin{pmatrix} j_1 & \dots & j_n \\ 1 & \dots & n \end{pmatrix} \right|. \quad \square \end{aligned}$$

Следствие 1.9.1. *Определитель произведения квадратных матриц одного и того же порядка равен произведению их определителей.*

Следствие 1.9.2. *Обратимая матрица является невырожденной.*

Доказательство. Пусть $AA^{-1} = I$. Тогда $|A||A^{-1}| = |I| = 1 \Rightarrow |A| \neq 0$. $\square$

Интересно заметить, что для следствия 1.9.1 есть и другие, менее прямые доказательства. Например, можно рассмотреть следующее соотношение для блочных матриц:

$$\begin{bmatrix} I & 0 \\ A & I \end{bmatrix} \begin{bmatrix} B & -I \\ 0 & A \end{bmatrix} = \begin{bmatrix} B & -I \\ AB & 0 \end{bmatrix}.$$

Определитель второй матрицы равен $|A||B|$, а ее умножение слева на первую матрицу — это преобразование, при котором к строкам от $(n+1)$ -й до $2n$ -й прибавляются линейные комбинации первых n строк. При таком преобразовании определитель не

меняется. Определитель третьей матрицы находится по теореме Лапласа, например, для последних n строк и равен

$$|AB|(-1)^n(-1)^{\sum_{i=1}^n(n+i)+\sum_{j=1}^n j} = |AB|(-1)^{n(n+1)} = |AB|.$$

Еще одна возможность — рассмотреть определитель $|AB|$ как функцию столбцов матрицы B и заметить, что эта функция полилинейна и равна нулю при совпадении столбцов. Если матрица A невырождена, то можно перейти к функции вида $|AB|/|A|$, которая равна 1 на столбцах единичной матрицы. Значит, $|AB|/|A| = |B|$. На этом пути, однако, надо отдельно рассмотреть случай вырожденной матрицы A . Это можно сделать, например, используя теорию ранга матрицы, которую мы разберем в следующем разделе.

Иногда по матрице A строятся матрицы, составленные из ее миноров

$$c_{(i_1, \dots, i_k), (j_1, \dots, j_k)} := A \begin{pmatrix} i_1, \dots, i_k \\ j_1, \dots, j_k \end{pmatrix}.$$

Будем считать, что A имеет размер $m \times n$ и определяющие минор номера упорядочены по возрастанию: $1 \leq i_1 < \dots < i_k \leq m$, $1 \leq j_1 < \dots < j_k \leq n$. Каждый из наборов индексных векторов $(i_1, \dots, i_k)$ и $(j_1, \dots, j_k)$ упорядочим *лексикографически*, а именно будем считать, что $(i_1, \dots, i_k) < (i'_1, \dots, i'_k)$, если имеется номер l , такой что

$$i_1 = i'_1, \quad \dots \quad i_{l-1} = i'_{l-1}, \quad i_l < i'_l.$$

Матрицу с элементами $c_{(i_1, \dots, i_k), (j_1, \dots, j_k)}$, в которой индексный вектор $(i_1, \dots, i_k)$ рассматривается как *мультииндекс* и указывает на строку и, аналогично, индексный вектор $(j_1, \dots, j_k)$ указывает на столбец, естественно называть *k -й минорной матрицей*, ассоциированной с матрицей A . Мультииндексы считаются упорядоченными лексикографически. Обозначение для k -й минорной матрицы: $C_k(A)$. Если, например, $m = 3$ и $n = 4$, то

$$C_2(A) =$$

$$= \begin{bmatrix} A \begin{pmatrix} 1, 2 \\ 1, 2 \end{pmatrix} & A \begin{pmatrix} 1, 2 \\ 1, 3 \end{pmatrix} & A \begin{pmatrix} 1, 2 \\ 1, 4 \end{pmatrix} & A \begin{pmatrix} 1, 2 \\ 2, 3 \end{pmatrix} & A \begin{pmatrix} 1, 2 \\ 2, 4 \end{pmatrix} & A \begin{pmatrix} 1, 2 \\ 3, 4 \end{pmatrix} \\ A \begin{pmatrix} 1, 3 \\ 1, 2 \end{pmatrix} & A \begin{pmatrix} 1, 3 \\ 1, 3 \end{pmatrix} & A \begin{pmatrix} 1, 3 \\ 1, 4 \end{pmatrix} & A \begin{pmatrix} 1, 3 \\ 2, 3 \end{pmatrix} & A \begin{pmatrix} 1, 3 \\ 2, 4 \end{pmatrix} & A \begin{pmatrix} 1, 3 \\ 3, 4 \end{pmatrix} \\ A \begin{pmatrix} 2, 3 \\ 1, 2 \end{pmatrix} & A \begin{pmatrix} 2, 3 \\ 1, 3 \end{pmatrix} & A \begin{pmatrix} 2, 3 \\ 1, 4 \end{pmatrix} & A \begin{pmatrix} 2, 3 \\ 2, 3 \end{pmatrix} & A \begin{pmatrix} 2, 3 \\ 2, 4 \end{pmatrix} & A \begin{pmatrix} 2, 3 \\ 3, 4 \end{pmatrix} \end{bmatrix}.$$

Основные свойства минорных матриц — прямое следствие формулы Бине–Коши.

Утверждение 1.9.1. *Если произведение матриц A и B существует, то существует и произведение их минорных матриц $C_k(A)$ и $C_k(B)$ и имеет место равенство*

$$C_k(A)C_k(B) = C_k(AB).$$

Если матрица A обратима, то матрица $C_k(A)$ также обратима и

$$(C_k(A))^{-1} = C_k(A^{-1}).$$

Задача 17. Пусть A — матрица размера $m \times n$ с линейно независимой системой столбцов. Докажите, что существует матрица B такая, что $BA = I_n$.

Задача 18. Докажите, что система линейных алгебраических уравнений с матрицей A имеет решение при любой правой части тогда и только тогда, когда однородная система вида $A^T u = 0$ имеет только нулевое решение $u = 0$.

1.10. Ранг матрицы

Пусть матрица A имеет ненулевой минор порядка r и в ней нет ненулевых миноров более высокого порядка. Такое число r называется *рангом матрицы A* . По определению ранг нулевой матрицы равен 0. Обозначение: $r = \text{rank } A$.

Если подматрица порядка k вложена в подматрицу порядка $k + 1$, то определитель второй подматрицы называется *окаймляющим минором* для определителя первой подматрицы. Ненулевой минор называется *базисным*, если для него все окаймляющие миноры равны нулю. Строки и столбцы, на которых он находится, также называют *базисными*.

Теорема 1.10.1 (ТЕОРЕМА О БАЗИСНОМ МИНОРЕ). *Строки (столбцы) матрицы, на которых расположен базисный минор, образуют базис в линейной оболочке строк (столбцов) данной матрицы. Порядок базисного минора равен рангу данной матрицы.*

Доказательство. Не ограничивая общности, будем считать, что базисный минор расположен в левом верхнем углу $m \times n$ -матрицы A . Пусть его порядок равен k . Соответствующую ему подматрицу обозначим через B .

Докажем, что любой столбец есть линейная комбинация первых k столбцов. Рассмотрим j -й столбец. Если $1 \leq j \leq k$, то утверждение очевидно. Пусть $j > k$. В силу невырожденности подматрицы B существуют числа $x_1, \dots, x_k$, удовлетворяющие уравнению

$$\begin{aligned}
 B \begin{bmatrix} x_1 \\ \dots \\ x_k \end{bmatrix} &= \begin{bmatrix} a_{1j} \\ \dots \\ a_{kj} \end{bmatrix} \Rightarrow \\
 \Rightarrow 0 &= \begin{vmatrix} & & a_{1j} \\ & B & \dots \\ a_{i1} & \dots & a_{ik} & a_{ij} \end{vmatrix} = \begin{vmatrix} & B & \dots & 0 \\ & & \dots & \dots \\ a_{i1} & \dots & a_{ik} & a_{ij} - \sum_{l=1}^k a_{il}x_l \end{vmatrix} \Rightarrow \\
 \Rightarrow a_{ij} - \sum_{l=1}^k a_{il}x_l &= 0 \quad \text{для всех } 1 \leq i \leq m.
 \end{aligned}$$

Таким образом, j -й столбец действительно получается как линейная комбинация первых k столбцов.

Докажем также, что первые k столбцов линейно независимы. Рассмотрим равную нулевому вектору линейную комбинацию этих столбцов с коэффициентами $x_1, \dots, x_k$. Тогда

$$B \begin{bmatrix} x_1 \\ \dots \\ x_k \end{bmatrix} = \begin{bmatrix} 0 \\ \dots \\ 0 \end{bmatrix} \Rightarrow \begin{bmatrix} x_1 \\ \dots \\ x_k \end{bmatrix} = B^{-1} \begin{bmatrix} 0 \\ \dots \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \dots \\ 0 \end{bmatrix}.$$

Линейная независимость доказана. Утверждение теоремы относительно строк получается с помощью перехода к транспонированной матрице.

Теперь докажем, что $\text{rang } A = k$. Рассмотрим произвольный минор порядка $l > k$. Столбцы матрицы A , на которых он расположен, непременно линейно зависимы, иначе мы имели бы $l > k$ линейно независимых векторов в векторном пространстве размерности k . Следовательно, столбцы минора порядка l также линейно зависимы $\Rightarrow$ хотя бы один из них есть линейная комбинация остальных столбцов $\Rightarrow$ минор порядка l равен нулю. $\square$

Как следствие этой теоремы можно получить еще одно доказательство для утверждения о том, что обратимая матрица A является невырожденной. От противного, если A имеет порядок n

и вырождена, то ее ранг строго меньше n . Поэтому ее столбцы линейно зависимы $\Rightarrow$ существуют не равные одновременно нулю числа $x_1, \dots, x_n$, такие что

$$A \begin{bmatrix} x_1 \\ \dots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \dots \\ 0 \end{bmatrix} \Rightarrow \begin{bmatrix} x_1 \\ \dots \\ x_n \end{bmatrix} = A^{-1} \begin{bmatrix} 0 \\ \dots \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \dots \\ 0 \end{bmatrix}.$$

Полученное противоречие означает, что матрица A должна быть невырожденной.

Следствие 1.10.1. *Размерность линейной оболочки столбцов матрицы совпадает с размерностью линейной оболочки ее строк и равна ее рангу.*

Доказательство. Согласно теореме о базисном миноре, размерность каждой линейной оболочки равна рангу матрицы. $\square$

Следствие 1.10.2. *Ранг не меняется при умножении матрицы слева или справа на обратимую матрицу.*

Доказательство. Докажем, что $\text{rank } AB = \text{rank } A$, если матрица B обратима. Согласно определению операции умножения матриц, линейная оболочка столбцов матрицы AB содержится в линейной оболочке столбцов матрицы A . Равенство $A = (AB)B^{-1}$ показывает, что линейная оболочка столбцов матрицы A содержится в линейной оболочке матрицы AB . Значит, эти линейные оболочки совпадают. По теореме о базисном миноре, их размерности равны рангам матриц A и AB .

Чтобы доказать равенство $\text{rank } BA = \text{rank } A$, перейдем к транспонированным матрицам: если $BA = C$, то $A^T B^T = C^T$. Далее используем уже доказанное и то, что ранг матрицы не меняется при транспонировании. $\square$

Следствие 1.10.3. *Ранг суммы матриц не превосходит суммы их рангов.*

Доказательство. Линейная оболочка столбцов матрицы $A + B$, конечно, содержится в линейной оболочке столбцов матрицы $C = [A, B]$, составленной из столбцов обеих матриц. Заметим также, что $\text{rank } C \leq \text{rank } A + \text{rank } B$. $\square$

Как выглядят матрицы ранга 1? Согласно теореме о базисном миноре, каждый столбец $m \times n$ -матрицы $A = [a_{ij}]$ ранга 1 пропорционален какому-то одному ненулевому столбцу. Пусть это будет столбец u с элементами $u_1, \dots, u_m$, а коэффициент

пропорциональности для j -го столбца пусть будет v_j . Тогда A есть произведение столбца u и строки $v^\top$ с элементами $v_1, \dots, v_n$:

$$A = uv^\top = \begin{bmatrix} u_1 \\ \dots \\ u_m \end{bmatrix} [v_1 \ \dots \ v_n] \Rightarrow a_{ij} = u_i v_j.$$

Обратим внимание на то, что равенство $a_{ij} = u_i v_j$ означает *разделение переменных*: функция a_{ij} от переменных i и j представляется произведением функции только от i и функции только от j .

Теорема 1.10.2. *Ранг матрицы A равен $r \neq 0$ в том и только том случае, когда она имеет вид*

$$A = \sum_{k=1}^r u_k v_k^\top,$$

где обе системы столбцов, $u_1, \dots, u_r$ и $v_1, \dots, v_r$, линейно независимы.

Доказательство. Пусть A имеет размер $m \times n$, и пусть столбцы, на которых расположен базисный минор, имеют вид

$$u_1 = \begin{bmatrix} u_{11} \\ \dots \\ u_{m1} \end{bmatrix}, \quad \dots, \quad u_r = \begin{bmatrix} u_{1r} \\ \dots \\ u_{mr} \end{bmatrix}.$$

Согласно теореме о базисном миноре j -й столбец есть линейная комбинация столбцов $u_1, \dots, u_r$. Обозначим коэффициенты этой линейной комбинации через $v_{1j}, \dots, v_{rj}$. Тогда

$$A = \underbrace{\begin{bmatrix} u_{11} & \dots & u_{1r} \\ u_{21} & \dots & u_{2r} \\ \dots & \dots & \dots \\ u_{m1} & \dots & u_{mr} \end{bmatrix}}_{=U} \underbrace{\begin{bmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ \dots & \dots & \dots & \dots \\ v_{r1} & v_{r2} & \dots & v_{rn} \end{bmatrix}}_{=V^\top} = UV^\top.$$

Обозначив столбцы матрицы V через $v_1, \dots, v_r$, находим

$$A = \sum_{k=1}^r u_k v_k^\top. \quad (*)$$

Ранг каждой из матриц U и V равен r : если бы он был меньше, то и ранг матрицы A был бы меньше, чем r . Следовательно, системы $u_1, \dots, u_r$ и $v_1, \dots, v_r$ обе линейно независимы.

Обратно, если A имеет вид (*), то $A = UV^T$, где $U = [u_1, \dots, u_r]$, $V = [v_1, \dots, v_r]$. Линейная независимость систем $u_1, \dots, u_r$ и $v_1, \dots, v_r$ означает, что

$$\text{rank } U = \text{rank } V = r.$$

Значит, в матрицах U и V^T имеются невырожденные подматрицы порядка r и их произведение будет невырожденной подматрицей порядка r в матрице A . Поэтому $r \leq \text{rank } A \leq \text{rank } U = \text{rank } V = r \Rightarrow \text{rank } A = r$. $\square$

Запись матрицы A ранга r в виде $A = UV^T$, где U и V имеют по r столбцов, называется *скелетным разложением* матрицы A . В качестве столбцов матрицы U можно выбрать базисные столбцы матрицы A . Можно построить также разложения, в которых матрица V^T составлена из базисных строк матрицы A .

Отметим также, что понятие ранга матриц используется в следующем довольно очевидном критерии совместности.

Теорема 1.10.3 (ТЕОРЕМА КРОНЕКЕРА–КАПЕЛЛИ). *Для совместности системы линейных алгебраических уравнений $Ax = b$ необходимо и достаточно условие*

$$\text{rank } A = \text{rank } [A, b].$$

Доказательство. Если система совместна, то столбец b является линейной комбинацией столбцов матрицы $A \Rightarrow$ все миноры матрицы $[A, b]$, окаймляющие базисный минор матрицы A , равны нулю $\Rightarrow \text{rank } A = \text{rank } [A, b]$. Если совпадают ранги, то в матрице $[A, b]$ имеется базисный минор на столбцах матрицы $A \Rightarrow b$ есть линейная комбинация столбцов матрицы A . $\square$

Задача 19. Ранг матрицы A равен r . Докажите, что подматрица B на пересечении любых r линейно независимых строк и r линейно независимых столбцов является невырожденной и при этом $A = CB^{-1}R$, где C и R — матрицы, составленные соответственно из столбцов и строк, содержащих подматрицу B .

Задача 20. A и B — квадратные матрицы ранга 1, и $AB = BA \neq 0$. Докажите, что ранг матрицы $A + B$ не больше 1.

Задача 21. Пусть $1 \leq k \leq (r+1)/2$ и в каждой из систем $u_1, \dots, u_r \in \mathbb{R}^{n \times 1}$ и $v_1, \dots, v_r \in \mathbb{R}^{n \times 1}$ любые k векторов линейно независимы. Докажите, что среди матриц $u_1 v_1^T, \dots, u_r v_r^T$ любые $2k - 1$ матриц линейно независимы.

1.11. Однородные системы

Теорема 1.11.1. Пусть V — векторное пространство всех решений однородной системы $Ax = 0$ с $m \times n$ -матрицей A ранга r . Тогда $\dim V = n - r$.

Доказательство. Пусть $a_1, \dots, a_n$ — столбцы матрицы A . Не ограничивая общности, можно считать, что базисный минор расположен на столбцах $a_1, \dots, a_r$. То, что x — решение системы $Ax = 0$, равносильно равенству $x_1 a_1 + \dots + x_n a_n = 0$. Неизвестные $x_1, \dots, x_r$ условимся называть *базисными*, а неизвестные $x_{r+1}, \dots, x_n$ — *свободными*. Название совершенно естественное: если для свободных неизвестных выбрать произвольные числовые значения, то обязательно найдутся однозначно определенные значения базисных неизвестных, для которых будет выполнено равенство

$$x_1 a_1 + \dots + x_r a_r = -x_{r+1} a_{r+1} - \dots - x_n a_n.$$

Достаточно учесть, что система $a_1, \dots, a_r$ образует базис в линейной оболочке столбцов матрицы A .

Построим решения $x^{(1)}, \dots, x^{(n-r)}$, соответствующие выбору

$$\begin{aligned} (x_{r+1}^{(1)}, \dots, x_n^{(1)}) &= (1, 0, 0, \dots, 0, 0), \\ (x_{r+1}^{(2)}, \dots, x_n^{(2)}) &= (0, 1, 0, \dots, 0, 0), \\ &\dots \dots \dots \\ (x_{r+1}^{(n-r)}, \dots, x_n^{(n-r)}) &= (0, 0, 0, \dots, 0, 1). \end{aligned}$$

Эти решения линейно независимы¹⁾:

$$\begin{aligned} \alpha_1 x^{(1)} + \dots + \alpha_{n-r} x^{(n-r)} &= (*, \dots, *, \alpha_1, \dots, \alpha_{n-r}) = \\ &= (0, 0, \dots, 0) \Rightarrow \alpha_1 = \dots = \alpha_{n-r} = 0. \end{aligned}$$

Далее, пусть $x = (x_1, \dots, x_r, x_{r+1}, \dots, x_n)$ — произвольное решение. Тогда вектор

$$y := x - x_{r+1} x^{(1)} - \dots - x_n x^{(n-r)} = (*, \dots, *, \underbrace{0, \dots, 0}_{n-r})$$

¹⁾ Символом $*$ обозначены координаты, не представляющие для нас интереса.

также будет решением и, более того, $y = 0$, так как значения всех свободных неизвестных для него равны нулю, а поскольку базисные неизвестные определяются однозначно, они тоже должны быть нулевыми. $\square$

Базис векторного пространства V иногда называют *фундаментальной системой решений* однородной системы $Ax = 0$.

Задача 22. Докажите, что если ранг матрицы порядка $n \geq 2$ равен $n - 1$, то ранг ее присоединенной матрицы равен 1.

1.12. Скалярное и векторное произведения

Скалярное произведение ненулевых геометрических векторов a и b определяется как число, равное произведению их длин на косинус угла $\phi = \phi(a, b)$ между ними. Обозначение: $(a, b) = |a||b| \cos \phi(a, b)$. Если хотя бы один из векторов нулевой, то скалярное произведение считается равным нулю. Вот основные свойства скалярного произведения:

- 1) $(a, a) \geq 0 \ \forall a$ и $(a, a) = 0 \Leftrightarrow a = 0$;
- 2) $(a, b) = (b, a) \ \forall a, b$ (симметричность);
- 3) $(\alpha a, c) = \alpha(a, c) \ \forall a, c, \ \forall \alpha \in \mathbb{R}$;
- 4) $(a + b, c) = (a, c) + (b, c) \ \forall a, b, c$.

Последние два свойства вместе означают *линейность по первому аргументу*. Из симметричности следует также линейность по второму аргументу.

Первые два свойства сразу же вытекают из определения. Линейность по первому аргументу очевидна, если $c = 0$ (нулевой вектор). Если $c \neq 0$, то введем декартову систему координат, в которой первая ось задается вектором c . Тогда величина $|a| \cos \phi(a, c)$ представляет собой первую координату вектора a . Далее нужно заметить, что при умножении вектора на число его координаты умножаются на это число, а при сложении векторов их координаты складываются.

Скалярное произведение можно ввести и для арифметических векторов из произвольного векторного пространства $V \subseteq V_n(\mathbb{R})$. Делается это уже *аксиоматически*: скалярным произведением

называется любая числовая функция, удовлетворяющая требованиям (1) – (4). После этого длиной арифметического вектора a объявляется величина

$$|a| := \sqrt{(a, a)},$$

а угол $\phi(a, b)$ между ненулевыми арифметическими векторами a и b определяется как число ϕ , такое что

$$\cos \phi(a, b) = \frac{(a, b)}{|a||b|}.$$

Напрашивается, конечно, вопрос об абсолютной величине правой части — не может ли она оказаться больше единицы?

Теорема 1.12.1 (Неравенство Коши–Буняковского–Шварца). *Из свойств (1)–(4) вытекает неравенство*

$$|(a, b)| \leq |a||b|.$$

Равенство имеет место в том и только том случае, когда векторы a и b линейно зависимы.

Доказательство. Если хотя бы один из векторов нулевой, то утверждения очевидны. Пусть оба вектора ненулевые. Рассмотрим функцию $f(t) := (a + tb, a + tb)$ и, используя свойства (1) – (4), находим, что это неотрицательный квадратный трехчлен:

$$\begin{aligned} f(t) &:= (a + tb, a + tb) = (a, a) + 2(a, b)t + (b, b)t^2 = \\ &= |a|^2 + 2(a, b)t + |b|^2 t^2 \geq 0 \quad \forall t \in \mathbb{R} \Rightarrow (a, b)^2 - |a|^2 |b|^2 \leq \\ &\leq 0 \quad (\text{дискриминант не может быть положительным}). \end{aligned}$$

Дискриминант равен нулю в том и только том случае, когда $a + tb = 0$ для некоторого числа t . $\square$

Геометрические векторы a и b называются *ортогональными*, если $(a, b) = 0$. При этом пишут $a \perp b$.

Точно так же называются арифметические векторы a и b из какого-либо векторного пространства, в котором каким-либо способом введено скалярное произведение. В этом случае нужно обратить внимание на то, что ортогональность векторов будет

зависеть от того, как именно введено скалярное произведение. Например, если $a = (a_1, \dots, a_n)$ и $b = (b_1, \dots, b_n)$, то формула

$$(a, b) := \sum_{i=1}^n \gamma_i a_i b_i$$

будет задавать *разные* скалярные произведения при любом выборе положительных чисел $\gamma_1, \dots, \gamma_n$.

Пусть $e_1, \dots, e_n$ — арифметические векторы, образующие базис некоторого векторного пространства V , в котором введено скалярное произведение. Если имеют место соотношения

$$(e_i, e_j) = \begin{cases} 1, & i = j, \\ 0, & i \neq j, \end{cases}$$

то система векторов $e_1, \dots, e_n$ называется *ортонормированной*.

Утверждение 1.12.1. Пусть $e_1, \dots, e_n$ — произвольная ортонормированная система, образующая базис векторного пространства V , в котором введено скалярное произведение.

Тогда для произвольных векторов $a = \sum_{i=1}^n a_i e_i$ и $b = \sum_{i=1}^n b_i e_i$ скалярное произведение вычисляется как сумма произведений соответствующих координат:

$$(a, b) = \sum_{i=1}^n a_i b_i.$$

Доказательство. Используем свойства (2) – (4) и ортонормированность:

$$(a, b) = \left(\sum_{i=1}^n a_i e_i, \sum_{j=1}^n b_j e_j \right) = \sum_{i=1}^n \sum_{j=1}^n a_i b_j (e_i, e_j) = \sum_{i=1}^n a_i b_i. \quad \square$$

В применении к геометрическим векторам данное утверждение дает очень простой метод вычисления скалярного произведения через координаты векторов в произвольной декартовой системе координат (декартовость означает, что оси определяются ортонормированным базисом).

Пример 1. Пусть нас интересует геометрическое место точек (x_1, x_2, x_3) , удовлетворяющих уравнению

$$A_0 + A_1 x_1 + A_2 x_2 + A_3 x_3 = 0 \quad (*)$$

при условии, что числа A_1, A_2, A_3 не равны одновременно нулю. В данном случае векторы (x_1, x_2, x_3) — это все решения системы линейных алгебраических уравнений, состоящей из единственного уравнения $A_1x_1 + A_2x_2 + A_3x_3 = -A_0$. Матрица коэффициентов состоит из одной ненулевой строки $A = [A_1, A_2, A_3]$, и ее ранг равен 1. Согласно теореме 1.11.1, множество решений соответствующей однородной системы — это векторное пространство размерности $3 - 1 = 2$ (число неизвестных минус ранг), т. е. линейная оболочка двух линейно независимых векторов и, другими словами, плоскость, проходящая через начало координат и натянутая на эти векторы. Конечно же, данная система совместна (например, в силу теоремы Кронекера–Капелли), и мы знаем, как устроено множество ее решений — это уже построенная плоскость, перенесенная параллельно в точку, представляющую собой какое-либо частное решение.

Уравнение (*) называется *общим уравнением плоскости* в трехмерном пространстве с некоторой аффинной системой координат. Если $A_0 + A_1x_1 + A_2x_2 + A_3x_3 = 0$, то точка с координатами (x_1, x_2, x_3) принадлежит данной плоскости. Заметим также, что *все точки, для которых $A_0 + A_1x_1 + A_2x_2 + A_3x_3 > 0$, находятся по одну сторону от данной плоскости, а точки, для которых $A_0 + A_1x_1 + A_2x_2 + A_3x_3 < 0$, лежат по другую сторону*. Для доказательства достаточно убедиться в том, что прямая, проходящая через пару точек вне этой плоскости, пересекает данную плоскость в том и только том случае, когда при подстановке их координат в общее уравнение получаются разные знаки.

Если система координат декартова, то *вектор $n := (A_1, A_2, A_3)$ будет ортогонален данной плоскости*. В самом деле, пусть (x_1, x_2, x_3) и (y_1, y_2, y_3) — произвольные точки плоскости, определяемой уравнением (*). Тогда

$$\begin{aligned} A_0 + A_1x_1 + A_2x_2 + A_3x_3 = 0, \quad A_0 + A_1y_1 + A_2y_2 + A_3y_3 = 0 &\Rightarrow \\ \Rightarrow A_1(x_1 - y_1) + A_2(x_2 - y_2) + A_3(x_3 - y_3) = 0 &\Rightarrow \\ \Rightarrow n \perp (x_1 - y_1, x_2 - y_2, x_3 - y_3). \end{aligned}$$

Вектор $n = (A_1, A_2, A_3)$ называется *нормалью* к плоскости $A_0 + A_1x_1 + A_2x_2 + A_3x_3 = 0$.

Пример 2. Предположим, что система координат декартова, и найдем расстояние от точки $z = (z_1, z_2, z_3)$ до плоскости

$A_0 + A_1x_1 + A_2x_2 + A_3x_3 = 0$ с нормалью $n = (A_1, A_2, A_3)$. Для этого рассмотрим прямую, состоящую из точек вида

$z + tn$, где t — произвольное вещественное число.

Нам уже понятно, что эта прямая ортогональна заданной плоскости. Найдём значение $t = t_0$, при котором прямая пересечёт плоскость:

$$\begin{aligned} A_0 + A_1(z_1 + t_0A_1) + A_2(z_2 + t_0A_2) + A_3(z_3 + t_0A_3) &= 0 \Rightarrow \\ \Rightarrow t_0 &= -\frac{A_0 + A_1z_1 + A_2z_2 + A_3z_3}{A_1^2 + A_2^2 + A_3^2}. \end{aligned}$$

Искомое расстояние равно длине вектора

$$|t_0n| = \frac{|A_0 + A_1z_1 + A_2z_2 + A_3z_3|}{\sqrt{A_1^2 + A_2^2 + A_3^2}}.$$

В арифметическом пространстве V_n для любого базиса $a_1, \dots, a_n$ можно ввести понятие *ориентации*. Для этого из векторов составляется матрица $A = [a_1, \dots, a_n]$ и рассматривается её определитель. Если $|A| > 0$, то базис называется *положительно ориентированным* или *положительным*, а если $|A| < 0$ — *отрицательно ориентированным* или *отрицательным*.

В трёхмерном геометрическом пространстве можно зафиксировать какую-то систему координат и после этого отождествлять точки с трёхмерными арифметическими векторами, составленными из координат точки. Базисные векторы выбранной системы координат имеют вид $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$ и образуют единичную матрицу $I = [e_1, e_2, e_3]$ с определителем, равным 1. Таким образом, базис выбранной системы координат оказывается положительно ориентированным. Система векторов e_2, e_1, e_3 также образует базис, но это будет уже отрицательно ориентированный базис. Легко видеть, что системы

$$e_1, e_2, e_3, \quad e_2, e_3, e_1, \quad e_3, e_1, e_2$$

ориентированы положительно, а системы

$$e_2, e_1, e_3, \quad e_1, e_3, e_2, \quad e_3, e_2, e_1$$

ориентированы отрицательно.

Векторное произведение линейно независимых геометрических векторов a и b определяется как вектор c , который является ортогональным каждому из векторов a и b , имеет длину

$|a||b|\sin\phi(a, b)$ и при этом система a, b, c является положительно ориентированным базисом. Если a и b линейно зависимы, то считается, что $c = 0$. Обозначение: $c = [a, b]$.

Величина $S(a, b, c) := ([a, b], c)$ называется *смешанным произведением* тройки векторов a, b, c .

Лемма 1.12.1. *Смешанное произведение тройки векторов a, b, c равно нулю, если векторы линейно зависимы. Для линейно независимых векторов оно равно объему параллелепипеда, натянутого на векторы a, b, c , взятому со знаком плюс, если тройка a, b, c положительно ориентирована, и минус, если эта тройка отрицательно ориентирована.*

Доказательство. Пусть радиус-векторы a, b, c линейно независимы. Объем натянутого на них параллелепипеда равен произведению площади параллелограмма, натянутого на векторы a и b , и длины перпендикуляра, опущенного из конечной точки радиус-вектора c на плоскость векторов a и b . Площадь параллелограмма равна $|a||b|\sin\phi(a, b)$. Вектор $[a, b]$ ортогонален плоскости векторов a и b , поэтому длина перпендикуляра равна абсолютной величине числа $|c|\cos\phi(c, [a, b])$. Остается учесть, что косинус положителен в случае положительно ориентированной тройки a, b, c и отрицателен в противном случае. $\square$

Следствие 1.12.1. *Смешанное произведение $S(a, b, c)$ является функцией, линейной по каждому из трех аргументов.*

Доказательство. Функция $S(a, b, c)$ линейна по третьему аргументу в силу ее определения. Тройки a, b, c и b, c, a имеют одну и ту же ориентацию, поэтому $S(a, b, c) = S(b, c, a)$. Аналогично, $S(a, b, c) = S(c, a, b)$. $\square$

Теорема 1.12.2. *Векторное произведение $[a, b]$ является векторно-значной функцией, линейной по каждому аргументу, и меняет знак при перестановке аргументов.*

Доказательство. Пусть $a = \alpha u + \beta v$, где α и β — произвольные числа, u и v — произвольные векторы. Введем вектор

$$h := [\alpha u + \beta v, b] - \alpha[u, b] - \beta[v, b].$$

Наша цель — доказать, что $h = 0$. Для этого мы используем свойства смешанного произведения:

$$(h, h) = S(\alpha u + \beta v, b, h) - \alpha S(u, b, h) - \beta S(v, b, h) = 0 \Rightarrow h = 0.$$

Равенство $[a, b] = -[b, a]$ непосредственно следует из определения векторного произведения. $\square$

Пусть исходная система координат декартова и определяется базисом $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$. Пусть даны векторы $a = (a_1, a_2, a_3)$ и $b = (b_1, b_2, b_3)$. Тогда, согласно теореме 1.12.2,

$$\begin{aligned}
 [a, b] &= [a_1 e_1 + a_2 e_2 + a_3 e_3, b_1 e_1 + b_2 e_2 + b_3 e_3] = \\
 &= \underbrace{a_1 b_1 [e_1, e_1] + a_2 b_2 [e_2, e_2] + a_3 b_3 [e_3, e_3]}_{=0} + \\
 &\quad + \underbrace{a_1 b_2 [e_1, e_2] + a_2 b_1 [e_2, e_1]}_{=(a_1 b_2 - a_2 b_1) e_3} + \underbrace{a_1 b_3 [e_1, e_3] + a_3 b_1 [e_3, e_1]}_{=-(a_1 b_3 - a_3 b_1) e_2} + \\
 &\quad + \underbrace{a_2 b_3 [e_2, e_3] + a_3 b_2 [e_3, e_2]}_{=(a_2 b_3 - a_3 b_2) e_1} = (a_2 b_3 - a_3 b_2) e_1 - (a_1 b_3 - a_3 b_1) e_2 + \\
 &\quad + (a_1 b_2 - a_2 b_1) e_3.
 \end{aligned}$$

Полученный результат легко запоминается, если его трактовать как применение теоремы Лапласа для третьей строки определителя

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ e_1 & e_2 & e_3 \end{vmatrix} = (a_2 b_3 - a_3 b_2) e_1 - (a_1 b_3 - a_3 b_1) e_2 + (a_1 b_2 - a_2 b_1) e_3.$$

Пусть имеется еще один вектор $c = (c_1, c_2, c_3)$. Тогда для смешанного произведения находим

$$\begin{aligned}
 S(a, b, c) &= ([a, b], c) = (a_2 b_3 - a_3 b_2) c_1 - (a_1 b_3 - a_3 b_1) c_2 + \\
 &\quad + (a_1 b_2 - a_2 b_1) c_3 = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}.
 \end{aligned}$$

Последняя формула раскрывает *геометрический смысл определителя* — в случае линейно независимых строк это объем параллелепипеда, натянутого на его строки, взятый со знаком плюс, если строки образуют положительно ориентированный базис, и минус в противном случае.

Нужно отметить, что в случае n -мерных арифметических векторов определитель, если он отличен от нуля, также представляет собой объем параллелепипеда, натянутого на его строки, — со знаком плюс в случае положительной ориентации системы строк и минус в противном случае. Доказательство этого утверждения должно, безусловно, опираться на определение объема для

множества точек в n -мерном пространстве — соответствующая теория обычно изучается в курсе математического анализа.

Задача 23. Докажите, что для произвольных геометрических векторов a, b, c выполняется тождество

$$[a, [b, c]] = (a, c)b - (a, b)c.$$

Задача 24. Докажите, что уравнение $[a, x] + [b, x] = [a, b]$ всегда имеет решение и найдите все решения для заданных векторов a и b .

1.13. Кривые второго порядка

Кривая второго порядка или квадрика — это геометрическое место точек (x_1, x_2) плоскости, координаты которых удовлетворяют уравнению

$$\underbrace{a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2}_{\text{квадратичная часть}} + \underbrace{2b_1x_1 + 2b_2x_2}_{\text{линейная часть}} + c = 0.$$

Квадратичная часть должна быть ненулевым многочленом, т. е. хотя бы одно из чисел a_{11}, a_{12}, a_{22} отлично от нуля. Коэффициент 2 в квадратичной части дает возможность записать уравнение в удобном матричном виде

$$x^T Ax + 2b^T x + c = 0, \quad A = \begin{bmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{bmatrix}, \quad b = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \quad x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix},$$

где $A = A^T$ — такая матрица называется *симметричной*, ниже это свойство нам очень поможет при упрощении вида уравнения. Ясно, что точкам (арифметическим векторам) однозначно ставятся в соответствие матрицы-столбцы:

$$(x_1, x_2) \leftrightarrow x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \quad (y_1, y_2) \leftrightarrow y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}.$$

Если система координат декартова, то скалярное произведение вычисляется по формуле $(x, y) = y^T x = x^T y = x_1 y_1 + x_2 y_2$, а уравнение кривой получает также вид

$$(Ax, x) + 2(b, x) + c = 0.$$

Коэффициент 2 в линейной части упрощает некоторые выкладки и, помимо этого, позволяет записать уравнение в виде

$$\begin{bmatrix} x_1 & x_2 & 1 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & b_1 \\ a_{12} & a_{22} & b_2 \\ b_1 & b_2 & c \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ 1 \end{bmatrix} = 0.$$

Чтобы понять, как могут выглядеть кривые второго порядка, попробуем упростить вид уравнения с помощью замены координат $x = Py$, где матрица P имеет вид

$$P = P(\phi) := \begin{bmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{bmatrix}.$$

Такая матрица называется *матрицей вращения* — вектор y при умножении на P слева поворачивается на угол ϕ против часовой стрелки. Исходное уравнение кривой преобразуется следующим образом:

$$(APy, Py) + 2(b, Py) + c = 0 \Leftrightarrow (P^T APy, y) + 2(P^T b, y) + c = 0.$$

Утверждение 1.13.1. Для любой симметричной матрицы $A \in \mathbb{R}^{2 \times 2}$ существует матрица вращения $P = P(\phi)$, такая что матрица $P^T AP$ приобретает диагональный вид

$$P^T AP = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix},$$

где вещественные числа λ_1 и λ_2 являются корнями квадратного уравнения

$$\begin{vmatrix} a_{11} - \lambda & a_{12} \\ a_{12} & a_{22} - \lambda \end{vmatrix} = \lambda^2 - (a_{11} + a_{22})\lambda + |A| = 0.$$

Доказательство. Для произвольного значения ϕ находим

$$\begin{aligned} (P^T AP)_{12} &= (P^T AP)_{21} = \\ &= a_{12}(\cos^2 \phi - \sin^2 \phi) + (a_{22} - a_{11}) \cos \phi \sin \phi = \\ &= a_{12} \cos 2\phi - \frac{a_{11} - a_{22}}{2} \sin 2\phi. \end{aligned}$$

Если $a_{12} = 0$, то матрица A уже диагональная и можно взять $\phi = 0$. Если $a_{12} \neq 0$, то ϕ следует выбрать из условия

$$\operatorname{ctg} 2\phi = \frac{a_{11} - a_{22}}{2a_{12}}.$$

Далее,

$$\lambda_1 = a_{11} \cos^2 \phi + 2a_{12} \cos \phi \sin \phi + a_{22} \sin^2 \phi,$$

$$\lambda_2 = a_{11} \sin^2 \phi - 2a_{12} \cos \phi \sin \phi + a_{22} \cos^2 \phi \Rightarrow$$

$$\Rightarrow \lambda_1 + \lambda_2 = a_{11} + a_{22}, \quad \lambda_1 \lambda_2 = |P^\top| |A| |P| = |A|. \quad \square$$

Следствие 1.13.1. Для любой кривой второго порядка существует декартова система координат, в которой точки (y_1, y_2) данной кривой удовлетворяют уравнению вида

$$\lambda_1 y_1^2 + \lambda_2 y_2^2 + 2\beta_1 y_1 + 2\beta_2 y_2 + c = 0.$$

Если оба числа, λ_1 и λ_2 , отличны от нуля, то возможно выделение полных квадратов:

$$\underbrace{\lambda_1 \left(y_1 + \frac{\beta_1}{\lambda_1}\right)^2}_{=\lambda_1 z_1^2} + \underbrace{\lambda_2 \left(y_2 + \frac{\beta_2}{\lambda_2}\right)^2}_{=\lambda_2 z_2^2} + \underbrace{\left(c - \frac{\beta_1^2}{\lambda_1} - \frac{\beta_2^2}{\lambda_2}\right)}_{=\gamma} = 0 \Leftrightarrow \lambda_1 z_1^2 + \lambda_2 z_2^2 + \gamma = 0.$$

В случае $\lambda_1 \neq 0, \lambda_2 = 0$ выделяется только один полный квадрат:

$$\underbrace{\lambda_1 \left(y_1 + \frac{\beta_1}{\lambda_1}\right)^2}_{=\lambda_1 z_1^2} + 2\beta_2 y_2 + \underbrace{\left(c - \frac{\beta_1^2}{\lambda_1}\right)}_{=\gamma} = 0 \Leftrightarrow \lambda_1 z_1^2 + 2\beta_2 y_2 + \gamma = 0.$$

Если $\beta_2 = 0$, то получается уравнение $\lambda_1 z_1^2 + \gamma = 0$. Если $\beta_2 \neq 0$, то можно сделать еще одну замену:

$$\lambda_1 z_1^2 + 2\beta_2 \underbrace{\left(y_2 + \frac{\gamma}{2\beta_2}\right)}_{=2\beta_2 z_2} = 0 \Leftrightarrow \lambda_1 z_1^2 + 2\beta_2 z_2 = 0.$$

У нас получилось три типа «простых» уравнений:

$$(1) \lambda_1 z_1^2 + \lambda_2 z_2^2 + \gamma = 0; \quad (2) \lambda_1 z_1^2 + \gamma = 0; \quad (3) \lambda_1 z_1^2 + 2\beta_2 z_2 = 0,$$

где коэффициенты $\lambda_1, \lambda_2, \beta$ отличны от нуля, а значение γ произвольное. Эти уравнения называются *приведенными уравнениями* кривой второго порядка. Сформулируем то, что мы доказали.

Теорема 1.13.1. Для произвольной кривой второго порядка существует декартова система координат, в которой кривая задается приведенным уравнением вида (1), (2) либо (3).

Приведенное уравнение вида (1) называется уравнением *эллиптического типа*, если λ_1 и λ_2 одного знака, и *гиперболического типа*, если знаки разные.

Уравнение эллиптического типа можно привести к одному из трех видов:

$$\frac{x_1^2}{a^2} + \frac{x_2^2}{b^2} = 1, \quad \frac{x_1^2}{a^2} + \frac{x_2^2}{b^2} = 0, \quad \frac{x_1^2}{a^2} + \frac{x_2^2}{b^2} = -1.$$

В третьем случае решений нет. Во втором случае решение состоит из одной точки $(0, 0)$. Первый случай самый интересный и дает кривую, которая называется *эллипсом*. Традиционно считается, что $a \geq b > 0$. Очевидно, что точки $(\pm a, 0)$ и $(0, \pm b)$ принадлежат эллипсу, а сам он целиком расположен внутри прямоугольника $[-a, a] \times [-b, b]$. Точки $(\pm c, 0)$, где $c = \sqrt{a^2 - b^2}$, называются *фокусами* эллипса. Величина $e := c/a$ называется *эксцентриситетом* эллипса. Прямые $x_1 = \pm a/e$ называются *директрисами* эллипса. Если $e = 0$, то эллипс превращается в окружность. В случае $e > 0$ прямые $x_2 = 0$ и $x_1 = 0$ называются *осями эллипса*, причем первая — *главной осью*.

Утверждение 1.13.2. *Эллипс представляет собой геометрическое место точек, для каждой из которых:*

- *сумма расстояний до его фокусов постоянна и равна $2a$;*
- *отношение расстояний до фокуса $(c, 0)$ и до директрисы $x_1 = a/e$ в случае $e > 0$ постоянно и равно эксцентриситету e ;*
- *отношение расстояний до фокуса $(-c, 0)$ и до директрисы $x_1 = -a/e$ в случае $e > 0$ постоянно и равно эксцентриситету e .*

Доказательство. Пусть точка (x_1, x_2) принадлежит эллипсу $\frac{x_1^2}{a^2} + \frac{x_2^2}{b^2} = 1$. Нетрудно вычислить, что расстояния до фокусов $(c, 0)$ и $(-c, 0)$ соответственно равны

$$\sqrt{(x_1 - c)^2 + x_2^2} = \sqrt{(x_1 - c)^2 + b^2(1 - x_1^2/a^2)} = |a - ex_1| = a - ex_1,$$

$$\sqrt{(x_1 + c)^2 + x_2^2} = \sqrt{(x_1 + c)^2 + b^2(1 - x_1^2/a^2)} = |a + ex_1| = a + ex_1.$$

Их сумма равна $2a$. По аналогии с вычислениями из примера 2 в разделе 1.12 можно найти, что расстояния до директрис $x_1 =$

$= a/e$ и $x_1 = -a/e$ равны $|x_1 - a/e|$ и $|x_1 + a/e|$. Следовательно,

$$\frac{|a - ex_1|}{|x_1 - a/e|} = \frac{|a + ex_1|}{|x_1 + a/e|} = e. \quad \square$$

Уравнение гиперболического типа приводится к одному из двух видов:

$$\frac{x_1^2}{a^2} - \frac{x_2^2}{b^2} = 1, \quad \frac{x_1^2}{a^2} - \frac{x_2^2}{b^2} = 0.$$

Во втором случае получается пара пересекающихся прямых. Первый случай дает кривую, которая называется *гиперболой*. Гипербола состоит из двух *ветвей* — одна в полуплоскости $x_1 \geq a$, другая в полуплоскости $x_1 \leq -a$. Точки $(\pm c, 0)$, где $c := \sqrt{a^2 + b^2}$, называются *фокусами* гиперболы, величина $e := c/a$ называется *эксцентриситетом* гиперболы, а прямые $x_1 = \pm a/e$ — ее *директрисами*.

Прямые $x_2 = \pm(b/a)x_1$ называются *асимптотами* гиперболы. Проверьте, что если (x_1, x_2) — точка гиперболы и $x_1^2 + x_2^2 \rightarrow \infty$, то расстояние от этой точки до ближайшей к ней асимптоты стремится к нулю.

Утверждение 1.13.3. *Гипербола представляет собой геометрическое место точек, для каждой из которых:*

- абсолютная величина разности расстояний до фокусов постоянна и равна $2a$;
- отношение расстояний до фокуса $(c, 0)$ и до директрисы $x_1 = a/e$ постоянно и равно эксцентриситету e ;
- отношение расстояний до фокуса $(-c, 0)$ и до директрисы $x_1 = -a/e$ постоянно и равно эксцентриситету e .

Доказательство следует той же схеме, как и для эллипса, и предоставляется читателю.

Приведенное уравнение вида (2) исследуется особенно легко — множество решений может быть пустым, состоять из одной прямой либо из пары параллельных прямых. Приведенное уравнение вида (3) дает кривую, которая называется *параболой*. Обычно оно приводится к стандартному виду $x_2^2 = 2px_1$, где $p > 0$. Точка $(p/2, 0)$ называется *фокусом* параболы, а прямая $x_1 = -p/2$ называется ее *директрисой*.

Утверждение 1.13.4. *Парабола представляет собой геометрическое место точек, равноудаленных от ее фокуса и от ее директрисы.*

Доказательство предоставляется читателю.

Обратим внимание на то, что эллипсы, гиперболы и параболы получаются при пересечении разными плоскостями одной и той же круговой конической поверхности, заданной уравнением $x_1^2 + x_2^2 - x_3^2 = 0$ в трехмерном пространстве — их можно увидеть, например, направляя на стену свет от лампочки под коническим абажуром.

Интересно отметить некоторые общие геометрические свойства кривых второго порядка. Например, рассмотрим кривую $(Ax, x) + 2(b, x) + c = 0$ и семейство ее хорд, параллельных заданному вектору $h \neq 0$. Если $(Ah, h) = 0$, то направление h называется *асимптотическим*, в противном случае — *неасимптотическим*. Легко видеть, что прямых с асимптотическим направлением мало: в эллиптическом случае их нет, в гиперболическом случае два направления $h = (a, \pm b)$, а в остальных случаях только одно: $h = (0, 1)$ для приведенного уравнения вида $\lambda_1 x_1^2 + \gamma = 0$ и $h = (1, 0)$ для параболы, заданной уравнением $x_2^2 = 2px_1$.

Предположим, что $(Ah, h) \neq 0$, и пусть хорда определяется точками x и $x + th$ при $t \neq 0$, принадлежащими данной кривой. Тогда

$$\begin{aligned} (A(x + th), x + th) + 2(b, x + th) + c &= 0, \\ (Ax, x) + 2(b, x) + c &= 0 \Rightarrow \\ \Rightarrow t^2(Ah, h) + 2t(Ax + b, h) &= 0 \Rightarrow t = -\frac{2(Ax + b, h)}{(Ah, h)}. \end{aligned}$$

Середина z данной хорды имеет вид

$$z = x + \frac{t}{2} h = x - \frac{(Ax + b, h)}{(Ah, h)} h \Rightarrow (Ah, z) = -(b, h).$$

Отсюда вытекает, что точки z (середины хорд, параллельных вектору h) лежат на одной прямой, определяемой уравнением $(Ah, z) = -(b, h)$.

Если кривая обладает центром симметрии в точке z , то эта точка, очевидно, принадлежит каждой из прямых, содержащих середины параллельных хорд. Тогда $(Az, h) = (Ah, z) = -(b, h)$ для любого вектора h , такого что $(Ah, h) \neq 0$. Отсюда нетрудно вывести, что равенство $(Az + b, h) = 0$ выполняется вообще для любого вектора $h \Rightarrow Az + b = 0$. Таким образом, точка z есть решение системы линейных алгебраических уравнений $Az = -b$.

Для приведенного уравнения типа (1) матрица A невырожденная, поэтому система имеет единственное решение, а соответствующая кривая (в частности, эллипс или гипербола) обладает единственным центром симметрии. Если множество решений приведенного уравнения типа (2) непусто, то центры симметрии заполняют целую прямую. Для приведенного уравнения типа (3) система имеет вид

$$\begin{bmatrix} \lambda_1^2 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} 0 \\ -2\beta \end{bmatrix}, \quad \beta \neq 0,$$

и, очевидно, является несовместной $\Rightarrow$ центра симметрии нет. Вывод совершенно естественный, так как кривая представляет собой параболу.

Для кривых немалый интерес представляют *касательные прямые*. В общем случае *алгебраическая кривая* задается уравнением $f(x) = 0$, где $f(x)$ — ненулевой многочлен от координат вектора x . Прямая

$$x = x^{(0)} + th$$

называется *касательной в точке* $x^{(0)}$, если многочлен $F(t) := f(x^{(0)} + th) - f(x^{(0)})$ делится на t^2 и данное условие определяет направление h однозначно. Для кривой второго порядка $f(x) = (Ax, x) + 2(b, x) + c \Rightarrow F(t) = (Ah, h)t^2 + 2(Ax^{(0)} + b, h)t$. Поэтому направление h определяется условием $(Ax^{(0)} + b, h) = 0$ однозначно, если $Ax^{(0)} + b \neq 0$. Прямая

$$(Ax^{(0)} + b, x) + (b, x^{(0)}) + c = 0$$

имеет нормаль $Ax^{(0)} + b$ и, значит, направлена по вектору h , ортогональному нормали. Очевидно также, что она проходит через точку $x = x^{(0)}$. Следовательно, эта прямая является касательной в точке $x^{(0)}$.

Равенство $Ax^{(0)} + b = 0$ для точки $x^{(0)}$, принадлежащей кривой второго порядка, возникает только в одном случае — когда кривая представляет собой пару прямых, пересекающихся в точке $x^{(0)}$. Согласно нашему определению, в этой точке касательная не существует.

В заключение заметим, что в разных ситуациях полезно иметь в виду следующие *параметрические представления*:

$$x_1 = a \cos \phi, \quad x_2 = b \sin \phi, \quad 0 \leq \phi < 2\pi \quad (\text{эллипс});$$

$$x_1 = a \operatorname{ch}(\phi), \quad x_2 = b \operatorname{sh}(\phi),$$

$$-\infty < \phi < +\infty \quad (\text{ветвь гиперболы при } x_1 \geq a).$$

Функции

$$\operatorname{ch}(\phi) := \frac{\exp(\phi) + \exp(-\phi)}{2}, \quad \operatorname{sh}(\phi) := \frac{\exp(\phi) - \exp(-\phi)}{2}$$

называются соответственно *гиперболическим косинусом* и *гиперболическим синусом*.

Задача 25. В эллипс с ненулевым эксцентриситетом вписан прямоугольник. Докажите, что его стороны параллельны осям эллипса.

Задача 26. Найдите все прямые, которые имеют ровно одну общую точку с каждой ветвью гиперболы.

Задача 27. Даны две параболы, причем одна из них получается из другой сдвигом (параллельным переносом) в некоторую точку и поворотом на угол $\pi/2$ вокруг этой точки. Докажите, что точки пересечения этих парабол лежат на одной окружности.

Задача 28. Дана плоскость $A_0 + A_1x_1 + A_2x_2 + A_3x_3 = 0$, для которой $A_0 \neq 0$, и круговой конус $x_1^2 + x_2^2 - x_3^2 = 0$. Докажите, что в сечении конуса данной плоскостью получается эллипс, гипербола или парабола соответственно в том и только том случае, когда $A_1^2 + A_2^2 < A_3^2$, $A_1^2 + A_2^2 > A_3^2$ или $A_1^2 + A_2^2 = A_3^2$.

Задача 29. Точка $A = (0, 0, 2)$ принадлежит сфере

$$x_1^2 + x_2^2 + (x_3 - 1)^2 = 1,$$

и рассматривается отображение этой сферы на плоскость $x_3 = 0$, при котором точка M сферы отображается в точку M' таким образом, что прямая MM' проходит через точку A ¹⁾. Докажите, что любая окружность на сфере, проходящая через точку A , отображается в прямую, а любая окружность, не проходящая через точку A , отображается в окружность на плоскости $x_3 = 0$.

Задача 30. В трехмерном геометрическом пространстве рассматривается множество точек (x_1, x_2, x_3) , удовлетворяющих уравнению²⁾

$$x_1^2 + x_2^2 - x_3^2 = 1.$$

¹⁾ Такое отображение называется стереографической проекцией.

²⁾ Такая поверхность называется однополостным гиперболоидом.

Докажите, что через каждую точку этой поверхности проходят ровно две прямые, состоящие целиком из точек этой поверхности.

1.14. Ступенчатые матрицы и треугольные разложения

Пусть $i \neq j$ и $E_{ij}^{(n)}$ — матрица порядка n , в которой все элементы нулевые, кроме единицы в позиции (i, j) . Рассмотрим преобразования $A \rightarrow PA$ и $A \rightarrow AQ$, где

$$P = I_m + \alpha E_{ij}^{(m)}, \quad Q = I_n + \alpha E_{ij}^{(n)}.$$

Легко сообразить, что первое преобразование заключается в том, что к i -й строке матрицы A прибавляется j -я, умноженная на число α , а во втором преобразовании к j -му столбцу матрицы A прибавляется i -й, умноженный на число α . Оба преобразования будем называть *элементарными*.

Кроме того, умножение матрицы A слева или справа на матрицу перестановки также будем считать элементарным преобразованием. Любые матрицы перестановки и любые матрицы такого же вида, как P и Q , будем называть *элементарными матрицами*. Заметим, что каждая из них обратима. Интерес к элементарным преобразованиям объясняется тем, что с их помощью совершенно произвольную матрицу можно привести к очень простому виду, например к ступенчатому виду.

Ступенчатой матрицей с числом ступеней r называется матрица, в которой все строки, кроме первых r , нулевые, первые r строк ненулевые и все элементы матрицы, расположенные слева и ниже первого слева ненулевого элемента каждой строки, равны нулю. Вот примерный портрет ступенчатой матрицы размера 4×8 :

$$\begin{bmatrix} 0 & \boxtimes & \times & \times & \times & \times & \times & \times \\ 0 & 0 & 0 & \boxtimes & \times & \times & \times & \times \\ 0 & 0 & 0 & 0 & 0 & 0 & \boxtimes & \times \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Крестиком в прямоугольнике обозначены заведомо ненулевые элементы, а просто крестиком — элементы с произвольными значениями. По определению нулевая матрица является ступенчатой с числом ступеней 0.

Теорема 1.14.1. Для любой матрицы A размера $m \times n$ существуют элементарные матрицы $P_1, \dots, P_N$, такие что матрица $P_N P_{N-1} \dots P_1 A$ является ступенчатой матрицей с числом ступеней $r = \text{rang } A$.

Доказательство. Все ясно, если $A = 0$. Предположим, что $A \neq 0$, и проведем индукцию по m . Случай $m = 1$ очевиден. Пусть $m > 1$. Предположим, что первым слева ненулевым столбцом является j -й столбец, и пусть $a_{ij} \neq 0$. Если $i = 1$, то положим $P_1 = I_m$. Если $i > 1$, то в качестве P_1 выберем матрицу перестановки, соответствующую транспозиции $(1, i)$. Тогда в матрице $B := P_1 A$ первые $j - 1$ столбцов окажутся нулевыми и $b_{1j} \neq 0$. Пусть

$$P_k := I_m + \alpha_{k1} E_{k1}, \quad \alpha_{k1} := -\frac{b_{kj}}{b_{1j}}, \quad 2 \leq k \leq m, \Rightarrow$$

$$\Rightarrow C := P_m P_{m-1} \dots P_2 P_1 A =$$

$$= \begin{bmatrix} 0 & \dots & 0 & b_{1j} & b_{1,j+1} & \dots & b_{1n} \\ 0 & \dots & 0 & 0 & c_{2,j+1} & \dots & c_{2n} \\ 0 & \dots & 0 & 0 & c_{3,j+1} & \dots & c_{3n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & c_{m,j+1} & \dots & c_{mn} \end{bmatrix}.$$

Обозначим через C' матрицу размера $(m-1) \times n$, полученную из C вычеркиванием первой строки. По индуктивному предположению существуют элементарные матрицы порядка $m-1$, такие что $P'_N P'_{N-1} \dots P'_{m+1} C'$ — ступенчатая матрица с числом ступеней $r-1$. Тогда каждая из матриц

$$P_k := \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \dots & & P'_k & \\ 0 & & & \end{bmatrix}$$

также будет элементарной, а матрица

$$D := P_N P_{N-1} \dots P_m \dots P_1 A$$

будет ступенчатой с числом ступеней r . То, что $r = \text{rang } A$, можно вывести, например, из линейной независимости первых r строк матрицы D . $\square$

Заметим, что при получении ступенчатой матрицы использовались только преобразования вида $A \rightarrow PA$. Можно еще больше

упростить вид ступенчатой матрицы, используя умножения справа, т. е. преобразования вида $A \rightarrow AQ$.

Утверждение 1.14.1. Для любой ступенчатой матрицы A с числом ступеней r существуют элементарные матрицы $Q_1, \dots, Q_N$, такие что $AQ_1Q_2 \dots Q_N$ — матрица, в которой отличны от нуля элементы в позициях (i, i) при $1 \leq i \leq r$, а все остальные элементы равны нулю.

Доказательство. С помощью перестановок столбцов можно перейти к ступенчатой матрице B , в которой ненулевой элемент i -й строки находится в позиции (i, i) . Далее, транспонированная матрица B^T имеет ровно r ненулевых столбцов, причем первых. Кроме того, в соответствующих столбцах выше этих ненулевых элементов расположены только нули. В силу только что доказанной теоремы, с помощью элементарных преобразований строк B^T приводится к ступенчатому виду, в котором как раз и будет ровно r ненулевых элементов в позициях (i, i) . $\square$

В итоге можно получить такую полезную теорему.

Теорема 1.14.2. Для любой $m \times n$ -матрицы ранга r существуют невырожденные матрицы P и Q , такие что матрица PAQ имеет вид

$$\begin{bmatrix} I_r & 0_{r \times (n-r)} \\ 0_{(m-r) \times r} & 0_{(m-r) \times (n-r)} \end{bmatrix}.$$

Доказательство. Пусть матрица имеет ровно r ненулевых элементов, расположенных в позициях (i, i) при $1 \leq i \leq r$. К нужному виду она легко приводится умножением слева или справа на некоторую невырожденную диагональную матрицу. $\square$

Теперь предположим, что A — невырожденная матрица порядка n . При приведении такой матрицы к ступенчатому виду получается, очевидно, невырожденная верхняя треугольная матрица.

Теорема 1.14.3. Для любой невырожденной матрицы A существует разложение

$$A = PLU,$$

где P — матрица перестановки, L — нижняя и U — верхняя треугольные матрицы, обе невырожденные.

Доказательство. Очевидно, что с помощью перестановок строк из A можно получить матрицу B , в которой все миноры,

расположенные в левом верхнем углу, отличны от нуля (такие матрицы иногда называют *строго регулярными*):

$$\left| B \begin{pmatrix} 1, \dots, k \\ 1, \dots, k \end{pmatrix} \right| \neq 0, \quad 1 \leq k \leq n.$$

Таким образом, для некоторой матрицы перестановки P имеем $A = PB$, где B — строго регулярная матрица. Остается доказать, что для B существует *треугольное разложение*, т. е. разложение вида $B = LU$, где L — нижняя и U — верхняя треугольные матрицы. Это довольно легко делается с помощью индукции по порядку матрицы n .

Случай $n = 1$ тривиален. Пусть $n > 1$. С помощью элементарных матриц

$$P_k = I_n + \alpha_{k1} E_{k1}, \quad \alpha_{k1} = -\frac{b_{k1}}{b_{11}}, \quad 2 \leq k \leq n,$$

получаем

$$C := P_n P_{n-1} \dots P_2 A = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ 0 & & & \\ \dots & & C' & \\ 0 & & & \end{bmatrix},$$

где C' имеет порядок $n - 1$. Заметим, что

$$P_k^{-1} = I_n - \alpha_{k1} E_{k1}, \quad 2 \leq k \leq n,$$

все эти матрицы являются нижними треугольными и поэтому их произведение $\hat{L} := P_2^{-1} \dots P_n^{-1}$ также будет нижней треугольной матрицей, притом с единицами на главной диагонали. Таким образом, $B = \hat{L}C$. Отсюда

$$\begin{aligned} B \begin{pmatrix} 1, \dots, k \\ 1, \dots, k \end{pmatrix} &= \hat{L} \begin{pmatrix} 1, \dots, k \\ 1, \dots, k \end{pmatrix} C \begin{pmatrix} 1, \dots, k \\ 1, \dots, k \end{pmatrix} \Rightarrow \\ &\Rightarrow \left| B \begin{pmatrix} 1, \dots, k \\ 1, \dots, k \end{pmatrix} \right| = \left| \hat{L} \begin{pmatrix} 1, \dots, k \\ 1, \dots, k \end{pmatrix} \right| \left| C \begin{pmatrix} 1, \dots, k \\ 1, \dots, k \end{pmatrix} \right| = \\ &= b_{11} \left| C' \begin{pmatrix} 1, \dots, k-1 \\ 1, \dots, k-1 \end{pmatrix} \right| \Rightarrow \left| C' \begin{pmatrix} 1, \dots, k-1 \\ 1, \dots, k-1 \end{pmatrix} \right| \neq 0, \quad 2 \leq k \leq n. \end{aligned}$$

Таким образом, матрица C' порядка $n - 1$ является строго регулярной и к ней можно применить индуктивное предположение. Доказательство завершается уже очевидным образом. $\square$

Задача 31. В $n \times n$ -матрице A выбраны строки с номерами $1 \leq i_1 < \dots < i_k \leq n$ и столбцы с номерами $1 \leq j_1 < \dots < j_k \leq n$. Системы номеров $1 \leq i_{k+1} < \dots < i_n \leq n$ и $1 \leq j_{k+1} < \dots < j_n \leq n$ являются дополнительными к выбранным системам. Предполагается, что $1 \leq k \leq n-1$. Докажите, что если $|A| = 1$, то

$$\left| A^{-1} \begin{pmatrix} j_{k+1} & \dots & j_n \\ i_{k+1} & \dots & i_n \end{pmatrix} \right| = (-1)^{i_1+\dots+i_k+j_1+\dots+j_k} \left| A \begin{pmatrix} i_1 & \dots & i_k \\ j_1 & \dots & j_k \end{pmatrix} \right|.$$

Задача 32. Докажите, что для любой невырожденной матрицы A существует разложение вида $A = LPU$, где P — матрица перестановки, L — нижняя и U — верхняя треугольные матрицы. Докажите также, что в любом таком разложении матрица P одна и та же.

1.15. Алгоритмы и оценки сложности вычислений

Сколько арифметических операций нужно, чтобы решить ту или иную задачу? Конечно, прежде чем ставить такой вопрос, необходимо еще доказать, что задача вообще решается с помощью арифметических операций над ее исходными данными. Например, число $\sqrt{2}$ нельзя получить, используя арифметические операции над рациональными числами.

Рассмотрим вопрос о решении системы $Ax = b$ с невырожденной вещественной матрицей A порядка n . Основная идея наиболее популярного метода — *метода исключения элементов* или, как его часто называют, *метода Гаусса* — привести матрицу A к треугольному виду с помощью элементарных преобразований строк, те же преобразования применить к правой части b , а потом уже вполне очевидным образом найти решение системы с треугольной матрицей. Приведение к треугольному виду выполняется таким образом:

- 1) $k := 1$.
- 2) Среди элементов k -го столбца в позициях (i, k) при $k \leq i \leq n$ найти ненулевой элемент, пусть это будет a_{ik} , и переставить k -ю и i -ю строки.
- 3) В k -м столбце преобразованной матрицы исключить все элементы ниже главной диагонали: для этого при $k+1 \leq i \leq n$ из i -й строки вычитается k -я, умноженная на число.

- 4) Увеличить значение k на единицу и, если новое значение меньше n , повторить те же действия начиная со второго пункта.

Данный алгоритм представляет собой цикл с параметром k , изменяющимся от 1 до $n - 1$ с шагом 1. Для каждого значения k число операций умножения имеет вид $(n - k)^2$, и нетрудно доказать (например по индукции), что общее число операций умножения таково:

$$\sum_{k=1}^{n-1} (n - k)^2 = \sum_{k=1}^{n-1} k^2 = \frac{1}{3} n^3 + an^2 + bn + c,$$

где a, b, c — некоторые числа, не зависящие от n . Их конкретные значения не очень интересны, так как *главный член* с ростом порядка n имеет, очевидно, вид $\frac{1}{3} n^3$. Такой же вид имеет главный член для общего числа вычитаний. Все остальные действия укладываются в $O(n^2)$ операций.

Можно ли получить алгоритм с меньшим числом арифметических действий, или, как говорят, меньшей *арифметической сложности*? В 1967 г. Штрассен предъявил алгоритм сложности $O(n^{\log_2 7})$. Поскольку $\log_2 7 < 3$, это алгоритм асимптотически меньшей сложности! Открытие Штрассена базируется на полученном им новом алгоритме для умножения $n \times n$ -матриц.

Пусть даны $n \times n$ -матрицы A и B и нужно вычислить их произведение $C = AB$. Известное нам правило «строка на столбец» выражается формулой

$$c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}$$

и, очевидно, дает алгоритм, в котором ровно n^3 умножений и $n^3 - n^2$ сложений.

По-видимому, впервые нетривиальный подход к умножению матриц был обнаружен Виноградом. Он обратил внимание на следующее легко проверяемое тождество:

$$\begin{aligned} \sum_{k=1}^{2m} a_{ik} b_{kj} &= \sum_{k=1}^m (a_{i,2k-1} + b_{2k,j})(b_{2k-1,j} + a_{i,2k}) - \\ &\quad - \sum_{k=1}^m a_{i,2k-1} a_{i,2k} - \sum_{k=1}^m b_{2k,j} b_{2k-1,j}. \end{aligned}$$

Если $n = 2m$, то для вычисления второй и третьей сумм справа достаточно $2nm = n^2$ умножений. Для первой суммы потребуется $n^2m = \frac{1}{2}n^3$ умножений — вдвое меньше, чем для правила «строка на столбец». Конечно, сложений окажется больше — их будет $3n^2m = \frac{3}{2}n^3$. Тем не менее алгоритм Винограда является одним из наиболее полезных нетривиальных алгоритмов умножения матриц в тех случаях, когда цена умножения существенно больше цены сложения.

Довольно общая идея, в том числе и в алгоритме Штрассена, заключается в следующем: придумать способ умножения блочных $p \times p$ -матриц

$$A = \begin{bmatrix} A_{11} & \dots & A_{1p} \\ \dots & \dots & \dots \\ A_{p1} & \dots & A_{pp} \end{bmatrix}, \quad B = \begin{bmatrix} B_{11} & \dots & B_{1p} \\ \dots & \dots & \dots \\ B_{p1} & \dots & B_{pp} \end{bmatrix},$$

$$A_{ij}, B_{ij} \in \mathbb{R}^{q \times q},$$

в котором имеется строго меньше чем p^3 умножений блоков, а после этого алгоритм для умножения матриц порядка $n = p^s$ строится по рекурсии.

Пусть число блочных умножений равно μ . Тогда на первом шаге рекурсии исходная задача сводится к μ задачам умножения матриц порядка p^{s-1} , на втором шаге появляется μ^2 задач умножения матриц порядка p^{s-2} и так далее. На последнем, s -м шаге мы обнаруживаем, что исходная задача редуцировалась к μ^s задачам умножения матриц порядка $p^{s-s} = 1$. Следовательно, общее число скалярных умножений оказывается равным μ^s . Если $\mu < p^3$, то

$$\mu^s = \mu^{\log_p n} = n^{\log_p \mu} < p^{3s} = n^3,$$

т. е. число скалярных умножений в новом алгоритме с ростом n асимптотически меньше, чем в классическом правиле «строка на столбец».

Остается найти подходящий алгоритм для блочных $p \times p$ -матриц для какого-то значения p . Штрассен сделал это для $p = 2$ и получил $\mu = 7$. Позже Виктор Пан заметил, что общий метод получения таких алгоритмов связан с построением специальных разложений для *трехмерных матриц* — таблиц, в которых эле-

менты снабжены тремя индексами. В самом деле, пусть C — блочная $p \times p$ -матрица, составленная из блоков C_{k_1, k_2} . Тогда

$$C_{k_1, k_2} = \sum_{i_1=1}^p \sum_{i_2=1}^p \sum_{j_1=1}^p \sum_{j_2=1}^p \gamma_{i_1, i_2, j_1, j_2, k_1, k_2} A_{i_1, i_2} B_{j_1, j_2},$$

где $\gamma_{i_1, i_2, j_1, j_2, k_1, k_2}$ — числа, равные 0 или 1, — их нетрудно найти, пользуясь определением операции умножения матриц.

Введем мультииндексы $i = (i_1, i_2)$, $j = (j_1, j_2)$, $k = (k_1, k_2)$ и будем писать

$$h_{ijk} := \gamma_{i_1, i_2, j_1, j_2, k_1, k_2}, \quad A_i := A_{i_1, i_2}, \quad B_j := B_{j_1, j_2}, \quad C_k := C_{k_1, k_2}.$$

Теперь попытаемся представить функцию h от мультииндексов i, j, k в виде суммы числовых функций с *разделенными переменными* i, j, k :

$$h_{ijk} = \sum_{\alpha=1}^R u_i^{(\alpha)} v_j^{(\alpha)} w_k^{(\alpha)}.$$

Совершенно очевидно, что какое-то разложение такого типа существует всегда. Нас, однако, интересует разложение с как можно меньшим числом слагаемых R . Минимально возможное число R называется *тензорным рангом* трехмерной матрицы с элементами h_{ijk} . Получение минимального разложения — это уже очень нетривиальная задача. Тем не менее, пусть получено какое-то разложение данного типа, не обязательно минимальное. Тогда

$$C_k = \sum_{\alpha=1}^R w_k^{(\alpha)} X_k^{(\alpha)} Y_k^{(\alpha)}, \quad X_k^{(\alpha)} = \sum_i u_i^{(\alpha)} A_i, \quad Y_k^{(\alpha)} = \sum_j v_j^{(\alpha)} B_j.$$

Эти формулы предлагают алгоритм, в котором ровно R умножений блоков. Остальные операции — это сложение блоков и умножение блока на число. В случае $p = 2$ можно найти бесконечно много разложений, для которых $R = 7$ ¹⁾. Итак, если $p = 2$, то мы получаем алгоритм умножения блочных 2×2 матриц с числом блочных умножений $\mu = R = 7$. Рекурсия приводит к алгоритму для $n \times n$ -матриц с числом скалярных умножений $n^{\log_2 7}$, если n — степень двойки, и $O(n^{\log_2 7})$ в общем случае. В качестве

¹⁾ С использованием компьютера построение таких разложений в данном частном случае реализуется на базе вполне естественных подходов и притом довольно легко, в общем случае дело обстоит иначе.

упражнения полезно проверить, что *общее число арифметических операций* также имеет вид $O(n^{\log_2 7})$.

В заключение отметим одно тождество, чем-то напоминающее тождество Винограда:

$$\begin{aligned} \sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n (a_{ij} b_{jk} x_{ki} + c_{jk} d_{ki} y_{ij}) = \\ = \sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n (a_{ij} + c_{jk})(b_{jk} + d_{ki})(x_{ki} + y_{ij}) - \\ - \sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n (a_{ij} + c_{jk}) d_{ki} x_{ki} - \sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n a_{ij} (b_{jk} + d_{ki}) y_{ij} - \\ - \sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n c_{jk} b_{jk} (x_{ki} + y_{ij}). \end{aligned}$$

Будем считать, что оно представляет собой равенство многочленов от букв x_{ki} и y_{ij} .

Рассмотрим $n \times n$ -матрицы $A = [a_{ij}]$, $B = [b_{jk}]$, $C = [c_{jk}]$, $D = [d_{ki}]$. Как легко заметить, коэффициент при x_{ki} в левой части — это в точности элемент матрицы AB в позиции (i, k) , а коэффициент при y_{ij} — это элемент произведения CD в позиции (j, i) . Вид правой части позволяет найти коэффициенты при этих буквах, затратив лишь $n^3 + 3n^2$ умножений!

В самом деле, очевидно, что первая сумма в правой части дает эти n^3 умножений. Обозначим через α_{ki} коэффициенты при x_{ki} для многочлена, определяемого второй суммой. Эти коэффициенты получаются таким образом:

$$u_{ik} := \sum_{j=1}^n (a_{ij} + c_{jk}), \quad \alpha_{ki} := u_{ik} d_{ki} \quad 1 \leq i, k \leq n.$$

Как видим, для получения α_{ki} умножений требуется ровно n^2 .

Аналогично, обозначим через β_{ij} коэффициенты при y_{ij} из третьей суммы. Для них нужно также n^2 умножений:

$$v_{ji} := \sum_{k=1}^n (b_{jk} + d_{ki}), \quad \beta_{ij} := a_{ij} v_{ji}, \quad 1 \leq i, j \leq n.$$

Теперь обозначим через γ_{ki} и δ_{ij} коэффициенты соответственно при x_{ki} и при y_{ij} в четвертой сумме. Потребуется n^2 умножений, чтобы найти

$$w_{jk} := c_{jk} b_{jk}, \quad 1 \leq j, k \leq n.$$

Далее,

$$\gamma_{ki} = \sum_{j=1}^n w_{jk}, \quad \delta_{ij} = \sum_{k=1}^n w_{jk}.$$

Окончательно, коэффициенты при x_{ki} и при y_{ij} для всей правой части имеют вид $\alpha_{ki} + \gamma_{ki}$ и $\beta_{ij} + \delta_{ij}$ соответственно. В итоге все суммы, кроме первой, дают вместе $3n^2$ умножений.

То, что у нас получилось, кажется поразительным: матрицы AB и CD можно получить за $n^3 + 3n^2$ умножений — два произведения практически по цене одного.

Задача 33. Придумайте алгоритм умножения блочных 10×10 -матриц, в котором будет меньше $10^3 = 1000$ умножений блоков.

Задача 34. Пусть имеется система $Ax = b$ с невырожденной матрицей A порядка n . Применение формул Крамера требует вычисления $n + 1$ определителей. Придумайте, как их можно найти, затратив лишь $O(n^3)$ арифметических операций.

Задача 35. Дана невырожденная матрица A порядка n и известно, что любые две матрицы порядка p можно перемножить, затратив не более sr^α арифметических операций, $s > 0$ и $2 < \alpha < 3$ — константы, не зависящие от p . Докажите, что матрица A^{-1} может быть вычислена с затратой $O(n^\alpha)$ арифметических операций.

1.16. Комплексные числа и комплексные матрицы

Комплексные числа можно ввести, например, как вещественные арифметические векторы с двумя координатами и разумным образом определенными операциями сложения и умножения. Это означает, что комплексные числа можно представлять точками (или радиус-векторами) на плоскости с декартовой системой координат. Именно так решается вопрос о наглядном представлении комплексных чисел — это точки (радиус-векторы) на комплексной плоскости. Итак, по определению, комплексное число имеет вид $z = (u, v)$, где $u, v \in \mathbb{R}$. Вещественное число u называется вещественной частью комплексного числа z , а v — его мнимой частью. Величина $\sqrt{u^2 + v^2}$ называется модулем комплексного числа z . Обозначения:

$$\operatorname{Re} z := u, \quad \operatorname{Im} z := v, \quad |z| := \sqrt{u^2 + v^2}.$$

Комплексное число вида $(u, 0)$, $u \in \mathbb{R}$, отождествляется с вещественным числом u . Комплексное число вида $(0, 1)$ называется *мнимой единицей* и обозначается $\mathbf{i} = (0, 1)$. Множество комплексных чисел обозначается $\mathbb{C}$ и расширяет множество вещественных чисел, т. е. $\mathbb{R} \subsetneq \mathbb{C}$.

Теперь мы должны ввести операции. Заметим, что у нас уже есть операция сложения арифметических векторов и операция умножения их на вещественные числа. Нетривиальный вопрос — как умножать арифметические векторы? Чтобы его решить, мы, конечно же, должны четко сформулировать, какие свойства мы ожидаем от операции умножения.

Вещественное число α отождествляется с вектором $(\alpha, 0)$, и мы будем писать $\alpha = (\alpha, 0)$. Таким образом, вот одно из требований к операции умножения:

- $(\alpha, 0)(a_1, a_2) = \alpha(a_1, a_2) = (\alpha a_1, \alpha a_2) \quad \forall \alpha \in \mathbb{R}, \forall (a_1, a_2) \in \mathbb{C}$ (согласованность).

Мы получаем естественную и удобную форму записи

$$a = (a_1, a_2) = a_1 + a_2 \mathbf{i} = \operatorname{Re} a + \operatorname{Im} a \mathbf{i}.$$

От умножения потребуем выполнения следующих свойств:

- $(a + b)c = ac + bc$, $c(a + b) = ca + cb$ (дистрибутивность умножения относительно сложения);
- $(\alpha a)(\beta b) = (\alpha\beta)ab \quad \forall \alpha, \beta \in \mathbb{R}, \forall a, b \in \mathbb{C}$ (билинейность произведения);
- уравнения $ax = b$ и $ya = b$ разрешимы при любом b и любом $a \neq 0$ (деление);
- $(ab)c = a(bc)$ (ассоциативность умножения);
- $ab = ba$ (коммутативность умножения).

Наша задача — *обеспечить все эти свойства*. Кроме того, введем также условие перемножения модулей:

- $|ab| = |a||b| \quad \forall a, b \in \mathbb{C}$.

Чтобы понять, как должна определяться операция умножения комплексных чисел, достаточно знать, какое число является квадратом мнимой единицы. Предположим, что $\mathbf{i}^2 = u + v\mathbf{i}$, $u, v \in \mathbb{R}$. Тогда

$$(a_1 + a_2 \mathbf{i})(b_1 + b_2 \mathbf{i}) = (a_1 b_1 + a_2 b_2 u) + (a_1 b_2 + a_2 b_1 + a_2 b_2 v) \mathbf{i}.$$

Запишем условие перемножения модулей:

$$|\mathbf{i}^2| = \sqrt{u^2 + v^2} = |\mathbf{i}|^2 = 1 \Rightarrow u^2 + v^2 = 1;$$

$$\begin{aligned}
 (a_1^2 + a_2^2)(b_1^2 + b_2^2) &= (a_1b_1 + a_2b_2u)^2 + (a_1b_2 + a_2b_1 + a_2b_2v)^2 \Rightarrow \\
 \Rightarrow 0 &= (1 - u^2 - v^2)a_2^2b_2^2 = 2a_1a_2b_1b_2(1 + u) + \\
 &\quad + 2a_2b_2(a_1b_2 + a_2b_1)v.
 \end{aligned}$$

В частности, при $a_1 = 0$ и $a_2 = b_1 = b_2 = 1$ находим $2v = 0 \Rightarrow v = 0$. Далее, при $a_1 = a_2 = b_1 = b_2 = 1$ находим $2(1 + u) = 0 \Rightarrow u = -1$.

Следовательно, $\mathbf{i}^2 = (-1, 0)$ и умножение комплексных чисел должно определяться следующим правилом:

$$(a_1 + a_2\mathbf{i})(b_1 + b_2\mathbf{i}) := (a_1b_1 - a_2b_2) + (a_1b_2 + a_2b_1)\mathbf{i}.$$

Все свойства из списка наших требований к умножению проверяются без особых трудностей.

Пусть z — ненулевое комплексное число. На комплексной плоскости оно представляется ненулевым радиус-вектором. Обозначим через ϕ угол, образуемый этим вектором с осью вещественных чисел. Число ϕ называется *аргументом* комплексного числа z . Его значение считается определенным с точностью до $2\pi k$, где k — целое число. Запись

$$z = |z|(\cos \phi + \mathbf{i} \sin \phi)$$

называется *тригонометрической формой* комплексного числа z .

Утверждение 1.16.1. При умножении ненулевых комплексных чисел их модули перемножаются, а аргументы складываются.

Доказательство. Пусть

$$\begin{aligned}
 a &= |a|(\cos \phi + \mathbf{i} \sin \phi), \quad b = |b|(\cos \psi + \mathbf{i} \sin \psi) \Rightarrow \\
 \Rightarrow ab &= |a||b|((\cos \phi \cos \psi - \sin \phi \sin \psi) + \\
 &\quad + \mathbf{i}(\sin \phi \cos \psi + \cos \phi \sin \psi)) = \\
 &= |a||b|(\cos(\phi + \psi) + \mathbf{i} \sin(\phi + \psi)). \quad \square
 \end{aligned}$$

Утверждение 1.16.2 (НЕРАВЕНСТВО ТРЕУГОЛЬНИКА). Для любых комплексных чисел a и b выполняется неравенство

$$|a + b| \leq |a| + |b|.$$

Доказательство. На комплексной плоскости числа 0 , a и $a + b$ задают вершины треугольника. Интересующее нас неравенство означает, что длина стороны в этом треугольнике не превосходит суммы длин остальных сторон. $\square$

Пусть $z = z_1 + i z_2$, $z_1, z_2 \in \mathbb{R}$. Тогда число $\bar{z} := z_1 - i z_2$ называется *сопряженным* числу z . На комплексной плоскости точки z и $\bar{z}$ расположены симметрично относительно оси вещественных чисел.

Утверждение 1.16.3. Для любых чисел $x, y \in \mathbb{C}$ имеют место равенства

$$\overline{x + y} = \bar{x} + \bar{y}, \quad \overline{xy} = \bar{x}\bar{y}.$$

Утверждение 1.16.4. Если $0 \neq x \in \mathbb{C}$, то

$$x^{-1} = \frac{\bar{x}}{|x|^2}.$$

Все понятия, введенные нами для вещественных арифметических векторов, остаются в силе и для комплексных арифметических векторов. В частности, можно говорить о линейно зависимых и независимых системах комплексных векторов и о базисе и размерности комплексного векторного пространства.

Множество всех комплексных матриц размера $m \times n$ обозначается $\mathbb{C}^{m \times n}$. Комплексные матрицы складываются и умножаются по тем же правилам, что и вещественные матрицы. Для квадратной комплексной матрицы определитель вычисляется по той же формуле, что и для вещественной матрицы. Понятие обратной матрицы вводится так же. Все свойства определителя те же.

Некоторые новые свойства связаны с операцией сопряжения для комплексных чисел. Матрица $B = [b_{ji}] \in \mathbb{C}^{n \times m}$ называется *сопряженной* к матрице $A = [a_{ij}] \in \mathbb{C}^{m \times n}$, если $b_{ji} = \overline{a_{ij}}$ для всех $1 \leq i \leq m$, $1 \leq j \leq n$. Обозначение: $B = A^*$.

Матрица A называется *самосопряженной* или *эрмитовой*, если $A^* = A$. Если $A^* = -A$, то A называется *косоэрмитовой*. Если $A^T = A$, то матрица A называется *симметричной*, а если $A^T = -A$, то *кососимметричной*. Квадратная матрица A называется *унитарной*, если она обратима и $A^{-1} = A^*$. Вещественная унитарная матрица называется *ортогональной*.

Утверждение 1.16.5. Пусть A и B — комплексные матрицы и произведение AB существует. Тогда $(AB)^* = B^*A^*$.

Утверждение 1.16.6. Если A — квадратная комплексная матрица, то $|A^*| = |A|$. Если матрица A обратима, то

$$(A^*)^{-1} = (A^{-1})^*.$$

Можно ли придумать «числа», которые задаются вещественными арифметическими векторами, скажем, с тремя координатами? Гамильтон пытался это сделать, но безуспешно. Позже Фробениус доказал, что это невозможно. Однако, Гамильтон обнаружил «почти числа» с четырьмя координатами, названные *кватернионами* — «почти» потому, что умножение кватернионов уже не обладает свойством коммутативности. Оказывается, других «почти чисел», для которых число координат больше четырех, уже нет — это также доказано Фробениусом.

Задача 36. Некто задумал ввести новую операцию умножения на множестве вещественных арифметических векторов вида (a_1, a_2) таким образом, чтобы сохранялись все требования к умножению, за исключением условия перемножения модулей. Пусть новое умножение определяется правилом $(0, 1)^2 := (u, v)$. Найдите все возможные значения для координат u и v .

Задача 37. Докажите, что любая квадратная матрица однозначно представима в виде суммы эрмитовой и косоеэрмитовой матриц.

Задача 38. Пусть $A \in \mathbb{C}^{m \times n}$ и $x \in \mathbb{C}^{n \times 1}$. Докажите, что из равенства $A^*Ax = 0$ вытекает равенство $Ax = 0$.

Задача 39. Пусть n — натуральное число и

$$\varepsilon = \cos(2\pi/n) + i \sin(2\pi/n).$$

Докажите, что $n \times n$ -матрица F с элементами $f_{ij} = \varepsilon^{(i-1)(j-1)}$ является обратимой и обратная матрица имеет вид

$$F^{-1} = \frac{1}{n} F^*.$$

Задача 40. Матрица порядка $n \geq 4$ имеет элементы, равные $\pm a$, где a — комплексное число, и является унитарной. Докажите, что n делится на 4.

Задача 41. Предположим, что на множестве вещественных арифметических векторов $V_n(\mathbb{R})$ введена ассоциативная

и дистрибутивная операция умножения, допускающая деление и согласованная с операцией умножения векторов на вещественные числа следующим образом:

$$(\alpha, 0, \dots, 0)(a_1, a_2, \dots, a_n) = (\alpha_1 a_1, \alpha_2 a_2, \dots, \alpha_n a_n),$$

$$\alpha, a_1, \dots, a_n \in \mathbb{R}.$$

Коммутативность умножения не предполагается. Пусть известно ¹⁾, что для каждого вектора $a \in V_n(\mathbb{R})$ имеется представление вида

$$a^2 = \alpha(a) \cdot \mathbf{1} + \beta(a) a, \quad \alpha(a), \beta(a) \in \mathbb{R}, \quad \mathbf{1} = (1, 0, \dots, 0).$$

Докажите, что множество L векторов $a \in V_n(\mathbb{R})$, таких что $a^2 = (\alpha, 0, \dots, 0)$ и $\alpha \leq 0$, должно быть векторным пространством. Докажите также, что любой вектор $z \in V_n(\mathbb{R})$ представляется в виде суммы $z = \alpha \cdot \mathbf{1} + a$, где $\alpha \in \mathbb{R}$ и $a \in L^2$.

¹⁾ Этот факт можно вывести из основной теоремы алгебры, которая у нас появится в гл. 4, и из теории линейных операторов, излагаемой в гл. 5.

²⁾ Отсюда уже не так трудно вывести, что для n возможны только три случая: $n = 1, 2, 4$.

Глава 2

ЧТО НУЖНО ЗНАТЬ О ГРУППАХ

2.1. Определение группы

Бинарной операцией на множестве G со значениями в множестве M называется отображение $f: G \times G \rightarrow M$, т. е. функция $f(a, b)$, зависящая от *двух* аргументов, a и b , определенная при всех $a, b \in G$ и такая, что ее значения являются элементами множества M . Для операции вводится какой-нибудь символ, часто $+$, $\times$, $\otimes$, $\cdot$ или просто пустое место. Чтобы подчеркнуть, что речь идет о совершенно общей ситуации, мы будем какое-то время использовать символ $*$, с его помощью результат операции записывается в виде

$$a * b := f(a, b).$$

Группой называется непустое множество G с бинарной операцией, обладающей следующими свойствами:

- $a * b \in G$ для любых $a, b \in G$ (замкнутость);
- $a * (b * c) = (a * b) * c$ для любых $a, b, c \in G$ (ассоциативность);
- для любых $a, b \in G$ существуют $x, y \in G$ такие, что $a * x = b$ и $y * a = b$ (существование правой и левой обратной операции).

Утверждение 2.1.1. *В группе G существует единственный элемент e , такой что для любого $a \in G$ имеют место равенства $a * e = e * a = a$.*

Доказательство. Зафиксируем произвольный элемент $a \in G$. Уравнение $a * x = a$ имеет хотя бы одно решение, пусть $e_{\Pi} \in G$ — одно из решений, т. е. $a * e_{\Pi} = a$. Возьмем произвольный элемент $b \in G$. Согласно определению группы, существует $y \in G$, такой что $y * a = b$. Тогда

$$a * e_{\Pi} = a \Rightarrow y * (a * e_{\Pi}) = y * a = b.$$

В то же время в силу ассоциативности $y * (a * e_{\Pi}) = (y * a) * e_{\Pi} = b * e_{\Pi}$. Таким образом, для любого $b \in G$ имеем $b * e_{\Pi} = b$.

Аналогично доказывается существование элемента $e_{\Lambda} \in G$, такого что для любого $b \in G$ выполняется равенство $e_{\Lambda} * b = b$. Докажем, что $e_{\Lambda} = e_{\Pi}$. Поскольку любой элемент сохраняется при умножении на e_{Π} справа, имеем $e_{\Lambda} * e_{\Pi} = e_{\Lambda}$. В то же время любой элемент сохраняется при умножении на e_{Λ} слева, поэтому $e_{\Lambda} * e_{\Pi} = e_{\Pi}$. Итак, $e := e_{\Pi} = e_{\Lambda}$.

Единственность доказывается следующим образом. Пусть $a * e_1 = e_1 * a = a$ и $e_2 * a = a * e_2 = a$ для всех $a \in G$. Тогда $e_1 = e_1 * e_2 = e_2$. $\square$

Элемент $e \in G$ со свойством $a * e = e * a = a \ \forall a \in G$ называется *нейтральным элементом* группы G .

Пусть a — произвольный элемент группы G . Элемент $b \in G$ со свойством $a * b = b * a = e$ называется *обратным элементом* для элемента a .

Утверждение 2.1.2. Пусть e — нейтральный элемент группы G . Тогда для любого элемента $a \in G$ существует единственный элемент $b \in G$, такой что

$$a * b = b * a = e.$$

Доказательство. Обозначим через b_{Π} и b_{Λ} решения уравнений $a * x = e$ и $y * a = e$. Тогда

$$b_{\Lambda} * (a * b_{\Pi}) = b_{\Lambda} * e = b_{\Lambda},$$

$$(b_{\Lambda} * a) * b_{\Pi} = e * b_{\Pi} = b_{\Pi}.$$

Из ассоциативности следует, что $b_{\Lambda} = b_{\Pi}$. Элемент $b := b_{\Lambda} = b_{\Pi}$ является искомым. Пусть b_1 и b_2 — два элемента с тем же свойством. Тогда

$$(b_1 * a) * b_2 = e * b_2 = b_2, \quad b_1 * (a * b_2) = b_1 * e = b_1 \Rightarrow b_1 = b_2. \quad \square$$

Эквивалентное определение группы. Группой называется непустое множество G с бинарной операцией, обладающей следующими свойствами:

- $a * b \in G \ \forall a, b \in G$;
- $a * (b * c) = (a * b) * c \ \forall a, b, c \in G$;
- $\exists e \in G : a * e = e * a = a \ \forall a \in G$;
- $\forall a \in G \exists b \in G : a * b = b * a = e$.

Доказательство эквивалентности определений. Пусть G — группа в смысле первого определения. Согласно вышеприведенным утверждениям в G имеется единственный нейтральный элемент и для каждого элемента существует единственный обратный элемент. Таким образом, выполнены все требования второго определения.

Пусть G — группа в смысле второго определения. Рассмотрим уравнение $a * x = b$. Если оно имеет решение, то это решение единственно. В самом деле, пусть c — обратный элемент для a . Тогда

$$a * x = b \Rightarrow c * (a * x) = (c * a) * x = e * x = x = c * b.$$

В то же время, взяв $x := c * b$, находим

$$a * x = a * (c * b) = (a * c) * b = e * b = b.$$

Аналогично рассматривается уравнение $y * a = b$. □

Обратим внимание на то, что в общем случае $a * b \neq b * a$. Если $a * b = b * a \ \forall a, b \in G$, то группа G называется *коммутативной* или *абелевой*.

Группа, имеющая конечное число элементов, называется *конечной группой*. Число элементов конечной группы G называется *порядком группы G* и обозначается $|G|$.

Примеры бинарных операций, не порождающих группу.

- G — множество геометрических векторов на плоскости, M — множество трехмерных векторов, $a * b := [a, b]$ — векторное произведение векторов $a, b \in G$. Эта операция не является замкнутой на множестве G , так как для линейно независимых векторов $[a, b] \in M \setminus G$.
- G — множество положительных рациональных чисел, $a * b := a/b$ — обычное деление. Эта операция замкнута и уравнения $a/x = b$ и $y/a = b$ всегда имеют решения. Но нет ассоциативности: $1/2 = (2/2)/2 \neq 2/(2/2) = 2$.
- G — множество натуральных чисел, $a * b := a + b$ — обычное сложение. Эта операция замкнута и ассоциативна. В таких случаях множество G называется *полугруппой*. Если к G добавить ноль, то получится полугруппа с нейтральным элементом — такие полугруппы называются *моноидами*. Обратных элементов нет, так как в G нет отрицательных чисел.

Пример бесконечной абелевой группы. Множество $\mathbb{Z}$ целых чисел относительно операции сложения.

Пример бесконечной неабелевой группы. Множество невырожденных матриц порядка n с вещественными элементами относительно операции умножения матриц. Эта группа называется *полной* или *общей линейной группой* и обозначается $GL(n, \mathbb{R})$. Множество вещественных матриц порядка n с определителем 1 относительно той же операции образует *специальную линейную группу*, которая обозначается $SL(n, \mathbb{R})$.

Пример конечной абелевой группы. Пусть n — натуральное число. Обозначим через $[a]$ множество всех целых чисел, имеющих при делении на n такой же остаток, как и число a . Множества вида $[a]$ называются *вычетами по модулю n* . Всего различных вычетов по модулю n имеется ровно n . Определим операцию сложения вычетов следующим образом:

$$[a] + [b] := [a + b].$$

Это определение корректно, так как из равенств

$$[a] = [\hat{a}], \quad [b] = [\hat{b}]$$

легко выводится, что $[a + b] = [\hat{a} + \hat{b}]$. Множество вычетов по модулю n относительно операции сложения вычетов является абелевой группой порядка n .

Пример конечной неабелевой группы. Пусть X — множество из n элементов и S_n — множество всех взаимно-однозначных отображений X на себя. Такие отображения называются *подстановками*. Операция композиции отображений превращает S_n в группу. Замкнутость, очевидно, есть. Ассоциативность всегда имеет место для композиции отображений. Нейтральный элемент — это тождественное отображение, обратные элементы задаются обратными отображениями. Группа S_n имеет порядок $n!$ и называется *симметрической группой степени n* .

Группы в геометрии. Один из подходов к описанию предмета геометрии — определять ее как науку о свойствах фигур, остающихся *инвариантными* (неизменными) при взаимно-однозначных преобразованиях пространства, образующих группу относительно композиции преобразований. Например, можно рассмотреть *аффинные преобразования* плоскости. Аффинным преобразованием называется композиция двух преобразований:

параллельного переноса и линейного преобразования. Чтобы определить линейное преобразование, фиксируется система координат и невырожденная вещественная матрица A порядка 2. Точка с координатами (x, y) преобразуется в точку с координатами $(\hat{x}, \hat{y})$ по правилу

$$\begin{bmatrix} \hat{x} \\ \hat{y} \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix}.$$

Можно доказать, что при любом аффинном преобразовании пересекающиеся прямые переходят в пересекающиеся прямые. Более того, пусть точки M, A, B переходят в точки $\widehat{M}, \widehat{A}, \widehat{B}$. Если M лежит на прямой между A и B , то $\widehat{M}$ находится на прямой между $\widehat{A}$ и $\widehat{B}$ и при этом $|AM|/|MB| = |\widehat{A}\widehat{M}|/|\widehat{M}\widehat{B}|$. Используя этот факт, можно получить, например, доказательство известной теоремы о том, что три медианы треугольника пересекаются в одной точке: с помощью некоторого аффинного преобразования любой треугольник можно перевести в равносторонний, для которого свойство медиан проверяется тривиально.

Задача 42. Докажите, что множество аффинных преобразований плоскости с операцией композиции преобразований образует группу.

Задача 43. Докажите, что существует аффинное преобразование, переводящее заданный треугольник в любой другой заданный треугольник.

Задача 44. Докажите, что если три точки M, A, B лежат на одной прямой, то при аффинном преобразовании их образы $\widehat{M}, \widehat{A}, \widehat{B}$ также лежат на одной прямой и сохраняется отношение $|AM|/|MB| = |\widehat{A}\widehat{M}|/|\widehat{M}\widehat{B}|$.

Задача 45. Пусть e — нейтральный элемент группы G и для любого элемента $a \in G$ имеет место равенство $a * a = e$. Докажите, что группа G является абелевой.

Задача 46. Докажите, что множество матриц вида

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ a_1 & 1 & 0 & 0 \\ a_2 & a_1 & 1 & 0 \\ a_3 & a_2 & a_1 & 1 \end{bmatrix},$$

где $a_1, a_2, a_3 \in \mathbb{Z}$, является абелевой группой относительно умножения матриц.

Задача 47. Докажите, что множество чисел вида $a + b\sqrt{3}$, где a, b — произвольные рациональные числа с условием $a^2 + b^2 \neq 0$, образует группу относительно операции умножения чисел.

2.2. Избыточность в определении группы

В рассмотренных выше определениях группы часть требований можно отбросить и получить как следствие других требований.

Теорема 2.2.1. Пусть G — непустое множество с бинарной операцией, которая имеет следующие свойства:

- $a * b \in G \quad \forall a, b \in G$;
- $a * (b * c) = (a * b) * c \quad \forall a, b \in G$;
- $\exists e \in G : a * e = a \quad \forall a \in G$ (существование правого нейтрального элемента);
- $\forall a \in G \exists b \in G : a * b = e$ (существование правого обратного элемента).

Тогда G является группой.

Доказательство. Докажем, что правый нейтральный элемент является также и левым нейтральным. Пусть $e * a = x$. Тогда для некоторого b имеем: $a * b = e$. Следовательно,

$$(e * a) * b = e * (a * b) = e * e = e = x * b = a * b.$$

Для некоторого c выполняется равенство $b * c = e$. Поэтому

$$\begin{aligned} x * b = a * b &\Rightarrow (x * b) * c = (a * b) * c = x * (b * c) = x * e = \\ &= x = a * (b * c) = a * e = a \Rightarrow x = a, \end{aligned}$$

что и требовалось доказать.

Далее, пусть $a * b = e$. Тогда

$$b * (a * b) = b * e = b = (b * a) * b.$$

Пусть элемент c обладает свойством $b * c = e$. Тогда

$$b = (b * a) * b \Rightarrow e = b * c = (b * a) * (b * c) = (b * a) * e = b * a. \quad \square$$

Задача 48. Докажите, что множество нижних треугольных матриц порядка n с целыми элементами и определите-

лем 1 является группой относительно операции умножения матриц. Найдите все значения n , при которых эта группа является абелевой.

Задача 49. Докажите, что все невырожденные вещественные $n \times n$ -матрицы, имеющие вид ¹⁾

$$\begin{bmatrix} a_0 & a_{n-1} & \dots & a_2 & a_1 \\ a_1 & a_0 & \ddots & \ddots & a_2 \\ \dots & \ddots & \ddots & \ddots & \dots \\ a_{n-2} & \ddots & \ddots & a_0 & a_{n-1} \\ a_{n-1} & a_{n-2} & \dots & a_1 & a_0 \end{bmatrix},$$

образуют группу относительно операции умножения матриц.

Задача 50. Пусть G — множество всех вещественных невырожденных $n \times n$ -матриц, в которых невырожденной является также любая подматрица, расположенная в левом верхнем углу. Является ли G группой относительно умножения матриц?

2.3. Аддитивные и мультипликативные группы

Группа называется *аддитивной*, если ее операция именуется сложением и обозначается знаком $+$. В аддитивной группе нейтральный элемент называется *нулевым* и обозначается символом 0 . Обратный элемент для a называется *противоположным* и обозначается $-a$. Аддитивная символика обычно применяется только для абелевых групп.

Пусть n — целое число. Определим n -кратное элемента a следующим образом:

- если $n > 0$, то

$$n \cdot a := \underbrace{a + \dots + a}_{n \text{ раз}};$$

- если $n = 0$, то

$$0 \cdot a := 0;$$

- если $n = -k$, $k > 0$, то

$$n \cdot a := k \cdot (-a).$$

¹⁾ Такие матрицы называются циркулянтными.

Утверждение 2.3.1. Пусть a — элемент аддитивной группы. Тогда

$$(m + n) \cdot a = m \cdot a + n \cdot a \quad \forall m, n \in \mathbb{Z}.$$

Доказательство. Если $m, n > 0$, то

$$(m + n) \cdot a = \underbrace{(a + \dots + a)}_{m \text{ раз}} + \underbrace{(a + \dots + a)}_{n \text{ раз}} = m \cdot a + n \cdot a.$$

Пусть $m > k > 0$ и $n = -k$. Тогда

$$\begin{aligned} (m + n) \cdot a &= \underbrace{a + \dots + a}_{m - k \text{ раз}} = \underbrace{(a + \dots + a)}_{m \text{ раз}} + \underbrace{((-a) + \dots + (-a))}_{k \text{ раз}} = \\ &= m \cdot a + n \cdot a. \end{aligned}$$

Остальные случаи разбираются аналогично. $\square$

Группа называется *мультипликативной*, если ее операция именуется умножением и обозначается пустым местом (иногда точкой). В мультипликативной группе нейтральный элемент называется *единичным* или *единицей*. Обычно для него используется обозначение e или даже 1 . Обратный для a элемент обозначается a^{-1} .

Пусть a — элемент мультипликативной группы и $n \in \mathbb{Z}$. Вот определение n -й степени элемента a :

- если $n > 0$, то

$$a^n := \underbrace{a \cdot \dots \cdot a}_{n \text{ раз}};$$

- если $n = 0$, то

$$a^0 := e;$$

- если $n = -k$, $k > 0$, то

$$a^n := (a^{-1})^k.$$

Утверждение 2.3.2. Пусть a — элемент мультипликативной группы. Тогда

$$a^{m+n} = a^m a^n \quad \forall m, n \in \mathbb{Z}.$$

Доказательство проводится по той же схеме, что и в случае кратных в аддитивной группе.

Пусть m — натуральное число. Говорят, что элемент a мультипликативной группы G имеет *порядок* m , если $a^m = e$ и $a^l \neq e$

при всех $1 \leq l \leq m - 1$. Обозначение: $m = \text{ord}(a)$. Если $a^k = e$ исключительно при $k = 0$, то a называется элементом *бесконечного порядка*. В этом и только этом случае все степени элемента a различны: $a^k \neq a^l$ при $k \neq l$.

Задача 51. Пусть $A \in \mathbb{Q}^{n \times n}$ — какая-то невырожденная матрица порядка n . Докажите, что множество всех матриц вида A^k , где $k \in \mathbb{Z}$, является группой относительно операции умножения матриц.

Задача 52. Пусть $A \in \mathbb{Q}^{n \times n}$ имеет вид

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{bmatrix}.$$

Докажите, что множество всех целых степеней матрицы A является группой по умножению матриц, в которой ровно n матриц. Найдите порядок элемента этой группы, имеющего вид $B = A^2$.

Задача 53. Пусть G — абелева группа, a и b — ее элементы порядка m и n соответственно. Докажите, что если числа m и n взаимно просты, то порядок элемента $c = ab$ равен mn . Верно ли это в случае, когда m и n имеют нетривиальный общий делитель?

2.4. Изоморфизмы групп

Рассмотрим два примера групп:

- 1) Группа G всех вещественных чисел относительно операции сложения чисел.
- 2) Группа $\hat{G}$ положительных вещественных чисел относительно операции умножения чисел.

Формально G и $\hat{G}$ — это разные группы. Но являются ли эти группы *различными в теории групп*? При изучении групп нас интересуют прежде всего свойства операций. Если эти свойства одни и те же для формально разных групп, то такие группы можно считать *одинаковыми с точки зрения свойств операций*.

Пусть G и $\hat{G}$ — группы с операциями $*$ и $\hat{*}$. Отображение $f: G \rightarrow \hat{G}$ называется *изоморфизмом*, если оно является *взаимно-однозначным* и *сохраняет операцию* в том смысле, что

$$f(a * b) = f(a) \hat{*} f(b) \quad \forall a, b \in G.$$

Будем говорить, что группа G *изоморфна* группе $\hat{G}$. Обозначение: $G \cong \hat{G}$.

Мы получаем бинарное отношение на множестве групп, которое, как несложно проверить, является рефлексивным, симметричным и транзитивным. Таким образом, все группы разбиваются на классы изоморфных между собой групп.

Утверждение 2.4.1. Пусть e и $\hat{e}$ — нейтральные элементы групп G и $\hat{G}$. Если $f: G \rightarrow \hat{G}$ — изоморфизм, то:

- $f(e) = \hat{e}$;
- $f(a^{-1}) = (f(a))^{-1} \quad \forall a \in G$.

Доказательство. Любой элемент группы $\hat{G}$ имеет вид $f(a)$ для некоторого $a \in G$. В силу сохранения операции

$$f(a) = f(a * e) = f(e * a) = f(a) \hat{*} f(e) = f(e) \hat{*} f(a).$$

Следовательно, $f(e) = \hat{e}$. Далее,

$$\hat{e} = f(e) = f(a * a^{-1}) = f(a^{-1} * a) = f(a) \hat{*} f(a^{-1}) = f(a^{-1}) \hat{*} f(a).$$

Значит, $(f(a))^{-1} = f(a^{-1})$. □

Если группы изоморфны, то существует хотя бы одно взаимно-однозначное и сохраняющее операцию отображение одной группы на другую. Таких отображений может быть и несколько. Изоморфизм группы G на себя называется *автоморфизмом*.

Утверждение 2.4.2. Пусть g — произвольно выбранный элемент группы G . Отображение $f(a) := gag^{-1}$, $a \in G$, является *автоморфизмом группы G* .

Доказательство. При данном отображении разные элементы переходят в разные: $gag^{-1} = bgg^{-1} \Rightarrow a = b$. Кроме того, для каждого элемента $b \in G$ имеется элемент, который в него переходит: $f(g^{-1}bg) = g(g^{-1}bg)g^{-1} = b$. Таким образом, отображение f является взаимно-однозначным. Сохранение операции проверяется очевидным образом: $f(a)f(b) = (gag^{-1})(gbg^{-1}) = g(ab)g^{-1} = f(ab)$. □

Отображение вида $f(a) = gag^{-1}$ при фиксированном $g \in G$ называется *внутренним автоморфизмом группы G* .

Задача 54. Докажите, что группа всех вещественных чисел по сложению изоморфна группе положительных вещественных чисел по умножению, но не изоморфна группе всех ненулевых вещественных чисел по умножению.

Задача 55. Докажите, что группа целых чисел относительно операции сложения чисел не изоморфна группе положительных рациональных чисел относительно операции умножения чисел.

Задача 56. Докажите, что аддитивная группа рациональных чисел не изоморфна аддитивной группе вещественных чисел.

Задача 57. Докажите, что множество автоморфизмов заданной группы образует группу относительно композиции автоморфизмов.

Задача 58. Найдите все автоморфизмы группы целых чисел по сложению.

Задача 59. Приведите пример группы, имеющей бесконечно много автоморфизмов.

2.5. Группа корней n -й степени из единицы

Рассмотрим множество C_n всех комплексных чисел z , таких что $z^n = 1$. Легко проверяется, что C_n является группой относительно операции умножения комплексных чисел.

Утверждение 2.5.1. В группе C_n всего n различных чисел.

Доказательство. Запишем z в тригонометрической форме:

$$z = \cos \phi + i \sin \phi.$$

Тогда

$$z^n = \cos n\phi + i \sin n\phi.$$

Равенство $z^n = 1$ означает, что

$$\cos n\phi = 1, \quad \sin n\phi = 0 \Leftrightarrow \phi = \frac{2\pi}{n} k, \quad k \in \mathbb{Z}.$$

Различные значения получаются при $k = 0, 1, \dots, n-1$. □

Пусть

$$\varepsilon = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \Rightarrow C_n = \{1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}\}, \quad \varepsilon^n = 1.$$

Корень $\zeta \in C_n$ называется *первообразным*, если его порядок в группе C_n равен n и, следовательно,

$$C_n = \{\zeta^k, k = 0, 1, \dots, n-1\}.$$

Утверждение 2.5.2. Корень ε^m является первообразным корнем n -й степени из 1 в том и только том случае, когда целые числа m и n взаимно просты.

Пусть $\phi(n)$ обозначает число взаимно простых с n натуральных чисел в промежутке от 1 до n . Функция $\phi(n)$ называется *функцией Эйлера*. Из утверждения 2.5.2 следует, что число первообразных корней n -й степени из 1 есть $\phi(n)$.

Теорема 2.5.1. Пусть $p_1, \dots, p_t$ — попарно различные простые числа и $s_1, \dots, s_t$ — натуральные числа. Тогда

$$\phi(p_1^{s_1} \dots p_t^{s_t}) = (p_1^{s_1} - p_1^{s_1-1}) \dots (p_t^{s_t} - p_t^{s_t-1}).$$

Доказательство. Прежде всего установим следующее свойство функции Эйлера: если $(m, n) = 1$ (т.е. m и n взаимно просты), то

$$\phi(mn) = \phi(m)\phi(n).$$

Рассмотрим целые числа вида

$$mx + ny \quad \text{при} \quad 0 \leq x \leq n-1, \quad 0 \leq y \leq m-1$$

и заметим, что все эти mn чисел имеют разные остатки при делении на mn . В самом деле, пусть

$$(mx_1 + ny_1) - (mx_2 + ny_2) = m(x_1 - x_2) + n(y_1 - y_2) : mn.$$

Тогда

$$m(x_1 - x_2) : n, \quad (m, n) = 1 \Rightarrow x_1 - x_2 : n.$$

Среди чисел в промежутке $-n+1 \leq x_1 - x_2 \leq n-1$ на n делится только 0, поэтому $x_1 = x_2$. Аналогично, $y_1 = y_2$. Чтобы найти значение $\phi(mn)$, достаточно просмотреть числа вида $mx + ny$ при $0 \leq x \leq n-1, 0 \leq y \leq m-1$ и посчитать, сколько из них являются взаимно простыми с mn .

Предположим, что простое число p является общим делителем чисел $mx + ny$ и mn . Поскольку m и n взаимно просты, либо $m : p$, либо $n : p$. В первом случае

$$mx + ny : p, \quad m : p \Rightarrow ny : p, \quad (n, p) = 1 \Rightarrow y : p.$$

Во втором случае $mx \vdots p$ и поэтому $x \vdots p$. Таким образом,

$$(mx + ny, mn) = 1 \Leftrightarrow (x, n) = 1, (y, m) = 1.$$

Таких пар x, y в промежутке $0 \leq x \leq n - 1, 0 \leq y \leq m - 1$ ровно $\phi(m)\phi(n)$.

Установленное свойство функции Эйлера приводит к формуле

$$\phi(p_1^{s_1} \dots p_t^{s_t}) = \phi(p_1^{s_1}) \dots \phi(p_t^{s_t}),$$

и уже вполне очевидный подсчет показывает, что в случае простого числа p

$$\phi(p^s) = p^s - p^{s-1}. \quad \square$$

Задача 60. Пусть ε — произвольный корень n -й степени из 1. Докажите, что коэффициенты многочлена

$$f(x) = (x - \varepsilon)(x - \varepsilon^2) \dots (x - \varepsilon^{n-1})$$

являются целыми числами.

2.6. Группы и подгруппы

В дальнейшем мы, как правило, будем использовать мультипликативную символику для групп. Пусть G — группа и H — некоторая часть элементов множества G . Если для любых $a, b \in H$ также $ab, a^{-1}, b^{-1} \in H$, то множество $H \subseteq G$ называется *подгруппой* группы G . Обозначение: $H \leq G$.

Любая подгруппа является сама группой относительно операции группы G . Каждая из подгрупп содержит единицу группы G . Очевидно, что множества $H = \{e\}$ и $H = G$ являются подгруппами. Они называются *тривиальными подгруппами*, первая из них называется *единичной*. Если группа аддитивная, то подгруппа, состоящая из одного лишь нулевого элемента, называется *нулевой*.

Пример 1. Множество четных подстановок образует подгруппу в симметрической группе S_n . Эта подгруппа называется *знакопеременной группой степени n* и обозначается A_n .

Пример 2. Пусть G — произвольная группа и a — любой из ее элементов. Множество $Z(a) := \{g \in G: ga = ag\}$ называется *централизатором* элемента a и, как нетрудно проверить, является подгруппой. Пересечение всех централизаторов

$Z(G) := \bigcap_{a \in G} Z(a)$ называется *центром* группы G — это подгруппа, в которой собраны все элементы, коммутирующие с каждым из элементов группы G .

Пример 3. Найдем все подгруппы в аддитивной группе целых чисел $\mathbb{Z}$. Пусть $H \leq \mathbb{Z}$ — ненулевая подгруппа. Тогда H содержит какие-то положительные целые числа. Пусть n — наименьшее из них. Возьмем теперь произвольное число $m \in H$ и поделим его с остатком на n :

$$m = nq + r, \quad 0 \leq r \leq n - 1.$$

Ясно, что $r \in H$ и поэтому $r = 0$, иначе m не было бы наименьшим положительным числом из H . Следовательно, H содержит только те числа, которые делятся на n . При этом все такие числа обязаны входить в H , иначе H не было бы подгруппой. Естественно использовать обозначение $H = n\mathbb{Z}$.

Пусть $A, B \subseteq G$. Определим *произведение множеств* A и B следующим образом:

$$AB := \{ab : a \in A, \quad b \in B\}.$$

Для аддитивной группы аналогично определяется *сумма множеств*:

$$A + B := \{a + b : a \in A, \quad b \in B\}.$$

Далее мы продолжаем работать с мультипликативными группами.

Утверждение 2.6.1. Для любой подгруппы $H \leq G$ и любого элемента $a \in G$ множество aHa^{-1} является подгруппой группы G .

Доказательство. Пусть $h_1, h_2 \in H$. Тогда $(ah_1a^{-1})(ah_2a^{-1}) = a(h_1h_2)a^{-1} \in aHa^{-1}$. Кроме того, $(aha)^{-1} = a^{-1}h^{-1}(a^{-1})^{-1}$. $\square$

Подгруппа aHa^{-1} называется *сопряженной* подгруппе H . Элемент aha^{-1} называется *сопряженным* элементу h .

Задача 61. Докажите, что порядок знакопеременной группы A_n равен $n!/2$. Найдите все подгруппы симметрической группы S_n , сопряженные подгруппе A_n .

2.7. Смежные классы и нормальные подгруппы

Пусть $H \leq G$ и $a \in G$. Множество $Ha = \{ha: h \in H\}$ называется *правым смежным классом* группы G по подгруппе H , а множество $aH = \{ah: h \in H\}$ — *левым смежным классом*.

Теорема 2.7.1 (ТЕОРЕМА ЛАГРАНЖА). *Порядок подгруппы в конечной группе является делителем порядка группы.*

Доказательство. Предположим, что правые смежные классы Ha и Hb имеют общий элемент c . Тогда

$$c = h_1a = h_2b.$$

H является группой $\Rightarrow Hh = H \forall h \in H$. Отсюда $Hc = Ha = Hb$. Следовательно, два правых смежных класса либо совпадают, либо не пересекаются. Значит, множество G является объединением конечного числа непересекающихся правых смежных классов. Остается заметить, что в любом правом смежном классе одно и то же число элементов, равное порядку подгруппы H . $\square$

Заметим, что в общем случае $Ha \neq aH$. Например, в группе $G = GL(n, \mathbb{R})$ невырожденных вещественных матриц порядка n подмножество H невырожденных верхних треугольных матриц является подгруппой. Однако произведение ah матриц

$$a = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \in G \quad \text{и} \quad h = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in H$$

нельзя представить в виде h_1a , где $h_1 \in H$, так как

$$aha^{-1} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ -1/2 & 3/2 \end{bmatrix} \notin H.$$

Операцию умножения подмножеств в мультипликативной группе можно рассматривать как бинарную операцию на множестве, скажем, правых смежных классов, но в общем случае она не будет замкнутой на этом множестве. Приведенный выше пример показывает, что произведение смежных классов $Ha \cdot Ha^{-1}$ не совпадает со смежным классом $H = He$, где e — единичная матрица, и поэтому не может совпадать ни с каким смежным классом.

В каком случае произведение любых правых смежных классов совпадает с каким-то правым смежным классом? Предположим, что $(Ha)(Hb) = Hc$. Тогда $ab \in Hc$ и, следовательно,

$Hc = H(ab)$. Таким образом, $(Ha)(Hb) = H(ab)$. Отсюда вытекает, что для любого $h \in H$ существует элемент $h_1 \in H$, такой что $ahb = h_1ab \Rightarrow ah = h_1a \Rightarrow aH \subseteq Ha \Rightarrow aHa^{-1} \subseteq H \subseteq a^{-1}Ha$.

Подгруппа $H \leq G$ называется *нормальной подгруппой* или *нормальным делителем*, если $aHa^{-1} \in H$ для любого элемента $a \in G$ и любого элемента $h \in H$. Другими словами, подгруппа H является нормальной в группе G , если она содержит любую сопряженную себе подгруппу. Обозначение: $H \trianglelefteq G$.

Утверждение 2.7.1. *Подгруппа содержит любую сопряженную себе подгруппу в том и только том случае, когда она совпадает с любой сопряженной себе подгруппой.*

Доказательство. Пусть $H \leq G$ и $aHa^{-1} \subseteq H$. В силу произвольности $a \in G$ включение выполняется также при замене a на a^{-1} . Поэтому для любого $h \in H$ имеем

$$h_1 := a^{-1}ha \in H \Rightarrow h = ah_1a^{-1} \Rightarrow H \subseteq aHa^{-1} \Rightarrow H = aHa^{-1}. \quad \square$$

Очевидно, что равенство $aHa^{-1} = H$ равносильно равенству $Ha = aH$. Таким образом, в случае нормальной подгруппы H правый смежный класс по подгруппе H для любого элемента совпадает с левым смежным классом для того же элемента.

Утверждение 2.7.2. *Для нормальной подгруппы множество ее смежных классов относительно операции умножения смежных классов является группой.*

Доказательство. Пусть $H \trianglelefteq G$. Обозначим через G/H множество смежных классов G по H . Поскольку $aH = Ha$ и $HH = H$, находим $(Ha)(Hb) = H(aH)b = H(Ha)b = (HH)(ab) = H(ab)$, т.е. $(Ha)(Hb) \in G/H$. Ассоциативность умножения смежных классов вытекает из ассоциативности умножения в группе G :

$$Ha \cdot (Hb \cdot Hc) = Ha \cdot Hbc = Habc = Hab \cdot Hc = (Ha \cdot Hb) \cdot Hc.$$

Единицей является смежный класс $He = H$. Поскольку $(Ha)(Ha^{-1}) = He = H$, обратным для смежного класса Ha является смежный класс Ha^{-1} . $\square$

Если $H \trianglelefteq G$, то группа смежных классов относительно умножения смежных классов называется *фактор-группой* группы G по подгруппе H и обозначается G/H .

Пример 1. В аддитивной группе $\mathbb{Z}$ множество $n\mathbb{Z}$ всех целых чисел, кратных натуральному числу n , является нормальной подгруппой, а фактор-группа $\mathbb{Z}/n\mathbb{Z}$ совпадает с группой вычетов по модулю n .

Пример 2. В любой группе G ее центр $Z(G) = \{a \in G: ag = ga \forall g \in G\}$ является нормальной подгруппой.

Может так случиться, что подгруппа H не является нормальной в группе G , но является нормальной подгруппой какой-то подгруппы $G_1 \leq G$. Множество

$$N(H) := \{g \in G: gHg^{-1} = H\}$$

называется *нормализатором* подгруппы H . Легко проверяемые свойства $N(H) \leq G$ и $H \leq N(H)$ вполне объясняют название. Подгруппа H нормальна в G тогда и только тогда, когда $G = N(H)$. Ясно также, что $G_1 \leq N(H)$, т.е. нормализатор является самой большой подгруппой, в которой H нормальна.

Задача 62. Докажите, что в группе простого порядка нетривиальных подгрупп нет.

Задача 63. Докажите, что в группе нечетного порядка ≥ 3 каждый элемент коммутирует хотя бы с одним элементом, кроме себя самого и единицы.

Задача 64. Докажите, что в группе четного порядка n любая подгруппа порядка $n/2$ нормальна.

Задача 65. Докажите, что если группа абелева, то любая ее подгруппа нормальна. Верно ли обратное утверждение?

Задача 66. Пусть G — мультипликативная группа вещественных невырожденных матриц порядка n , H_1 — подмножество матриц с определителем 1, H_2 — подмножество невырожденных верхних треугольных матриц. Докажите, что H_1 и H_2 являются подгруппами G . Выясните, являются ли они нормальными подгруппами.

Задача 67. Докажите, что множество внутренних автоморфизмов группы G является нормальной подгруппой в группе всех ее автоморфизмов. Докажите также, что подгруппа внутренних автоморфизмов изоморфна фактор-группе группы G по ее центру $Z(G)$.

Задача 68. Пусть $A, B \leq G$ и G — конечная группа. Докажите, что число элементов в произведении AB равно

$$|AB| = \frac{|A||B|}{|A \cap B|}.$$

Задача 69. Пусть $H < G$. Докажите, что конечную группу G нельзя представить в виде объединения подгрупп, сопряженных с подгруппой H .

Задача 70. Пусть $A \trianglelefteq G$ и $B \leq G$. Доказать, что $AB \leq G$.

Задача 71. Элемент группы G , представимый в виде $c = aba^{-1}b^{-1}$, называется коммутатором элементов a и b . Множество $C(G)$ всех произведений любого конечного числа коммутаторов называется коммутантом группы G . Докажите, что $C(G) \leq G$.

Задача 72. Пусть $H \leq A_4$ и известно, что H содержит тройной цикл (123) и является нормальной подгруппой в A_4 . Докажите, что $H = A_4$.

Задача 73. Докажите, что в знакопеременной группе A_5 нет нетривиальных (отличных от нее самой и от единичной подгруппы) нормальных подгрупп.

2.8. Циклические группы

Пусть a — произвольный элемент группы G . Рассмотрим множество всех его целых степеней:

$$\langle a \rangle := \{a^k, \quad k \in \mathbb{Z}\}.$$

Группа G называется *циклической*, если $G = \langle a \rangle$ для некоторого $a \in G$.

Группа C_n является примером циклической группы порядка n , но в определенном смысле она же является единственной циклической группой порядка n . Группа целых чисел $\mathbb{Z}$ по сложению является примером бесконечной циклической группы.

Теорема 2.8.1. Все циклические группы порядка n изоморфны. Все бесконечные циклические группы также изоморфны.

Доказательство. Пусть $G = \langle a \rangle$ и $\hat{G} = \langle \hat{a} \rangle$. Искомое отображение определим правилом $f: a^k \rightarrow \hat{a}^k$. Но будет ли такое определение корректным?

Если группы имеют разное число элементов, например $|G| = 2$ и $|\hat{G}| = 3$, то такого отображения просто не существует! В самом деле, $f(e) = \hat{e}$ и одновременно $f(e) = f(a^2) = \hat{a}^2 \neq \hat{e}$.

Однако, по условию конечные группы G и $\hat{G}$ имеют один и тот же порядок. Пусть $n = |G| = |\hat{G}|$. Тогда

$$a^k = a^l \Leftrightarrow k - l : n \Leftrightarrow \hat{a}^k = \hat{a}^l,$$

поэтому отображение определено корректно. Элементы $a^0, \dots, a^{n-1}$ — это все различные элементы группы G , а их образы $\hat{a}^0, \dots, \hat{a}^{n-1}$ — это все различные элементы группы $\hat{G}$. Значит, отображение f взаимно-однозначно.

Оно сохраняет операцию, так как

$$f(a^k a^l) = f(a^{k+l}) = \hat{a}^{k+l} = \hat{a}^k \hat{a}^l = f(a^k) f(a^l).$$

Таким образом, отображение f является изоморфизмом. Случай бесконечных групп разбирается аналогично. $\square$

Теорема 2.8.2. *Любая подгруппа циклической группы является циклической группой.*

Доказательство. Пусть подгруппа $H \leq G = \langle a \rangle$ отлична от единичной подгруппы. Тогда в H имеются какие-то элементы вида a^k как при отрицательных, так и при положительных целых k . Пусть m — наименьшее натуральное m такое, что $a^m \in H$. Рассмотрим произвольный элемент $a^k \in H$ и поделим k на m с остатком:

$$k = mq + r, \quad 0 \leq r \leq m - 1.$$

Тогда $a^r = a^k ((a^m)^{-1})^q \in H$ и, следовательно, $r = 0$, иначе m не было бы наименьшим. Итак, $k : m$, т.е. любой элемент из H имеет вид h^q , где $h := a^m$. Поскольку H является подгруппой, все целые степени элемента h обязаны входить в H . Таким образом, $H = \langle h \rangle$. $\square$

Задача 74. Докажите, что циклическая группа всегда абелева, и приведите примеры конечных и бесконечных абелевых групп, которые не являются циклическими.

Задача 75. Докажите, что в любой бесконечной группе имеется бесконечно много нетривиальных подгрупп.

Задача 76. Найдите число автоморфизмов для циклической группы порядка 2014.

Задача 77. Пусть X — непустое подмножество элементов конечной группы G порядка n и X_k — множество всех k -членных произведений элементов из множества X (произведений вида $x_1 \dots x_k$, где $x_i \in X$). Докажите, что множество $H = X_1 \cup \dots \cup X_n$ является подгруппой в G .

Задача 78. Найдите с точностью до изоморфизма все группы порядка 4 и 6.

2.9. Действие группы на множестве

Нередко с элементами мультипликативной группы G ассоциируются взаимно-однозначные отображения некоторого непустого множества X на себя. В таких случаях говорят, что определено *действие группы G на множестве X* .

При этом разные элементы группы G могут соответствовать одному и тому же отображению, но требуется, чтобы для любых $g_1, g_2 \in G$ и для каждого $x \in X$ выполнялось равенство

$$(g_1 g_2)(x) = g_1(g_2(x)).$$

Отсюда следует, что единичному элементу $e \in G$ должно соответствовать тождественное отображение: $e(e(x)) = e^2(x) = e(x)$ и в силу взаимной однозначности каждый элемент множества X имеет вид $e(x)$. Заметим также, что обратному элементу соответствует обратное отображение:

$$y = g(x) \Rightarrow g^{-1}(y) = g^{-1}(g(x)) = (g^{-1}g)(x) = e(x) = x.$$

Действие группы на множестве может задаваться по-разному. Если $X = G$, то действие G на G можно определить, например, как *действие умножением*: $g(x) := gx$. Или же как *действие сопряжением*: $g(x) := xgx^{-1}$. В конкретных ситуациях надо оговаривать, как именно определяется действие.

Для фиксированного $x \in X$ множество $G(x) := \{g(x) \in X : g \in G\}$ называется *орбитой* элемента $x \in X$. Множество $G_x := \{g \in G : g(x) = x\}$ называется *стабилизатором* элемента $x \in X$. Для фиксированного элемента g группы G множество $X_g := \{x \in X : g(x) = x\}$ называется *множеством неподвижных точек* для $g \in G$.

Утверждение 2.9.1. Стабилизатор G_x элемента $x \in G$ является подгруппой в G .

Доказательство. Пусть $g_1(x) = x$ и $g_2(x) = x$. Тогда, конечно же, $(g_1g_2)(x) = g_1(g_2(x)) = x$ и $g_1^{-1}(x) = x$. $\square$

Утверждение 2.9.2. *Длина орбиты $G(x)$ равна числу правых (левых) смежных классов группы G по стабилизатору G_x .*

Доказательство. Равенство $g_1(x) = g_2(x)$ равносильно равенству $(g_2^{-1}g_1)(x) = x$, т.е. $g_2^{-1}g_1 \in G_x$. А это равносильно равенству смежных классов $g_1G_x = g_2G_x$. $\square$

Пусть $X = G$ и G действует на $X = G$ сопряжением. Элементы x и gxg^{-1} называются *сопряженными*. Орбита $G(x) = \{gxg^{-1} : g \in G\}$ — это множество всех элементов, сопряженных элементу x . Длина этой орбиты равна числу правых (левых) смежных классов G по стабилизатору G_x . Вследствие теоремы Лагранжа, число сопряженных элементов для элемента x является делителем порядка группы. Центр группы G состоит из таких ее элементов, которые сопряжены только сами с собой (их орбиты имеют длину 1).

Теорема 2.9.1. *Пусть порядок группы есть степень простого числа. Тогда в этой группе имеется элемент, отличный от единицы и коммутирующий с любым элементом группы.*

Доказательство. Пусть порядок группы равен p^s , где p — простое число. Множество элементов группы разбивается на непересекающиеся классы сопряженных между собой элементов — это орбиты при действии группы на самой себе сопряжением. Длина каждой орбиты неединичной длины кратна p . Орбиты длины 1 обязательно имеются: такова орбита единичного элемента. Поэтому орбит единичной длины как минимум p . Значит, одна из них порождается элементом $x \neq e$. Для нее находим $gxg^{-1} = x \ \forall g \in G \Leftrightarrow gx = xg \ \forall g \in G$. $\square$

Теорема 2.9.2 (ТЕОРЕМА БЕРНСАЙДА). *В случае конечной группы G число различных орбит конечного множества X равно*

$$\frac{1}{|G|} \sum_{g \in G} |X_g| = \frac{1}{|G|} \sum_{x \in X} |G_x|.$$

Доказательство. Пары (g, x) со свойством $g(x) = x$ можно сосчитать двумя различными способами:

$$\sum_{g \in G} |X_g| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|G(x)|}. \quad \square$$

Пример. Рассмотрим вращения куба вокруг оси, проходящей через его центр, причем такие вращения, которые совмещают куб с самим собой. Это тождественное вращение плюс по три вращения вокруг осей, проходящих через центры противоположных граней, плюс по два вращения вокруг осей, проходящих через пары наиболее удаленных друг от друга (диаметральных) вершин, плюс по одному вращению вокруг осей, проходящих через середины противоположных ребер. Таким образом получаем 24 вращения.

Чтобы доказать, что композиция двух вращений является вращением, достаточно заметить, что любое вращение на угол ϕ вокруг некоторой оси есть композиция двух симметрий относительно проходящих через эту ось плоскостей, угол между которыми равен $\phi/2$. При этом одна из этих плоскостей может быть произвольной плоскостью, содержащей ось вращения. Таким образом, заданные вращения Φ и Ψ могут быть записаны в виде композиций двух симметрий: $\Phi = AB$ и $\Psi = BD$, где B — симметричное отражение относительно плоскости, проходящей через оси вращений Φ и Ψ . Композиция $\Phi\Psi = ABBD = AD$ оказывается композицией двух симметрий A и D и поэтому является вращением вокруг прямой, по которой пересекаются плоскости неподвижных точек при симметриях A и D . Возможно и чисто алгебраическое доказательство, но оно будет доступно после изучения блочной жордановой формы для ортогональных матриц (см. раздел 5.12).

Чтобы доказать, что в группе G всех вращений куба ровно 24 вращения, рассмотрим действие этой группы на множестве вершин куба. Вершин всего 8. При этом, как несложно проверить, орбита только одна. Возьмем произвольную вершину x . Если вращение оставляет x на месте, то оно оставляет на месте и наиболее удаленную от x вершину. Значит, стабилизатор вершины x содержит три вращения вокруг оси, проходящей через диаметрально противоположные вершины. Поэтому $|G| = 8 \cdot 3 = 24$.

Задача 79. Каждая грань куба закрашивается одной из двух красок. При этом раскраски считаются одинаковыми, если они совпадают при вращении куба. Докажите, что разных раскрасок ровно 10.

Задача 80. Докажите, что в группе порядка 8 имеется нормальная подгруппа порядка 4.

Задача 81. Докажите, что в симметрической группе степени n две подстановки являются сопряженными в том и только том случае, когда они разлагаются в произведение одного и того же числа независимых циклов с одним и тем же набором длин.

Задача 82. Найдите число разных орбит сопряженных элементов в группе S_{13} .

2.10. Группа движений

Взаимно-однозначное отображение плоскости на себя, при котором расстояние между любой парой точек равно расстоянию между их образами, называется *движением плоскости*. В планиметрии геометрические фигуры считаются равными (конгруэнтными), если одну можно совместить с другой с помощью некоторого движения плоскости. Множество всех движений относительно операции композиции (последовательного выполнения) отображений является группой. Взаимно-однозначное отображение пространства, сохраняющее расстояние, также называется движением.

Теорема 2.10.1 (ТЕОРЕМА ШАЛЯ). Любое движение плоскости представляет собой параллельный перенос, поворот вокруг точки на некоторый угол, симметричное отражение относительно некоторой прямой или композиция параллельного переноса и симметрии относительно прямой (скользящая симметрия).

Доказательство. Заметим, что движение плоскости полностью определяется, если известны образы вершин какого-либо треугольника. Опираясь на это наблюдение, легко убедиться в том, что в случае ровно одной неподвижной точки мы получаем не что иное, как поворот вокруг этой точки на некоторый угол. Если вообще все точки неподвижны, то движение является тождественным преобразованием. Если неподвижных точек больше чем одна, то имеется целая прямая неподвижных точек, и если при этом хотя бы одна точка не является неподвижной, то движение должно быть симметрией относительно данной прямой. Случай, когда неподвижных точек нет, мы оставляем читателю. $\square$

Задача 83. Докажите, что множество всех движений плоскости, совмещающих правильный n -й угольник с самим собой, является группой с числом элементов $2n$.

Задача 84. Докажите, что группа движений плоскости не является абелевой.

Задача 85. Докажите, что если отображение плоскости в плоскость сохраняет расстояние, то оно взаимно-однозначно, т. е. является движением.

Задача 86. Докажите, что множество всех движений, совмещающих куб с самим собой, является группой. Докажите, что порядок этой группы равен 48.

Задача 87. Найдите порядок группы движений, переводящих в себя правильный тетраэдр.

2.11. Группа дробно-линейных преобразований комплексной плоскости

Отображение комплексной плоскости вида

$$z \rightarrow f(z) = \frac{a_{11}z + a_{12}}{a_{21}z + a_{22}}$$

называется *дробно-линейным преобразованием*, если

$$\det \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \neq 0, \quad a_{ij} \in \mathbb{C}.$$

Заметим, что отображение определено при всех $z \in \mathbb{C}$, кроме, возможно, одного, при котором знаменатель обращается в нуль.

Задача 88. Докажите, что множество дробно-линейных преобразований комплексной плоскости является группой относительно композиции преобразований.

Задача 89. Докажите, что дробно-линейные преобразования с вещественными коэффициентами, подчиненными условию $a_{11}a_{22} - a_{12}a_{21} = 1$, образуют группу относительно композиции преобразований и переводят точки верхней полуплоскости в точки верхней полуплоскости. Докажите также, что для любой пары точек верхней полуплоскости найдется преобразование такого вида, переводящее одну точку в другую.

Задача 90. Докажите, что любое движение комплексной плоскости задается отображением вида

$$z \rightarrow az + b \quad \text{либо} \quad z \rightarrow a\bar{z} + b, \quad \text{где} \quad a, b \in \mathbb{C}, \quad |a| = 1.$$

Задача 91. Докажите, что преобразование

$$f(z) = \frac{z-1}{z+1}$$

переводит мнимую ось в единичную окружность (окружность радиуса 1 с центром в точке $z=0$), а правую полуплоскость — во внутренность единичного круга.

Задача 92. Докажите, что для произвольных дробно-линейных преобразований $f(z)$ и $g(z)$ с неконстантными многочленами в знаменателях существуют специальные дробно-линейные преобразования $h_1(z) = a_1z + b_1$ и $h_2(z) = a_2z + b_2$, такие что

$$f = h_1 g h_2, \quad \text{т.е.} \quad f(z) = h_1(g(h_2(z))).$$

Задача 93. Докажите, что при дробно-линейном преобразовании любая прямая (окружность) переходит в прямую либо в окружность.

2.12. Гомоморфизмы групп

Отображение $f: G \rightarrow \hat{G}$ группы G в группу $\hat{G}$ называется гомоморфизмом, если оно сохраняет операцию, т.е.

$$f(ab) = f(a)f(b) \quad \forall a, b \in G.$$

Отличие от изоморфизма в том, что не требуется взаимной однозначности.

Ядром гомоморфизма называется множество элементов группы G , отображаемых в единицу группы $\hat{G}$. Обозначение: $\ker f$.

Образом гомоморфизма называется множество элементов группы $\hat{G}$, в которые отображается хотя бы один элемент группы G . Обозначение: $\operatorname{im} f = f(G)$.

Теорема 2.12.1. Если f — гомоморфизм группы G в группу $\hat{G}$, то

$$\ker f \trianglelefteq G, \quad \operatorname{im} f \leq \hat{G}, \quad \operatorname{im} f \cong G / \ker f.$$

Доказательство. Пусть $H = \ker f$ и $a, b \in H$. Тогда $f(a) = f(b) = \hat{e}$, где $\hat{e}$ — единица группы $\hat{G}$. В силу сохранения операции

$$f(ab) = f(a)f(b) = \hat{e}\hat{e} = \hat{e} \Rightarrow ab \in H,$$

$$\hat{e} = f(e) = f(aa^{-1}) = f(a)f(a^{-1}) = \hat{e}f(a^{-1}) = f(a^{-1}) \Rightarrow a^{-1} \in H.$$

Таким образом, H является подгруппой в G . Кроме того, для любого $h \in H$ и любого $g \in G$ имеем

$$\begin{aligned} f(ghg^{-1}) &= f(g)f(h)f(g^{-1}) = f(g)f(h)f(g^{-1}) = f(g)f(g^{-1}) = \\ &= f(gg^{-1}) = f(e) = \hat{e} \Rightarrow ghg^{-1} \in H. \end{aligned}$$

Поэтому H — нормальная подгруппа в G .

Пусть $R = \text{im } f$. Возьмем два произвольных элемента из R . Пусть они имеют вид $f(a)$ и $f(b)$ для каких-то $a, b \in G$. Тогда

$$f(a)f(b) = f(ab) \Rightarrow f(a)f(b) \in R.$$

Далее,

$$\begin{aligned} f(aa^{-1}) &= f(a)f(a^{-1}) = f(a^{-1})f(a) = \hat{e} \Rightarrow \\ &\Rightarrow (f(a))^{-1} = f(a^{-1}) \Rightarrow (f(a))^{-1} \in R. \end{aligned}$$

Таким образом, $R \leq \hat{G}$.

Отображение $\phi: G/H \rightarrow R$ определим следующим образом:

$$\phi(Ha) := f(a), \quad a \in G.$$

Поскольку определение использует произвольный элемент a из смежного класса Ha , необходимо показать, что образ смежного класса не зависит от выбора a . Пусть $Ha = Hb$. Тогда $b = ha$ для некоторого $h \in H$ и, значит,

$$f(b) = f(ha) = f(h)f(a) = \hat{e}f(a) = f(a).$$

Таким образом, отображение ϕ определено корректно.

Произвольный элемент группы R имеет вид $f(a)$ и при отображении ϕ представляет собой образ смежного класса Ha . Кроме того, если $f(a) = f(b)$, то

$$f(ab^{-1}) = \hat{e} \Rightarrow ab^{-1} \in H \Rightarrow Ha = Hb,$$

т.е. разные смежные классы переводятся в разные элементы группы R . Доказана взаимная однозначность отображения ϕ .

Сохранение операции при отображении ϕ вытекает из сохранения операции при гомоморфизме f :

$$\phi(HaHb) = \phi(Hab) = f(ab) = f(a)f(b). \quad \square$$

Замечательным следствием этой теоремы о гомоморфизме является то, что все образы при гомоморфизмах данной группы можно описать, ничего не зная о той группе, в которую отобра-

жаются элементы. Достаточно рассмотреть всевозможные нормальные подгруппы данной группы и соответствующие факторгруппы.

Пример 1. Пусть G — мультипликативная группа и $\hat{G}$ — группа ее внутренних автоморфизмов, т.е. отображений вида $\hat{g}(a) = gag^{-1}$, действующих на всех элементах $a \in G$ и задаваемых произвольным фиксированным элементом $g \in G$. Отображение $f: g \rightarrow \hat{g}$ сохраняет операцию и поэтому является гомоморфизмом G на $\hat{G}$:

$$g_1 \rightarrow \hat{g}_1(a) = g_1 a g_1^{-1}, \quad g_2 \rightarrow \hat{g}_2(a) = g_2 a g_2^{-1} \Rightarrow \\ \Rightarrow (g_1 g_2)(a) = g_1(g_2(a)) = g_1(g_2 a g_2^{-1}) g_1^{-1} = (g_1 g_2) a (g_1 g_2)^{-1}.$$

Его ядро состоит из тех и только тех элементов $g \in G$, для которых

$$gag^{-1} = a \quad \forall a \in G \quad \Leftrightarrow \quad ga = ag \quad \forall a \in G.$$

Таким образом, $\ker f = Z(G)$, где $Z(G)$ — центр группы G . Согласно теореме о гомоморфизме, $\hat{G} \cong G/Z(G)$.

Пример 2. Рассмотрим три многочлена от четырех переменных:

$$p_1 = x_1 x_2 + x_3 x_4, \quad p_2 = x_1 x_3 + x_2 x_4, \quad p_3 = x_1 x_4 + x_2 x_3.$$

Любая подстановка $\sigma \in S_4$ однозначно определяет перестановку многочленов p_1, p_2, p_3 . Пусть таким образом определяется отображение $f: S_4 \rightarrow S_3$. Оно является гомоморфизмом, а его ядро состоит из четырех подстановок:

$$\sigma_1 = e, \quad \sigma_2 = (12)(34), \quad \sigma_3 = (13)(24), \quad \sigma_4 = (14)(23).$$

Согласно теореме о гомоморфизме, ядро является нормальной подгруппой в S_4 . Эта подгруппа называется *четверной группой Клейна* и обозначается K_4 .

Задача 94. Найдите число гомоморфизмов циклической группы порядка 4 в циклическую группу порядка 2016.

Задача 95. Пусть $\mathbb{C}^*$ — мультипликативная группа ненулевых комплексных чисел и C_n — группа корней n -й степени из 1. Докажите, что

$$\mathbb{C}^*/C_n \cong \mathbb{C}^*.$$

Задача 96. В группе G даны подгруппы $H \trianglelefteq G$ и $K \leq G$. Докажите, что

$$HK \leq G, \quad H \trianglelefteq HK, \quad H \cap K \trianglelefteq K \quad \text{и} \quad HK/H \cong K/(H \cap K).$$

Задача 97. Докажите, что если группа внутренних автоморфизмов группы G является циклической, то сама группа G является абелевой.

2.13. Теорема Кэли о конечных группах

Теорема 2.13.1 (ТЕОРЕМА КЭЛИ). Любая группа порядка n изоморфна некоторой подгруппе симметрической группы S_n .

Доказательство. Пусть $G = \{g_1, g_2, \dots, g_n\}$ и $b \in G$. Рассмотрим следующее отображение Кэли:

$$\sigma(b) := \begin{pmatrix} g_1 & g_2 & \dots & g_n \\ bg_1 & bg_2 & \dots & bg_n \end{pmatrix}.$$

Пусть $a \in G$ и соответствующая ему подстановка имеет вид

$$\sigma(a) = \begin{pmatrix} bg_1 & bg_2 & \dots & bg_n \\ a(bg_1) & a(bg_2) & \dots & a(bg_n) \end{pmatrix}.$$

Тогда, как видим, $\sigma(ab) = \sigma(a)\sigma(b)$, т.е. подстановка, поставленная в соответствие ab , есть произведение (композиция) подстановок, соответствующих a и b . Следовательно, отображение $\sigma: G \rightarrow S_n$ является гомоморфизмом G в группу S_n . Образ группы G при гомоморфизме есть подгруппа группы S_n . Поскольку при отображении Кэли разные элементы соответствуют разным подстановкам, мы получаем изоморфизм группы G и ее образа. $\square$

Задача 98. Пусть a — элемент порядка k в группе порядка n . Докажите, что при отображении Кэли элементу a соответствует подстановка σ , являющаяся произведением n/k независимых циклов длины k .

Задача 99. Порядок группы G равен $2^s t$, где t — нечетное число. Докажите, что если порядок элемента $a \in G$ равен 2^s , а порядок элемента $b \in G$ равен t , то порядок элемента ab делится на 2^s .

2.14. Конечно порожденные абелевы группы

В группе G выберем какие-то элементы $a_1, \dots, a_s \in G$ и будем рассматривать всевозможные подгруппы, которые их содержат. Пусть H — пересечение всех таких подгрупп. Несложно проверить, что H будет подгруппой в G . Таким образом, H является минимальной подгруппой, содержащей элементы $a_1, \dots, a_s$. Говорят, что подгруппа H *порождена элементами* $a_1, \dots, a_s$. Обозначение: $H = \langle a_1, \dots, a_s \rangle$.

Группа G называется *конечно порожденной*, если $G = \langle a_1, \dots, a_s \rangle$ для каких-то элементов $a_1, \dots, a_s \in G$. Уже известный нам пример — это циклические группы, которые определяются как группы, порожденные каким-то одним своим элементом. Они же играют ключевую роль при описании строения произвольной конечно порожденной группы в случае, если она является абелевой.

Пусть G — аддитивная абелева группа и заданы ее подгруппы $G_1, \dots, G_s \leq G$. Если любой элемент $g \in G$ имеет и притом единственное представление в виде

$$g = g_1 + \dots + g_s, \quad g_i \in G_i, \quad 1 \leq i \leq s,$$

то группа G называется *прямой суммой* подгрупп $G_1, \dots, G_s$. Обозначение:

$$G = G_1 \oplus \dots \oplus G_s.$$

В случае мультипликативной абелевой группы аналогичным образом вводится понятие *прямого произведения* подгрупп, а вместо знака $\oplus$ применяется символ $\times$.

Теорема 2.14.1. *Любая аддитивная конечно порожденная абелева группа G является прямой суммой конечного числа циклических подгрупп*

$$G = G_1 \oplus \dots \oplus G_s,$$

упорядоченных таким образом, что если группа G_{i+1} конечна, то G_i также конечна и ее порядок является делителем порядка группы G_{i+1} ¹⁾.

Доказательство. Пусть s — минимальное число элементов, порождающих абелеву группу G . Систему элементов, порождающих G , назовем *минимальной*, если в ней ровно s элементов.

¹⁾ Обратим внимание на то, что допускается равенство $|G_{i+1}| = |G_i|$.

Если $a_1, \dots, a_s$ — минимальная система, то любой элемент $a \in G$ имеет вид

$$a = n_1 a_1 + \dots + n_s a_s, \quad n_1, \dots, n_s \in \mathbb{Z}.$$

Если целые числа $n_1, \dots, n_s$ определяются по a единственным образом, то теорема доказана, так как можно взять $G_i := \langle a_i \rangle$. Каждая подгруппа G_i будет бесконечной циклической группой.

Изучим случай неединственности. Теперь хотя бы для одного набора не равных одновременно нулю целых чисел $n_1, \dots, n_s$ получается равенство

$$n_1 a_1 + \dots + n_s a_s = 0.$$

Равенства такого вида будем называть *нетривиальными соотношениями* между элементами $a_1, \dots, a_s$.

Рассмотрим всевозможные минимальные системы порождающих G элементов и всевозможные нетривиальные соотношения между элементами каждой из систем. Пусть система $a_1, \dots, a_s$ обладает нетривиальным соотношением указанного выше вида, в котором n_1 является минимальным положительным среди всех коэффициентов любых нетривиальных соотношений хотя бы с одним положительным коэффициентом для всевозможных минимальных систем, порождающих группу G . Тогда можно сделать два наблюдения:

- если $m_1 a_1 + \dots + m_s a_s = 0$, то число n_1 является делителем числа m_1 ;
- каждый из коэффициентов $n_2, \dots, n_s$ делится на n_1 .

Для доказательства первого утверждения рассмотрим деление с остатком:

$$m_1 = n_1 q + r, \quad 0 \leq r < n_1.$$

Если $r > 0$, то получаем противоречие с минимальностью n_1 :

$$(m_1 - n_1 q) a_1 + (m_2 - n_2 q) a_2 + \dots + (m_s - n_s q) a_s = 0,$$

$$0 < r = m_1 - n_1 q < n_1.$$

Чтобы доказать второе утверждение от противного, предположим, что, скажем, n_2 не делится на n_1 . Тогда $n_2 = n_1 q + r$, где q — целое число и $0 < r < n_1$. Нетрудно проверить, что группа G порождается элементами

$$b_1 := a_2, \quad b_2 := a_1 + q a_2, \quad b_3 := a_3, \dots, b_s := a_s,$$

для которых имеется нетривиальное соотношение вида

$$rb_1 + n_1b_2 + n_3b_3 + \dots + n_sb_s = 0, \quad 0 < r < n_1.$$

Опять получаем противоречие с минимальностью n_1 .

Итак, $n_i = n_1q_i$ для каких-то целых q_i . Положим

$$b := a_1 + q_2a_2 + \dots + q_sa_s.$$

Тогда $n_1b = 0$ и $kb \neq 0$ при $0 < k < n_1$. Это значит, что циклическая группа $G_1 := \langle b \rangle$ имеет порядок n_1 . Несложно проверяется, что G порождается элементами $b, a_2, \dots, a_s$. Кроме того, в случае

$$m_1b + (m_2a_2 + \dots + m_sa_s) = 0$$

мы получаем также

$$m_1a_1 + (m_2 + q_2m_1)a_2 + \dots + (m_s + q_sm_1)a_s = 0.$$

Значит, m_1 делится на n_1 и поэтому $m_1b = 0$ и, как следствие, $m_2a_2 + \dots + m_sa_s = 0$. Таким образом,

$$G = G_1 \oplus H, \quad \text{где } G_1 = \langle b \rangle, \quad H := \langle a_2, \dots, a_s \rangle.$$

Кроме того, минимальный положительный коэффициент в нетривиальных соотношениях между элементами, порождающими группу H , обязательно будет делиться на n_1 . В самом деле, пусть

$$m_2a_2 + \dots + m_sa_s = 0.$$

Тогда, учитывая определение элемента b и равенство $n_1b = 0$, находим

$$n_1b + m_2a_2 + \dots + m_sa_s = 0.$$

Между порождающими группу G элементами $b, a_2, \dots, a_s$ мы получаем нетривиальное соотношение, в котором коэффициент n_1 является минимальным положительным во всех нетривиальных соотношениях для всех минимальных систем, порождающих группу G . В силу отмеченного выше второго наблюдения каждый из коэффициентов $m_2, \dots, m_s$ должен делиться на n_1 .

Доказательство завершается индукцией по s . □

Группа, в которой порядок каждого элемента представляет собой некоторую зависящую от элемента степень одного и того же простого числа p , называется *примарной группой* или *p-группой*.

Следствие 2.14.1. *Любая конечная абелева группа является прямой суммой примарных циклических групп.*

Доказательство содержится в предлагаемых ниже задачах 100 и 101.

Задача 100. Докажите, что циклическая группа порядка $n = n_1 n_2 \dots n_t$ с попарно взаимно простыми числами $n_1, n_2, \dots, n_t$ является прямой суммой циклических групп порядков $n_1, n_2, \dots, n_t$.

Задача 101. Докажите, что любая конечная абелева группа является прямой суммой циклических групп, порядки которых суть какие-то простые числа в каких-то степенях.

Задача 102. Докажите, что в конечной абелевой группе существует элемент, порядок которого равен наименьшему общему кратному порядков всех элементов данной группы.

Задача 103. Порядок некоторой конечной группы совпадает с наименьшим общим кратным порядков всех ее элементов. Обязана ли эта группа быть циклической?

Задача 104. Докажите, что конечно порожденная группа, в которой каждый неединичный элемент имеет порядок 2, будет конечной ¹⁾.

Задача 105. Докажите, что аддитивная группа рациональных чисел не является конечно порожденной.

Задача 106. Докажите, что ни для какой конечной группы множество автоморфизмов не может содержать ровно три разных автоморфизма.

¹⁾ Задача связана с довольно трудной проблемой Бернсайда: вытекает ли конечность конечно порожденной группы из конечности порядков ее элементов? В общем случае ответ оказался отрицательным.

Глава 3

КОЛЬЦА, ПОЛЯ, МНОГОЧЛЕНЫ

3.1. Определения кольца и поля

Пусть на одном и том же множестве K определены две замкнутые бинарные операции. Первая из них называется *сложением* и превращает K в аддитивную абелеву группу, вторая называется *умножением* и связана с первой законами *дистрибутивности*:

$$(a + b)c = ac + bc, \quad a(b + c) = ab + ac \quad \forall a, b, c \in K.$$

В таких случаях множество K называется *кольцом*.

Нейтральный элемент по сложению называется *нулевым элементом* кольца и обозначается символом 0 . Если других элементов нет, то кольцо называется *нулевым*. Если произведение двух ненулевых элементов кольца равно 0 , то каждый из этих элементов называется *делителем нуля*.

Утверждение 3.1.1. Для любого элемента a в произвольном кольце K имеет место равенство $0 \cdot a = a \cdot 0 = 0$.

Доказательство. В силу дистрибутивности

$$\begin{aligned} 0 \cdot a &= (0 + 0)a = 0 \cdot a + 0 \cdot a \Rightarrow \\ &\Rightarrow (-0 \cdot a) + 0 \cdot a = 0 = ((-0 \cdot a) + 0 \cdot a) + 0 \cdot a = 0 \cdot a. \end{aligned}$$

Равенство $a \cdot 0 = 0$ получается аналогично. □

Если умножение ассоциативно, то кольцо называется *ассоциативным*. Если умножение коммутативно, то кольцо называется *коммутативным*.

Пример неассоциативного и некоммутативного кольца: множество векторов в трехмерном пространстве с операциями сложения ($c = a + b$) и векторного умножения векторов ($c = a \times b = [a, b]$). В дальнейшем мы будем рассматривать только ассоциативные кольца.

Элемент $e \in K$ со свойством $ae = ea = a \forall a \in K$ называется *единичным элементом* или *единицей* кольца K . Если такой элемент существует, то кольцо называется *кольцом с единицей*. Легко доказывается, что единица может быть только одна. Элемент a кольца K с единицей e называется *обратимым* или *делителем единицы*, если существует $b \in K$, такой что $ab = ba = e$.

Ассоциативное коммутативное кольцо без делителей нуля называется *целостным кольцом* или *областью целостности*.

Кольцо целых чисел. Множество целых чисел $\mathbb{Z}$ с операциями сложения и умножения чисел является целостным кольцом с единицей. Здесь два делителя единицы: 1 и -1 .

Кольцо гауссовых чисел. Комплексные числа вида $a + bi$ при целых a и b называются *гауссовыми числами*. Множество всех таких чисел обозначается $\mathbb{Z}[i]$. Операции сложения и умножения комплексных чисел превращают $\mathbb{Z}[i]$ в целостное кольцо с единицей. Это кольцо интересно тем, что в нем имеют место многие замечательные свойства кольца целых чисел, в частности, вводится понятие простых чисел и доказывается аналог *основной теоремы арифметики* — о том, что любое число, кроме делителей единицы, имеет разложение на простые множители, которое определяется однозначно с точностью до перестановки множителей и умножения их на какие-то делители единицы.

Кольцо квадратных матриц. Множество вещественных $n \times n$ -матриц с операциями сложения и умножения матриц является ассоциативным некоммутативным кольцом с единицей. Нулевым элементом является нулевая матрица, единичным элементом — единичная матрица (диагональная матрица с числом 1 на главной диагонали). При $n \geq 2$ в этом кольце имеются делители нуля. Например:

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Кольцо вычетов по модулю n . Напомним, что *вычетом* по модулю n называется множество всех целых чисел, имеющих при делении на n один и тот же остаток. Если целое число a входит в такое множество, то оно однозначно определяет остаток при делении на n , а значит и все множество целых чисел с одним и тем же остатком. Поэтому соответствующий вычет однозначно определяется любым входящим в него числом. Для вычета,

содержащего число a , мы используем обозначение $[a]$. Сложение и умножение вычетов определяется следующим образом:

$$[a] + [b] := [a + b], \quad [a][b] := [ab].$$

Важно понимать, что такого рода определения нуждаются в проверке их корректности. В данном случае нужно убедиться в том, что если $[a] = [a']$ и $[b] = [b']$, то $[a + b] = [a' + b']$ и $[ab] = [a'b']$. Кольцо вычетов по модулю n является конечным ассоциативным коммутативным кольцом с единицей $e = [1]$ и нулем $0 = [0]$. Если n составное, т. е. $n = ab$ при $a, b \neq n$, то $[a], [b] \neq 0$ и в то же время $[a][b] = [ab] = [n] = 0$, т. е. вычеты $[a]$ и $[b]$ являются делителями нуля. Кольцо вычетов по модулю n обозначается $\mathbb{Z}_n$.

Часто для обозначения вычетов $[a]$ и $[b]$ используются сами числа a и b . При этом говорится, что операции выполняются по модулю n ; если $[c] = [a] + [b]$ или $[c] = [a][b]$, то применяется запись

$$c = a + b \pmod{n} \quad \text{или} \quad c = ab \pmod{n}.$$

Пусть K — ассоциативное коммутативное кольцо, в котором есть хотя бы один ненулевой элемент и для любых ненулевых элементов a и b существует ненулевой элемент x такой, что $ax = b$. Такое кольцо называется *полем*.

Согласно определению, в поле должно быть не менее двух элементов: заведомо есть нулевой элемент и должен быть единичный элемент, не совпадающий с нулевым. Ясно, что множество ненулевых элементов поля образует группу по умножению. Эта группа называется *мультипликативной группой поля*. Все элементы поля образуют группу по сложению, которая называется *аддитивной группой поля*.

Утверждение 3.1.2. *В поле делителей нуля нет.*

Доказательство. Пусть $ab = 0$. Если $a \neq 0$, то существует элемент x , такой что $ax = e$. Используя ассоциативность и коммутативность умножения, находим $0 = x \cdot 0 = x(ab) = (xa)b = eb = b$, т. е. $b = 0$. Аналогично, если $b \neq 0$, то $a = 0$. $\square$

Свойства операций произвольного поля по сути те же, что и хорошо знакомые со школы свойства операций сложения и умножения рациональных или вещественных чисел. Для матриц с элементами из поля K операции сложения и умножения матриц определяются так же, как и для вещественных матриц.

Более того, точно таким же образом вводится понятие определителя для квадратных матриц с элементами из K и доказываются те же основные свойства определителя. Никак не меняется понятие обратной матрицы: матрица B называется обратной к $n \times n$ -матрице A , если $AB = BA = I$ (единичная матрица порядка n). Имеет место такое же определение ранга матрицы, справедлива та же теорема о базисном миноре и ее следствия. Все, что известно о системах линейных алгебраических уравнений с вещественными коэффициентами и вещественной правой частью, остается в силе для случаев, когда коэффициенты, правая часть и решение берутся из произвольного заданного поля.

Заметим также, что понятие определителя имеет смысл для матриц с элементами из произвольного ассоциативного коммутативного кольца K . При его вычислении получается некоторый элемент из K . Можно проверить, что и в этом случае определитель обладает рядом привычных свойств¹⁾:

- как функция столбцов (строк) матрицы — определитель является линейной функцией по каждому из аргументов при фиксации остальных аргументов (такие функции называются *полилинейными* или *мультилинейными*);
- определитель меняет знак при перестановке двух разных столбцов (строк);
- определитель не меняется при прибавлении к столбцу (строке) линейной комбинации других столбцов (строк);
- определитель не меняется при транспонировании матрицы;
- определитель произведения матриц равен произведению определителей матриц-сомножителей.

Отображение $f: K \rightarrow \hat{K}$ кольца K в кольцо $\hat{K}$ называется *гомоморфизмом*, если оно сохраняет операции:

$$f(a + b) = f(a) + f(b), \quad f(ab) = f(a)f(b) \quad \forall a, b \in K.$$

В случае взаимной однозначности гомоморфизм называется *изоморфизмом*.

¹⁾ В качестве упражнения проведите аккуратные доказательства этих свойств. Обратите внимание на то, что утверждение о равенстве нулю определителя с парой одинаковых столбцов в случае кольца $\mathbb{Z}_2$ не является прямым следствием утверждения об изменении знака при перестановке двух разных столбцов.

Задача 107. Докажите, что если кольцо изоморфно полю, то оно само является полем.

Задача 108. Докажите, что множество функций, непрерывных на заданном отрезке вещественной оси, относительно операций сложения и умножения функций является ассоциативным коммутативным кольцом с единицей. Является ли это кольцо целостным?

Задача 109. Найдите все делители единицы в кольце гауссовых чисел.

Задача 110. Докажите, что множество вещественных чисел вида $a + b\sqrt{5}$ при всех $a, b \in \mathbb{Q}$ относительно операций сложения и умножения чисел является полем.

Задача 111. Пусть $a, b \in K$, где K — ассоциативное кольцо с единицей e . Докажите, что из обратимости элемента $e + ab$ вытекает обратимость элемента $e + ba$.

Задача 112. Пусть K — произвольное бесконечное поле, m и n — произвольные фиксированные натуральные числа. Докажите, что среди $m \times n$ -матриц с элементами из K существует такая матрица ранга 1, в которой все элементы различны.

Задача 113. Докажите, что все вещественные $n \times n$ -матрицы вида

$$\begin{bmatrix} a_0 & a_{n-1} & \ddots & a_2 & a_1 \\ a_1 & a_0 & \ddots & \ddots & a_2 \\ \ddots & \ddots & \ddots & \ddots & \ddots \\ a_{n-2} & \ddots & \ddots & a_0 & a_{n-1} \\ a_{n-1} & a_{n-2} & \ddots & a_1 & a_0 \end{bmatrix}$$

образуют ассоциативное коммутативное кольцо с единицей относительно операций сложения и умножения матриц. Выясните, есть ли в этом кольце делители нуля.

Задача 114. Пусть K — ассоциативное коммутативное кольцо с единицей и L — кольцо $n \times n$ -матриц с элементами из K . Докажите, что матрица $A \in L$ обратима тогда и только тогда, когда $\det A$ является обратимым элементом кольца K .

3.2. Поле вычетов

Хорошо известные примеры полей: рациональные числа $\mathbb{Q}$, вещественные числа $\mathbb{R}$, комплексные числа $\mathbb{C}$. Но существуют и *конечные поля*, в которых число элементов конечно.

Теорема 3.2.1. *Кольцо вычетов по модулю n является полем в том и только том случае, когда число n простое.*

Доказательство. Мы уже знаем, что если n составное, то делители нуля в $\mathbb{Z}_n$ есть. Пусть $n = p$ — простое число. Множество ненулевых вычетов имеет вид

$$\mathbb{Z}_p^* = \{ [1], \dots, [p-1] \}.$$

Докажем, что для любых $[a], [b] \in \mathbb{Z}_p^*$ существует $[x] \in \mathbb{Z}_p^*$, такой что $[a][x] = [b]$. Для этого достаточно проверить, что вычеты $[a][1], \dots, [a][p-1]$ являются разными ненулевыми вычетами — тогда среди них обязательно есть вычет $[b]$. Данные вычеты определяются остатками при делении на p :

$$\begin{aligned} 1 \cdot a &= pq_1 + r_1, & 0 \leq r_1 \leq p-1, \\ 2 \cdot a &= pq_2 + r_2, & 0 \leq r_2 \leq p-1, \\ &\dots & \dots \\ (p-1) \cdot a &= pq_{p-1} + r_{p-1}, & 0 \leq r_{p-1} \leq p-1. \end{aligned}$$

Пусть $r_i = r_j$. Тогда

$$(i-j)a : p, \quad (a, p) = 1 \Rightarrow i-j : p.$$

Среди целых чисел от $-p+1$ до $p-1$ на p делится только 0. Следовательно, $i=j$ и мы доказали, что остатки $r_1, \dots, r_{p-1}$ разные. Ни один из них не равен нулю, иначе число ia делилось бы на p , что невозможно при $1 \leq i \leq p-1$. Таким образом, остатки $r_1, \dots, r_{p-1}$ представляют собой перестановку чисел $1, \dots, p-1$. $\square$

В качестве следствия легко получается *малая теорема Ферма*: если p простое и $(a, p) = 1$, то $a^{p-1} - 1 : p$. Достаточно перемножить рассмотренные выше равенства и заметить, что $(p-1)! = r_1 \dots r_{p-1}$. В результате находим

$$(p-1)!(a^{p-1} - 1) : p, \quad ((p-1)!, p) = 1 \Rightarrow a^{p-1} - 1 : p.$$

Теорему о поле вычетов можно превратить в несколько более общее и более абстрактное утверждение.

Теорема 3.2.2. *Конечное ассоциативное коммутативное кольцо является полем тогда и только тогда, когда в нем нет делителей нуля.*

Доказательство. Если делители нуля есть, то это не поле. Пусть их нет. Предположим, что кольцо имеет m ненулевых элементов $a_1, \dots, a_m$. Тогда элементы $a_k a_1, a_k a_2, \dots, a_k a_m$ должны быть разными: если $a_k a_i = a_k a_j$, то $a_k(a_i - a_j) = 0$. Поскольку делителей нуля нет и $a_k \neq 0$, получаем $a_i = a_j$. Значит, для любых a_k и a_l уравнение $a_k x = a_l$ имеет решение в данном кольце. $\square$

Существенно более трудным оказывается следующее интересное утверждение.

Теорема 3.2.3 (МАЛАЯ ТЕОРЕМА ВЕДДЕРБЕРНА). *Конечное ассоциативное кольцо с единицей и без делителей нуля является полем.*

Мы отложим доказательство до выяснения связи полей и линейных пространств.

Задача 115. *Посчитайте число различных невырожденных матриц с коэффициентами из поля вычетов по простому модулю p .*

Задача 116. *Пусть p — простое число. Найдите сумму и произведение всех ненулевых вычетов по модулю p .*

Задача 117. *Пусть a и b — произвольные элементы поля вычетов по простому модулю p . Докажите равенство*

$$(a + b)^p = a^p + b^p.$$

Задача 118. *Пусть n — натуральное число и $\mathbb{Z}_n^* := \{[a] \in \mathbb{Z}_n : (a, n) = 1\}$. Докажите, что множество $\mathbb{Z}_n^*$ является группой относительно операции умножения вычетов по модулю n .*

Задача 119. *Докажите следующую теорему Эйлера: если a и n — взаимно простые натуральные числа, то*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Задача 120. *Докажите, что в поле $\mathbb{Z}_p$ при простом $p \geq 3$ число элементов a , для которых уравнение $x^2 = a$ имеет решение $x \in \mathbb{Z}_p$, равно $(p - 1)/2 + 1$.*

3.3. Кольцо многочленов

Всюду в дальнейшем мы будем рассматривать только ассоциативные кольца.

Многочленом от переменной (буквы, символа) x над кольцом K называется *формальное выражение* вида

$$a(x) = a_0 + a_1x + a_2x^2 + \dots,$$

где коэффициенты $a_0, a_1, a_2, \dots$ принадлежат K и лишь конечное их число отлично от нуля. Многочлен однозначно сопоставляется с бесконечной последовательностью элементов кольца K , в которой имеется лишь конечное число ненулевых элементов. Множество всех многочленов от x над K обозначается $K[x]$.

Выражение $a_i x^i$ называется *одночленом*. Если $a_i \neq 0$, то одночлен называется ненулевым одночленом степени i . В записи многочлена нулевые одночлены можно опускать. Многочлен, все коэффициенты которого являются нулями, называется *нулевым*.

Если $a_n \neq 0$ и $a_k = 0$ при $k > n$, то n называется *степенью* многочлена $a(x)$. Обозначение: $n = \deg a(x)$. Коэффициент a_n называется *старшим коэффициентом* многочлена. Коэффициент a_0 называется *свободным членом* многочлена. Степень нулевого многочлена считается неопределенной. Нулевой многочлен и многочлены нулевой степени естественно ассоциируются с элементами кольца K и называются *константами*.

Равенство многочленов определяется именно как равенство формальных выражений. Если

$$b(x) = b_0 + b_1x + b_2x^2 + \dots,$$

то мы пишем $a(x) = b(x)$ в том и только том случае, когда $a_i = b_i$ при всех i .

Взяв $\theta \in K$, мы можем найти *значение* многочлена $a(x)$ в точке θ , получаемое при замене x на θ :

$$a(\theta) := a_0 + a_1\theta + \dots + a_n\theta^n \in K.$$

Если $f(\theta) = 0$, то θ называется *корнем* или *нулем* многочлена $f(x)$.

Мы имеем право также рассматривать многочлен $f(x)$ как функцию $f(\theta)$, определенную при всех $\theta \in K$. Если многочлены равны как формальные выражения, то соответствующие им функции будут принимать одинаковые значения при

одних и тех же значениях аргумента. Обратное верно, если кольцо K бесконечно и целостно (об этом позже, см. следствие 3.4.3), и, вообще говоря, неверно, если кольцо K конечно. Вот пример *равных* функций, определяемых *разными* многочленами $f(x), g(x) \in \mathbb{Z}_2[x]$:

$$f(x) = 1, \quad g(x) = 1 + x + x^2.$$

Многочлены можно складывать и умножать. Суммой многочленов $a(x)$ и $b(x)$ называется многочлен $c(x)$ с коэффициентами

$$c_i := a_i + b_i, \quad i = 0, 1, \dots$$

Обозначение: $c(x) = a(x) + b(x)$.

Произведением многочленов $a(x)$ и $b(x)$ называется многочлен $d(x)$ с коэффициентами

$$d_i := a_0 b_i + a_1 b_{i-1} + \dots + a_i b_0, \quad i = 0, 1, \dots$$

Обозначение: $d(x) = a(x)b(x)$.

Утверждение 3.3.1. *В случае произвольного кольца K степень произведения двух ненулевых многочленов не выше суммы их степеней. Если старшие коэффициенты не являются делителями нуля, то степень произведения равна сумме степеней. То же верно, если K — кольцо с единицей и хотя бы один из старших коэффициентов двух ненулевых многочленов является обратимым.*

Доказательство. Пусть $m = \deg a(x)$ и $n = \deg b(x)$. Тогда при $i = k + l > m + n$ имеем $k > m$ или $l > n$, поэтому $a_k = 0$ или $b_l = 0$ и в любом случае $a_k b_l = 0$. Таким образом, $d_i = 0$ при $i > m + n$. Заметим также, что $d_{m+n} = a_m b_n$. В случае обратимости a_m или b_n имеем $d_{m+n} \neq 0$. $\square$

Утверждение 3.3.2. *Множество многочленов $K[x]$ с операциями сложения и умножения многочленов образует кольцо. Кольцо $K[x]$ наследует от K такие свойства, как ассоциативность, коммутативность, наличие единицы и отсутствие делителей нуля. Если K — поле, то $K[x]$ является целостным кольцом с единицей.*

Доказательство является рутинным упражнением. Отметим лишь причину отсутствия делителей нуля: если в K их нет, то

$$\deg(a(x)b(x)) = \deg a(x) + \deg b(x),$$

поэтому нулевой многочлен не может получиться при умножении ненулевых многочленов.

Задача 121. Найдите число различных многочленов степени 10 над $\mathbb{Z}_2$. Сколько из них различны как функции, определенные на $\mathbb{Z}_2$?

Задача 122. Может ли кольцо быть изоморфным своему строго меньшему подкольцу?

3.4. Деление с остатком и алгоритм Евклида

Всюду далее считаем, что K — целостное кольцо с единицей 1.

Пусть $a(x), b(x) \in K[x]$ и $b(x) \neq 0$. Говорят, что многочлен $a(x)$ делится с остатком на многочлен $b(x) \neq 0$, если для некоторых многочленов $q(x), r(x) \in K[x]$ выполняется равенство $a(x) = q(x)b(x) + r(x)$, $r(x) = 0$ либо $\deg r(x) \leq \deg b(x) - 1$.

Многочлены $r(x)$ и $q(x)$ называются соответственно *остатком* и *неполным частным*.

Теорема 3.4.1. Пусть K — целостное кольцо с единицей и старший коэффициент многочлена $b(x)$ над K является обратимым. Тогда для любого многочлена $a(x)$ над K деление с остатком на $b(x)$ выполнимо и остаток и неполное частное определены однозначно.

Доказательство. При обратимости старшего коэффициента для $b(x)$ деление с остатком реализуется по известному со школы методу деления столбиком. Допустим, что получились два разных представления:

$$a(x) = q_1(x)b(x) + r_1(x), \quad \deg r_1(x) \leq \deg b(x) - 1,$$

$$a(x) = q_2(x)b(x) + r_2(x), \quad \deg r_2(x) \leq \deg b(x) - 1.$$

Вычитая второе из первого, находим

$$(q_2(x) - q_1(x))b(x) = r_1(x) - r_2(x).$$

Если $q_1(x) \neq q_2(x)$, то это невозможно, так как степень многочлена слева не меньше степени многочлена $b(x)$, а степень многочлена справа строго меньше этой степени. $\square$

Теорема 3.4.2 (ТЕОРЕМА БЕЗУ). *Остаток при делении многочлена $f(x) \in K[x]$ на многочлен $x - \theta$, $\theta \in K$, есть многочлен-константа $f(\theta)$.*

Доказательство. Старший коэффициент многочлена (двучлена) $x - \theta$ является обратимым, поэтому деление с остатком выполнимо:

$$f(x) = q(x)(x - \theta) + r(x) \Rightarrow f(\theta) = q(\theta)(\theta - \theta) + r(\theta) = r(\theta). \quad \square$$

Следствие 3.4.1. *Если $\theta \in K$ — корень многочлена $f(x) \in K[x]$, то существует многочлен $q(x) \in K[x]$, такой что $f(x) = q(x)(x - \theta)$.*

Следствие 3.4.2. *Многочлен степени n не может иметь более n различных корней.*

Следствие 3.4.3. *Пусть K — бесконечное целостное кольцо с единицей. Тогда многочлены $a(x)$ и $b(x)$ равны как функции от $x \in K$ в том и только том случае, когда они имеют одинаковые коэффициенты при одинаковых степенях переменной x .*

Доказательство. Если многочлен $c(x) := a(x) - b(x)$ не является нулевым и принимает нулевое значение в бесконечном числе точек, то число его различных корней больше его степени. Такой многочлен не может быть ненулевым. $\square$

Пусть при делении $a(x)$ на $b(x)$ остаток равен нулю. Тогда мы говорим, что $a(x)$ делится на $b(x)$, а $b(x)$ делит $a(x)$. Используются два типа обозначений:

$$a(x) : b(x) \quad (a \text{ делится на } b) \quad \Leftrightarrow \quad b(x) \mid a(x) \quad (b \text{ делит } a).$$

В этом же случае $b(x)$ называется делителем $a(x)$.

Если $d(x) \mid a(x)$ и $d(x) \mid b(x)$, то $d(x)$ называется общим делителем многочленов $a(x)$ и $b(x)$. Делитель называется нетривиальным, если он сам и соответствующее ему частное не являются делителями единицы.

Заметим, что в случае кольца многочленов над полем делителем единицы является любая ненулевая константа. Если $K = \mathbb{Z}$, то делителей единицы два: 1 и -1 .

Наибольшим общим делителем многочленов $a(x)$ и $b(x)$ называется такой общий делитель, который делится на любой общий делитель этих многочленов. Запись $(a(x), b(x)) = d(x)$

означает, что $d(x)$ является наибольшим общим делителем для $a(x)$ и $b(x)$.

Утверждение 3.4.1. *Наибольший общий делитель в кольце многочленов над целостным кольцом с единицей определяется однозначно с точностью до умножения на делитель единицы.*

Доказательство. Если $d_1(x)$ и $d_2(x)$ — наибольшие общие делители для одной пары многочленов над кольцом K , то $d_1(x) \mid d_2(x)$ и $d_2(x) \mid d_1(x)$, т. е. имеют место разложения

$$d_2(x) = d_1(x)q_1(x), \quad d_1(x) = d_2(x)q_2(x).$$

Отсюда $\deg d_1(x) \leq \deg d_2(x)$ и $\deg d_2(x) \leq \deg d_1(x)$. Значит, $\deg d_1(x) = \deg d_2(x)$ и поэтому $\deg q_1(x) = \deg q_2(x) = 0$. Таким образом, q_1 и q_2 являются константами. Пусть a — старший коэффициент многочлена $d_2(x)$. Благодаря тому что в K делителей нуля нет, находим

$$a = a(q_1q_2) \Rightarrow a(1 - q_1q_2) = 0 \Rightarrow q_1q_2 = 1. \quad \square$$

Многочлены $a(x)$ и $b(x)$ называются *взаимно простыми*, если любой их общий делитель является делителем единицы. В этом и только этом случае $(a(x), b(x)) = 1$.

Теорема 3.4.3 (АЛГОРИТМ ЕВКЛИДА). *Пусть K — поле и заданы отличные от констант многочлены $a(x), b(x) \in K[x]$. Положим*

$$r_0(x) := a(x), \quad r_1(x) := b(x)$$

и рассмотрим следующую последовательность делений с остатком:

$$r_0(x) = q_2(x)r_1(x) + r_2(x), \quad \deg r_2(x) < \deg r_1(x),$$

$$r_1(x) = q_3(x)r_2(x) + r_3(x), \quad \deg r_3(x) < \deg r_2(x),$$

...

$$r_{k-2}(x) = q_k(x)r_{k-1}(x) + r_k(x), \quad \deg r_k(x) < \deg r_{k-1}(x),$$

$$r_{k-1}(x) = q_{k+1}(x)r_k(x).$$

Такая последовательность всегда существует, а последний ненулевой остаток $r_k(x)$ является наибольшим общим делителем многочленов $a(x)$ и $b(x)$.

Доказательство. Степени остатков не могут понижаться бесконечное число раз. Значит, существует последний ненулевой остаток. Пусть это $r_k(x)$. Из последнего соотношения ясно, что

$r_k(x) \mid r_{k-1}(x)$. Из предпоследнего находим: $r_k(x) \mid r_{k-2}(x)$. Про-
сматривая соотношения снизу вверх, приходим к выводу о том,
что $r_k(x)$ является общим делителем для $r_0(x)$ и $r_1(x)$. Далее,
пусть $d(x)$ — произвольный общий делитель многочленов $r_0(x)$
и $r_1(x)$. Из первого соотношения видим, что $r_2(x) : d(x)$. Про-
сматривая соотношения сверху вниз, получаем $r_k(x) : d(x)$. $\square$

Следствие 3.4.4 (ТЕОРЕМА О НАИБОЛЬШЕМ ОБЩЕМ ДЕЛИ-
ТЕЛЕ). Для отличных от констант многочленов $a(x)$ и $b(x)$
над полем K и их наибольшего общего делителя $d(x) \in K[x]$
существуют многочлены $u(x), v(x) \in K[x]$, такие что

$$a(x)u(x) + b(x)v(x) = d(x),$$

$$\deg u(x) < \deg b(x), \quad \deg v(x) < \deg a(x).$$

Доказательство. Рассмотрим первое соотношение алгоритма
Евклида

$$r_0 = q_2 r_1 + r_2$$

и запишем его в матричном виде:

$$\begin{bmatrix} r_1 \\ r_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_2 \end{bmatrix} \begin{bmatrix} r_0 \\ r_1 \end{bmatrix}.$$

Аналогично, при всех $2 \leq i \leq k$ находим

$$\begin{bmatrix} r_{i-1} \\ r_i \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix} \begin{bmatrix} r_{i-2} \\ r_{i-1} \end{bmatrix} = \begin{bmatrix} f_i & g_i \\ u_i & v_i \end{bmatrix} \begin{bmatrix} r_0 \\ r_1 \end{bmatrix},$$

где

$$\begin{bmatrix} f_i & g_i \\ u_i & v_i \end{bmatrix} := \begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -q_{i-1} \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & -q_2 \end{bmatrix}.$$

В итоге находим

$$\begin{bmatrix} r_{k-1} \\ r_k \end{bmatrix} = \begin{bmatrix} f_k & g_k \\ u_k & v_k \end{bmatrix} \begin{bmatrix} r_0 \\ r_1 \end{bmatrix} \Rightarrow r_k = u_k r_0 + v_k r_1.$$

Таким образом,

$$a(x)u(x) + b(x)v(x) = r_k(x) \quad \text{при} \quad u(x) := u_k(x), \quad v(x) := v_k(x).$$

Кроме того, при всех $3 \leq i \leq k$

$$\begin{bmatrix} f_i & g_i \\ u_i & v_i \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix} \begin{bmatrix} f_{i-1} & g_{i-1} \\ u_{i-1} & v_{i-1} \end{bmatrix},$$

откуда

$$\deg u_i = \deg q_i + \deg u_{i-1}, \quad \deg v_i = \deg q_i + \deg v_{i-1}.$$

Заметив, что $\deg u_2 = 0$ и $\deg v_2 = \deg q_2$, получаем

$$\deg u_k = \deg q_3 + \deg q_4 + \dots + \deg q_k = \deg r_1 - \deg r_{k-1} < \deg r_1,$$

$$\deg v_k = \deg q_2 + \deg q_3 + \dots + \deg q_k = \deg r_0 - \deg r_{k-1} < \deg r_0. \quad \square$$

Задача 123. Найдите все делители единицы в кольце 2×2 -матриц с целочисленными элементами.

Задача 124. Найдите наибольший общий делитель многочленов $x^{15} - 1$ и $x^{10} - 1$ над полем K в трех случаях: $K = \mathbb{Q}$, $K = \mathbb{Z}_2$, $K = \mathbb{Z}_5$.

3.5. Разложение на неприводимые множители

Пусть K — целостное кольцо с единицей. Отличный от делителя единицы ненулевой элемент $a \in K$ называется *неприводимым* в K , если из равенства $a = bc$ для каких-то $b, c \in K$ следует, что b или c является делителем единицы. Под *разложением на неприводимые множители* понимается представление элемента из K в виде произведения неприводимых элементов.

Разложение на неприводимые множители называется *однозначным*, если любое аналогичное разложение получается из него перенумерацией множителей и умножением их на делители единицы. Целостное кольцо с единицей, в котором любой элемент, отличный от делителя единицы, имеет однозначное разложение на неприводимые множители, называется *факториальным* или *гауссовым*.

Если K — целостное кольцо с единицей, то таким же будет и кольцо $K[x]$. Многочлен $p(x) \in K[x]$ называется *неприводимым над K* , если он не имеет нетривиальных делителей в кольце $K[x]$. Конечно, это определение согласуется с приведенным выше понятием неприводимости в произвольном целостном кольце с единицей.

Пример. Каждый из многочленов $f_1(x) = 7$, $f_2(x) = 17$, $f_3(x) = x^2 + 1$ не является делителем единицы в $\mathbb{Z}[x]$ и неприводим над $\mathbb{Z}$. При этом f_1 и f_2 являются в $\mathbb{Q}[x]$ делителями единицы, понятия приводимости или неприводимости для них не рассматриваются. Многочлен-константа $f(x) = 4$ приводим над $\mathbb{Z}$, но оказывается делителем единицы над $\mathbb{Q}$.

Лемма 3.5.1. Пусть рассматриваются многочлены над полем. Тогда

$$a(x)b(x) : c(x), \quad (b(x), c(x)) = 1 \Rightarrow a(x) : c(x).$$

Доказательство. По теореме о наибольшем общем делителе для некоторых многочленов $u(x)$ и $v(x)$ над тем же полем

$$b(x)u(x) + c(x)v(x) = 1 \Rightarrow$$

$$\Rightarrow (a(x)b(x))u(x) + c(x)a(x)v(x) = a(x) \Rightarrow a(x) : c(x). \quad \square$$

Теорема 3.5.1. Для любого отличного от константы многочлена над полем существует однозначное разложение на неприводимые множители.

Доказательство. Существование очевидно. Чтобы доказать однозначность, рассмотрим два разложения:

$$p_1 p_2 \dots p_s = q_1 q_2 \dots q_t.$$

Предположим, что p_1 не делится на q_1 . В силу неприводимости $(p_1, q_1) = 1$, поэтому по предыдущей лемме

$$p_2 p_3 \dots p_s : q_1.$$

Повторяя это рассуждение, мы установим, что существует многочлен p_i , который делится на многочлен q_1 . После перенумерации можно считать, что $p_1 : q_1$. В силу неприводимости получаем равенство $p_1 = c q_1$, где c — ненулевая константа. Таким образом,

$$q_1 (c p_2 p_3 \dots p_s - q_2 q_3 \dots q_t) = 0.$$

Поскольку в кольце многочленов над полем делителей нуля нет, отсюда получаем равенство следующих двух разложений на неприводимые множители:

$$(c p_2) p_3 \dots p_s = q_2 q_3 \dots q_t.$$

Для завершения доказательства можно провести индукцию по s . $\square$

Задача 125. Пусть n — простое число и a — рациональное число. Докажите, что многочлен $f(x) = x^n - a$ приводим над полем рациональных чисел в том и только том случае, когда $a = b^n$ для некоторого рационального числа b . Верно ли это утверждение в случае составного числа n ?

Задача 126. Докажите, что любое ненулевое гауссово число (комплексное число вида $a + bi$ при целых a и b) имеет конечное число делителей в кольце гауссовых чисел.

Задача 127. Пусть K — множество комплексных чисел вида $a + i\sqrt{3}b$, где $a, b \in \mathbb{Z}$. Докажите, что K является целостным кольцом с единицей, в котором число 4 имеет несколько разных разложений на неприводимые множители.

3.6. Многочлены с целыми коэффициентами

Рассмотрим вопрос о неприводимости над полем рациональных чисел многочлена с целыми коэффициентами. Его решение основано на следующей лемме.

Лемма 3.6.1 (ЛЕММА ГАУССА). Пусть $a(x), b(x), c(x) \in \mathbb{Z}[x]$ и $c(x) = a(x)b(x)$. Если все коэффициенты многочлена $c(x)$ делятся на простое число p , то это же верно для всех коэффициентов хотя бы одного из многочленов $a(x)$ или $b(x)$.

Доказательство. Пусть

$$\begin{aligned} c_0 + c_1x + \dots + c_{m+n}x^{m+n} = \\ = (a_0 + a_1x + \dots + a_mx^m)(b_0 + b_1x + \dots + b_nx^n). \end{aligned}$$

От противного, допустим, что $p \nmid a_i$ и $p \nmid b_j$. Давайте считать, что

$$p \mid a_0, \dots, p \mid a_{i-1}, p \nmid a_i \quad \text{и} \quad p \mid b_0, \dots, p \mid b_{j-1}, p \nmid b_j.$$

Тогда

$$c_{i+j} = a_ib_j + (a_{i-1}b_{j+1} + \dots + a_0b_{j+i}) + (a_{i+1}b_{j-1} + \dots + a_{i+j}b_0).$$

Число a_ib_j не делится на p , а две скобки делятся на p . Поэтому c_{i+j} не может делиться на p . $\square$

Теорема 3.6.1. Пусть $c(x) \in \mathbb{Z}[x]$. Тогда $c(x)$ нельзя представить в виде произведения целых многочленов ненулевой степени в том и только том случае, когда $c(x)$ неприводим над $\mathbb{Q}$.

Доказательство. Предположим, что многочлен $c(x) \in \mathbb{Z}[x]$ является произведением целых многочленов ненулевой степени. Тогда он очевидно приводим над $\mathbb{Q}$. Теперь предположим, что $c(x)$ приводим над $\mathbb{Q}$:

$$c(x) = a(x)b(x), \quad a(x), b(x) \in \mathbb{Q}[x], \quad m = \deg a(x), \quad n = \deg b(x).$$

Пусть для целых чисел A и B многочлены $a_1(x) := Aa(x)$ и $b_1(x) := Bb(x)$ оказываются многочленами с целыми коэффициентами, причем $\deg a_1(x) = m$ и $\deg b_1(x) = n$. Разложим число AB в произведение простых чисел:

$$AB = p_1 p_2 \dots p_s,$$

и рассмотрим равенство многочленов с целыми коэффициентами:

$$(p_1 p_2 \dots p_s) c(x) = a_1(x) b_1(x).$$

По лемме Гаусса все коэффициенты хотя бы одного из многочленов $a_1(x)$ или $b_1(x)$ делятся на p_1 . Поделив обе части равенства многочленов на p_1 , получаем новое равенство многочленов с целыми коэффициентами:

$$(p_2 p_3 \dots p_s) c(x) = a_2(x) b_2(x), \quad \text{где} \quad \deg a_2(x) = m, \quad \deg b_2(x) = n.$$

Применяя лемму Гаусса s раз, приходим к равенству

$$c(x) = a_{s+1}(x) b_{s+1}(x),$$

где многочлены $a_{s+1}(x)$ и $b_{s+1}(x)$ имеют целые коэффициенты, а их степени равны соответственно m и n . $\square$.

Теорема 3.6.2. *Кольцо $\mathbb{Z}[x]$ является факториальным.*

Доказательство. Многочлен $f(x) \in \mathbb{Z}[x]$ является также многочленом над $\mathbb{Q}$, поэтому он разлагается в произведение неприводимых многочленов с рациональными коэффициентами. Последовательное применение доказанной выше теоремы дает разложение того же многочлена в произведение многочленов с целыми коэффициентами, которые получаются из многочленов исходного разложения с помощью умножения на какие-то ненулевые целые числа. Таким образом можно получить представление

$$f(x) = p_1 \dots p_k f_1(x) \dots f_s(x),$$

где $p_1, \dots, p_k$ — простые числа, а $f_1(x), \dots, f_s(x)$ — целые многочлены положительной степени, обладающие тем свойством, что коэффициенты каждого из них не имеют нетривиального (отличного от делителя единицы) общего делителя. Это и будет разложение на неприводимые множители над $\mathbb{Z}$.

Пусть имеется еще одно разложение

$$f(x) = q_1 \dots q_l g_1(x) \dots g_t(x),$$

где $q_1, \dots, q_l$ — простые числа и $g_1(x), \dots, g_t(x)$ — неприводимые над $\mathbb{Z}$ многочлены положительной степени. Ясно, что

коэффициенты любого многочлена $g_i(x)$ не могут иметь нетривиальный общий делитель, иначе он будет приводимым над $\mathbb{Z}$. В силу леммы Гаусса, какое-то из чисел q_j должно делиться на p_i . Но это означает, что p_i равно какому-то из чисел q_j . По той же причине каждое q_j равно какому-то из чисел p_i . В итоге $k = l$ и числа $p_1, \dots, p_k$ получаются перестановкой чисел $q_1, \dots, q_k$. Следовательно,

$$f_1(x) \dots f_s(x) = g_1(x) \dots g_t(x).$$

Множители слева и справа являются неприводимыми многочленами над $\mathbb{Q}$, где однозначность разложения уже доказана. Следовательно, $s = t$ и после перенумерации справедливы соотношения

$$A_i f_i(x) = B_i g_i(x), \quad A_i, B_i \in \mathbb{Z}, \quad 1 \leq i \leq s.$$

В этом месте существенно, что коэффициенты каждого из многочленов $f_i(x)$ и $g_i(x)$ не имеют нетривиального общего делителя. Поэтому еще одно применение леммы Гаусса приводит нас к выводу о том, что A_i получается из B_i умножением на ± 1 . $\square$

При выяснении неприводимости конкретных многочленов весьма полезно следующее достаточное условие неприводимости.

Теорема 3.6.3 (ПРИЗНАК ЭЙЗЕНШТЕЙНА). Пусть $f(x) \in \mathbb{Z}[x]$. Если старший коэффициент $f(x)$ не делится на простое число p , все остальные коэффициенты делятся на p , но свободный член не делится на p^2 , то $f(x)$ неприводим над $\mathbb{Q}$.

Доказательство. От противного, пусть $f(x)$ разлагается в произведение рациональных многочленов степени m и n . Тогда $f(x)$ разлагается в произведение целых многочленов тех же степеней:

$$\begin{aligned} f_0 + f_1 x + \dots + f_{m+n} x^{m+n} = \\ = (a_0 + a_1 x + \dots + a_m x^m)(b_0 + b_1 x + \dots + b_n x^n). \end{aligned}$$

Число $a_0 b_0$ не делится на p^2 , но делится на p . Следовательно, ровно одно из чисел, a_0 либо b_0 , делится на p . Пусть это a_0 , тогда b_0 не делится на p . Среди коэффициентов a_i есть не делящийся на p . Поэтому существует номер i такой, что

$$p \mid a_0, \dots, p \mid a_{i-1}, \quad p \nmid a_i.$$

Тогда $f_i = a_i b_0 + (a_{i-1} b_1 + \dots + a_0 b_i)$. Произведение $a_i b_0$ не делится на p , а число в скобках делится. Поэтому f_i не может

делиться на p . По условию это невозможно при $i < t + n$. Следовательно, $i = t + n$ и, так как $i \leq t$, откуда получаем $n = 0$. $\square$

Задача 128. Докажите, что многочлен $f(x) = 2x^{1986} + 8x^{1955} + 27$ является неприводимым над $\mathbb{Q}$.

Задача 129. Пусть p — простое число. Докажите, что многочлен

$$f(x) = \frac{(x+1)^p - 1}{x}$$

неприводим над $\mathbb{Q}$.

Задача 130. Пусть $f(x) = 1 + x + \dots + x^{p-1}$ — многочлен с коэффициентами из поля вычетов по простому модулю p . Найдите разложение многочлена $f(x)$ на неприводимые над этим полем множители.

3.7. Круговые многочлены

Важный класс многочленов с целыми коэффициентами — это *круговые* или *циклотомические* многочлены, определяемые следующим образом:

$$\Phi_n(x) = \prod_{1 \leq k \leq n, (k,n)=1} (x - \varepsilon_n^k), \quad \varepsilon_n = \cos(2\pi/n) + i \sin(2\pi/n).$$

Они называются также *многочленами деления круга*. Корни многочлена $\Phi_n(x)$ — это в точности все первообразные корни степени n из единицы.

Утверждение 3.7.1. Многочлен $\Phi_n(x)$ имеет целые коэффициенты.

Доказательство. Каждый корень степени n является первообразным корнем однозначно определенной степени $d | n$ (это его порядок как элемента группы корней степени n). Поэтому

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Далее по индукции. $\square$

Известно, что круговые многочлены неприводимы. Мы отложим доказательство до обсуждения алгебраического понятия производной многочлена и его связи с наличием или отсутствием кратных корней.

Задача 131. Докажите, что сумма коэффициентов кругового многочлена $\Phi_n(x)$ равна простому числу p , если n — степень числа p , а если n не является степенью простого числа, то сумма равна 1.

3.8. Поле частных

Пусть K — произвольное целостное кольцо, в котором есть хотя бы один ненулевой элемент. Рассмотрим множество *формальных частных* или *дробей*

$$\frac{a}{b}, \quad \text{где } a, b \in K, \quad b \neq 0.$$

Любое формальное частное ассоциируется с упорядоченной парой элементов кольца K , в которой второй элемент не равен нулю. По очевидной аналогии с рациональными числами, можно называть a числителем, а b — знаменателем.

По определению,

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc.$$

Данное бинарное отношение является рефлексивным, симметричным и транзитивным. Приведем доказательство транзитивности (в нем используется отсутствие делителей нуля в K):

$$\begin{aligned} \frac{a}{b} = \frac{c}{d}, \quad \frac{c}{d} = \frac{p}{q} &\Rightarrow ad = bc, \quad cq = dp \Rightarrow \\ adq = bcq = bdp &\Rightarrow aq = bp \Rightarrow \frac{a}{b} = \frac{p}{q}. \end{aligned}$$

Таким образом, все множество формальных частных разбивается на непересекающиеся классы равных между собой частных. Для обозначения класса используется любой его представитель.

Определим операцию сложения формальных частных следующим образом:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}.$$

Здесь нужна проверка корректности определения, которая заключается в следующем.

Утверждение 3.8.1.

$$\frac{a}{b} = \frac{a_1}{b_1}, \quad \frac{c}{d} = \frac{c_1}{d_1} \Rightarrow \frac{ad + bc}{bd} = \frac{a_1d_1 + b_1c_1}{b_1d_1}.$$

Доказательство. $(ad + cb)b_1d_1 - (a_1d_1 + c_1b_1)bd =$
 $= dd_1(ab_1 - a_1b) + bb_1(cd_1 - c_1d) = 0. \quad \square$

Вот определение операции умножения формальных частных:

$$\frac{a}{b} \frac{c}{d} := \frac{ac}{bd}.$$

Как и для сложения, следует проверить корректность определения.

Утверждение 3.8.2. $\frac{a}{b} = \frac{a_1}{b_1}, \quad \frac{c}{d} = \frac{c_1}{d_1} \Rightarrow \frac{ac}{bd} = \frac{a_1c_1}{b_1d_1}.$

Доказательство. $ab_1 = ba_1, \quad cd_1 = dc_1 \Rightarrow$
 $\Rightarrow acb_1d_1 = bda_1c_1. \quad \square$

Теорема 3.8.1. Для любого целостного кольца с хотя бы одним ненулевым элементом множество его формальных частных с операциями сложения и умножения образует поле.

Доказательство. Начнем с проверки ассоциативности сложения:

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{p}{q} = \frac{(ad + bc)q + bdp}{bdq}, \quad \frac{a}{b} + \left(\frac{c}{d} + \frac{p}{q}\right) = \frac{b(cq + dp) + adq}{bdq},$$

$$(ad + bc)q + bdp - b(cq + dp) - adq = adq + bcq - bcq - adq = 0.$$

Нулевой элемент по сложению есть формальное частное вида

$$0 := \frac{0}{b}, \quad b \neq 0.$$

Противоположный элемент имеет такой вид:

$$-\frac{a}{b} = \frac{-a}{b}.$$

Коммутативность сложения дробей очевидна. При проверке дистрибутивности вновь используется отсутствие делителей нуля:

$$\left(\frac{a}{b} + \frac{c}{d}\right) \frac{p}{q} = \frac{(ad + bc)p}{bdq},$$

$$\frac{a}{b} \frac{p}{q} + \frac{c}{d} \frac{p}{q} = \frac{ap}{bq} + \frac{cp}{dq} = \frac{apdq + bqcp}{bq dq} = \frac{apd + bcp}{bdq} = \frac{(ad + bc)p}{bdq}.$$

Коммутативность умножения очевидна. Единичный элемент имеет вид

$$1 := \frac{a}{a}, \quad a \neq 0.$$

Обратный элемент для дроби с ненулевым числителем определяется таким образом:

$$\left(\frac{a}{b}\right)^{-1} := \frac{b}{a}. \quad \square$$

Фиксируем произвольный ненулевой элемент $b \in K$ и рассмотрим отображение, определенное для любого $a \in K$:

$$\phi: a \rightarrow \frac{ab}{b}.$$

Нетрудно проверить, что при этом отображении разные элементы переходят в разные дроби, поэтому каждый элемент исходного кольца однозначно сопоставляется с некоторой дробью. Кроме того, сумма и произведение элементов переходят в сумму и произведение дробей, ассоциированных с этими элементами посредством отображения ϕ . Все это дает основание говорить, что исходное целостное кольцо *вложено* в свое поле частных.

Если $K = \mathbb{Z}$ — кольцо целых чисел, то поле частных строится так же, как поле рациональных чисел. Общеизвестно, что $\mathbb{Z}$ считается частью $\mathbb{Q}$.

Пусть K — целостное кольцо и $K[x]$ — кольцо многочленов над K . Поле частных для $K[x]$, т.е. поле формальных дробей вида

$$\frac{f(x)}{g(x)}, \quad f(x), g(x) \in K[x], \quad g(x) \neq 0,$$

называется *полем рациональных функций* на K . Обозначение для поля рациональных функций: $K(x)$ (круглые скобки вместо квадратных скобок для кольца многочленов от x). Естественным образом считается, что $K[x] \subset K(x)$.

Задача 132. *Рассматриваются рациональные функции над $\mathbb{Z}_2$, для которых степень числителя и знаменателя не выше 2. Найдите число различных рациональных функций такого вида.*

3.9. Многочлены от нескольких переменных

Пусть K — целостное кольцо с единицей и $K_1 := K[x]$ — кольцо многочленов над K . Мы уже знаем, что кольцо K_1 также является целостным кольцом с единицей.

Пусть теперь $K_1[y]$ — кольцо многочленов от y с коэффициентами из K_1 . Любой элемент кольца

$$K_1[y] = (K[x])[y]$$

имеет вид

$$f(x, y) = \sum_i \sum_j a_{ij} x^i y^j,$$

где i, j — неотрицательные целые числа и a_{ij} — элементы из K , среди которых лишь конечное число отличается от нуля, т.е. в сумме присутствует конечное число членов. Условимся писать $K[x, y] = (K[x])[y]$ — это кольцо многочленов от переменных x и y с коэффициентами из K .

Аналогичным образом строится кольцо

$$K[x_1, x_2, \dots, x_n] := (K[x_1, \dots, x_{n-1}])[x_n].$$

Это целостное кольцо с единицей. Его элементы называются многочленами от переменных $x_1, \dots, x_n$ и имеют вид суммы одночленов

$$a_{i_1, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}, \quad a_{i_1, \dots, i_n} \in K.$$

Если $a_{i_1, \dots, i_n} \neq 0$, то одночлен называется ненулевым, в этом случае сумма $i_1 + \dots + i_n$ называется его степенью. Степенью многочлена называется максимальная степень его ненулевых одночленов.

Многочлен называется *однородным*, если он отличен от ненулевой константы и состоит из одночленов одной и той же степени.

Удобно ввести *мультииндекс* $i := (i_1, \dots, i_n)$ и писать $x := (x_1, \dots, x_n)$ и $x^i := x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$. С помощью мультииндексов запись многочлена от n переменных по виду ничем не отличается от записи многочлена от одной переменной:

$$f(x_1, \dots, x_n) = f(x) = \sum_i a_i x^i,$$

$$x = (x_1, \dots, x_n), \quad i = (i_1, \dots, i_n).$$

Каноническим представлением многочлена считается такое представление, в котором одночлен с мультииндексом i встречается только один раз. Два многочлена называются равными, если в своих канонических представлениях они имеют одни и те же коэффициенты в одночленах с одним и тем же мультииндексом.

Возьмем $\alpha_1, \dots, \alpha_n \in K$. Значением многочлена $f(x_1, \dots, x_n)$ в точке $(\alpha_1, \dots, \alpha_n)$ называется

$$f(\alpha_1, \dots, \alpha_n) := \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} \alpha_1^{i_1} \dots \alpha_n^{i_n}.$$

Как и для многочлена от одной переменной, для многочленов от n переменных вводится понятие делителя: мы пишем

$$g(x_1, \dots, x_n) : f(x_1, \dots, x_n) \quad \text{или} \quad f(x_1, \dots, x_n) \mid g(x_1, \dots, x_n),$$

если существует многочлен $h(x_1, \dots, x_n)$ над K , с которым выполняется равенство

$$g(x_1, \dots, x_n) = f(x_1, \dots, x_n)h(x_1, \dots, x_n).$$

Теорема 3.9.1. *Если K — факториальное кольцо, то кольцо $K[x_1, \dots, x_n]$ также является факториальным.*

Мы наметим лишь схему доказательства. Достаточно установить, что кольцо $K[x]$ является факториальным. Для этого построим поле частных для K . Обозначим это поле через L . Уже доказано, что для многочленов от одной переменной над любым полем, в том числе и над L , имеет место однозначное разложение на неприводимые множители. Далее можно сформулировать абстрактный аналог леммы Гаусса для многочленов $a(x)$ и $b(x)$ над произвольным факториальным кольцом, произведение которых $c(x) = a(x)b(x)$ делится на неприводимый элемент p этого кольца, и почти слово в слово переписать доказательство теоремы о факториальности кольца $\mathbb{Z}[x]$.

Задача 133. *Два многочлена от n переменных над бесконечным полем принимают одинаковые значения в бесконечном числе различных точек. Равны ли эти многочлены?*

Задача 134. *Покажите, что теорема о наибольшем общем делителе для многочленов от двух и большего числа переменных неверна.*

Задача 135. *Поле K вложено в поле M и многочлены $f(x_1, \dots, x_n)$ и $g(x_1, \dots, x_n)$ над полем K имеют общий множитель степени ≥ 1 над полем M . Докажите, что они имеют общий множитель степени ≥ 1 также над полем K .*

Задача 136. *Многочлены $f(x_1, \dots, x_n)$ и $g(x_1, \dots, x_n)$ с целыми коэффициентами имеют общий множитель $h(x_1, \dots, x_n)$ в кольце многочленов с рациональными коэффициентами.*

Докажите, что для некоторого рационального числа α многочлен αh имеет целые коэффициенты и является общим делителем многочленов f и g в кольце многочленов с целыми коэффициентами.

Задача 137. Докажите, что многочлен $x^2 + y^2 - 1$ приводим над полем $\mathbb{Z}_2$ и неприводим над любым полем $\mathbb{Z}_p$ при простом $p \geq 3$.

Задача 138. Докажите, что любой делитель однородного многочлена является однородным многочленом.

Задача 139. В поле K выбрано подмножество X из m различных элементов и рассматривается множество точек

$$D := \underbrace{X \times \dots \times X}_n = \{(\alpha_1, \dots, \alpha_n) : \alpha_1, \dots, \alpha_n \in X\}.$$

Дан многочлен $f(x_1, \dots, x_n)$ над полем K . Докажите, что число его корней, принадлежащих D , т.е. таких точек $(\alpha_1, \dots, \alpha_n) \in D$, в которых $f(\alpha_1, \dots, \alpha_n) = 0$, не больше чем $\deg f \cdot m^{n-1}$.

Задача 140. Выясните, является ли многочлен $f(x, y, z) = x^{25} + y^{25} + z^{25}$ неприводимым над $\mathbb{Z}_5$.

Задача 141. Пусть K — поле. Докажите, что многочлен от n переменных над K вида

$$f(x_1, \dots, x_n) := \det \begin{bmatrix} x_1 & x_1^2 & \dots & x_1^n \\ x_2 & x_2^2 & \dots & x_2^n \\ \dots & \dots & \dots & \dots \\ x_n & x_n^2 & \dots & x_n^n \end{bmatrix}$$

делится на $x_i - x_j$ при $i \neq j$. Найдите его разложение на неприводимые множители.

Задача 142. Над полем K задан многочлен от n^2 переменных x_{ij} , $1 \leq i, j \leq n$, который определяется следующим образом:

$$f(x_{11}, x_{21}, \dots, x_{nn}) := \det \begin{bmatrix} x_{11} & \dots & x_{1n} \\ \dots & \dots & \dots \\ x_{n1} & \dots & x_{nn} \end{bmatrix}.$$

Докажите, что этот многочлен неприводим над K .

3.10. Матрица Сильвестра и результат

Пусть даны многочлены

$$\begin{aligned} f(x, a_0, \dots, a_m) &= a_0 + a_1x + \dots + a_mx^m, \\ g(x, b_0, \dots, b_n) &= b_0 + b_1x + \dots + b_nx^n. \end{aligned} \quad (*)$$

Квадратная матрица вида

$$S(f, g) = \left[\begin{array}{cccc} a_m & a_{m-1} & \dots & a_0 \\ & a_m & a_{m-1} & \dots & a_0 \\ & & \dots & \dots & \dots \\ & & & a_m & a_{m-1} & \dots & a_0 \\ b_n & b_{n-1} & \dots & b_0 \\ & b_n & b_{n-1} & \dots & b_0 \\ & & \dots & \dots & \dots & \dots \\ & & & b_n & b_{n-1} & \dots & b_0 \end{array} \right] \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \begin{array}{l} n \text{ строк} \\ \\ \\ t \text{ строк} \end{array}$$

называется ассоциированной с ними *матрицей Сильвестра* или *результант-матрицей*. Ее определитель

$$R(a_0, \dots, a_m, b_0, \dots, b_n) := \det S(f, g)$$

называется *результантом* многочленов f и g .

Утверждение 3.10.1. *Результант R многочленов f и g вида (*) является многочленом от $a_0, \dots, a_m, b_0, \dots, b_n$, и выполняется равенство*

$$fu + gv = R,$$

где $u(x, a_0, \dots, a_m, b_0, \dots, b_n)$, $v(x, a_0, \dots, a_m, b_0, \dots, b_n)$ — некоторые многочлены с целыми коэффициентами.

Доказательство. Результант-матрицу $S = S(f, g)$ можно рассматривать как матрицу над полем рациональных функций $\mathbb{Q}(x, a_0, \dots, a_m, b_0, \dots, b_n)$. Используем легко проверяемое равенство

$$S \begin{bmatrix} x^{m+n-1} \\ x^{m+n-2} \\ \dots \\ x \\ 1 \end{bmatrix} = \begin{bmatrix} fp \\ gq \end{bmatrix}, \quad \text{где} \quad p = \begin{bmatrix} x^{n-1} \\ x^{n-2} \\ \dots \\ x \\ 1 \end{bmatrix}, \quad q = \begin{bmatrix} x^{m-1} \\ x^{m-2} \\ \dots \\ x \\ 1 \end{bmatrix},$$

и формулы Крамера. Для последнего элемента столбца, на который умножается матрица S , находим

$$1 \cdot R = R',$$

где R' — определитель матрицы, которая отличается от S заменой последнего столбца на столбец $\begin{bmatrix} fp \\ gq \end{bmatrix}$. $\square$

Вот замечательное, хотя и очевидное, следствие: если $f = g = 0$, то $R = 0$. При этом система полиномиальных уравнений $f = g = 0$ устанавливает связь между переменными $x, a_0, \dots, a_m, b_0, \dots, b_n$, а в уравнении $R = 0$ переменная x не присутствует. Таким образом, при решении системы полиномиальных уравнений результат позволяет исключить одну из переменных, в нашем случае x .

Утверждение 3.10.2. *Предположим, что многочлены f и g вида (*) допускают разложения*

$$f = a_m \prod_{i=1}^m (x - \alpha_i), \quad g = b_n \prod_{j=1}^n (x - \beta_j).$$

Тогда для результата многочленов f и g справедливо представление

$$R = a_m^n b_n^m \prod_{i=1}^m \prod_{j=1}^n (\alpha_i - \beta_j).$$

Доказательство. Будем считать, что f и g — многочлены от буквы x над полем рациональных функций $\mathbb{Q}(a_m, \alpha_1, \dots, \alpha_m, b_n, \beta_1, \dots, \beta_n)$. Полагаем, что элементы результат-матрицы S для f и g принадлежат этому же полю. Кроме того, будем использовать матрицы над тем же полем, определяемые следующим образом:

$$W(\xi_1, \dots, \xi_s) = \begin{bmatrix} \xi_1^{s-1} & \xi_2^{s-1} & \dots & \xi_s^{s-1} \\ \xi_1^{s-2} & \xi_2^{s-2} & \dots & \xi_s^{s-2} \\ \dots & \dots & \dots & \dots \\ \xi_1 & \xi_2 & \dots & \xi_s \\ 1 & 1 & \dots & 1 \end{bmatrix}.$$

Матрица V , полученная из $W(\xi_1, \dots, \xi_s)$ перестановкой строк в обратном порядке, называется *матрицей Вандермонда*. Так же называется транспонированная матрица V^T . В разделе 1.6 была

получена формула для определителя Вандермонда $|V|$. Применяя ее и учитывая изменение знака при перестановках, находим

$$|W(\xi_1, \dots, \xi_s)| = \prod_{1 \leq i < j \leq s} (\xi_i - \xi_j).$$

Введем в рассмотрение следующие матрицы:

$$Z = W(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n), \quad Z_1 = W(\alpha_1, \dots, \alpha_m),$$

$$Z_2 = W(\beta_1, \dots, \beta_n),$$

$$D_1 = \begin{bmatrix} g(\alpha_1) & & \\ & \ddots & \\ & & g(\alpha_m) \end{bmatrix}, \quad D_2 = \begin{bmatrix} f(\beta_1) & & \\ & \ddots & \\ & & f(\beta_n) \end{bmatrix}.$$

Прямая проверка дает нам равенство

$$SW = \begin{bmatrix} 0_{n \times m} & D_2 W_2 \\ D_1 W_1 & 0_{m \times n} \end{bmatrix}.$$

С помощью разложения Лапласа находим определитель матрицы в правой части:

$$\begin{aligned} (-1)^{mn} |D_1| |D_2| |W_1| |W_2| &= \\ &= (-1)^{mn} \prod_{i=1}^m g(\alpha_i) \prod_{j=1}^n f(\beta_j) \prod_{1 \leq i_1 < i_2 \leq m} (\alpha_{i_1} - \alpha_{i_2}) \times \\ &\times \prod_{1 \leq j_1 < j_2 \leq n} (\alpha_{j_1} - \alpha_{j_2}) = b_n^m a_n^m \left(\prod_{i=1}^m \prod_{j=1}^n (\alpha_i - \beta_j) \right)^2 \times \\ &\times \prod_{1 \leq i_1 < i_2 \leq m} (\alpha_{i_1} - \alpha_{i_2}) \prod_{1 \leq j_1 < j_2 \leq n} (\alpha_{j_1} - \alpha_{j_2}). \end{aligned}$$

Определитель матрицы в левой части равен

$$R|W| = R \prod_{i=1}^m \prod_{j=1}^n (\alpha_i - \beta_j) \prod_{1 \leq i_1 < i_2 \leq m} (\alpha_{i_1} - \alpha_{i_2}) \prod_{1 \leq j_1 < j_2 \leq n} (\alpha_{j_1} - \alpha_{j_2}).$$

В левой и правой части полученного равенства многочленов имеется общий ненулевой множитель. Искомое выражение для результата возникает после его сокращения — здесь мы опираемся на целостность кольца многочленов. $\square$

Следствие 3.10.1. Пусть f и g — многочлены от буквы x вида (*) с коэффициентами $a_0, \dots, a_m$ и $b_0, \dots, b_n$ из произвольного поля и при этом $a_m \neq 0$ и $b_n \neq 0$. Тогда f и g имеют нетривиальный общий делитель в том и только том случае, когда их результат равен нулю.

Задача 143. Докажите, что степень наибольшего общего делителя многочленов $f(x)$ и $g(x)$ над некоторым полем равна сумме их степеней минус ранг ассоциированной с ними результат-матрицы.

3.11. Симметрические многочлены

Многочлен $f(x_1, \dots, x_n)$ называется *симметрическим*, если

$$f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = f(x_1, \dots, x_n) \quad \forall \sigma \in S_n.$$

Вот простейшие примеры симметрических многочленов:

$$E_1(x_1, \dots, x_n) = x_1 + x_2 + \dots + x_n, \quad E_n(x_1, \dots, x_n) = x_1 x_2 \dots x_n.$$

Обобщая эти примеры, положим

$$E_k(x_1, \dots, x_n) := \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} \dots x_{i_k}, \quad 1 \leq k \leq n.$$

Такие многочлены называются *элементарными симметрическими многочленами*.

Элементарные симметрические многочлены возникают при описании связи между корнями многочлена и его коэффициентами.

Теорема 3.11.1 (ТЕОРЕМА ВИЕТА). Пусть $x_1, \dots, x_n \in L$, где L — поле, содержащее в себе поле K . Если многочлен над K имеет вид

$$\begin{aligned} f(x) &= a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + a_n x^n = \\ &= (x - x_1)(x - x_2) \dots (x - x_n), \end{aligned}$$

то для его коэффициентов имеют место формулы

$$a_k = (-1)^{n-k} E_{n-k}(x_1, \dots, x_n), \quad 0 \leq k \leq n-1, \quad a_n = 1.$$

Доказательство проводится раскрытием скобок очевидным образом.

Теорема 3.11.2. *Для любого симметрического многочлена $f(x_1, \dots, x_n)$ существует единственный многочлен $g(z_1, \dots, z_n)$, такой что*

$$f(x_1, \dots, x_n) = g(E_1(x_1, \dots, x_n), \dots, E_n(x_1, \dots, x_n)).$$

Доказательство. Примем специальный порядок для ненулевых одночленов, входящих в каноническое представление многочлена $f(x)$, $x = (x_1, \dots, x_n)$. А именно, введем *словарный порядок* для мультииндексов:

$$\begin{aligned} i = (i_1, \dots, i_n) > j = (j_1, \dots, j_n) &\Leftrightarrow \\ \Leftrightarrow \exists k : i_1 = j_1, \dots, i_{k-1} = j_{k-1}, i_k > j_k. \end{aligned}$$

Порядок для ненулевых одночленов соответствует порядку для их мультииндексов. В частности,

$$x_1 > x_2 > \dots > x_n.$$

Из симметричности многочлена $f(x)$ вытекает, что если $a_i x^i$ — его старший одночлен по словарному порядку, то мультииндекс $i = (i_1, \dots, i_n)$ обладает следующим свойством:

$$i_1 \geq i_2 \geq \dots \geq i_n.$$

В самом деле, если для некоторой подстановки $\sigma \in S_n$ в составе $f(x)$ имеется одночлен

$$a_i x_{\sigma(1)}^{i_1} \dots x_{\sigma(n)}^{i_n},$$

то в силу симметричности должен присутствовать и одночлен

$$a_i x_1^{i_1} \dots x_n^{i_n}.$$

Рассмотрим новый симметрический многочлен

$$f_1(x) := f(x) - a_i E^j,$$

$$E = (E_1(x), \dots, E_n(x)), \quad j = (j_1, \dots, j_n),$$

$$j_1 := i_1 - i_2, \quad j_2 := i_2 - i_3, \quad \dots, \quad j_{n-1} := i_{n-1} - i_n, \quad j_n := i_n,$$

и заметим, что его старший одночлен строго меньше старшего одночлена для $f(x)$. Аналогичным образом из $f_1(x)$ получается симметрический многочлен $f_2(x)$, для которого старший одночлен еще меньше. И так далее.

Примем во внимание, что одночленов, которые по словарному порядку меньше заданного одночлена, имеется конечное число. Поэтому рано или поздно мы придем к нулевому многочлену, а в итоге $f(x)$ окажется суммой одночленов от $E_1, \dots, E_n$. Данная сумма и определяет искомым многочлен $g(z_1, \dots, z_n)$, для которого $f(x) = g(E_1(x), \dots, E_n(x))$.

Для доказательства единственности достаточно установить следующее:

$$G(x) := g(E_1(x), \dots, E_n(x)) = 0 \Rightarrow g(z_1, \dots, z_n) = 0.$$

От противного, пусть $g(z) \neq 0$, $z = (z_1, \dots, z_n)$. С каждым ненулевым одночленом $a_j z^j$ в составе $g(z)$ свяжем одночлен $a_j x^i$, где

$$i_1 = j_1 + \dots + j_n, \quad i_2 = j_2 + \dots + j_n, \quad \dots, \quad i_{n-1} = j_{n-1} + j_n, \quad i_n = j_n,$$

и выберем мультииндекс j , соответствующий наибольшему i по словарному порядку. Запишем

$$G(x) = a_j x^i + R(x)$$

и заметим, что одночлен $a_j x^i$ строго больше в словарном смысле, чем любой одночлен в составе $R(x)$. Поэтому равенство $G(x) = 0$ невозможно. $\square$

Еще один пример симметрического многочлена от n переменных:

$$D(x_1, \dots, x_n) := \prod_{1 \leq i < j \leq n} (x_i - x_j)^2.$$

Значение D в случае, когда $x_1, \dots, x_n$ — корни многочлена от одной переменной

$$f(x) = x^n + a_{n-1}x + \dots + a_0 = (x - x_1) \dots (x - x_n),$$

называется *дискриминантом* многочлена $f(x)$. Для квадратного многочлена

$$x^2 + bx + c = (x - x_1)(x - x_2)$$

дискриминант равен

$$D = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = b^2 - 4c.$$

Из доказанной нами теоремы следует, что дискриминант всегда вычисляется по коэффициентам с помощью конечного числа арифметических операций, знание корней не требуется.

Если старший коэффициент многочлена $f(x)$ степени n отличен от единицы и равен a , то дискриминант определяется как дискриминант многочлена $f(x)/a$, умноженный на a^{2n-2} . Можно доказать, что в этом случае он также является многочленом от коэффициентов многочлена $f(x)$.

Задача 144. Докажите, что кольцо многочленов от n переменных над некоторым полем изоморфно своему собственному подкольцу, состоящему из всех симметрических многочленов.

Задача 145. Найдите сумму

$$S = x_1^3 + \dots + x_n^3,$$

где $x_1, \dots, x_n$ — корни многочлена $f(x) = x^n + x + 1$.

Задача 146. Пусть $\varepsilon = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ и $f(x_1, \dots, x_n)$ — симметрический многочлен с целыми коэффициентами. Докажите, что значение $f(x_1, \dots, x_n)$ в точке $(1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1})$ является целым числом.

Задача 147. Найдите кубический многочлен, корнями которого являются квадраты корней многочлена $x^3 - 2x - 5$.

Задача 148. Докажите, что произвольный симметрический многочлен от переменных $x_2, \dots, x_n$ является многочленом от x_1 и элементарных симметрических многочленов $E_1, \dots, E_n$ от переменных $x_1, x_2, \dots, x_n$.

Задача 149. Докажите, что произвольная рациональная функция от переменных $x_1, \dots, x_n$ над полем рациональных чисел является рациональной функцией от $x = x_1 + 2x_2 + \dots + nx_n$ над полем симметрических рациональных функций от $x_1, \dots, x_n$.

Задача 150. Докажите, что суммы вида

$$s_k(x_1, \dots, x_n) := \sum_{i=1}^n x_i^k$$

и элементарные симметрические многочлены $E_k(x_1, \dots, x_n)$ связаны следующими рекуррентными соотношениями ¹⁾:

$$s_l + \sum_{k=1}^{l-1} (-1)^k s_{l-k} E_k + (-1)^l l E_l = 0 \quad \text{при } 1 \leq l \leq n,$$

$$s_l + \sum_{k=1}^n (-1)^k s_{l-k} E_k = 0 \quad \text{при } l > n.$$

Задача 151. Докажите, что дискриминант многочлена $x^n - 1 \in \mathbb{C}[x]$ равен

$$D = (-1)^{(n-1)(n+2)/2} n^n.$$

¹⁾ Их называют соотношениями Ньютона, а величины s_k — суммами Ньютона.

Глава 4

ЛИНЕЙНЫЕ ПРОСТРАНСТВА, ПОЛЯ И ИХ РАСШИРЕНИЯ

4.1. Линейные пространства и подпространства

Будем считать, что фиксировано произвольное поле K , элементы которого называются *числами*, и задано непустое множество V , элементы которого называются *векторами*.

Пусть на V определена *операция сложения векторов*, которая обозначается знаком $+$ и превращает V в абелеву группу. Нулевой элемент этой группы называется *нулевым вектором*. В этом разделе нулевой вектор обозначается полужирным символом $\mathbf{0}$, чтобы отличать его от числа 0 в поле K . Заметим также, что для нуля в поле и для нулевого вектора часто применяется один и тот же символ 0 . Смысл всегда ясен из контекста, поэтому затруднений не возникает. К такому стилю мы перейдем в последующих разделах.

Пусть имеется также *операция умножения вектора на число*. Она обозначается пустым местом или точкой, а ее результатом является вектор

$$w = \alpha v \in V, \quad \alpha \in K, \quad v \in V.$$

Пусть операция сложения векторов и операция умножения вектора на число обладают еще и такими свойствами:

- 1) $(\alpha\beta)v = \alpha(\beta v) \quad \forall \alpha, \beta \in K, \forall v \in V$
(ассоциативность умножения на число);
- 2) $(\alpha + \beta)v = \alpha v + \beta v \quad \forall \alpha, \beta \in K, \forall v \in V$
(дистрибутивность по сложению чисел);
- 3) $\alpha(u + v) = \alpha u + \alpha v \quad \forall \alpha \in K, \forall u, v \in V$
(дистрибутивность по сложению векторов);
- 4) $1 \cdot v = v \quad \forall v \in V, \quad 1 \text{ — единица поля } K.$

В таких случаях V называется *линейным пространством над полем K* или *векторным пространством над полем K* .

Утверждение 4.1.1. $0 \cdot v = 0$ для любого вектора $v \in V$.

Доказательство.

$$0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v \Rightarrow 0 \cdot v = 0. \quad \square$$

Утверждение 4.1.2. $(-1) \cdot v = -v$ для любого вектора $v \in V$.

$$\begin{aligned} \text{Доказательство. } 0 &= 0 \cdot v = (1 + (-1)) \cdot v = \\ &= 1 \cdot v + (-1) \cdot v = v + (-1) \cdot v \Rightarrow (-1) \cdot v = -v. \quad \square \end{aligned}$$

Заметим, что аксиома $1 \cdot v = v \forall v \in V$ равносильна утверждению о том, что любой вектор можно получить путем умножения некоторого вектора на некоторое число. Данное утверждение очевидно следует из этой аксиомы. В то же время, если $v = \alpha w$ для какого-то числа $\alpha \in K$ и какого-то вектора $w \in V$, то в силу ассоциативности умножения на число получаем

$$1 \cdot v = 1 \cdot (\alpha w) = (1 \cdot \alpha)w = \alpha w = v.$$

Пример 1. Множество $V = K^{m \times n}$ всех матриц размера $m \times n$ с элементами из поля K является линейным пространством над полем K . Сложение векторов в данном случае — это сложение матриц, определяемое как поэлементное сложение. Умножение вектора на число — это умножение матрицы на число, определяемое как поэлементное умножение.

Пример 2. Пусть $V = C[0, 1]$ — множество вещественных функций, непрерывных на отрезке $[0, 1]$. Оно является линейным пространством над полем вещественных чисел $\mathbb{R}$. Сложение векторов в данном случае — это поточечное сложение функций, умножение вектора на число — это умножение функции на число. Важно, что в результате этих операций будут получаться функции, которые также непрерывны на отрезке $[0, 1]$.

Пусть V — линейное пространство над полем K . Непустое подмножество $L \subseteq V$ называется *подпространством* в V , если оно обладает следующим свойством:

$$u, v \in L, \alpha, \beta \in K \Rightarrow \alpha u + \beta v \in L.$$

По аналогии с группами и подгруппами, для подпространства L в V будем использовать обозначение $L \leq V$. Ясно, что L также

является линейным пространством над полем K . Два *тривиальных* подпространства — это *нулевое подпространство*, состоящее из одного нулевого вектора, и подпространство L , совпадающее с V . Остальные подпространства называются *нетривиальными*.

Простой и важный для алгебры метод конструирования подпространств заключается в следующем. Возьмем произвольные векторы $v_1, \dots, v_n$ и числа $\alpha_1, \dots, \alpha_n$. Выражение

$$\alpha_1 v_1 + \dots + \alpha_n v_n$$

называется *линейной комбинацией* векторов $v_1, \dots, v_n$, а числа $\alpha_1, \dots, \alpha_n$ называются ее коэффициентами. Множество всевозможных линейных комбинаций заданных векторов $v_1, \dots, v_n$ называется их *линейной оболочкой* и обозначается

$$L(v_1, \dots, v_n) = \langle v_1, \dots, v_n \rangle := \{ \alpha_1 v_1 + \dots + \alpha_n v_n : \alpha_1, \dots, \alpha_n \in K \}.$$

Легко проверяется, что линейная оболочка любой конечной системы векторов линейного пространства V является подпространством.

Если уже имеются какие-то подпространства, то можно строить их пересечения в теоретико-множественном смысле и суммы как суммы множеств аддитивной группы:

$$L + M := \{ u + v : u \in L, v \in M \}.$$

Утверждение 4.1.3. *Сумма и пересечение подпространств в пространстве V также являются подпространствами:*

$$L \leq V, M \leq V \Rightarrow L + M \leq V, L \cap M \leq V.$$

Доказательство. Пусть $u, v \in L + M$. Тогда $u = u_1 + u_2$ и $v = v_1 + v_2$, где $u_1, v_1 \in L$ и $u_2, v_2 \in M$. Следовательно,

$$\begin{aligned} u + v &= (u_1 + v_1) + (u_2 + v_2), \quad u_1 + v_1 \in L, \quad u_2 + v_2 \in M \Rightarrow \\ &\Rightarrow u + v \in L + M. \end{aligned}$$

Аналогично, если $\alpha \in K$, то $\alpha u = \alpha u_1 + \alpha u_2$, $\alpha u_1 \in L$, $\alpha u_2 \in M \Rightarrow \alpha u \in L + M$. Таким образом, мы доказали, что $L + M \leq V$. Случай $L \cap M$ разбирается по той же схеме. $\square$

Можно рассматривать суммы любого конечного числа подпространств $L_1, \dots, L_s$, их сумма $L = L_1 + \dots + L_s := \{ x \in V : x = x_1 + \dots + x_s, x_i \in L_i, 1 \leq i \leq s \}$ также будет подпространством. Нетрудно проверить, что пересечение *любого* (необяза-

тельно конечного) числа подпространств является подпространством. Пересечение всех подпространств, содержащих заданные векторы $v_1, \dots, v_n$, совпадает с их линейной оболочкой. Пересечение L всех подпространств, содержащих заданное непустое множество $M \subseteq V$, также является подпространством. Оно называется *линейной оболочкой множества M* и состоит из линейных комбинаций любых конечных систем векторов, принадлежащих M . Обозначение: $L = \langle M \rangle$.

Пусть L_1 и L_2 — подпространства в пространствах матриц-столбцов над общим полем. Линейная оболочка множества кронекеровых произведений (см. раздел 1.7) $\{v_1 \otimes v_2: v_1 \in L_1, v_2 \in L_2\}$ называется *тензорным произведением* подпространств L_1 и L_2 и обозначается $L_1 \otimes L_2$.

Пусть A — матрица размера $m \times n$ над полем K . Множество векторов

$$L := \{x \in K^{n \times 1}: Ax = 0\}$$

называется *ядром* или *нуль-пространством* матрицы A . Обозначение: $L = \ker A$. Множество векторов

$$M := \{y \in K^{m \times 1}: \exists x \in K^{n \times 1}, y = Ax\}$$

называется *образом* матрицы A . Обозначение: $M = \operatorname{im} A$.

Утверждение 4.1.4. *Ядро матрицы $A \in K^{m \times n}$ над полем K является подпространством в $K^{n \times 1}$, а ее образ — подпространством в $K^{m \times 1}$.*

Доказательство. Пусть $x_1, x_2 \in \ker A$ и $\alpha \in K$. Тогда

$$A(x_1 + x_2) = Ax_1 + Ax_2 = 0 \Rightarrow x_1 + x_2 \in \ker A,$$

$$A(\alpha x_1) = \alpha Ax_1 = 0 \Rightarrow \alpha x_1 \in \ker A.$$

Пусть $y_1, y_2 \in \operatorname{im} A$. Тогда $y_1 = Ax_1$ и $y_2 = Ax_2$ для каких-то векторов $x_1, x_2 \in K^{n \times 1}$. Следовательно,

$$y_1 + y_2 = Ax_1 + Ax_2 = A(x_1 + x_2) \Rightarrow y_1 + y_2 \in \operatorname{im} A,$$

$$\alpha y_1 = \alpha Ax_1 = A(\alpha x_1) \Rightarrow \alpha y_1 \in \operatorname{im} A. \quad \square$$

Пусть V и W — линейные пространства над полем K . Отображение $f: V \rightarrow W$ называется *гомоморфизмом*, если оно сохраняет операции, т. е. $f(x + y) = f(x) + f(y)$ и $f(\alpha x) = \alpha f(x)$ для всех векторов $x, y \in V$ и любого числа $\alpha \in K$. В случае взаимной однозначности гомоморфизм называется *изоморфизмом*, при этом пространства V и W называются *изоморфными*.

Задача 152. Докажите, что группа целых чисел с операцией сложения не может быть аддитивной группой линейного пространства над каким-либо полем.

Задача 153. Приведите пример линейного пространства, в котором ровно 64 вектора.

Задача 154. Докажите, что линейное пространство над бесконечным полем K нельзя представить в виде объединения конечного числа нетривиальных подпространств.

4.2. Базисы и размерность

Линейная комбинация векторов называется *тривиальной*, если все ее коэффициенты являются нулевыми. Конечная система векторов называется *линейно зависимой*, если для них существует нетривиальная линейная комбинация, дающая нулевой вектор. В противном случае система векторов называется *линейно независимой*. Проверка линейной независимости векторов $v_1, \dots, v_n$ состоит в следующем: надо доказать, что равенство

$$\alpha_1 v_1 + \dots + \alpha_n v_n = 0$$

влечет за собой равенство

$$\alpha_1 = \dots = \alpha_n = 0.$$

Линейное пространство V над полем K называется *бесконечномерным*, если в нем можно найти любое сколь угодно большое число линейно независимых векторов, и *конечномерным* в противном случае. Если пространство конечномерно, то его *размерностью* называется максимальное число линейно независимых векторов в этом пространстве. Обозначение для размерности: $\dim V$.

Система векторов $v_1, \dots, v_n$ в конечномерном пространстве V над полем K называется *базисом*, если:

- $V = \langle v_1, \dots, v_n \rangle$;
- векторы $v_1, \dots, v_n$ линейно независимы.

Лемма 4.2.1. Пусть A — матрица размера $m \times n$ над полем K и $m < n$. Тогда столбцы матрицы A линейно зависимы как векторы пространства $K^{m \times 1}$.

Доказательство. Чтобы установить линейную зависимость столбцов матрицы A , достаточно найти нетривиальное (отличное

от нулевого) решение однородной системы линейных алгебраических уравнений:

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0,$$

...

$$a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0.$$

Рассуждение проведем индукцией по m . Если $m = 1$, то нетривиальное решение строится очевидным образом.

Пусть $m \geq 2$. Если первый столбец матрицы A нулевой, то можно взять

$$x_1 = 1, \quad x_2 = \dots = x_n = 0.$$

Если первый столбец ненулевой, то без ограничения общности будем считать, что $a_{11} \neq 0$. Преобразуем систему уравнений следующим образом: первое уравнение оставим как есть, а при $2 \leq i \leq m$ из i -го уравнения вычтем первое, умноженное на коэффициент a_{i1}/a_{11} . Новая система уравнений равносильна исходной системе, но имеет более простой вид:

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0,$$

$$b_{22}x_2 + \dots + b_{2n}x_n = 0,$$

...

$$b_{m2}x_2 + \dots + b_{mn}x_n = 0,$$

где

$$b_{ij} := a_{ij} - \frac{a_{i1}}{a_{11}} a_{1j}, \quad 2 \leq i \leq m, \quad 2 \leq j \leq n.$$

В однородной системе

$$b_{22}x_2 + \dots + b_{2n}x_n = 0,$$

...

$$b_{m2}x_2 + \dots + b_{mn}x_n = 0$$

число уравнений и число неизвестных равны $m - 1$ и $n - 1$. При этом

$$m < n \Rightarrow m - 1 < n - 1.$$

По индуктивному предположению данная система имеет нетривиальное решение $x_2, \dots, x_n$. Возьмем эти значения и положим

$$x_1 := -(a_{12}x_2 + \dots + a_{1n}x_n)/a_{11}.$$

Тем самым мы получим нетривиальное решение исходной системы. $\square$

Лемма 4.2.2. В произвольном линейном пространстве даны две системы векторов, $u_1, \dots, u_n$ и $v_1, \dots, v_m$. Если векторы

первой системы линейно независимы и содержатся в линейной оболочке векторов второй системы, то $n \leq m$.

Доказательство. Пусть векторы принадлежат пространству V над полем K . Согласно условию, каждый из векторов первой системы является линейной комбинацией векторов второй системы:

$$u_1 = a_{11}v_1 + \dots + a_{m1}v_m,$$

...

$$u_n = a_{1n}v_1 + \dots + a_{mn}v_m,$$

где $a_{ij} \in K$. Рассмотрим однородную систему линейных алгебраических уравнений:

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0,$$

...

$$a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0,$$

и предположим от противного, что $m < n$. Тогда, согласно предыдущей лемме, существует нетривиальное решение этой системы. Взяв это решение, находим

$$x_1u_1 + \dots + x_nu_n = 0,$$

что противоречит линейной независимости векторов $u_1, \dots, u_n$. $\square$

Теорема 4.2.1. *В конечномерном пространстве число векторов в любом его базисе равно его размерности.*

Доказательство. Пусть $n = \dim V$. По определению размерности, существует система из n линейно независимых векторов $u_1, \dots, u_n$ и для любой линейно независимой системы векторов, в частности для базиса $v_1, \dots, v_m$, имеет место неравенство $m \leq n$. По определению базиса, векторы $u_1, \dots, u_n$ принадлежат линейной оболочке векторов $v_1, \dots, v_m$ и поэтому, согласно предыдущей лемме, $n \leq m$. Следовательно, $m = n$. $\square$

Теорема 4.2.2. *В конечномерном пространстве любую линейно независимую систему можно дополнить до базиса.*

Доказательство. Возьмем линейно независимую систему $u_1, \dots, u_m$ и какой-то базис $v_1, \dots, v_n$. Рассмотрим упорядоченную последовательность векторов

$$u_1, \dots, u_m, v_1, \dots, v_n.$$

Данная система является линейно зависимой и в ней заведомо имеется вектор, который является линейной комбинацией векторов слева от него. Это может быть только один из векторов $v_1, \dots, v_n$. Рассмотрим систему без этого вектора. Если $m + n - 1 > n$, то и эта система линейно зависима и в ней есть вектор, который является линейной комбинацией векторов слева. Выбросим этот вектор и перейдем к системе из еще меньшего числа векторов. И так далее. В итоге останется ровно n векторов, среди которых непременно будут векторы $u_1, \dots, u_m$, так как ни один из них не является линейной комбинацией векторов, расположенных слева. Оставшаяся система такова, что любой из векторов $v_1, \dots, v_n$ является линейной комбинацией ее векторов. Поэтому какая-то ее подсистема будет базисом. Вследствие того что в любом базисе должно быть n векторов, эта система сама и является базисом. $\square$

Теорема 4.2.3 (ТЕОРЕМА ГРАССМАНА). Пусть V_1 и V_2 — конечномерные подпространства одного и того же линейного пространства. Тогда

$$\dim(V_1 + V_2) = \dim V_1 + \dim V_2 - \dim V_1 \cap V_2.$$

Доказательство. Пусть $u_1, \dots, u_m$ — базис $V_1 \cap V_2$. Заметим, что $V_1 \cap V_2$ является подпространством в V_1 и одновременно в V_2 , и построим выбранный в нем базис сначала до базиса V_1 , а затем до базиса V_2 :

$$u_1, \dots, u_m, v_1, \dots, v_k \text{ — базис } V_1,$$

$$u_1, \dots, u_m, w_1, \dots, w_l \text{ — базис } V_2.$$

Легко видеть, что $V_1 + V_2$ является линейной оболочкой векторов

$$u_1, \dots, u_m, v_1, \dots, v_k, w_1, \dots, w_l.$$

Остается доказать линейную независимость этих векторов. Пусть

$$\alpha_1 u_1 + \dots + \alpha_m u_m + \beta_1 v_1 + \dots + \beta_k v_k + \gamma_1 w_1 + \dots + \gamma_l w_l = 0.$$

Отсюда ясно, что

$$\gamma_1 w_1 + \dots + \gamma_l w_l \in V_1 \cap V_2 \Rightarrow \gamma_1 = \dots = \gamma_l = 0 \Rightarrow$$

$$\alpha_1 = \dots = \alpha_m = \beta_1 = \dots = \beta_k = 0.$$

Таким образом, $\dim(V_1 + V_2) = m + k + l = (m + k) + (m + l) - m$. $\square$

Суммой подпространств $V_1, \dots, V_k$ называется множество векторов v , допускающих представление в виде

$$v = v_1 + \dots + v_k, \quad v_1 \in V_1, \dots, v_k \in V_k.$$

Такое представление называется *разложением вектора по подпространствам*. Если векторы v_i в разложении по подпространствам определяются однозначно, то такая сумма подпространств $V = V_1 + \dots + V_k$ называется *прямой суммой*. Обозначение для прямой суммы:

$$V = V_1 \oplus \dots \oplus V_k.$$

Задача 155. *Всегда ли сумма ядра и образа квадратной матрицы является прямой суммой?*

Задача 156. *Дана матрица A размеров $m \times n$ над полем K . Докажите, что*

$$\dim \ker A + \dim \operatorname{im} A = n.$$

Задача 157. *Найдите размерность суммы подпространства $n \times n$ -матриц с нулевой суммой элементов в каждой строке и подпространства $n \times n$ -матриц с нулевой суммой элементов в каждом столбце.*

Задача 158. *Сколько различных подпространств имеет линейное пространство матриц размера 2×2 над полем вычетов по модулю 2?*

Задача 159. *Пусть V — вещественное линейное пространство функций, определенных на отрезке $[a, b]$. Докажите, что для линейной независимости функций $f_1(x), \dots, f_n(x)$ необходимо и достаточно существование точек $x_1, \dots, x_n \in [0, 1]$, таких что матрица*

$$A = \begin{bmatrix} f_1(x_1) & \dots & f_n(x_1) \\ \dots & & \dots \\ f_1(x_n) & \dots & f_n(x_n) \end{bmatrix}$$

является обратной.

Задача 160. *Докажите линейную независимость функций $\sin x, \sin 2x, \dots, \sin nx$ как векторов вещественного линейного пространства функций на произвольно заданном отрезке $[a, b]$.*

4.3. Конечные и алгебраические расширения полей

Пусть L — поле и $K \subseteq L$ — непустое подмножество, обладающее следующими свойствами:

- $a, b \in K \Rightarrow a + b, ab \in K$;
- $0 \neq a \in K \Rightarrow a^{-1} \in K$; $a \in K \Rightarrow -a \in K$.

В таких случаях K называется *подполем* в L , а поле L — *расширением* поля K . По аналогии с группами и подгруппами будем писать $K \leq L$. Если $K \neq L$, то подполе K называется *собственным*. Естественно, K само является полем относительно тех же операций сложения и умножения, которые действуют в поле L .

При изучении полей можно (и, как мы увидим позже, очень полезно) рассматривать более широкое поле L как линейное пространство над своим подполем K . Числа из L играют роль векторов. Сложение векторов в данном случае — это обычное сложение чисел поля L . Умножение вектора на число из поля K — это умножение числа из L на число из $K \leq L$. Принято говорить, что поле L является *конечным расширением* поля K , если пространство L над K конечномерно. Для размерности этого пространства используются обозначения $(L : K) = \dim(L : K) = \dim_K L$. Размерность пространства L над K называется также *размерностью расширения*¹⁾.

Пример 1. Поле комплексных чисел $\mathbb{C}$ является конечным расширением поля вещественных чисел $\mathbb{R}$. В данном случае $\dim(\mathbb{C} : \mathbb{R}) = 2$.

Пример 2. Поле вещественных чисел $\mathbb{R}$ как линейное пространство над полем рациональных чисел $\mathbb{Q}$ является бесконечномерным. Если бы оно имело конечную размерность n , то любое вещественное число можно было бы представить в виде

$$\alpha_1 z_1 + \dots + \alpha_n z_n, \quad \alpha_1, \dots, \alpha_n \in \mathbb{Q},$$

где $z_1, \dots, z_n$ — некоторые фиксированные вещественные числа. Из счетности множества рациональных чисел нетрудно вывести,

¹⁾ Часто встречается также термин *степень расширения*, но в этой книге мы используем его не для размерности, а для числа p в случае так называемых *радикальных* расширений — когда поле L получается из K присоединением всех корней двучлена $x^p - a$, где $a \in K$ (см. раздел 7.7).

что множество чисел такого вида должно быть счетным. Однако известно, что множество вещественных чисел не является счетным.

Теорема 4.3.1. *Предположим, что поле L является промежуточным полем между полями K и M :*

$$K \leqslant L \leqslant M.$$

Тогда расширение M над K конечно в том и только том случае, когда расширение M над L и расширение L над K оба конечны. При этом

$$\dim(M : K) = \dim(M : L) \dim(L : K).$$

Доказательство. Пусть пространство M над K конечномерно и $w_1, \dots, w_n$ — его базис. Тогда любое число $z \in M$ имеет вид

$$z = \gamma_1 w_1 + \dots + \gamma_n w_n, \quad \gamma_1, \dots, \gamma_n \in K.$$

Данное выражение можно рассматривать также как линейную комбинацию с коэффициентами из поля L . Поэтому пространство M над L также конечномерно и $m := \dim(M : L) \leqslant n$. В то же время L является подпространством в пространстве M над K , поэтому оно конечномерно и $l := \dim(L : K) \leqslant n$.

Рассмотрим два базиса:

$u_1, \dots, u_l$ — базис L над K и $v_1, \dots, v_m$ — базис M над L .

Пусть z — произвольное число из M . Оно допускает однозначно определенное разложение

$$z = \sum_{i=1}^m \beta_i v_i, \quad \text{где } \beta_i \in L, \quad 1 \leqslant i \leqslant m.$$

Каждый коэффициент $\beta_i \in L$ имеет однозначно определенное разложение

$$\beta_i = \sum_{j=1}^l a_{ij} u_j, \quad \text{где } a_{ij} \in K, \quad 1 \leqslant j \leqslant l.$$

Таким образом, любое число $z \in M$ однозначно представимо в виде линейной комбинации ml векторов $u_j v_i \in M$:

$$z = \sum_{i=1}^m \sum_{j=1}^l a_{ij} (u_j v_i), \quad a_{ij} \in K.$$

Следовательно, $n = ml$.

□

Пусть поле L является расширением поля K . Число $\alpha \in L$ называется *алгебраическим над K* , если оно является корнем ненулевого многочлена с коэффициентами из K . Ненулевой многочлен над K минимальной степени, для которого α является корнем, называется *минимальным многочленом* для числа α и *приведенным минимальным многочленом*, если старший коэффициент равен 1. Расширение $L \supseteq K$ называется *алгебраическим расширением* поля K , если любое число из L является алгебраическим над полем K . Поле K называется *алгебраически замкнутым*, если любое алгебраическое над K число принадлежит K .

Утверждение 4.3.1. *Минимальный многочлен над полем K является неприводимым над K .*

Доказательство. Если минимальный многочлен для числа α приводим над K , то α является корнем какого-то множителя в нетривиальном разложении минимального многочлена на неприводимые множители. $\square$

Утверждение 4.3.2. *Любое конечное расширение поля является алгебраическим, причем степень любого минимального многочлена не выше размерности расширения.*

Доказательство. Пусть $n = \dim(L : K)$ и $\alpha \in L$. Тогда числа

$$1, \alpha, \dots, \alpha^n$$

линейно зависимы как векторы пространства L над полем K . Поэтому для некоторых не равных одновременно нулю чисел $a_0, a_1, \dots, a_n \in K$ имеем

$$a_0 \cdot 1 + a_1 \cdot \alpha + \dots + a_n \cdot \alpha^n = 0.$$

Многочлен

$$f(x) := a_0 + a_1 x + \dots + a_n x^n$$

имеет коэффициенты из K , не является нулевым и при этом $f(\alpha) = 0$. $\square$

Задача 161. Пусть $p_1 < \dots < p_n$ — произвольная последовательность простых чисел. Докажите, что числа $\ln p_1, \dots, \ln p_n$ линейно независимы над полем рациональных чисел $\mathbb{Q}$.

Задача 162. Найдите минимальный многочлен для числа $\sqrt[7]{8}$ над полем рациональных чисел $\mathbb{Q}$.

Задача 163. Докажите, что поле комплексных чисел $\mathbb{C}$ не является алгебраическим расширением поля рациональных чисел $\mathbb{Q}$.

4.4. Присоединение корня

Пусть поле M является расширением поля K и число $\theta \in M \setminus K$ алгебраично над K . Обозначим через $K(\theta)$ минимальное расширение поля K , содержащее число θ . Минимальность означает, что θ не принадлежит никакому собственному подполю поля $K(\theta)$. Принято говорить, что поле $K(\theta)$ получается из поля K присоединением числа θ . В нашем случае θ — это корень какого-то ненулевого многочлена над K , в частности своего минимального многочлена.

Теорема 4.4.1. Пусть поле M есть расширение поля K и $f(x) \in K[x]$ — минимальный многочлен степени n для $\theta \in M \setminus K$. Тогда расширение $K \leq K(\theta)$ является конечным расширением размерности n ,

$$K(\theta) = L,$$

где

$$L := \{a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1} : a_0, a_1, \dots, a_{n-1} \in K\}.$$

Доказательство. Ясно, что $L \subseteq K(\theta)$. Чтобы доказать равенство, достаточно установить, что L является полем.

Множество L очевидно является замкнутым относительно операции сложения чисел. Установим его замкнутость относительно умножения чисел. Числа $u, v \in L$ имеют вид

$$u = \phi(\theta), \quad v = \psi(\theta), \quad \text{где } \phi(x), \psi(x) \in K[x].$$

Рассмотрим произведение многочленов $\phi(x)\psi(x)$ и поделим его с остатком на $f(x)$:

$$\phi(x)\psi(x) = q(x)f(x) + r(x),$$

где

$$\deg r(x) \leq n - 1 \quad \text{либо} \quad r(x) = 0.$$

Отсюда

$$uv = \phi(\theta)\psi(\theta) = r(\theta) \in L.$$

Пусть $u \neq 0$. Тогда $\phi(x) \neq 0$ и можно считать, что $\deg \phi(x) \leq n - 1$. Многочлены $\phi(x)$ и $f(x)$ взаимно просты, иначе минималь-

ный многочлен $f(x)$ оказался бы приводимым над K . По теореме о наибольшем общем делителе существуют многочлены над K , такие что

$$\begin{aligned}\phi(x)p(x) + f(x)q(x) &= 1, \quad \deg p(x) < \deg f(x) = n \Rightarrow \\ &\Rightarrow \phi(\theta)p(\theta) = 1 \Rightarrow 1/u \in L.\end{aligned}$$

По самому построению линейное пространство L является линейной оболочкой векторов $1, \theta, \dots, \theta^{n-1}$. Чтобы доказать линейную независимость этих векторов над полем K , рассмотрим равенство

$$a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1} = 0.$$

Если хотя бы один из коэффициентов данной линейной комбинации не равен нулю, то θ будет корнем многочлена над K , степень которого строго меньше n . Это противоречит минимальности многочлена $f(x)$. Следовательно, $a_0 = \dots = a_{n-1} = 0$. $\square$

В наших рассуждениях число θ было взято из уже существующего расширения M поля K . Рассмотрим более тонкий вопрос — о существовании поля M , в котором имеется корень θ заданного неприводимого многочлена $f(x)$ с коэффициентами из поля K .

Пусть $f(x)$ — произвольный ненулевой многочлен из кольца $K[x]$. Для любого многочлена $\phi(x) \in K[x]$ множество многочленов

$$[\phi(x)] := \{g(x) \in K[x] : g(x) - \phi(x) \div f(x)\}$$

называется *вычетом по модулю $f(x)$* . Эти вычеты можно складывать и умножать:

$$[\phi(x)] + [\psi(x)] := [\phi(x) + \psi(x)], \quad [\phi(x)][\psi(x)] = [\phi(x)\psi(x)].$$

Несложно проверяется, что эти операции сложения и умножения вычетов в кольце многочленов $K[x]$ определены корректно и превращают множество вычетов по модулю $f(x)$ в ассоциативное коммутативное кольцо с единицей, в котором вычеты, порожденные многочленами-константами, естественным образом отождествляются с числами из K .

Лемма 4.4.1. *Кольцо вычетов по неприводимому над полем K многочлену $f(x)$ является полем, содержащим поле K .*

Доказательство. Пусть $[\phi(x)] \neq 0$. Тогда многочлен $\phi(x)$ взаимно прост с многочленом $f(x)$ и по теореме о наибольшем

общем делителе существуют многочлены $p(x)$ и $q(x)$ из $K[x]$, такие что

$$\phi(x)p(x) + f(x)q(x) = 1 \Rightarrow [\phi(x)p(x)] = [\phi(x)][p(x)] = [1].$$

Таким образом, любой ненулевой вычет является обратимым в кольце вычетов. $\square$

Теорема 4.4.2. Для любого поля K и любого неприводимого над K многочлена $f(x)$ существует расширение M поля K и число $\theta \in M$, такое что $f(\theta) = 0$.

Доказательство. В качестве M рассмотрим поле вычетов по модулю

$$f(x) = a_0 + a_1x + \dots + a_nx^n, \quad a_0, a_1, \dots, a_n \in K.$$

Этот же многочлен можно рассматривать как многочлен над M :

$$f(x) = [a_0] + [a_1]x + \dots + [a_n]x^n.$$

Положим $\theta := [x]$. Тогда

$$\begin{aligned} f(\theta) &= f([x]) = [a_0] + [a_1][x] + \dots + [a_n][x]^n = \\ &= [a_0 + a_1x + \dots + a_nx^n] = [f(x)] = 0. \end{aligned}$$

Таким образом, поле M является искомым. $\square$

Задача 164. Докажите, что $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$.

Задача 165. Пусть θ — корень многочлена $f(x) = x^4 - 10x + 1 \in \mathbb{Q}[x]$. Найдите размерность расширения $\mathbb{Q} \leq \mathbb{Q}(\theta)$.

Задача 166. Пусть числа a и b являются алгебраическими над полем K . Докажите, что числа $a + b$ и ab также будут алгебраическими над K .

Задача 167. Приведите пример алгебраического расширения, которое не является конечным.

Задача 168. Пусть $p_1 < \dots < p_n$ — последовательность простых чисел. Докажите, что числа $\sqrt{p_1}, \dots, \sqrt{p_n}$ линейно независимы над полем рациональных чисел.

Задача 169. Бесконечное поле K вложено в поле M , и число промежуточных полей между K и M конечно. Докажите, что $M = K(\theta)$ для какого-то числа $\theta \in M$.

4.5. Поле разложения

Пусть $f(x)$ — многочлен степени $n \geq 1$ над полем K . Его *полем разложения* над K называется расширение M поля K , которое обладает следующими свойствами:

- поле M содержит все n корней многочлена $f(x)$, т.е. над M имеет место разложение

$$f(x) = a(x - \theta_1) \dots (x - \theta_n), \quad \theta_1, \dots, \theta_n \in M, \quad a \in K;$$

- если $K \leq L \leq M$ и поле L содержит все корни многочлена $f(x)$, то $L = M$.

Теорема 4.5.1. *Любой отличный от константы многочлен над полем K обладает полем разложения над K .*

Доказательство. Рассмотрим разложение данного многочлена на неприводимые множители над K и построим поле $K_1 \geq K$ путем присоединения к K корня какого-либо из неприводимых множителей. Над K_1 наш многочлен распадается уже на большее число неприводимых множителей. Присоединим какой-либо из их корней. И так далее. В итоге получится поле M' , содержащее K и все корни заданного многочлена. Пусть множество M является пересечением всех подполей поля M' , которые содержат K и все корни нашего многочлена. Несложно проверяется, что пересечение любого числа подполей есть поле. Поле M и будет искомым полем разложения заданного многочлена. $\square$

Наша ближайшая цель — доказать, что поле разложения заданного многочлена определяется по существу однозначно. Несмотря на то что при его построении могут получаться формально разные поля, все они будут неразличимы с точки зрения свойств их операций. Способ отождествления формально разных полей связан с понятием изоморфизма полей.

Пусть K и $\hat{K}$ — два поля. Отображение $\phi: K \rightarrow \hat{K}$ называется *изоморфизмом*, если оно является взаимно-однозначным и сохраняет операции в том смысле, что

$$\phi(a + b) = \phi(a) + \phi(b), \quad \phi(ab) = \phi(a)\phi(b) \quad \forall a, b \in K.$$

В таких случаях поле K называется *изоморфным* полю $\hat{K}$. Обозначение: $K \cong \hat{K}$.

На множестве всех полей мы получаем бинарное отношение эквивалентности, которое разбивает все множество полей на классы изоморфных между собой полей.

Изоморфизм $\phi: K \rightarrow \hat{K}$ естественным образом порождает взаимно-однозначное отображение кольца многочленов $K[x]$ на кольцо $\hat{K}[x]$:

$$f(x) = a_0 + a_1x + \dots + a_nx^n \rightarrow \hat{f}(x) = \hat{a}_0 + \hat{a}_1x + \dots + \hat{a}_nx^n,$$

где

$$\hat{a}_i := \phi(a_i), \quad 0 \leq i \leq n.$$

Многочлены $f(x)$ и $\hat{f}(x)$ будем называть *соответствующими*.

Если есть более широкое поле $L \supseteq K$, то ϕ можно попытаться доопределить на L так, чтобы получился какой-то изоморфизм поля L на какое-то поле $\hat{L} \supseteq \hat{K}$. В таких случаях говорят, что изоморфизм поля K *продолжается* до изоморфизма поля L .

Лемма 4.5.1. *Любой изоморфизм полей $\phi: K \rightarrow \hat{K}$ продолжается до изоморфизма полей $\psi: K(\theta) \rightarrow \hat{K}(\hat{\theta})$, где θ и $\hat{\theta}$ — заданные корни соответствующих неприводимых многочленов $f(x) \in K[x]$ и $\hat{f}(x) \in \hat{K}[x]$.*

Доказательство. Рассмотрим пару соответствующих многочленов

$$\begin{aligned} f(x) &= a_0 + a_1x + \dots + a_nx^n \in K[x], \\ \hat{f}(x) &= \hat{a}_0 + \hat{a}_1x + \dots + \hat{a}_nx^n \in \hat{K}[x]. \end{aligned}$$

Легко видеть, что они имеют одну и ту же степень $n = \deg f(x) = \deg \hat{f}(x) \geq 1$ и неприводимость $f(x)$ имеет место в том и только том случае, когда неприводим $\hat{f}(x)$.

Можно считать, что элементы θ и $\hat{\theta}$ принадлежат каким-то полям разложения соответствующих неприводимых многочленов $f(x)$ и $\hat{f}(x)$. Мы хотим доопределить ϕ на $K(\theta)$ так, чтобы это был изоморфизм. Если это возможно, то число $\phi(\theta)$ должно быть корнем многочлена $\hat{f}(\theta)$. В самом деле, пусть

$$f(x) = a_0 + a_1x + \dots + a_nx^n \leftrightarrow \hat{f}(x) = \hat{a}_0 + \hat{a}_1x + \dots + \hat{a}_nx^n.$$

Тогда в силу сохранения операций

$$a_0 + a_1\theta + \dots + a_n\theta^n = 0 \Rightarrow \hat{a}_0 + \hat{a}_1\phi(\theta) + \dots + \hat{a}_n(\phi(\theta))^n = 0.$$

Мы уже знаем, как устроены поля, возникающие при присоединении корня неприводимого многочлена:

$$\begin{aligned} K(\theta) &= \{c_0 + c_1\theta + \dots + c_{n-1}\theta^{n-1} : c_0, \dots, c_{n-1} \in K\}, \\ \hat{K}(\hat{\theta}) &= \{\hat{c}_0 + \hat{c}_1\hat{\theta} + \dots + \hat{c}_{n-1}\hat{\theta}^{n-1} : \hat{c}_0, \dots, \hat{c}_{n-1} \in \hat{K}\}. \end{aligned}$$

Поэтому искомое отображение $\psi: K(\theta) \rightarrow \widehat{K}(\widehat{\theta})$ кажется вполне естественным определить следующим образом:

$$\begin{aligned}\psi(c_0 + c_1\theta + \dots + c_{n-1}\theta^{n-1}) &:= \widehat{c}_0 + \widehat{c}_1\widehat{\theta} + \dots + \widehat{c}_{n-1}\widehat{\theta}^{n-1}, \\ \widehat{c}_i &:= \phi(c_i), \quad 0 \leq i \leq n-1.\end{aligned}$$

Ясно, что $\psi(a) = \phi(a) \quad \forall a \in K$, т.е. ψ совпадает с ϕ на K , но имеет более широкую область определения.

Докажем, что ψ является изоморфизмом полей $K(\theta)$ и $\widehat{K}(\widehat{\theta})$. Взаимная однозначность очевидна. Сохранение сложения тоже очевидно. Установим сохранение операции умножения. Пусть

$$\begin{aligned}u &= c_0 + c_1\theta + \dots + c_{n-1}\theta^{n-1} = c(\theta), \\ c(x) &:= c_0 + c_1x + \dots + c_{n-1}x^{n-1}, \\ v &= d_0 + d_1\theta + \dots + d_{n-1}\theta^{n-1} = d(\theta), \\ d(x) &:= d_0 + d_1x + \dots + d_{n-1}x^{n-1}.\end{aligned}$$

Тогда

$$\psi(u) = \widehat{c}(\widehat{\theta}), \quad \psi(v) = \widehat{d}(\widehat{\theta}).$$

Поделим $c(x)d(x)$ с остатком на $f(x)$:

$$c(x)d(x) = f(x)q(x) + r(x) \leftrightarrow \widehat{c}(x)\widehat{d}(x) = \widehat{f}(x)\widehat{q}(x) + \widehat{r}(x).$$

Отсюда

$$\psi(uv) = \psi(r(\theta)) = \widehat{r}(\widehat{\theta}) = \psi(u)\psi(v). \quad \square$$

Теорема 4.5.2. *Любой изоморфизм полей продолжается до изоморфизма заданных полей разложения соответствующих многочленов.*

Доказательство. Рассмотрим изоморфизм $\phi: K \rightarrow \widehat{K}$ и пару соответствующих многочленов $f(x)$ и $\widehat{f}(x)$. Разложение $f(x)$ на неприводимые множители порождает разложение $\widehat{f}(x)$ на соответствующие неприводимые множители:

$$\begin{aligned}f(x) = f_1(x) \dots f_s(x) &\leftrightarrow \widehat{f}(x) = \widehat{f}_1(x) \dots \widehat{f}_s(x), \\ f_i(x) &\leftrightarrow \widehat{f}_i(x), \quad 1 \leq i \leq s.\end{aligned}$$

Пусть $\Pi \geq K$ и $\widehat{\Pi} \geq \widehat{K}$ — заданные поля разложения для $f(x)$ и $\widehat{f}(x)$.

Обозначим через m число корней многочлена $f(x)$, не принадлежащих полю K , и проведем индукцию по m . Случай $m = 0$ тривиален, так как $\Pi = K$ и $\widehat{\Pi} = \widehat{K}$. Пусть $m \geq 1$ и $\theta \in \Pi \setminus K$ —

корень, скажем, множителя $f_1(x)$. Тогда $\deg f_1(x) \geq 2$. Согласно доказанной выше лемме, изоморфизм ϕ продолжается до изоморфизма ψ полей $K(\theta)$ и $\hat{K}(\theta)$. По индуктивному предположению, ψ продолжается до изоморфизма полей разложения многочленов $f(x)$ и $\hat{f}(x)$, так как число корней $f(x)$ вне поля $K(\theta)$ строго меньше m . $\square$

Следствие 4.5.1. Любые поля разложения одного и того же многочлена над одним и тем же полем изоморфны.

Доказательство. Пусть Π и $\hat{\Pi}$ — два поля разложения одного и того же многочлена. Согласно доказанной теореме, тождественное отображение $\phi: K \rightarrow \hat{K} = K$ продолжается до изоморфизма полей Π и $\hat{\Pi}$. $\square$

Задача 170. Докажите, что размерность поля разложения многочлена степени n не выше $n!$.

Задача 171. Найдите размерность поля разложения многочлена $f(x) = x^4 + 1$ над полем рациональных чисел $\mathbb{Q}$.

Задача 172. Найдите размерность поля разложения многочлена $f(x) = x^4 + 1$ над полем вычетов по модулю p для $p = 2, 3, 5$.

4.6. Производная многочлена и кратные корни

Пусть M — поле разложения многочлена $f(x)$ над полем K . Корень $a \in M$ многочлена $f(x)$ над полем K называется корнем кратности s , если

$$f(x) = (x - a)^s g(x), \quad g(x) \in M[x], \quad g(a) \neq 0,$$

s — неотрицательное целое число.

Если $s = 1$, то корень называется *простым*. Если $s \geq 2$, то корень называется *кратным*. Многочлен называется *сепарабельным*, если в его разложении на неприводимые множители каждый множитель имеет только простые корни в своем поле разложения. Элемент расширения поля K называется *сепарабельным*, если все корни его минимального многочлена над K являются простыми.

Чтобы узнать, имеет ли многочлен кратные корни, совсем не обязательно знать корни! Этот вопрос проясняется с помощью производной данного многочлена.

В алгебре под *производной* многочлена

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

понимается многочлен вида

$$f'(x) := a_1 + 2a_2x + \dots + na_nx^{n-1}.$$

Утверждение 4.6.1. Для двух многочленов, $f(x)$ и $g(x)$, справедливы соотношения

$$\begin{aligned}(f(x) + g(x))' &= f'(x) + g'(x), \\ (f(x)g(x))' &= f'(x)g(x) + f(x)g'(x), \\ (f(g(x)))' &= f'(g(x))g'(x).\end{aligned}$$

Теорема 4.6.1. Многочлен $f(x)$ над полем K имеет только простые корни в своем поле разложения в том и только том случае, когда $f(x)$ и его производная $f'(x)$ взаимно просты.

Доказательство. Пусть

$$f(x) = (x - a)^s g(x), \quad \text{где } g(a) \neq 0.$$

Если $s \geq 2$, то

$$f'(x) = s(x - a)^{s-1}g(x) + (x - a)^s g'(x) \Rightarrow f'(a) = 0.$$

Таким образом, в случае кратного корня a многочлены $f(x)$ и $f'(x)$ с коэффициентами из поля K имеют общий корень в некотором расширении поля K и поэтому обладают нетривиальным общим делителем над исходным полем K .

Если $s = 1$, то $f'(x) = g(x) + (x - a)g'(x) \Rightarrow f'(a) \neq 0$. Если все корни $f(x)$ простые, то ни один из них не является корнем $f'(x)$. Для этого необходима взаимная простота многочленов $f(x)$ и $f'(x)$. $\square$

Задача 173. Докажите, что многочлен

$$f(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \dots + \frac{x^n}{n!}$$

не имеет кратных корней.

Задача 174. Является ли многочлен $f(x) = x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$ сепарабельным?

Задача 175. Пусть $L = \mathbb{Z}_2(y)$ — поле рациональных функций от y над полем $\mathbb{Z}_2$. Докажите, что многочлен $f(x) = x^2 - y$ неприводим над L , но имеет кратный корень в своем поле разложения.

Задача 176. Докажите, что дискриминант приведенного многочлена $f(x)$ с точностью до знака равен результату многочленов $f(x)$ и $f'(x)$.¹⁾

4.7. Неприводимость круговых многочленов

Многочлен $x^n - 1 \in \mathbb{Q}[x]$ не имеет кратных корней, так как у него нет общих корней с производной $(x^n - 1)' = nx^{n-1}$. Взяв простое число p и перейдя к вычетам, мы можем считать, что $x^n - 1 \in \mathbb{Z}_p[x]$. Если $p \mid n$, то $(x^n - 1)' = 0$ по модулю p , поэтому кратные корни должны быть. Если же $p \nmid n$, то единственным корнем уравнения $nx^{n-1} = 0$ является $x = 0$. В данном случае кратных корней нет.

Этот факт используется в разных ситуациях, в том числе и для доказательства неприводимости круговых многочленов $\Phi_n(x) \in \mathbb{Z}[x]$. Напомним, что $\Phi_n(x)$ — это многочлен со старшим коэффициентом 1, корни которого суть все первообразные корни степени n из единицы. В разделе 3.7 доказано, что коэффициенты этих многочленов являются целыми.

Теорема 4.7.1. *Круговые многочлены $\Phi_n(x)$ неприводимы над кольцом целых чисел.*

Доказательство. Пусть ε — произвольный первообразный корень степени n из единицы и простое число p не делит n . Тогда ε^p — еще один первообразный корень. Обозначим через $f(x)$ и $g(x)$ приведенные минимальные многочлены для ε и ε^p над полем $\mathbb{Q}$. Каждый из них является делителем многочлена $x^n - 1 \in \mathbb{Z}[x]$, и с помощью леммы Гаусса нетрудно показать, что $f(x), g(x) \in \mathbb{Z}[x]$. Многочлены $f(x)$ и $g(x)$ неприводимы над полем $\mathbb{Q}$ (что, как мы знаем, равносильно неприводимости над кольцом $\mathbb{Z}$).

Докажем, что $f(x) = g(x)$. Если это не так, то $f(x)$ и $g(x)$ взаимно просты и $g(x^p)$ делится на $f(x)$. Поэтому имеют место разложения

$$\begin{aligned} x^n - 1 &= f(x)g(x)h(x), & g(x^p) &= f(x)q(x), \\ h(x), q(x) &\in \mathbb{Z}[x]. \end{aligned}$$

При переходе к вычетам по простому модулю p они очевидно сохраняются как равенства в кольце $\mathbb{Z}_p[x]$. В этом кольце

¹⁾ Определение результата и дискриминанта см. в разделах 3.10 и 3.11.

$g(x^p) = (g(x))^p$ — прямое следствие тождества $(a + b)^p = a^p + b^p$, где a и b — произвольные элементы поля $\mathbb{Z}_p$. Из факториальности кольца $\mathbb{Z}_p[x]$ вытекает, что любой неприводимый множитель многочлена $f(x)$ делит $g(x)$. Следовательно, многочлен $x^n - 1 \in \mathbb{Z}_p[x]$ обладает кратным корнем, что невозможно при $p \nmid n$. Таким образом, $f(x) = g(x)$.

Возьмем произвольное целое число $1 \leq k \leq n - 1$, взаимно простое с n , и рассмотрим разложение на простые множители $k = p_1^{s_1} \dots p_t^{s_t}$. Ясно, что $p_1, \dots, p_t \nmid n$. Поэтому каждое число в последовательности

$$\varepsilon, \varepsilon^{p_1}, \varepsilon^{p_1^2}, \dots, \varepsilon^{p_1^{s_1}}, \varepsilon^{p_1^{s_1} p_2}, \varepsilon^{p_1^{s_1} p_2^2}, \dots, \varepsilon^{p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}} = \varepsilon^k$$

является корнем $f(x)$. Значит, ε^k является корнем $f(x)$ для всех $1 \leq k \leq n - 1$, взаимно простых с n . Следовательно, $f(x) = \Phi_n(x)$. $\square$

Задача 177. *Покажите, что круговые многочлены $\Phi_n(x)$ могут быть приводимы как многочлены над полем вычетов по простому модулю p .*

4.8. Малая теорема Веддерберна

Эта теорема была сформулирована, когда мы познакомились с полями вычетов (теорема 3.2.3). Она утверждает, что *конечное ассоциативное кольцо с единицей и без делителей нуля является полем*.

Доказательство. Пусть речь идет о кольце K . Обозначим через Z множество всех элементов $a \in K$ таких, что $ab = ba \forall b \in K$. Легко проверяется, что Z — поле. Число его элементов обозначим через q . Очевидно, что K можно рассматривать как конечномерное линейное пространство над полем Z . Поэтому число элементов кольца K имеет вид q^n , где n — натуральное число. Наша задача — доказать, что $n = 1$.

Из условий теоремы вытекает, что множество K^* ненулевых элементов кольца K является мультипликативной группой и может быть представлено как объединение непересекающихся классов сопряженности. Число элементов, сопряженных с элементом $a \in K^*$, равно числу смежных классов группы K^* по подгруппе $C(a) = \{b \in K^* : ab = ba\}$. Отдельные классы сопряженности, состоящие из одного элемента, образуют ненулевые элементы поля Z . Пусть $a_1, \dots, a_t$ — элементы из различных

классов сопряженности, содержащих более одного элемента. Тогда

$$q^n - 1 = q - 1 + \sum_{i=1}^t \frac{q^n - 1}{|C(a_i)|}.$$

По теореме Лагранжа порядок подгруппы делит порядок группы $\Rightarrow q^n - 1 \vdots |C(a_i)|$. Если к $C(a_i)$ добавить нулевой элемент, то получится кольцо, которое можно рассматривать как конечномерное линейное пространство над полем Z . Следовательно, $|C(a_i)| = q^{n_i} - 1$ для какого-то натурального числа n_i . Легко доказывается, что

$$q^n - 1 \vdots q^{n_i} - 1 \Leftrightarrow n \vdots n_i.$$

Используя круговые многочлены, находим

$$q^n - 1 = \prod_{d|n} \Phi_d(q), \quad q^{n_i} - 1 = \prod_{d|n_i} \Phi_d(q), \quad n \vdots n_i \Rightarrow \frac{q^n - 1}{q^{n_i} - 1} \vdots \Phi_n(q).$$

В итоге $q - 1 \vdots \Phi_n(q)$. Но при $n \geq 2$ это невозможно — в силу того что для каждого первообразного корня ε^k выполняется неравенство $|q - \varepsilon^k| > q - 1 \Rightarrow |\Phi_n(q)| > q - 1$. Следовательно, $n = 1$. $\square$

Задача 178. *Может ли конечное поле быть подполем бесконечного поля?*

4.9. Конечные поля

В поле K рассмотрим n -кратные единицы $n \cdot 1 = 1 + \dots + 1$ (n раз) и предположим, что $n \cdot 1 = 0$ для какого-то натурального числа n . Наименьшее n с таким свойством называется *характеристикой* поля K . Если $n \cdot 1 \neq 0$ при всех натуральных n , то считается, что поле имеет характеристику 0. Обозначение для характеристики: $\text{char } K$.

Утверждение 4.9.1. *Характеристика поля либо равна нулю, либо является простым числом.*

Доказательство. Если ненулевая характеристика поля является составным числом $n = kl$, то $0 = n \cdot 1 = (k \cdot 1)(l \cdot 1)$, т. е. имеются делители нуля. В поле их не бывает, поэтому n должно быть простым числом. $\square$

Поле нулевой характеристики обязательно имеет бесконечно много элементов. Поэтому любое конечное поле обладает положительной характеристикой.

Утверждение 4.9.2. *В конечном поле характеристики p число элементов имеет вид p^s , где s — натуральное число.*

Доказательство. Обозначим данное конечное поле через L . Несложно убедиться в том, что множество $K := \{k \cdot 1 : k = 0, 1, \dots, p-1\}$ является подполем, изоморфным полю $\mathbb{Z}_p$. При отождествлении изоморфных полей можно считать, что L является расширением поля $\mathbb{Z}_p$. Очевидно, что это расширение конечно. Пусть s — размерность поля L как линейного пространства над полем $\mathbb{Z}_p$. Тогда любой элемент $a \in L$ имеет однозначное разложение по базису $a_1, \dots, a_s \in L$:

$$a = \alpha_1 a_1 + \dots + \alpha_s a_s, \quad \alpha_1, \dots, \alpha_s \in \mathbb{Z}_p.$$

Отсюда вытекает, что число элементов в поле L равно p^s . $\square$

Мы уже знаем, что для любого простого p имеется конечное поле $\mathbb{Z}_p$, в котором ровно p элементов. Для любого ли натурального числа s существует поле, в котором ровно p^s элементов?

Теорема 4.9.1. *Для любого простого числа p и натурального числа s существует поле, в котором ровно $n = p^s$ элементов. Все поля из n элементов изоморфны.*

Доказательство. Если известно, что L — поле с числом элементов $n = p^s$, то его мультипликативная группа имеет порядок $n - 1$. Поэтому для любого $0 \neq a \in L$ имеет место равенство $a^{n-1} = 1$ и, следовательно, все элементы поля L являются корнями многочлена

$$f(x) := x^n - x \in \mathbb{Z}_p.$$

Обозначим через M поле разложения данного многочлена и теперь *определим* L как множество всех элементов $a \in M$, для которых $a^n = a$. Пусть $a, b \in L$. Тогда

$$\begin{aligned} (a+b)^p &= a^p + b^p \Rightarrow (a+b)^{p^2} = (a^p + b^p)^p = a^{p^2} + b^{p^2} \Rightarrow \dots \\ &\dots \Rightarrow (a+b)^n = a^n + b^n = a + b, \end{aligned}$$

$$(ab)^n = a^n b^n = ab, \quad (a^{-1})^n = (a^n)^{-1} = a^{-1}.$$

Таким образом, множество всех корней многочлена $f(x) = x^n - x$ является полем и поэтому $M = L$.

Многочлен n -й степени не может иметь больше чем n корней. Поэтому остается понять, почему у многочлена $f(x) = x^n - x$ не может быть кратных корней. Для этого вычислим производную многочлена $f(x)$ по модулю p :

$$f'(x) = nx^{n-1} - 1 = -1 \pmod{p}.$$

Производная является ненулевой константой, поэтому $f(x)$ и $f'(x)$ взаимно просты. Следовательно, все корни многочлена $f(x)$ простые, т.е. он имеет n различных корней. Это означает, что в поле M ровно n элементов.

Из нашего рассуждения ясно, что искомое поле непременно является полем разложения многочлена $f(x) = x^n - x \in \mathbb{Z}_p$. Ранее уже было доказано, что все поля разложения одного и того же многочлена над одним и тем же полем изоморфны. $\square$

Задача 179. Пусть K — поле положительной характеристики p . Докажите, что неприводимый многочлен $f(x)$ над K имеет кратный корень в том и только том случае, когда он имеет вид $f(x) = g(x^p)$ для какого-то многочлена $g(x) \in K[x]$.

Задача 180. Может ли многочлен, неприводимый над конечным полем, иметь кратные корни?

Задача 181. Существует ли линейное пространство, в котором ровно 10 векторов?

4.10. Мультипликативная группа конечного поля

Теорема 4.10.1. Для любого конечного поля его мультипликативная группа является циклической.

Сначала мы установим простую лемму об абелевых группах.

Лемма 4.10.1. Пусть a и b — элементы порядка m и n в некоторой абелевой группе. Если m и n взаимно просты, то порядок элемента ab равен mn .

Доказательство. Пусть e — единичный элемент и k — порядок элемента ab . Тогда $(ab)^k = e \Rightarrow a^{kn} = e, b^{km} = e \Rightarrow kn : m, km : n$. Вследствие взаимной простоты m и n находим $k : m, k : n \Rightarrow k : mn$. Таким образом, $(ab)^{mn} = e$ и $(ab)^k \neq e$ при $1 \leq k < mn$. $\square$

Доказательство теоремы. Пусть дано конечное поле с числом элементов $n = p^s$, где p — простое число, s — натуральное

число, G — множество ненулевых элементов поля, образующих мультипликативную группу. Рассмотрим разложение числа $m := |G| = n - 1$ на простые множители: $m = p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}$. Все корни уравнения $x^{m/p_i} = 1$ принадлежат G , и их число строго меньше m . Поэтому существует элемент $a_i \in G$ такой, что $a_i^{m/p_i} \neq 1$. Положим $b_i := a_i^{m/p_i^{s_i}}$. Тогда $b_i^{p_i^{s_i}} = 1$, но $b_i^{p_i^{s_i-1}} \neq 1$. Отсюда следует, что порядок элемента b_i равен $p_i^{s_i}$. Согласно предыдущей лемме, порядок элемента $\theta := b_1 \dots b_t$ равен $p_1^{s_1} \dots p_t^{s_t} = m$. Тем самым цикличность группы G доказана¹⁾. $\square$

Следствие 4.10.1. *Конечное поле M с числом элементов p^s , где p — простое число и s — натуральное число, получается присоединением к полю $\mathbb{Z}_p$ одного единственного элемента θ , т.е.*

$$M = \mathbb{Z}_p(\theta).$$

При этом θ является корнем неприводимого над $\mathbb{Z}_p$ многочлена степени s .

Чтобы получить поле с числом элементов p^s , достаточно найти неприводимый над $\mathbb{Z}_p$ многочлен $\phi(x)$ степени s . Искомое поле будет полем вычетов по модулю $\phi(x)$.

Задача 182. Найдите неприводимый над $\mathbb{Z}_2$ многочлен степени 3 и постройте таблицу умножения для поля из 8 элементов.

Задача 183. Докажите, что любой неприводимый над полем $\mathbb{Z}_p$ многочлен степени s является делителем многочлена $x^{p^s} - x$.

Задача 184. Поле K вложено в конечное поле M . Докажите, что $M = K(\theta)$ для некоторого $\theta \in M$.

Задача 185. Число элементов поля M равно p^s , где p — простое число, s — натуральное число. Докажите, что число разных изоморфизмов поля M на M равно s и эти изоморфизмы образуют циклическую группу относительно композиции изоморфизмов.

¹⁾ Другое доказательство: по теореме 2.14.1 мультипликативная группа поля представляет собой прямое произведение циклических подгрупп, причем их порядки суть делители максимального из них. Если максимальный порядок равен $h < n - 1$, то уравнение $x^h - 1 = 0$ должно иметь более h корней. Поэтому $h = n - 1$.

4.11. Расширения полей в геометрии

Расширения полей играют ключевую роль при изучении геометрических задач на построение с помощью циркуля и линейки. Поставим задачу таким образом: на плоскости задан отрезок длины 1, требуется построить отрезок длины a .

С помощью циркуля и линейки легко строятся прямые, образующие декартову систему координат, и любые точки с рациональными координатами. Если точка берется случайно, то будем считать, что она имеет рациональные координаты. Это очень разумное соглашение, так как при случайном выборе такая точка может возникнуть, а метод построения должен работать при любом случайном выборе. Таким образом, на начальном этапе можно считать, что нам доступны любые точки с координатами из поля $\mathbb{Q}_0 := \mathbb{Q}$.

Будем считать, что алгоритм построения представляет собой последовательность этапов, причем на k -м этапе доступны точки с координатами из поля $\mathbb{Q}_k$, а на $k + 1$ -м этапе — точки с координатами из поля $\mathbb{Q}_{k+1} \supseteq \mathbb{Q}_k$. Новые точки возникают следующим образом:

- при пересечении двух прямых, проведенных через пары точек с координатами из поля $\mathbb{Q}_k$;
- при пересечении прямой, проведенной через пару точек с координатами из поля $\mathbb{Q}_k$, и окружности, для которой центр и какая-то из ее точек имеют координаты из поля $\mathbb{Q}_k$;
- при пересечении двух окружностей вышеуказанного вида;
- при случайном выборе точки на плоскости или на уже имеющихся прямых или окружностях.

Каждое из вышеперечисленных действий дает точки с координатами, принадлежащими тому же самому полю $\mathbb{Q}_k$ либо его расширению вида $\mathbb{Q}_k(\sqrt{D_k})$, где $D_k \in \mathbb{Q}_k$. Исключив совпадающие поля, мы получаем цепочку расширений полей

$$\mathbb{Q}_0 < \mathbb{Q}_1 < \dots < \mathbb{Q}_s,$$

где

$$\mathbb{Q}_k = \mathbb{Q}_{k-1}(\sqrt{D_k}), \quad D_k \in \mathbb{Q}_{k-1}, \quad 1 \leq k \leq s.$$

Построение заканчивается при условии $a \in \mathbb{Q}_s$.

Утверждение 4.11.1. $\dim(\mathbb{Q}_s : \mathbb{Q}_0) = 2^s$.

Доказательство. Достаточно заметить, что

$$\dim(\mathbb{Q}_k : \mathbb{Q}_{k-1}) = 2, \quad 1 \leq k \leq s.$$

□

Рассмотрим, например, задачу о построении правильного p -угольника в случае простого числа сторон p . Требуется построить отрезок длины $a = \cos(2\pi/p)$. Пусть

$$\varepsilon = \cos(2\pi/p) + i \sin(2\pi/p) \Rightarrow a = (\varepsilon + \varepsilon^{-1})/2.$$

Отсюда ясно, что ε является корнем многочлена

$$x^2 - 2ax + 1 \in \mathbb{Q}_s[x], \quad \varepsilon \in \mathbb{Q}_{s+1} := \mathbb{Q}_s(\varepsilon).$$

Поле $\mathbb{Q}(\varepsilon)$ является промежуточным полем между $\mathbb{Q}$ и $\mathbb{Q}_{s+1}$:

$$\mathbb{Q} < \mathbb{Q}(\varepsilon) \leq \mathbb{Q}_{s+1}.$$

По теореме о размерностях расширений, число $n := \dim(\mathbb{Q}(\varepsilon) : \mathbb{Q})$ должно быть делителем числа $\dim(\mathbb{Q}_{s+1} : \mathbb{Q}) = 2^{s+1}$. В случае простого p минимальным многочленом над $\mathbb{Q}$ для ε оказывается многочлен $f(x) = 1 + x + \dots + x^{p-1}$. Минимальность вытекает из неприводимости данного многочлена над $\mathbb{Q}$. Вопрос можно свести к вопросу о неприводимости многочлена $f(x+1) = ((x+1)^p - 1)/x$, который решается, например, применением признака Эйзенштейна.

Таким образом, $n = p - 1$. Значит, если построение правильного p -угольника при простом p возможно, то $p = 2^d + 1$ для некоторого натурального числа d .

Задача 186. Докажите неразрешимость индийской задачи об удвоении куба, в которой с помощью циркуля и линейки требуется построить отрезок длины $\sqrt[3]{2}$.

Задача 187. Докажите, что с помощью циркуля и линейки произвольный угол невозможно разделить на три равные части.

Задача 188. Докажите, что с помощью циркуля и линейки построение треугольника по трем биссектрисам невозможно.

4.12. Основная теорема алгебры

Теорема 4.12.1 (ОСНОВНАЯ ТЕОРЕМА АЛГЕБРЫ). Любой многочлен положительной степени с комплексными коэффициентами имеет комплексный корень.

Эта теорема играет очень важную роль в алгебре, хотя «основной» называется исключительно в силу традиции. В некоторых частных случаях существование корня почти очевидно. Например, совсем просто доказывается, что любой вещественный

многочлен $f(x)$ нечетной степени имеет вещественный корень: если старший коэффициент положителен, то $f(x) \rightarrow +\infty$ при $x \rightarrow +\infty$ и $f(x) \rightarrow -\infty$ при $x \rightarrow -\infty \Rightarrow$ непрерывная функция $f(x)$ от вещественной переменной x принимает значения разных знаков на концах некоторого отрезка и поэтому принимает значение нуль в какой-то точке этого отрезка. Заметим, что в любом доказательстве так или иначе используется свойство непрерывности функции $f(x)$.

Первое полное доказательство получено Гауссом. На сегодняшний день имеется уже не менее десятка различных доказательств. Мы рассмотрим одно из них, основанное на лемме Даламбера, — по той причине, что при абсолютно строгом изложении оно требует минимального объема знаний.

Лемма 4.12.1 (ЛЕММА ДАЛАМБЕРА). Пусть $f(x)$ — отличный от константы многочлен с комплексными коэффициентами и $f(z_0) \neq 0$ для комплексного числа z_0 . Тогда существует комплексное число z , такое что $|f(z)| < |f(z_0)|$.

Доказательство. Запишем $x = z_0 + h$ и рассмотрим $f(x)$ как многочлен от h :

$$f(z_0 + h) = f(z_0) + b_k h^k + b_{k+1} h^{k+1} + \dots + b_n h^n,$$

где

$$b_k \neq 0, \quad n = \deg f(x).$$

Будем искать z в виде $z = z_0 + h$, где $h = th_0$ при $t > 0$ и $h_0^k = -f(z_0)/b_k$. Пусть

$$c := (|b_{k+1} h_0^{k+1}| + \dots + |b_n h_0^n|)/|f(z_0)|.$$

Тогда при $0 < t < \min(1, 1/c)$ получаем

$$\begin{aligned} |f(z_0 + th_0)| &\leq |f(z_0)|(1 - t^k + ct^{k+1}) \leq \\ &\leq |f(z_0)|(1 - t^k(1 - ct)) < |f(z_0)|. \quad \square \end{aligned}$$

Лемма 4.12.2 (О РОСТЕ МОДУЛЯ МНОГОЧЛЕНА). Пусть $f(x)$ — многочлен с комплексными коэффициентами и степень $\deg f(x) \geq 1$. Тогда

$$\forall M > 0 \exists R > 0 : |x| > R \Rightarrow |f(x)| > M.$$

Доказательство. Пусть $f(x) = a_0 + a_1x + \dots + a_nx^n$, $a_n \neq 0$. При любом $x \in \mathbb{C}$ справедливо неравенство

$$\begin{aligned} |f(x)| &= |a_nx^n + (a_0 + \dots + a_{n-1}x^{n-1})| \geq \\ &\geq |a_nx^n| - |a_0 + \dots + a_{n-1}x^{n-1}| = \\ &= |a_n||x|^n \left(1 - \frac{|a_0|}{|a_n||x|^{n-1}} - \dots - \frac{|a_{n-1}|}{|a_n||x|} \right). \end{aligned}$$

При $|x| > 1$ правая часть больше $|a_n||x|^n(1 - c/|x|)$, где $c := (|a_0| + \dots + |a_{n-1}|)/|a_n|$. Если $|x| > 2c$, то она больше $|x|^n|a_n|/2$. Таким образом,

$$|x| > R := \max(1, 2c, \sqrt[n]{2M/|a_n|}) \Rightarrow |f(x)| \geq |x|^n|a_n|/2 > M. \quad \square$$

Далее нам нужно понятие сходящейся последовательности комплексных чисел z_k , $k = 1, 2, \dots$, и понятие непрерывности для вещественной функции $F(z)$, определенной в точках z комплексной плоскости. Последовательность $z_k \in \mathbb{C}$ называется *сходящейся к точке* $z_0 \in \mathbb{C}$, если

$$\forall \varepsilon > 0 \exists N : k > N \Rightarrow |z_k - z_0| < \varepsilon.$$

В этом случае мы пишем $z_k \rightarrow z_0$, а точка z_0 называется *пределом* последовательности z_k . Функция $F(z)$ называется *непрерывной в точке* $z_0 \in \mathbb{C}$, если для любой последовательности z_k , сходящейся к z_0 , последовательность $F(z_k)$ сходится к $F(z_0)$. Множество, состоящее из каких-то точек комплексной плоскости, называется *ограниченным*, если оно содержится в некотором круге комплексной плоскости. Множество называется *замкнутым*, если для любой сходящейся последовательности точек этого множества ее предел также принадлежит этому множеству.

Лемма 4.12.3 (ТЕОРЕМА БОЛЬЦАНО–ВЕЙЕРШТРАССА). *Из любой последовательности точек замкнутого ограниченного множества комплексной плоскости можно выделить подпоследовательность, сходящуюся к точке этого же множества.*

Доказательство. Если точки $z_k = u_k + iv_k$ принадлежат кругу $|z| \leq R$, то

$$-R \leq u_k \leq R, \quad -R \leq v_k \leq R.$$

В курсе математического анализа доказывается теорема Больцано–Вейерштрасса о том, что из любой ограниченной последовательности вещественных чисел можно выделить сходящуюся подпоследовательность. В силу этой теоремы существует сходящаяся подпоследовательность $u_{k_l} \rightarrow u_0$. Далее, по той же теореме существует сходящаяся подпоследовательность $v_{k_{l_m}} \rightarrow v_0$. Следовательно,

$$z_{k_{l_m}} = u_{k_{l_m}} + i v_{k_{l_m}} \rightarrow z_0 := u_0 + i v_0 \in L. \quad \square$$

Лемма 4.12.4 (ТЕОРЕМА ВЕЙЕРШТРАССА). Пусть вещественная функция $F(z)$ является непрерывной во всех точках замкнутого ограниченного множества $L \subset \mathbb{C}$. Тогда существуют точки $z_{\min}, z_{\max} \in L$, такие что

$$F(z_{\min}) \leq F(z) \leq F(z_{\max}) \quad \forall z \in L.$$

Доказательство. Функция $F(z)$ ограничена снизу и сверху. Если бы не было ограниченности снизу, то нашлась бы последовательность $z_k \in L$, такая что $F(z_k) \rightarrow -\infty$. Возьмем сходящуюся подпоследовательность $z_{k_l} \rightarrow z_0$. В силу непрерывности функции $F(z)$ имеем: $F(z_{k_l}) \rightarrow F(z_0)$, а это невозможно, так как $F(z_{k_l}) \rightarrow -\infty$. Аналогично доказывается ограниченность сверху.

Обозначим через c_1 точную нижнюю грань множества значений $F(z)$ при $z \in L$. Согласно определению точной нижней грани, существует последовательность z_k со следующим свойством:

$$c_1 \leq F(z_k) \leq c_1 - \varepsilon_k, \quad \varepsilon_k > 0, \quad \varepsilon_k \rightarrow 0.$$

Выделив из нее сходящуюся подпоследовательность $z_{k_l} \rightarrow z_{\min} \in L$, находим

$$F(z_{k_l}) \rightarrow F(z_{\min}) = c_1 \leq F(z) \quad \forall z \in L.$$

Существование точки $z_{\max}$ устанавливается аналогичным образом. $\square$

Лемма 4.12.5. Для любого многочлена $f(x) \in \mathbb{C}[x]$ вещественная функция $F(z) := |f(z)|$ непрерывна во всех точках комплексной плоскости.

Доказательство. Чтобы установить непрерывность в точке $z_0 \in \mathbb{C}$, положим $z = z_0 + h$ и рассмотрим заданный многочлен как функцию от $h \in \mathbb{C}$:

$$f(z_0 + h) = f(z_0) + b_1 h + \dots + b_n h^n, \quad n = \deg f(x).$$

Пусть $c := |b_1| + \dots + |b_n|$. Тогда при $|h| \leq 1$

$$|F(z_0 + h) - F(z_0)| = ||f(z_0 + h)| - |f(z_0)|| \leq \\ \leq |f(z_0 + h) - f(z_0)| \leq c|h|. \quad \square$$

Доказательство основной теоремы алгебры. Пусть $f(x)$ — заданный многочлен. Положим $M := |f(0)|$. Если $M = 0$, то все доказано. Поэтому рассмотрим случай $M > 0$. По лемме о росте модуля многочлена существует $R > 0$ такое, что при $|z| > R$ выполняется неравенство $|f(z)| > M$. Круг $|z| \leq R$ является замкнутым ограниченным множеством комплексной плоскости, функция $F(z) = |f(z)|$ непрерывна во всех точках этого круга. Поэтому, согласно теореме Вейерштрасса, в данном круге есть точка $z_{\min}$, в которой функция $F(z)$ принимает свое минимальное значение на данном круге. Но это же значение будет минимальным значением этой функции на всей комплексной плоскости, так как $|f(z_{\min})| \leq |f(0)| < |f(z)|$ при всех $|z| > R$. Если $f(z_{\min}) \neq 0$, то по лемме Даламбера найдется точка комплексной плоскости, в которой значение модуля многочлена еще меньше. Следовательно, $f(z_{\min}) = 0$. $\square$

Утверждение 4.12.1. Для любого многочлена $f(x) \in \mathbb{C}[x]$ степени $n \geq 1$ со старшим коэффициентом a_n существуют разные комплексные числа $x_1, \dots, x_t$ и натуральные числа $\alpha_1, \dots, \alpha_t$ такие, что

$$f(x) = a_n(x - x_1)^{\alpha_1} \dots (x - x_t)^{\alpha_t}, \quad \alpha_1 + \dots + \alpha_t = n.$$

Для доказательства достаточно вспомнить теорему Безу. Число α_i называется *кратностью* корня x_i . Часто говорят также, что комплексный многочлен степени $n \geq 1$ имеет n комплексных корней с учетом кратностей.

Следствие 4.12.1. Поле комплексных чисел является алгебраически замкнутым.

Весьма полезно знать о том, что для любого поля существует такое его расширение, которое является алгебраически замкнутым. Но к доказательству этого не очень простого утверждения мы пока не готовы (см. раздел 8.9).

В заключение рассмотрим свойства корней вещественных многочленов. Пусть $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{R}[x]$. Если комплексное число z имеет вид $z = u + iv$, то число $\bar{z} := u - iv$

называется *комплексно-сопряженным* к числу z . Легко проверяется, что если $z_1, z_2 \in \mathbb{C}$, то $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ и $\overline{z_1 z_2} = \overline{z_1} \overline{z_2}$. Отсюда

$$f(z) = a_0 + a_1 z + \dots + a_n z^n = 0 \Rightarrow \overline{f(z)} = a_0 + a_1 \bar{z} + \dots + a_n \bar{z}^n = 0.$$

Таким образом, если вещественный многочлен $f(x)$ имеет не вещественный корень z , то он имеет также комплексно-сопряженный не вещественный корень $\bar{z}$.

Утверждение 4.12.2. Вещественный многочлен степени $n \geq 1$ со старшим коэффициентом a_n имеет разложение

$$f(x) = a_n \prod_{i=1}^s (x - \xi_i) \prod_{j=1}^t (x^2 + p_j x + q_j),$$

$$x^2 + p_j x + q_j = (x - z_j)(x - \bar{z}_j), \quad p_i, q_j \in \mathbb{R},$$

$$\xi_i \in \mathbb{R}, \quad 1 \leq i \leq s, \quad z_j \in \mathbb{C} \setminus \mathbb{R}, \quad 1 \leq j \leq t, \quad s + 2t = n.$$

Задача 189. Докажите, что отображение $z \rightarrow \bar{z}$ является единственным изоморфизмом, который отображает поле $\mathbb{C}$ на себя, оставляет на месте каждое число из поля $\mathbb{R}$ и не является тождественным отображением.

Задача 190. Не опираясь на основную теорему алгебры, докажите, что из факта существования комплексного корня для произвольного вещественного многочлена положительной степени вытекает существование комплексного корня для произвольного комплексного многочлена положительной степени.

Задача 191. Пусть имеется вещественный многочлен положительной степени и L — его поле разложения над $\mathbb{R}$. Докажите, что $\dim(L : \mathbb{R}) = 2^d$, где d — неотрицательное целое число.

Задача 192. Докажите, что множество всех алгебраических над $\mathbb{Q}$ чисел образует поле, которое является алгебраически замкнутым.

Глава 5

ЛИНЕЙНЫЕ ОПЕРАТОРЫ

5.1. Определение линейного оператора

Пусть V и W — линейные пространства над одним и тем же полем $\mathbb{P}$. Отображение (оператор) $A: V \rightarrow W$ называется *линейным оператором*, если

$$A(\alpha x + \beta y) = \alpha A(x) + \beta A(y) \quad \forall x, y \in V, \quad \forall \alpha, \beta \in \mathbb{P}.$$

Иногда V называют *пространством прообразов*, а W — *пространством образов* оператора A . Если $W = V$, то говорят, что оператор A *действует на пространстве V* . Часто (почти всегда) скобки опускаются: $A(x) = Ax$. Если $W = \mathbb{P}$, то оператор называют также *функционалом*.

Множество всех линейных операторов, переводящих векторы из V в векторы из W , само является линейным пространством над тем же полем $\mathbb{P}$. *Сложение операторов* и *умножение оператора на число* определяются совершенно естественным образом ¹⁾:

$$(A + B)(x) := A(x) + B(x), \quad (\alpha A)(x) := \alpha A(x).$$

Нулевой оператор переводит любой вектор в нулевой вектор и обозначается так же, как число 0. Для пространства всех линейных операторов из V в W примем обозначения $\mathcal{L}(V, W) = \mathcal{L}_{\mathbb{P}}(V, W)$.

Нередко приходится рассматривать и произведение AB операторов $B: V \rightarrow Z$ и $A: Z \rightarrow W$, где Z — еще одно пространство

¹⁾ Тривиально проверяется, что линейность операторов A и B влечет за собой линейность операторов $A + B$ и αA .

над тем же полем $\mathbb{P}$. *Произведение операторов* определяется так же, как композиция функций:

$$(AB)(x) := A(B(x)).$$

Без труда проверяется, что в случае линейных операторов A и B произведение также является линейным оператором. Заметим, что оператор αA можно рассматривать как произведение оператора A и *скалярного оператора*, умножающего каждый вектор из пространства W на число α .

Тождественное отображение $x \rightarrow x$, конечно же, является линейным оператором. Такой оператор часто называется *единичным*. Рассмотрим единичные операторы $I_V: V \rightarrow V$ и $I_W: W \rightarrow W$ и предположим, что для оператора $A: V \rightarrow W$ существует оператор $B: W \rightarrow V$, такой что $BA = I_V$ и $AB = I_W$. В таких случаях оператор A называется *обратимым*. Легко доказывается, что оператор B определяется однозначно. Он называется *обратным оператором* для A и обозначается A^{-1} .

Обратимое отображение очевидно является взаимно-однозначным. Поэтому если A — обратимый линейный оператор, то A^{-1} также является линейным оператором. В другой, уже известной нам терминологии, линейный оператор — это не что иное, как гомоморфизм пространства V в пространство W . Обратимый линейный оператор реализует изоморфизм пространств V и W .

Пример 1. Пусть $V = \mathbb{P}^n$, $W = \mathbb{P}^m$, $A \in \mathbb{P}^{m \times n}$. Правило $x \rightarrow Ax$ (умножение матрицы A на вектор $x \in V$) задает линейный оператор.

Пример 2. Пусть $V = W = \mathbb{R}[x]$ — бесконечномерное линейное пространство всех вещественных многочленов от переменной x . Легко проверить, что оператор дифференцирования $f(x) \rightarrow f'(x)$ (многочлен переводится в свою производную) является линейным.

Пример 3. Пусть V — произвольное линейное пространство, представленное прямой суммой $V = L \oplus M$. Тогда любой вектор $x \in V$ однозначно записывается в виде $x = x_L + x_M$, где $x_L \in L$ и $x_M \in M$. Оператор $x \rightarrow x_L$ является линейным и называется *проектором на подпространство L вдоль подпространства M* .

Пусть L — какое-то подмножество векторов из V . Тогда, по определению, AL — это множество всех векторов $y \in W$ вида

$y = Ax$, где $x \in L$. Если L — подпространство пространства V , то для любого линейного оператора $A: V \rightarrow W$ множество AL будет, как легко видеть, подпространством пространства W .

Подпространство $AV \subseteq W$ называется *образом* оператора A и обозначается $\text{im } A$. Его размерность называется *рангом* оператора. Обозначение: $\text{rank } A = \dim \text{im } A$.

Множество всех векторов из V , которые переводятся в нулевой вектор пространства W , называется *ядром* оператора A и обозначается $\ker A$. В случае линейного оператора $A: V \rightarrow W$ ядро является подпространством в V , его размерность называется *дефектом оператора* A . Обозначение: $\text{def } A = \dim \ker A$.

Теорема 5.1.1. Пусть $A: V \rightarrow W$ — произвольный линейный оператор и пространство V конечномерно. Тогда

$$\text{rank } A + \text{def } A = \dim V.$$

Доказательство. Пусть $n = \dim V$ и $d = \text{def } A$. Выберем в ядре какой-либо базис $x_1, \dots, x_d$ и дополним его до базиса $x_1, \dots, x_d, x_{d+1}, \dots, x_n$ пространства V . Тогда $\text{im } A = \langle Ax_{d+1}, \dots, Ax_n \rangle$ и, кроме того, векторы $Ax_{d+1}, \dots, Ax_n$ линейно независимы:

$$\begin{aligned} \alpha_{d+1}Ax_{d+1} + \dots + \alpha_nAx_n &= 0 \Rightarrow \\ \Rightarrow A(\alpha_{d+1}x_{d+1} + \dots + \alpha_nx_n) &= 0 \Rightarrow \\ \Rightarrow z := \alpha_{d+1}x_{d+1} + \dots + \alpha_nx_n &\in \ker A = \langle x_1, \dots, x_d \rangle \Rightarrow \\ \Rightarrow z = 0 \Rightarrow \alpha_{d+1} = \dots = \alpha_n &= 0. \quad \square \end{aligned}$$

Задача 193. Докажите, что линейный оператор $A: V \rightarrow V$ является проектором в том и только том случае, когда $A^2 = A$.

Задача 194. Линейный оператор A удовлетворяет уравнению $A^2 + A + I = 0$. Докажите, что он обратим.

Задача 195. Докажите, что линейный оператор $A: V \rightarrow V$ коммутирует со всеми линейными операторами, действующими на пространстве V над полем $\mathbb{P}$, в том и только том случае, когда он является оператором умножения на некоторое число из поля $\mathbb{P}$.

Задача 196. Сумма двух линейных операторов, действующих на конечномерном пространстве V , является обратимым

оператором, а произведение — нулевым оператором. Докажите, что сумма рангов этих операторов равна размерности пространства V .

5.2. Операторы и матрицы

Утверждение 5.2.1. Если пространство V конечномерно, то линейный оператор $A: V \rightarrow W$ полностью определяется образами базисных векторов пространства V .

Доказательство. Пусть $e_1, \dots, e_n$ — произвольный базис пространства V . Тогда любой вектор $x \in V$ имеет однозначное разложение

$$x = \sum_{j=1}^n x_j e_j, \quad x_1, \dots, x_n \in \mathbb{P},$$

и, в силу линейности оператора A ,

$$Ax = \sum_{j=1}^n x_j Ae_j.$$

Таким образом, для каждого вектора $x \in V$ его образ Ax однозначно определяется, если известны векторы $Ae_1, \dots, Ae_n$. $\square$

Теперь предположим, что пространство W также конечномерно, пусть оно имеет размерность m и базис $f_1, \dots, f_m$. Рассмотрим коэффициенты $a_{ij} \in \mathbb{P}$ разложений

$$Ae_j = \sum_{i=1}^m a_{ij} f_i, \quad 1 \leq j \leq n,$$

и составим из них $m \times n$ -матрицу

$$M = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{bmatrix}.$$

Матрица M однозначно определяется линейным оператором A , базисом $e_1, \dots, e_n$ пространства прообразов и базисом $f_1, \dots, f_m$ пространства образов. Для краткости будем говорить, что заданы базисы e и f , и примем обозначение $M = [A]_{fe}$. Кроме того, если векторы $x \in V$ и $y \in W$ имеют разложения

$$x = \sum_{j=1}^n x_j e_j, \quad y = \sum_{i=1}^m y_i f_i,$$

то условимся писать

$$[x]_e := \begin{bmatrix} x_1 \\ \dots \\ x_n \end{bmatrix}, \quad [y]_f := \begin{bmatrix} y_1 \\ \dots \\ y_m \end{bmatrix}.$$

Матрица $M = [A]_{fe}$ называется *матрицей линейного оператора* или *представлением линейного оператора в базисах e и f* . Ее роль проясняется следующим наблюдением.

Утверждение 5.2.2. Для любого вектора $x \in V$ выполняется равенство

$$[Ax]_f = [A]_{fe}[x]_e.$$

Доказательство.

$$Ax = \sum_{j=1}^n x_j A e_j = \sum_{j=1}^n x_j \sum_{i=1}^m a_{ij} f_i = \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} x_j \right) f_i. \quad \square$$

Утверждение 5.2.3. Пусть V и W — линейные пространства над полем $\mathbb{P}$ размерностей n и m соответственно. Тогда пространство линейных операторов $\mathcal{L}_{\mathbb{P}}(V, W)$ изоморфно линейному пространству матриц $\mathbb{P}^{m \times n}$.

Доказательство. Искомый изоморфизм — это отображение $A \rightarrow [A]_{fe}$, которое, очевидно, сохраняет операцию сложения операторов и операцию умножения оператора на число: $[A + B]_{fe} = [A]_{fe} + [B]_{fe}$, $[\alpha A]_{fe} = \alpha [A]_{fe}$. $\square$

Вместо базисов e и f мы можем взять какие-то другие базисы g и h , составленные соответственно из векторов $g_1, \dots, g_n$ и $h_1, \dots, h_m$. Как связаны между собой матрицы $[A]_{fe}$ и $[A]_{hg}$?

Прежде всего нужно понять, как связаны координаты одного и того же вектора в разных базисах. Пусть имеются разложения вектора $x \in V$ в базисах e и g :

$$x = \sum_{l=1}^n x_l e_l = \sum_{j=1}^n x'_j g_j \Rightarrow [x]_e = \begin{bmatrix} x_1 \\ \dots \\ x_n \end{bmatrix}, \quad [x]_g = \begin{bmatrix} x'_1 \\ \dots \\ x'_n \end{bmatrix}.$$

Рассмотрим коэффициенты p_{lj} разложений

$$g_j = \sum_{l=1}^n p_{lj} e_l, \quad 1 \leq j \leq n,$$

и образуем из них $n \times n$ -матрицу $P_{eg} = [p_{lj}]$. Матрица P_{eg} называется *матрицей перехода* от базиса g к базису e .

Утверждение 5.2.4. Для любого вектора $x \in V$ выполняется равенство

$$[x]_e = P_{eg}[x]_g.$$

Доказательство.

$$x = \sum_{j=1}^n x'_j g_j = \sum_{j=1}^n x'_j \sum_{l=1}^n p_{lj} e_l = \sum_{l=1}^n \left(\sum_{j=1}^n p_{lj} x'_j \right) e_j. \quad \square$$

Следствие 5.2.1. Матрица перехода P_{eg} невырождена и $P_{eg}^{-1} = P_{ge}$.

Утверждение 5.2.5. Пусть P_{eg} — матрица перехода от базиса g к базису e пространства V и Q_{hf} — матрица перехода от базиса f к базису h пространства W . Тогда для любого линейного оператора $A: V \rightarrow W$ имеет место равенство

$$[A]_{hg} = Q_{hf} [A]_{fe} P_{eg}.$$

Доказательство. Матрица $[A]_{hg}$ — это единственная матрица, удовлетворяющая равенству $[Ax]_h = [A]_{hg}[x]_g$ для всех векторов $x \in V$. В то же время

$$\begin{aligned} [Ax]_h &= Q_{hf}[Ax]_f = Q_{hf}[A]_{fe}[x]_e = (Q_{hf}[A]_{fe}P_{eg})[x]_g \Rightarrow \\ &\Rightarrow [A]_{hg} = Q_{hf}[A]_{fe}P_{eg}. \quad \square \end{aligned}$$

Матрицы A, B над одним и тем же полем называются *эквивалентными*, если для каких-то невырожденных матриц P и Q над тем же полем выполняется равенство $B = QAP$.

Утверждение 5.2.6. Эквивалентные матрицы и только они представляют некоторый, один и тот же, линейный оператор при подходящем выборе базисов.

Доказательство. Если матрицы A и B представляют один и тот же линейный оператор в разных базисах, то они эквивалентны в силу утверждения 5.2.5. Обратно, предположим, что матрица A имеет размер $m \times n$ и $B = QAP$. Рассмотрим линейный оператор умножения векторов на матрицу A . Сама матрица A является его представлением в базисах, составленных из столбцов единичных матриц порядка n и порядка m . Обозначим столбцы матрицы P через $g_1, \dots, g_n$, а через $h_1, \dots, h_m$ — столбцы матрицы Q^{-1} . Равенство $Q^{-1}B = AP$ показывает, что каждый вектор Ag_j есть линейная комбинация векторов $h_1, \dots, h_m$ с коэффициентами из j -го столбца матрицы B . Это означает, что B — матрица того же оператора в базисах g и h . $\square$

Теорема 5.2.1. *Для эквивалентности матриц A и B над одним и тем же полем необходимо и достаточно совпадение их размеров и рангов.*

Доказательство. Необходимость почти очевидна: совпадение размеров сразу же следует из определения эквивалентных матриц, известно также, что ранг сохраняется при умножении на невырожденные матрицы. Чтобы установить достаточность, заметим, что эквивалентность матриц — это бинарное отношение на множестве матриц, обладающее всеми свойствами общего отношения эквивалентности на абстрактном множестве. Поэтому нам достаточно показать, что любая $m \times n$ -матрица A ранга r эквивалентна одной и той же матрице, имеющей вид $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} = QAP$, где I_r — единичная матрица порядка r . Матрицы Q и P можно получить как произведения очень простых матриц, умножение на которые реализует так называемые *элементарные преобразования*. К таковым относятся перестановки строк (столбцов), прибавление к строке (столбцу) другой строки (другого столбца), умножение строки (столбца) на ненулевое число. $\square$

Следствие 5.2.2. *В случае конечномерных пространств V и W для любого линейного оператора $A: V \rightarrow W$ ранга r существуют базисы, в которых он представляется матрицей вида $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$.*

Предположим, что нам известна только матрица линейного оператора, но мы не знаем базисов. Из данного следствия мы видим, что одна только матрица может давать очень скудную информацию о свойствах оператора. Скоро мы поймем, что ситуация будет существенно иной, если пространство образов совпадает с пространством прообразов и известно, что в них выбран один и тот же базис.

Матрица $[A]_e := [A]_{ee}$ называется *матрицей линейного оператора A в базисе e* . Выбрав какой-то другой базис g , получаем

$$[A]_g = P_{eg}^{-1} [A]_e P_{eg},$$

где P_{eg} — матрица перехода от базиса g к базису e . Матрицы A и B над общим полем, связанные соотношением $B = P^{-1}AP$, где P — невырожденная матрица над тем же полем, называются *подобными*.

Утверждение 5.2.7. *Подобные матрицы и только они представляют некоторый, один и тот же, линейный оператор $A: V \rightarrow V$ при подходящем выборе базиса пространства V .*

Доказательство сходно с доказательством утверждения 5.2.6 и предоставляется читателю в качестве упражнения.

Задача 197. Пусть V, W, Z — конечномерные линейные пространства над одним и тем же полем и заданы произвольные линейные операторы $B: V \rightarrow Z$ и $A: Z \rightarrow W$. Докажите, что

$$\operatorname{rank} A + \operatorname{rank} B - \operatorname{rank} AB \leq \dim Z.$$

Задача 198. Матрицы A, B, C, X, Y порядка n над одним и тем же полем удовлетворяют равенству $XA + BY = C$. Докажите эквивалентность матриц

$$L = \begin{bmatrix} A & 0 \\ C & B \end{bmatrix} \quad \text{и} \quad D = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$

Задача 199. Докажите, что произвольная матрица порядка n подобна верхней почти треугольной матрице, которая может быть вычислена за конечное число арифметических операций вида $O(n^3)$. Матрица называется верхней почти треугольной, если она имеет нулевые элементы в позициях i, j при $i > j + 1$.

5.3. Характеристический многочлен

Характеристическим многочленом матрицы A порядка n над полем $\mathbb{P}$ называется многочлен $\det(A - \lambda I_n) \in \mathbb{P}[\lambda]$. Очевидно, что это многочлен степени n и при умножении на $(-1)^n$ он превращается в многочлен $\det(\lambda I_n - A)$ со старшим коэффициентом, равным 1. Такой многочлен называется *приведенным характеристическим многочленом*.

Коэффициенты характеристического многочлена выражаются через главные миноры матрицы A . Напомним, что *главным минором* квадратной матрицы называется определитель подматрицы, расположенной на пересечении строк и столбцов с одинаковыми номерами.

Утверждение 5.3.1. Пусть A — матрица порядка n . Тогда

$$\det(A - \lambda I_n) = \sum_{k=0}^n s_k (-\lambda)^k,$$

где $s_n = 1$ и s_k — сумма главных миноров порядка $n - k$ при $0 \leq k \leq n - 1$.

Доказательство. Определитель $\det(A - \lambda I_n)$ является суммой взятых с определенными знаками произведений элементов матрицы $B(\lambda) = A - \lambda I_n$. Чтобы получить коэффициент при $(-\lambda)^k$, эту сумму преобразуем в сумму одночленов от λ и приведем подобные члены. Заметим, что при любых фиксированных номерах $1 \leq i_1 < \dots < i_k \leq n$ сумма всех членов определителя $|B(\lambda)|$, содержащих элементы главной диагонали в позициях $(i_1, i_1), \dots, (i_k, i_k)$, имеет вид $b_{i_1 i_1} \dots b_{i_k i_k} B_{i_1, \dots, i_k}$, где $B_{i_1, \dots, i_k} = B_{i_1, \dots, i_k}(\lambda)$ — главный минор матрицы $B(\lambda)$, возникающий после вычеркивания строк и столбцов с номерами $i_1, \dots, i_k$. Рассмотрим одночлены, которые соответствуют этой сумме и получаются при выборе λ при раскрытии двучленов $b_{i_1 i_1} = a_{i_1 i_1} - \lambda, \dots, b_{i_k i_k} = a_{i_k i_k} - \lambda$. Очевидно, что вклад в коэффициент при $(-\lambda)^k$ от таких одночленов равен $|B_{i_1, \dots, i_k}(0)|$ ¹⁾. □

Свободный член характеристического многочлена — это определитель матрицы A , а коэффициент при $(-\lambda)^{n-1}$ — это сумма элементов главной диагонали, называемая *следом* матрицы A . Обозначение для следа: $\text{tr } A$.

Характеристическим многочленом оператора A , действующего в n -мерном пространстве V , называется характеристический многочлен представляющей его матрицы $[A]_e$ в произвольно

¹⁾ Наметим и другой вариант рассуждения. Скоро мы докажем, что среди матриц над полем разложения многочлена $\det(A - \lambda I_n)$ можно выбрать невырожденную матрицу P таким образом, что матрица $P^{-1}AP$ будет верхней треугольной. Утверждение 5.3.1 совершенно очевидно для случая верхней треугольной матрицы, а общий случай сводится к нему в силу двух причин. Во-первых, характеристические многочлены подобных матриц совпадают (утверждение 5.3.2). Во-вторых, сумма главных миноров порядка k для подобных матриц одна и та же. Для доказательства удобно использовать минорные матрицы (см. раздел 1.9): сумма главных миноров порядка k для A равна сумме элементов главной диагонали для $C_k(A)$. Согласно утверждению 1.9.1, $C_k(P^{-1}AP) = (C_k(P))^{-1}C_k(A)C_k(P)$. Чтобы показать, что сумма элементов главной диагонали для подобных матриц одна и та же, опираемся на то, что коэффициент при $(-\lambda)^{n-1}$ равен сумме элементов главной диагонали — это особенно легко проверяемая часть утверждения 5.3.1.

выбранном базисе ϵ . Конечно, это определение имеет смысл только в том случае, если многочлен получается один и тот же при любом выборе базиса. Это действительно так и вытекает из следующего утверждения.

Утверждение 5.3.2. *Характеристические многочлены подобных матриц совпадают.*

Доказательство. Пусть $A, B, P \in \mathbb{P}^{n \times n}$ и $B = P^{-1}AP$. Тогда

$$\begin{aligned} \det(B - \lambda I_n) &= \det(P^{-1}AP - \lambda P^{-1}I_n P) = \\ &= \det P \det(A - \lambda I_n) \det P^{-1} = \det(A - \lambda I_n). \quad \square \end{aligned}$$

Таким образом, величины s_k определяются по матрице оператора, но не зависят от выбора базиса для построения этой матрицы. В частности, для линейного оператора $A: V \rightarrow V$ мы получаем возможность ввести полезные понятия *определителя оператора* и *следа оператора*:

$$\det A := \det [A]_e = s_0, \quad \operatorname{tr} A := \operatorname{tr} [A]_e = s_{n-1}.$$

Пример. Оператор дифференцирования на пространстве многочленов от t степени не выше $n-1$ в базисе $1, t, \frac{t^2}{2}, \dots, \frac{t^{n-1}}{(n-1)!}$ представляется двухдиагональной матрицей

$$A = \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ & & & 0 \end{bmatrix}$$

с характеристическим многочленом $f_A(\lambda) = (-\lambda)^n$.

Нетрудно понять, что матрица A не может быть подобна никакой диагональной матрице. В самом деле, характеристический многочлен диагональной матрицы

$$B = \begin{bmatrix} b_1 & & \\ & \ddots & \\ & & b_n \end{bmatrix}$$

имеет вид

$$f_B(\lambda) = (b_1 - \lambda) \dots (b_n - \lambda).$$

Если A и B подобны, то, согласно утверждению 5.3.2,

$$f_A(\lambda) = f_B(\lambda) \Rightarrow b_1 = \dots = b_n = 0 \Rightarrow B = 0.$$

Значит, если матрица A подобна диагональной матрице, то эта диагональная матрица должна быть нулевой. Но ненулевая матрица не может быть подобна нулевой матрице. Как видим, *не всякая матрица подобна диагональной и равенство характеристических многочленов недостаточно для подобия!*

Пусть A — произвольный оператор в пространстве над полем $\mathbb{P}$. Для любого многочлена $f(\lambda) = \sum_{k=0}^m f_k \lambda^k \in \mathbb{P}[\lambda]$ можно определить соответствующий ему *многочлен от оператора A* :

$$f(A) := \sum_{k=0}^m f_k A^k.$$

Теорема 5.3.1 (ТЕОРЕМА КЭЛИ–ГАМИЛЬТОНА¹⁾). Пусть V — конечномерное пространство над полем $\mathbb{P}$, $A: V \rightarrow V$ — линейный оператор и $f(\lambda)$ — его характеристический многочлен. Тогда $f(A) = 0$.

Доказательство. Достаточно рассмотреть случай, когда $A = [a_{ij}]$ — матрица порядка n . Пусть $e_1, \dots, e_n$ — столбцы единичной матрицы порядка n . Тогда, очевидно,

$$Ae_1 = a_{11}e_1 + a_{21}e_2 + \dots + e_{n1}e_n,$$

$$\dots \dots \dots$$

$$Ae_n = a_{1n}e_1 + a_{2n}e_2 + \dots + e_{nn}e_n.$$

Теперь образуем блочную матрицу вида

$$\mathcal{A} = \begin{bmatrix} a_{11}I_n - A & a_{21}I_n & \dots & a_{n1}I_n \\ a_{12}I_n & a_{22}I_n - A & \dots & a_{n2}I_n \\ \dots & \dots & \dots & \dots \\ a_{1n}I_n & a_{2n}I_n & \dots & a_{nn}I_n \end{bmatrix}$$

и заметим, что

$$A \begin{bmatrix} e_1 \\ \dots \\ e_n \end{bmatrix} = \begin{bmatrix} 0 \\ \dots \\ 0 \end{bmatrix}. \quad (*)$$

Можно считать, что $\mathcal{A} \in K^{n \times n}$, где $K = \{g(A): g(\lambda) \in \mathbb{P}[\lambda]\}$ — кольцо многочленов от матрицы A . Ясно, что это коммутативное ассоциативное кольцо с единицей. Поэтому для матриц над

¹⁾ Мы сохраняем англоязычный порядок фамилий авторов: Caley и Hamilton.

кольцом K остаются в силе основные факты теории определителей. В данном случае определитель $\det A$ является элементом кольца K (т.е. многочленом от матрицы A) и, как нетрудно заметить, равен $f^T(A)$, где $f^T(\lambda)$ — характеристический многочлен транспонированной матрицы A^T . Тривиально проверяется, что $f^T(\lambda) = f(\lambda)$. Кроме того, мы имеем право рассмотреть присоединенную матрицу $\hat{A}$. Напомним, что в позиции i, j присоединенной матрицы размещается алгебраическое дополнение элемента исходной матрицы, расположенного в позиции j, i . При умножении на присоединенную матрицу получаем

$$\hat{A}A = \begin{bmatrix} f(A) & & \\ & \ddots & \\ & & f(A) \end{bmatrix}.$$

Используя равенство (*), находим, что матрица $f(A) \in K \subseteq \mathbb{P}^{n \times n}$ удовлетворяет соотношениям

$$f(A)e_1 = \dots = f(A)e_n = 0,$$

откуда очевидно следует, что $f(A) = 0$. □

Многочлен $g(\lambda) \in \mathbb{P}[\lambda]$ называется *аннулирующим* матрицу $A \in \mathbb{P}^{n \times n}$ или оператор A на n -мерном пространстве над полем $\mathbb{P}$, если $g(A) = 0$. Теорема Кэли–Гамильтона утверждает, что характеристический многочлен для A является аннулирующим. Аннулирующий многочлен минимальной степени называется *минимальным многочленом* для A .

Утверждение 5.3.3. *Для любого оператора на конечно-мерном пространстве минимальный многочлен является делителем характеристического многочлена и вообще любого аннулирующего многочлена.*

Доказательство. Если бы остаток при делении аннулирующего многочлена на минимальный был ненулевым, то он был бы аннулирующим многочленом меньшей степени. □

Следствие 5.3.1. *Минимальный многочлен определяется однозначно с точностью до умножения на ненулевое число.*

Задача 200. *Найдите минимальный многочлен для оператора дифференцирования на пространстве многочленов степени не выше $n - 1$.*

Задача 201. Докажите, что приведенный характеристический многочлен матрицы

$$A = \begin{bmatrix} 0 & & & -a_0 \\ 1 & 0 & & -a_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{bmatrix}$$

имеет вид $f_A(\lambda) = a_0 + a_1\lambda + \dots + a_{n-1}\lambda^{n-1} + \lambda^n$.¹⁾

Задача 202. Матрицы A и B порядка n имеют приведенные характеристические многочлены соответственно вида

$$f_A(\lambda) = \prod_{i=1}^n (\lambda - \lambda_i), \quad f_B(\lambda) = \prod_{i=1}^n (\lambda - \mu_i).$$

Найти характеристический многочлен линейного оператора $X \rightarrow AX + XB$, действующего на пространстве $n \times n$ -матриц X .

Задача 203. Докажите, что для произвольных линейных операторов A и B на одном и том же конечномерном пространстве над произвольным полем характеристические многочлены произведений AB и BA совпадают.

Задача 204. Даны $m \times n$ -матрицы A и B над общим полем. Как связаны между собой характеристические многочлены матриц AB^T и $B^T A$?

5.4. Матричные многочлены и подобие

Матричный многочлен над полем $\mathbb{P}$ от буквы λ — это многочлен вида

$$A(\lambda) = \sum_{k=0}^m A_k \lambda^k$$

с коэффициентами из кольца матриц одного и того же порядка n над полем $\mathbb{P}$. Если $A_m \neq 0$, то m называется его степенью и обозначается $\deg A(\lambda) = m$. Подчеркнем, что если $n \geq 2$, то мы имеем дело с многочленом над некоммутативным кольцом. В то же время, матричный многочлен можно также рассматривать

¹⁾ Матрица A называется матрицей Фробениуса или сопровождающей матрицей многочлена $f(\lambda)$.

как матрицу над коммутативным кольцом $\mathbb{P}[\lambda]$, ее элементы являются многочленами над полем $\mathbb{P}$.

Наша цель в этом разделе — доказать, что подобие матриц A и B равносильно *унимодулярной эквивалентности* матричных двучленов $A(\lambda) = A - \lambda I$ и $B(\lambda) = B - \lambda I$, где I — единичная матрица.

Матрица $P(\lambda) \in (\mathbb{P}[\lambda])^{n \times n}$ называется *унимодулярной*, если ее определитель есть ненулевая константа. В этом случае элементы обратной матрицы $P^{-1}(\lambda)$ будут также многочленами от λ , а ее определитель — ненулевая константа. Поэтому обратная матрица также унимодулярная. Матричный многочлен $A(\lambda)$ называется *унимодулярно эквивалентным* матричному многочлену $B(\lambda)$, если существуют унимодулярные матрицы $P(\lambda), Q(\lambda) \in (\mathbb{P}[\lambda])^{n \times n}$ такие, что $B(\lambda) = Q(\lambda)A(\lambda)P(\lambda)$. Бинарное отношение унимодулярной эквивалентности обладает всеми свойствами отношения эквивалентности.

К элементарным унимодулярным преобразованиям матрицы $A(\lambda)$ будем относить перестановки строк (столбцов), прибавление к строке (столбцу) другой строки (другого столбца) с предварительным умножением на некоторый многочлен от λ , умножение строки (столбца) на ненулевое число. Эти преобразования реализуются с помощью умножения матрицы $A(\lambda)$ слева или справа на некоторую унимодулярную матрицу.

Теорема 5.4.1. *Любой ненулевой матричный многочлен $A(\lambda)$ элементарными унимодулярными преобразованиями приводится к диагональному виду*

$$F(\lambda) = \begin{bmatrix} F_r(\lambda) & 0 \\ 0 & 0 \end{bmatrix}, \quad F_r(\lambda) = \begin{bmatrix} f_1(\lambda) & & \\ & \ddots & \\ & & f_r(\lambda) \end{bmatrix},$$

где каждый из многочленов $f_1(\lambda), \dots, f_r(\lambda)$ имеет старший коэффициент 1 и при $1 \leq k \leq r-1$ многочлен $f_k(\lambda)$ является делителем многочлена $f_{k+1}(\lambda)$. Число r и многочлены $f_1(\lambda), \dots, f_r(\lambda)$ не зависят от использованных преобразований и определяются по матрице $A(\lambda)$ однозначно. Более того, при всех $1 \leq k \leq r$ произведение $f_1(\lambda) \dots f_k(\lambda)$ равно наибольшему общему делителю всех миноров порядка k матрицы $A(\lambda)$ с точностью до умножения на ненулевое число.

Доказательство. Проведем индукцию по порядку матрицы n . Случай $n = 1$ очевиден. Пусть $n \geq 2$. Обозначим че-

рез $B(\lambda)$ матрицу, в которой элемент $b_{11}(\lambda)$ является ненулевым многочленом наименьшей степени среди элементов в этой позиции во всех матричных многочленах, получаемых из $A(\lambda)$ с помощью конечной последовательности элементарных унимодулярных преобразований. Тогда каждый элемент первого столбца и первой строки матрицы $B(\lambda)$ обязан делиться на $b_{11}(\lambda)$ — иначе с помощью элементарных унимодулярных преобразований можно получить матрицу, в которой появится многочлен меньшей степени. Следовательно, матрица $A(\lambda)$ приводится к виду

$$B(\lambda) = \begin{bmatrix} b_{11}(\lambda) & 0 \\ 0 & C(\lambda) \end{bmatrix},$$

где матрица $C(\lambda)$ имеет порядок $n - 1$, и если $C(\lambda) \neq 0$, то для нее можно применить индуктивное предположение. Остается заметить, что любое элементарное унимодулярное преобразование с точностью до умножения на ненулевое число сохраняет наибольший общий делитель всех миноров порядка k . $\square$

Следствие 5.4.1. *Любая унимодулярная матрица с помощью конечной последовательности элементарных унимодулярных преобразований приводится к единичной матрице.*

Следствие 5.4.2. *Наличие или отсутствие унимодулярной эквивалентности двух матричных многочленов можно выяснить за конечное число арифметических операций.*

Теорема 5.4.2. *Квадратные матрицы A и B над общим полем подобны тогда и только тогда, когда матричные многочлены $A(\lambda) = A - \lambda I$ и $B(\lambda) = B - \lambda I$ унимодулярно эквивалентны.*

Доказательство. Нетривиальная часть — вывести подобие из соотношения $B(\lambda) = Q(\lambda)A(\lambda)P(\lambda)$ и унимодулярности матриц $P(\lambda)$ и $Q(\lambda)$. Для этого заметим, что для многочленов в некоммутативном кольце можно также выполнять деление с остатком, если делитель имеет обратимый старший коэффициент. В некоммутативном случае имеются два способа деления с остатком — слева и справа. Мы будем делить на многочлен первой степени $B(\lambda) = B - \lambda I$, поэтому ненулевые остатки будут обычными матрицами (многочленами нулевой степени):

$$P(\lambda) = X_1(\lambda)B(\lambda) + R_1,$$

$$Q(\lambda) = B(\lambda)X_2(\lambda) + R_2.$$

Рассмотрим разность

$$\begin{aligned} R_2 A(\lambda) R_1 - B(\lambda) &= (Q(\lambda) - B(\lambda) X_2(\lambda)) A(\lambda) (P(\lambda) - \\ &- X_1(\lambda) B(\lambda)) - Q(\lambda) A(\lambda) P(\lambda) = B(\lambda) X_2(\lambda) A(\lambda) X_1(\lambda) B(\lambda) - \\ &- B(\lambda) X_2(\lambda) \underline{A(\lambda) P(\lambda)} - \underline{Q(\lambda) A(\lambda)} X_1(\lambda) B(\lambda). \end{aligned}$$

Используя унимодулярную эквивалентность матриц $A(\lambda)$ и $B(\lambda)$, подчеркнутые многочлены запишем в виде

$$A(\lambda) P(\lambda) = Q^{-1}(\lambda) B(\lambda), \quad Q(\lambda) A(\lambda) = B(\lambda) P^{-1}(\lambda).$$

В результате получаем

$$\begin{aligned} R_2 A(\lambda) R_1 - B(\lambda) &= \\ &= B(\lambda) (X_2(\lambda) A(\lambda) X_1(\lambda) - Q^{-1}(\lambda) B(\lambda) - P^{-1}(\lambda) B(\lambda)) B(\lambda). \end{aligned}$$

Если подчеркнутый многочлен в скобках отличен от нуля, то степень правой части не меньше 2. В то же время слева стоит многочлен степени не выше 1. Следовательно, правая часть равна нулю $\Rightarrow R_2(A - \lambda I)R_1 = B - \lambda I \Rightarrow R_2 A R_1 = B$, $R_2 R_1 = I$. $\square$

Следствие 5.4.3. *Наличие или отсутствие подобия двух матриц над произвольным полем можно выяснить за конечное число арифметических операций над этим полем.*

Задача 205. *Докажите, что квадратная матрица над произвольным полем подобна своей транспонированной матрице.*

Задача 206. *Докажите, что матрицы*

$$\begin{bmatrix} a_1 & a_2 & 1 \\ 1 & 0 & 0 \\ 0 & a_3 & 0 \end{bmatrix} \quad \text{и} \quad \begin{bmatrix} a_1 & a_2 & a_3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

подобны при любых значениях a_1, a_2, a_3 .

Задача 207. *Пусть $\sigma(1), \dots, \sigma(n)$ — произвольная перестановка чисел $1, \dots, n$. Докажите, что произвольная верхняя треугольная матрица с диагональными элементами $\lambda_1, \dots, \lambda_n$ подобна некоторой верхней треугольной матрице с диагональными элементами $\lambda_{\sigma(1)}, \dots, \lambda_{\sigma(n)}$.*

5.5. Собственные значения и собственные векторы

Пусть $f_A(\lambda) = \det(A - \lambda I)$ — характеристический многочлен матрицы A порядка n над полем $\mathbb{P}$. Предположим, что он имеет корень, принадлежащий полю $\mathbb{P}$. Обозначим этот корень той же буквой λ , т.е. далее полагаем, что λ — это число из поля $\mathbb{P}$. Поскольку $\det(A - \lambda I) = 0$, однородное уравнение $(A - \lambda I)x = 0$ имеет нетривиальное решение $x \in \mathbb{P}^n$ и, следовательно,

$$Ax = \lambda x, \quad x \neq 0. \quad (*)$$

Соотношение $(*)$ можно рассматривать и без какой-либо связи с характеристическим многочленом. Более того, оно имеет смысл, если считать, что A — некоторый линейный оператор на каком-то пространстве V над полем $\mathbb{P}$, $x \in V$ и $\lambda \in \mathbb{P}$. Число λ и вектор $x \neq 0$, связанные соотношением $(*)$, называются *собственным значением* и *собственным вектором* матрицы или оператора A .

Связь собственных значений и корней характеристического многочлена описывается следующим, в действительности уже полученным нами, утверждением.

Утверждение 5.5.1. *Собственные значения линейного оператора на конечномерном пространстве и только они являются корнями его характеристического многочлена.*

Обратим внимание на ясный геометрический смысл собственного вектора: при действии на него оператором A он просто умножается на соответствующее ему собственное значение.

Если в пространстве V имеется базис из собственных векторов оператора, то в этом базисе данный оператор представляется, очевидно, диагональной матрицей. Такой оператор называется *оператором простой структуры* или *диагонализуемым оператором*.

Простым достаточным условием диагонализуемости является простота собственных значений и предположение о том, что поле разложения характеристического многочлена содержится в поле $\mathbb{P}$. Собственное значение называется *простым*, если оно является простым корнем характеристического многочлена. В противном случае собственное значение называется *кратным*. Говорят, что собственное значение имеет *алгебраическую кратность* k , если для характеристического многочлена оно является корнем кратности k . Упомянутое выше условие диагонализуемости вытекает из следующей теоремы.

Теорема 5.5.1. Если собственные векторы $x_1, \dots, x_k$ линейного оператора A соответствуют попарно различным собственным значениям $\lambda_1, \dots, \lambda_k$, то они линейно независимы.

Доказательство. Рассмотрим равную нулю линейную комбинацию данных собственных векторов и подействуем на нее оператором A :

$$\sum_{i=1}^k \alpha_i x_i = 0 \Rightarrow \sum_{i=1}^k \alpha_i \lambda_i x_i = 0.$$

Из последнего равенства вычтем равенство

$$\lambda_k \left(\sum_{i=1}^k \alpha_i x_i \right) = 0 \Rightarrow \sum_{i=1}^{k-1} \alpha_i (\lambda_i - \lambda_k) x_i = 0.$$

Далее очевидным образом применяется индукция по k . □

Пусть λ — собственное значение линейного оператора A : $V \rightarrow V$. Множество L_λ всех векторов $x \in V$, таких что $Ax = \lambda x$, называется *собственным подпространством* оператора A , отвечающим данному собственному значению λ . То, что L_λ будет подпространством в V , проверяется тривиальным образом. Каждый ненулевой вектор из L_λ является собственным вектором для λ , и очевидно, что L_λ содержит все собственные векторы, соответствующие λ . Размерность пространства L_λ называется *геометрической кратностью* собственного значения λ .

Утверждение 5.5.2. Геометрическая кратность собственного значения меньше или равна его алгебраической кратности.

Доказательство. Пусть линейный оператор A действует в n -мерном пространстве V над полем $\mathbb{P}$, и пусть λ_1 — его собственное значение геометрической кратности l . Выберем базис $e_1, \dots, e_n$ пространства V таким образом, чтобы векторы $e_1, \dots, e_l$ составили базис собственного подпространства для λ_1 . В этом базисе матрица оператора A примет вид

$$[A]_e = \begin{bmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{bmatrix}, \quad A_{11} = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_1 \end{bmatrix} \in \mathbb{P}^{l \times l}.$$

Поэтому характеристический многочлен представляет собой произведение

$$\det(A_{11} - \lambda I_l) \det(A_{22} - \lambda I_{n-l}) = (\lambda_1 - \lambda)^l \det(A_{22} - \lambda I_{n-l}).$$

Отсюда видно, что l не может быть больше алгебраической кратности корня λ_1 . $\square$

Вопрос о существовании собственных значений, а значит и собственных подпространств, — это вопрос о том, имеет ли характеристический многочлен корни в поле $\mathbb{P}$. Мы уже знаем, впрочем, что всегда можно перейти к более широкому полю разложения характеристического многочлена, в котором он будет иметь n корней с учетом кратностей. Довольно естественным образом исходное n -мерное пространство V можно сделать подмножеством нового n -мерного пространства над этим более широким полем и доопределить действие оператора на новом пространстве.

Задача 208. Пусть A — матрица порядка n и ранга r . Докажите, что матрица $I + A$ имеет собственное значение 1 алгебраической кратности не меньше $n - r$.

Задача 209. Матрица $A = [a_{ij}]$ порядка n имеет верхний почти треугольный вид, т.е. $a_{ij} = 0$ при $i > j + 1$. Кроме того, $a_{i+1,i} \neq 0$ при $1 \leq i \leq n - 1$. Докажите, что если матрица A диагонализуема, то она имеет n попарно различных собственных значений.

Задача 210. Докажите, что диагонализуемая матрица ранга r обладает ненулевым главным минором порядка r .

Задача 211. Комплексная матрица A порядка n обратима, совпадает со своей сопряженной матрицей и известно, что окаймляющая ее матрица

$$C = \begin{bmatrix} A & B \\ B^* & 0 \end{bmatrix}, \quad B \in \mathbb{C}^{n \times r}$$

также является обратимой. Докажите, что матрица $B^* A^{-1} B$ обратима и матрица

$$D := \begin{bmatrix} A^{-1} & 0 \\ 0 & (B^* A^{-1} B)^{-1} \end{bmatrix} C$$

имеет собственные значения 1 и $(1 \pm \sqrt{5})/2$ алгебраической кратности $n - r$ и r соответственно.

Задача 212. Пусть λ — собственное значение матрицы $A \in \mathbb{C}^{n \times n}$. Докажите, что

$$\left| \lambda - \frac{\operatorname{tr} A}{n} \right|^2 \leq \frac{n-1}{n} \sum_{i=1}^n \sum_{j=1}^n \left| a_{ij} - \frac{\operatorname{tr} A}{n} \right|^2.$$

Задача 213. Все элементы матрицы $A \in \mathbb{R}^{n \times n}$ неотрицательны, а суммы элементов в каждой строке одинаковы и равны λ . Докажите, что λ является наибольшим по модулю собственным значением матрицы A .

Задача 214. Придумайте, как найти алгебраические кратности собственных значений комплексной матрицы, не вычисляя сами собственные значения. Докажите, что это можно сделать за конечное число арифметических операций.

5.6. Теорема Шура и нормальные матрицы

Здесь мы получим еще одно достаточное условие диагонализуемости, применяемое для *комплексных матриц*. Оно имеет вид $AA^* = A^*A$ — матрица коммутирует со своей сопряженной матрицей. Такие комплексные матрицы называются *нормальными*. То, что из нормальности следует диагонализуемость, не так уж и очевидно и в действительности связано с рядом важных понятий линейной алгебры. Мы докажем, что любая нормальная матрица *унитарно подобна* диагональной матрице (подобие реализуется с помощью унитарной матрицы).

Пусть V — комплексное пространство, для любой пары векторов $x, y \in V$ определено комплексное число (x, y) и при этом имеют место такие свойства:

- $(x, x) \geq 0 \quad \forall x \in V$ и $(x, x) = 0 \Leftrightarrow x = 0$;
- $(x, y) = \overline{(y, x)} \quad \forall x, y \in V$ (черта означает комплексное сопряжение);
- $(x + y, z) = (x, z) + (y, z) \quad \forall x, y, z \in V$;
- $(\alpha x, y) = \alpha (x, y) \quad \forall x, y \in V, \forall \alpha \in \mathbb{C}$.

В таких случаях число (x, y) называется *скалярным произведением* векторов x и y . Величина $\|x\| := \sqrt{(x, x)}$ называется *длиной* вектора x . Кроме того, скалярное произведение дает возможность ввести абстрактное понятие ортогональности векторов: $x, y \in V$ называются *ортогональными*, если $(x, y) = 0$ — в этом

случае пишем $x \perp y$. Вектор x называется *ортгогональным* множеству $L \subseteq V$, если x ортгогонален любому вектору из L .

Пример 1. Формула $(x, y) := y^*x$ задает *естественное скалярное произведение* векторов $x, y \in \mathbb{C}^n$.

Пример 2. Пусть $H \in \mathbb{C}^{n \times n}$ и $H = H^*$ — такая матрица называется *самосопряженной* или *эрмитовой*. Кроме того, пусть в естественном скалярном произведении имеет место неравенство $(Hx, x) = x^*Hx > 0$ для любого ненулевого вектора $x \in \mathbb{C}^n$ — такая матрица называется *положительно определенной*. В этом случае правило $(x, y)_H := y^*Hx$ задает некоторое скалярное произведение на $\mathbb{C}^n$. Более того, можно даже доказать, что *любое* скалярное произведение на $\mathbb{C}^n$ представляется в таком виде с некоторой положительно определенной матрицей H .

Система векторов $q_1, \dots, q_k \in V$ называется *ортонормированной*, если $(q_i, q_j) = 0$ при $i \neq j$ и 1 при $i = j$. Если $q_1, \dots, q_k$ — векторы-столбцы из пространства $\mathbb{C}^n$ с естественным скалярным произведением, то ортонормированность равносильна матричному равенству

$$Q_k^* Q_k = I_k, \quad \text{где } Q_k = [q_1, \dots, q_k].$$

Матрица $Q \in \mathbb{C}^{n \times n}$ со свойством $Q^*Q = I$ называется *унитарной*, а если ее элементы вещественны — *ортгогональной*.

Примеры унитарных матриц.

1. Зафиксируем индексы $1 \leq k < l \leq n$ и построим матрицу, которая отличается от единичной матрицы I_n лишь в позициях $(kk), (kl), (lk), (ll)$ — там размещается блок вида

$$R(\phi) = \begin{bmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{bmatrix}, \quad \phi \in \mathbb{R}.$$

Такая матрица является ортгогональной при любом выборе ϕ и называется *матрицей вращения*. Преобразование $x \rightarrow R(\phi)x$ действительно поворачивает вектор $x \in \mathbb{R}^2$ на угол ϕ против часовой стрелки.

2. Матрица $Q := I_n - 2uu^*$, где $u \in \mathbb{C}^n$ и $u^*u = 1$, унитарна и называется *матрицей отражения* (относительно подпространства $L := \{x \in \mathbb{C}^n : u^*x = 0\}$).

3. Пусть $\varepsilon \in \mathbb{C}$ — первообразный корень степени n из единицы. Матрица вида

$$F_n = \begin{bmatrix} \varepsilon^{0 \cdot 0} & \varepsilon^{0 \cdot 1} & \dots & \varepsilon^{0 \cdot (n-1)} \\ \varepsilon^{1 \cdot 0} & \varepsilon^{1 \cdot 1} & \dots & \varepsilon^{1 \cdot (n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \varepsilon^{(n-1) \cdot 0} & \varepsilon^{(n-1) \cdot 1} & \dots & \varepsilon^{(n-1) \cdot (n-1)} \end{bmatrix}$$

называется *матрицей Фурье* порядка n . Унитарной является матрица $Q := \frac{1}{\sqrt{n}} F_n$.

Теорема 5.6.1 (ПРОЦЕСС ОРТОГОНАЛИЗАЦИИ ГРАМ–ШМИДТА). Пусть V — пространство со скалярным произведением и векторы $x_1, \dots, x_k \in V$ линейно независимы. Тогда существует ортонормированная система векторов $q_1, \dots, q_k$, для которых $\langle q_l, \dots, q_l \rangle = \langle x_1, \dots, x_l \rangle$ при $1 \leq l \leq k$.

Доказательство. Положим $q_1 := x_1 / \|x_1\|$. Далее, пусть уже определены векторы $q_1, \dots, q_l$. Если $l < k$, то q_{l+1} получается следующим образом:

$$p_{l+1} = x_l - \sum_{i=1}^l \langle x_l, q_i \rangle q_i, \quad q_{l+1} := p_{l+1} / \|p_{l+1}\|. \quad \square$$

Следствие 5.6.1. Любую ортонормированную систему в конечномерном пространстве со скалярным произведением можно достроить до ортонормированного базиса.

Следствие 5.6.2 (ТЕОРЕМА О ПЕРПЕНДИКУЛЯРЕ). Пусть в комплексном или вещественном линейном пространстве V введено скалярное произведение и L — произвольное конечномерное подпространство. Тогда для любого вектора $x \in V$ существуют единственные векторы $z \in L$ и $h \perp L$ такие, что $x = z + h$.

Вектор z называется *ортогональной проекцией* вектора x на подпространство L , а вектор h — *перпендикуляром*, опущенным из вектора x на подпространство L .

Следствие 5.6.3. Любую невырожденную матрицу $A \in \mathbb{C}^{n \times n}$ можно представить в виде $A = QR$, где матрицы Q и R соответственно унитарная и верхняя треугольная.

Теорема 5.6.2 (ТЕОРЕМА ШУРА). Для любой матрицы $A \in \mathbb{C}^{n \times n}$ существует унитарная матрица Q , для которой матрица $T := Q^{-1}AQ$ будет верхней треугольной.

Доказательство. Проведем индукцию по n . Для этого выберем произвольный собственный вектор p_1 длины 1 (в естественном скалярном произведении) и, согласно следствию 5.6.1, построим содержащий его ортонормированный базис $p_1, p_2, \dots, p_n$. Матрица $P = [p_1, \dots, p_n]$ будет унитарной. Пусть $Ap_1 = \lambda_1 p_1$. Тогда, очевидно,

$$P^{-1}AP = \begin{bmatrix} \lambda_1 & b \\ 0 & A_1 \end{bmatrix}, \quad b \in \mathbb{C}^{1 \times (n-1)}, \quad A_1 \in \mathbb{C}^{(n-1) \times (n-1)}.$$

Согласно индуктивному предположению, $T_1 = P_1^{-1}A_1P_1$ имеет верхний треугольный вид для некоторой унитарной матрицы P_1 порядка $n-1$. Пусть

$$T := Q^{-1}AQ, \quad Q := P \begin{bmatrix} 1 & 0 \\ 0 & P_1 \end{bmatrix}.$$

Легко проверяется, что T — верхняя треугольная матрица, а Q — унитарная. $\square$

Теорема 5.6.3. *Комплексная $n \times n$ -матрица A является нормальной тогда и только тогда, когда она имеет вид $A = Q\Lambda Q^{-1}$, где комплексные матрицы Λ и Q являются соответственно диагональной и унитарной.*

Доказательство. Если $A = Q\Lambda Q^{-1}$, то нормальность очевидна. Если матрица A нормальная, то применяем теорему Шура и получаем верхнюю треугольную матрицу $T = Q^{-1}AQ$, которая в силу унитарности матрицы Q также является нормальной. Остается лишь убедиться в том, что верхняя треугольная матрица является нормальной в том и только том случае, когда она диагональная. $\square$

Следствие 5.6.4. *Любая нормальная матрица является диагонализуемой.*

Задача 215. Докажите, что нормальность комплексной матрицы A равносильна существованию комплексного многочлена $f(\lambda)$, для которого $A^* = f(A)$.

Задача 216. Докажите, что для любой матрицы $A \in \mathbb{C}^n$ существует однозначно определенное разложение $A = H_1 + iH_2$, где матрицы H_1 и H_2 эрмитовы.

Задача 217. Докажите, что из положительной определенности комплексной матрицы следует ее эрмитовость.

Задача 218. Докажите, что для любой эрмитовой матрицы H матрица $Q = (I - iH)^{-1}(I + iH)$ является унитарной.

Любую ли унитарную матрицу можно представить в таком виде?

Задача 219. Дана вещественная симметричная матрица A . Докажите, что существует ортогональная матрица Q , для которой главная диагональ матрицы QAQ^{-1} состоит из одинаковых элементов.

Задача 220. Пусть F_n — матрица Фурье порядка n . Докажите, что столбцы матрицы $Q = \frac{1}{\sqrt{n}} F_n$ образуют ортонормированный базис из собственных векторов для любой циркулянтной матрицы, т.е. матрицы вида

$$A = \begin{bmatrix} a_0 & a_{n-1} & \dots & a_2 & a_1 \\ a_1 & a_0 & \dots & a_3 & a_2 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n-2} & a_{n-3} & \dots & a_0 & a_{n-1} \\ a_{n-1} & a_{n-2} & \dots & a_1 & a_0 \end{bmatrix} \in \mathbb{C}^{n \times n}.$$

5.7. Сингулярное разложение

Изученные нами свойства нормальных и, в особенности, эрмитовых матриц позволяют получить одно из самых популярных матричных разложений — *сингулярное разложение* комплексной матрицы. Оно является специальным случаем скелетного разложения комплексной матрицы (см. раздел 1.10).

Пусть дана матрица $A \in \mathbb{C}^{m \times n}$, $\sigma_1, \dots, \sigma_r$ — неотрицательные вещественные числа и каждая из систем векторов $u_1, \dots, u_r \in \mathbb{C}^n$ и $v_1, \dots, v_r \in \mathbb{C}^m$ ортонормирована в естественном скалярном произведении пространств $\mathbb{C}^n$ и $\mathbb{C}^m$. Представление матрицы в виде

$$A = \sum_{k=1}^r \sigma_k v_k u_k^* = V_r \Sigma_r U_r^*,$$

$$V_r = [v_1, \dots, v_r], \quad \Sigma_r = \begin{bmatrix} \sigma_1 & & \\ & \ddots & \\ & & \sigma_r \end{bmatrix}, \quad U_r = [u_1, \dots, u_r],$$

называется *сингулярным разложением* матрицы A . Число σ_k называется *k -м сингулярным числом*, u_k — соответствующим ему *правым* и v_k — *левым сингулярным вектором*.

Предположим, что имеется сингулярное разложение $A = V_r \Sigma_r U_r^*$. Мы знаем, что любую ортонормированную систему

можно достроить до ортонормированного базиса. Поэтому существуют унитарные матрицы вида $U = [U_r, \hat{U}]$ и $V = [V_r, \hat{V}]$, в которых первые r столбцов те же, что в матрицах U_r и V_r . Далее, из равенства $A = V_r \Sigma_r U_r^*$ выводим

$$A = [V_r, \hat{V}] \begin{bmatrix} \Sigma_r U^* \\ 0_{(m-r) \times r} \end{bmatrix} = [V_r, \hat{V}] \begin{bmatrix} \Sigma_r & 0_{r \times (n-r)} \\ 0_{(m-r) \times r} & 0_{(m-r) \times (n-r)} \end{bmatrix} \begin{bmatrix} U_r^* \\ \hat{U}^* \end{bmatrix} = V \Sigma U^*.$$

Отсюда следует, что *число ненулевых сингулярных чисел равно рангу матрицы A* .

Полученное нами разложение $A = V \Sigma U^*$ также называется *сингулярным разложением* или *полным сингулярным разложением* матрицы A . Поскольку порядок слагаемых в сумме может быть произвольным, их всегда можно расположить по невозрастанию сингулярных чисел. При стандартной нумерации

$$\sigma_1 \geq \dots \geq \sigma_{r_0} > \sigma_{r_0+1} = \dots = \sigma_r = 0, \quad r_0 = \text{rank } A,$$

первые $r_0 = \text{rank } A$ столбцов унитарных матриц U и V составлены из правых и левых сингулярных векторов, отвечающих ненулевым сингулярным числам. Наибольшее сингулярное число называется *старшим*. Понятно также, что матрица будет той же, если мы уберем слагаемые с нулевыми сингулярными числами.

Теорема 5.7.1. *Для любой комплексной матрицы A существует сингулярное разложение $A = V_r \Sigma_r U_r^*$, в котором все сингулярные числа отличны от нуля и их число r равно рангу матрицы A .*

Доказательство. Пусть $A \in \mathbb{C}^{m \times n}$ и $r = \text{rank } A$. Запишем скелетное разложение матрицы A в виде

$$A = B_1 B_2^*, \quad B_1 \in \mathbb{C}^{m \times r}, \quad B_2 \in \mathbb{C}^{n \times r}.$$

Столбцы матриц B_1 и B_2 линейно независимы. Проведя их ортогонализацию, получаем разложения $B_1 = Q_1 R_1$ и $B_2 = Q_2 R_2$, где столбцы матриц Q_1 и Q_2 ортонормированы, а R_1 и R_2 — невырожденные матрицы порядка r . Таким образом, $A = Q_1 R Q_2^*$, где $R = R_1 R_2^*$ — невырожденная матрица порядка r .

Матрица $R^* R$ эрмитова, и ее собственные значения положительны. Эрмитовость: $(R^* R)^* = R^* (R^*)^* = R^* R$. Положительность собственных значений:

$$R^* R x = \lambda x, \quad x \neq 0 \Rightarrow \lambda(x, x) = (R^* R x, x) = (R x, R x) \geq 0,$$

равенство нулю невозможно, так как $Rx \neq 0$ при $x \neq 0$ в силу невырожденности матрицы R . Пусть столбцы матрицы Q образуют ортонормированный базис из собственных векторов матрицы R^*R для собственных значений $\lambda_1 \geq \dots \geq \lambda_r > 0$. Тогда Q — унитарная матрица порядка r и выполняется равенство

$$R^*R = Q\Sigma_r^2Q^*, \quad \Sigma_r = \begin{bmatrix} \sqrt{\lambda_1} & & \\ & \ddots & \\ & & \sqrt{\lambda_r} \end{bmatrix} \Rightarrow$$

$$\Rightarrow \underbrace{((R^{-1})^*Q\Sigma_r)}_{=Z} \underbrace{(\Sigma_rQ^*R^{-1})}_{=Z^*} = I_r \Rightarrow R = Z\Sigma_rQ^*, \quad ZZ^* = I_r.$$

Следовательно,

$$A = \underbrace{Q_1Z}_{=V_r} \Sigma_r \underbrace{Q^*Q_2^*}_{U_r^*} = V_r\Sigma_rU_r^*.$$

Несложно проверяется, что столбцы матриц $V_r := Q_1Z$ и $U_r = Q_2Q$ ортонормированы. $\square$

Следствие 5.7.1. Для любой матрицы $A \in \mathbb{C}^{m \times n}$ ранга r существует разложение

$$A = V\Sigma U^*,$$

где матрицы $U \in \mathbb{C}^{n \times n}$ и $V \in \mathbb{C}^{m \times m}$ унитарные, а матрица Σ имеет вид

$$\Sigma = \begin{bmatrix} \Sigma_r & 0_{r \times (n-r)} \\ 0_{(m-r) \times r} & 0_{(m-r) \times (n-r)} \end{bmatrix}, \quad \Sigma_r = \begin{bmatrix} \sigma_1 & & \\ & \ddots & \\ & & \sigma_r \end{bmatrix},$$

$$\sigma_1 \geq \dots \geq \sigma_r > 0.$$

Следствие 5.7.2. Ненулевые сингулярные числа однозначно определяются по матрице A и совпадают с корнями квадратными из ненулевых собственных значений каждой из эрмитовых матриц A^*A и AA^* .

Доказательство. Пусть $A = V\Sigma U^*$ — полное сингулярное разложение матрицы A . Тогда, очевидно, $A^*A = U\Sigma^2U^* = U\Sigma^2U^{-1} \Rightarrow$ первые $r = \text{rank } A$ столбцов матрицы U представляют собой собственные векторы матрицы A^*A , соответствующие ее ненулевым собственным значениям. Аналогично, $AA^* = V\Sigma^2V^* = V\Sigma^2V^{-1} \Rightarrow$ первые r столбцов матрицы V суть

собственные векторы для ненулевых собственных значений матрицы AA^* . Обратим внимание на то, что A^*A и AA^* — эрмитовы матрицы с неотрицательными собственными значениями. $\square$

Следствие 5.7.3. Пусть $u_1, \dots, u_m$ и $v_1, \dots, v_n$ — столбцы матриц U и V из полного сингулярного разложения $A = V\Sigma U^*$, и предположим, что ранг матрицы A равен r и ненулевыми являются первые r сингулярных чисел. Тогда

$$Au_k = \begin{cases} \sigma_k v_k, & 1 \leq k \leq r, \\ 0, & r+1 \leq k \leq n, \end{cases} \quad A^*v_k = \begin{cases} \sigma_k u_k, & 1 \leq k \leq r, \\ 0, & r+1 \leq k \leq m. \end{cases}$$

Следствие 5.7.4.

$$\ker A = \langle u_{r+1}, \dots, u_n \rangle, \quad \operatorname{im} A = \langle v_1, \dots, v_r \rangle,$$

$$\ker A^* = \langle v_{r+1}, \dots, v_m \rangle, \quad \operatorname{im} A^* = \langle u_1, \dots, u_r \rangle.$$

Подпространства L и M пространства, в котором введено скалярное произведение, называются *ортогональными*, если $(x, y) = 0$ для любого $x \in L$ и любого $y \in M$.

Следствие 5.7.5. Пространства $\ker A$ и $\operatorname{im} A^*$ и пространства $\ker A^*$ и $\operatorname{im} A$ — это две пары ортогональных подпространств в естественном скалярном произведении пространств $\mathbb{C}^n$ и $\mathbb{C}^m$. При этом

$$\mathbb{C}^n = \ker A \oplus \operatorname{im} A^*, \quad \mathbb{C}^m = \ker A^* \oplus \operatorname{im} A.$$

Следствие 5.7.6 (альтернатива Фредгольма). Рассматривается система линейных алгебраических уравнений с комплексной матрицей A . Либо система имеет решение при любой правой части, либо сопряженная однородная система $A^*y = 0$ имеет нетривиальное решение.

Следствие 5.7.7. Пусть матрица A порядка n невырождена и ее сингулярное разложение имеет вид $A = \sum_{k=1}^n \sigma_k v_k u_k^*$.

Тогда $A^{-1} = \sum_{k=1}^n \frac{1}{\sigma_k} u_k v_k^*$ — сингулярное разложение обратной матрицы.

Величина

$$\|A\| := \max_{x \neq 0} \frac{\|Ax\|}{\|x\|}$$

называется *спектральной нормой* матрицы A . Напомним, что $\|x\|$ — это длина вектора x в естественном скалярном произведении: по определению $\|x\| = \sqrt{(x, x)}$.

Утверждение 5.7.1. *Спектральная норма матрицы равна ее старшему сингулярному числу.*

Доказательство. Рассмотрим полное сингулярное разложение $A = V\Sigma U^*$ и заметим, что длина вектора сохраняется при его умножении на любую унитарную матрицу. После этого остается проверить равенство $\|\Sigma\| = \sigma_1$, где σ_1 — старшее сингулярное число. $\square$

Утверждение 5.7.2. *Пусть $A = \sum_{l=1}^r \sigma_l v_l u_l^*$ — сингулярное разложение, в котором сингулярные числа упорядочены по невозрастанию, и при $1 \leq k < r$ рассматриваются матрицы $A_k := \sum_{l=1}^k \sigma_l v_l u_l^*$. Тогда $\|A - A_k\| = \sigma_{k+1}$.*

Если $r = \text{rank } A$, то, очевидно, ранг матрицы A_k равен k . Таким образом, A_k может рассматриваться как приближение ранга $k < r$ к матрице A ранга r . Утверждение 5.7.2 дает нам погрешность данного приближения. Доказательство элементарно и предоставляется читателю. В действительности можно доказать очень важное и содержательное дополнение к данному утверждению.

Теорема 5.7.2. *Пусть $\sigma_1 \geq \dots \geq \sigma_r > 0$ — ненулевые сингулярные числа матрицы A ранга r . Тогда $\|A - B\| \geq \sigma_{k+1}$ для любой матрицы B ранга не выше $k < r$.*

Доказательство. Пусть $A = V\Sigma U^*$ — полное сингулярное разложение комплексной матрицы A размера $m \times n$. Нам нужны столбцы матриц $U = [u_1, \dots, u_n]$ и $V = [v_1, \dots, v_m]$ и подпространство $L := \langle u_1, \dots, u_{k+1} \rangle$. В силу теоремы Грассмана

$$\begin{aligned} \dim L \cap \ker B &= \dim L + \dim \ker B - \dim (L + \ker B) \geq \\ &\geq (k+1) + (n-k) - n \geq 1. \end{aligned}$$

Следовательно, имеется ненулевой вектор $z \in L \cap \ker B$. Тогда

$$\|A - B\| \geq \frac{\|(A - B)z\|}{\|z\|} = \frac{\|Az\|}{\|z\|} \geq \min_{0 \neq x \in L} \frac{\|Ax\|}{\|x\|} = \sigma_{k+1}.$$

Поясним последнее равенство:

$$\begin{aligned} x \in L \Rightarrow x = \sum_{i=1}^{k+1} \xi_i u_i \Rightarrow Ax = \sum_{i=1}^{k+1} \xi_i \sigma_i v_i \Rightarrow \\ \Rightarrow \frac{\|Ax\|^2}{\|x\|^2} = \frac{\sum_{i=1}^{k+1} \sigma_i^2 |\xi_i|^2}{\sum_{i=1}^{k+1} |\xi_i|^2} \geq \sigma_{k+1}^2. \end{aligned}$$

Чтобы получить равенство, можно взять $\xi_1 = \dots = \xi_k = 0$ и $\xi_{k+1} = 1$. $\square$

Сингулярное разложение квадратной матрицы порядка n тесно связано с еще одним интересным разложением. Перепишав полное сингулярное разложение в виде

$$A = V \Sigma U^* = \underbrace{(V \Sigma V^*)}_{=H} \underbrace{(V U^*)}_{=Q} = H Q,$$

мы получаем равенство $A = H Q$, в котором H — эрмитова матрица с неотрицательными собственными значениями, Q — унитарная матрица. Такое разложение называется *полярным разложением*. Если $n = 1$, то оно равносильно представлению комплексного числа в тригонометрической форме.

Задача 221. Пусть $A \in \mathbb{C}^{m \times n}$, $r = \text{rank } A$ и выполняются равенства $A U_r = V_r \Sigma_r$, $A^* V_r = U_r \Sigma_r$, где матрицы $U_r \in \mathbb{C}^{n \times r}$ и $V_r \in \mathbb{C}^{m \times r}$ имеют ортонормированные столбцы и Σ_r — диагональная матрица порядка r с положительными числами на главной диагонали. Верно ли, что $A = V_r \Sigma_r U_r^*$?

Задача 222. Пусть $A = A^\top$ — симметричная комплексная матрица. Докажите, что полное сингулярное разложение для нее можно найти в виде $A = V \Sigma V^\top$, где V — унитарная матрица и Σ — диагональная матрица с неотрицательными элементами.

Задача 223. Пусть A — $m \times n$ -матрица ранга r и $A = \sum_{k=1}^r \sigma_k v_k u_k^*$ — ее сингулярное разложение. Докажите, что для любого вектора $b \in \mathbb{C}^m$ вектор

$$z = \sum_{k=1}^r \frac{(b, v_k)}{\sigma_k} u_k$$

имеет наименьшую длину среди всех векторов y таких, что ¹⁾

$$\|b - Ay\| = \min_{x \in \mathbb{C}^n} \|b - Ax\|.$$

Задача 224. Пусть λ — наибольшее по модулю собственное значение ²⁾ матрицы $A \in \mathbb{C}^{n \times n}$. Докажите, что $|\lambda| = \lim_{k \rightarrow \infty} \|A^k\|^{1/k}$.

5.8. Инвариантные пространства и прямая сумма операторов

Подпространство L линейного пространства V называется *инвариантным пространством* относительно оператора $A: V \rightarrow V$, если $AL \subseteq L$.

Инвариантность означает, что любой вектор из L при действии на него оператором A переходит в вектор, также принадлежащий L . Это дает возможность рассматривать тот же оператор на более узком множестве, а именно на подпространстве L . Оператор $B: L \rightarrow L$ называется *сужением оператора A на подпространство L* или *индуцированным оператором*, если $Bx = Ax$ для любого вектора $x \in L$. Обозначение: $B = A|_L$.

Очевидно, любое собственное подпространство является инвариантным. Еще два важных примера — это ядро и образ линейного оператора A :

$$\ker A := \{x \in V : Ax = 0\},$$

$$\operatorname{im} A = AV := \{y \in V : \exists x \in V, y = Ax\}.$$

Эти подпространства порождают целое семейство примеров.

Утверждение 5.8.1. Для произвольного линейного оператора $A: V \rightarrow V$ и произвольного многочлена $f(\lambda)$ ядро $\ker f(A)$ и образ $\operatorname{im} f(A)$ являются подпространствами, инвариантными относительно A .

Доказательство. Инвариантность следует из того, что оператор A коммутирует с оператором $f(A)$. Для ядра: если

¹⁾ Такие векторы y называются псевдорешениями системы $Ax = b$, которая может и не иметь решений. Псевдорешение наименьшей длины называется нормальным псевдорешением.

²⁾ В этом случае величина $|\lambda|$ называется спектральным радиусом матрицы A .

$f(A)x = 0$, то $f(A)Ax = A(f(A)x) = 0$. Для образа: если $y = f(A)x$, то $Ay = Af(A)x = f(A)(Ax)$. $\square$

Теперь предположим, что пространство $V = V_1 \oplus \dots \oplus V_s$ является прямой суммой своих подпространств $V_1, \dots, V_s$. Напомним, что в этом случае любой вектор из V однозначно раскладывается по подпространствам $V_1, \dots, V_s$. Предположим, что заданы линейные операторы $A_i: V_i \rightarrow V_i$, и пусть оператор A действует на V по следующему правилу:

$$x = x_1 + \dots + x_s, \quad x_i \in V_i \Rightarrow Ax := A_1x_1 + \dots + A_sx_s.$$

Легко видеть, что A — корректно определенный линейный оператор на пространстве V , а подпространства $V_1, \dots, V_s$ являются для него инвариантными. Такой оператор A называется *прямой суммой операторов* $A_1, \dots, A_s$. Обозначение: $A = A_1 \oplus \dots \oplus A_s$.

Прямой суммой матриц $A_1, \dots, A_s$ называется блочная матрица вида

$$A = A_1 \oplus \dots \oplus A_s := \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_s \end{bmatrix}.$$

Лемма 5.8.1. *Предположим, что многочлен $f(\lambda)$ допускает разложение $f(\lambda) = f_1(\lambda)f_2(\lambda)$ с взаимно простыми множителями. Тогда*

$$\ker f(A) = \ker f_1(A) \oplus \ker f_2(A).$$

Кроме того, сужения $f_1(A)|_{\ker f_2(A)}$ и $f_2(A)|_{\ker f_1(A)}$ являются обратимыми операторами соответственно на подпространствах $\ker f_2(A)$ и $\ker f_1(A)$.

Доказательство. Из взаимной простоты выводится существование многочленов $g_1(\lambda), g_2(\lambda)$ таких, что $f_1(\lambda)g_1(\lambda) + f_2(\lambda)g_2(\lambda) = 1 \Rightarrow f_1(A)g_1(A) + f_2(A)g_2(A) = I$. Отсюда для любого вектора x получаем

$$x = x_1 + x_2, \quad x_1 = f_2(A)g_2(A)x, \quad x_2 = f_1(A)g_1(A)x.$$

Если $x \in \ker f(A)$, то, очевидно, $f_1(A)x_1 = 0$ и $f_2(A)x_2 = 0$. Значит, $\ker f(A) = \ker f_1(A) + \ker f_2(A)$. Пересечение ядер является нулевым подпространством:

$$x \in \ker f_1(A) \cap \ker f_2(A) \Rightarrow x = g_1(A)f_1(A)x + g_2(A)f_2(A)x = 0.$$

Поэтому сумма ядер — прямая, а операторы $f_1(A)|_{\ker f_2(A)}$ и $f_2(A)|_{\ker f_1(A)}$ имеют нулевые ядра и, следовательно, обратимы. $\square$

Заметим, что лемма включает и малоинтересный случай — когда $\ker f(A) = 0$. Тем не менее она приводит к нетривиальным разложениям при разумном выборе многочлена $f(\lambda)$, например таком, как в следующей лемме.

Лемма 5.8.2. Пусть многочлен $f(\lambda) = f_1(\lambda)f_2(\lambda)$ является характеристическим многочленом линейного оператора A и множители $f_1(\lambda)$ и $f_2(\lambda)$ взаимно просты. Тогда A есть прямая сумма сужений $A_1 = A|_{\ker f_1(A)}$ и $A_2 = A|_{\ker f_2(A)}$ и при этом характеристические многочлены операторов A_1 и A_2 с точностью до ненулевых множителей совпадают соответственно с $f_1(\lambda)$ и $f_2(\lambda)$.

Доказательство. Равенство $A = A_1 \oplus A_2$ вытекает из леммы 5.8.1. Матрица оператора A в базисе, составленном из базисов подпространств $\ker f_1(A)$ и $\ker f_2(A)$, имеет блочный вид

$$[A] = \begin{bmatrix} [A_1] & \\ & [A_2] \end{bmatrix}.$$

Поэтому характеристический многочлен для A является произведением характеристических многочленов для A_1 и A_2 . Обозначив их через $F_1(\lambda)$ и $F_2(\lambda)$, находим $f(\lambda) = f_1(\lambda)f_2(\lambda) = F_1(\lambda)F_2(\lambda)$. Далее, матрицу $[A]$ можно рассматривать как матрицу над полем, содержащим поле разложения многочлена $f(\lambda)$, и считать, что это матрица оператора на пространстве над этим полем. Пусть λ_i — произвольный корень многочлена $F_i(\lambda)$, а значит и некоторое собственное значение оператора A . Пусть x_i — соответствующий ему собственный вектор из подпространства $\ker f_i(A)$. Тогда

$$Ax_i = \lambda_i x_i \Rightarrow 0 = f_i(A)x_i = f_i(\lambda_i)x_i \Rightarrow f_i(\lambda_i) = 0.$$

Отсюда вытекает взаимная простота многочленов $f_1(\lambda)$ и $F_2(\lambda)$ и многочленов $f_2(\lambda)$ и $F_1(\lambda)$. Следовательно, $f_1(\lambda) : F_1(\lambda)$, $f_2(\lambda) : F_2(\lambda) \Rightarrow \deg F_1(\lambda) \leq \deg f_1(\lambda)$, $\deg F_2(\lambda) \leq \deg f_2(\lambda)$. Кроме того, $\deg f_1(\lambda) + \deg f_2(\lambda) = \deg F_1(\lambda) + \deg F_2(\lambda) \Rightarrow \deg f_1(\lambda) = \deg F_1(\lambda)$ и $\deg f_2(\lambda) = \deg F_2(\lambda)$. $\square$

Теорема 5.8.1. *Предположим, что приведенный характеристический многочлен линейного оператора A на n -мерном пространстве над полем $\mathbb{P}$ имеет вид*

$$f(\lambda) = \prod_{i=1}^s f_i(\lambda), \quad f_i(\lambda) = (\lambda - \lambda_i)^{k_i},$$

где $\lambda_1, \dots, \lambda_s \in \mathbb{P}$ — попарно различные собственные значения алгебраических кратностей $k_1, \dots, k_s$ соответственно. Тогда пространство V расщепляется в прямую сумму инвариантных относительно A подпространств $V_i = \ker f_i(A)$ размерности k_i , а оператор A — в прямую сумму операторов на этих подпространствах:

$$V = V_1 \oplus \dots \oplus V_s, \quad V_i = \ker (A - \lambda_i I)^{k_i}, \quad \dim V_i = k_i, \\ A = A_1 \oplus \dots \oplus A_s, \quad A_i = A|_{V_i}, \quad 1 \leq i \leq s. \quad (*)$$

Доказательство. В силу теоремы Кэли–Гамильтона

$$\ker f(A) = V.$$

Чтобы получить разложения, последовательно применяем лемму 5.8.1. Обозначим через W_i сумму подпространств V_j , а через $g_i(\lambda)$ — произведение многочленов $f_j(\lambda)$ при всех $j \neq i$. Тогда многочлены $f_i(\lambda)$ и $g_i(\lambda)$ взаимно просты и $V = V_i \oplus W_i$, где $V_i = \ker f_i(A)$ и $W_i = \ker g_i(A)$. Согласно лемме 5.8.2, $f_i(\lambda)$ — это характеристический многочлен оператора $A_i \Rightarrow \dim V_i = \deg f_i(\lambda) = k_i$. $\square$

Подпространство $V_i = \ker (A - \lambda_i I)^{k_i}$ называется *корневым пространством* для собственного значения λ_i , принадлежащие ему векторы называются *корневыми*. Разложение (*) называется *корневым разложением* оператора A .

Задача 225. Докажите, что для диагонализуемости линейного оператора на комплексном конечномерном пространстве необходимо и достаточно, чтобы для любого собственного значения геометрическая кратность совпадала с алгебраической кратностью.

Задача 226. Найдите все инвариантные подпространства оператора дифференцирования на бесконечномерном пространстве многочленов $\mathbb{P}[\lambda]$ над произвольным полем $\mathbb{P}$.

Задача 227. Комплексные матрицы $A_1, \dots, A_s$ коммутируют, т.е. $A_i A_j = A_j A_i$ при всех $1 \leq i, j \leq s$. Докажите, что эти матрицы имеют общий собственный вектор.

Задача 228. Для матрицы A порядка n имеет место равенство

$$\operatorname{rank}(I - A) = n - \operatorname{rank} A.$$

Докажите, что $A^2 = A$.

5.9. Нильпотентные операторы и корневое разложение

Линейный оператор $A: V \rightarrow V$ называется *нильпотентным*, если $A^k = 0$ для некоторого натурального числа k . Если при этом $A^{k-1} \neq 0$, то k называется *индексом нильпотентности*.

Лемма 5.9.1. Для нильпотентности линейного оператора A на n -мерном пространстве необходимо и достаточно, чтобы он имел нулевое собственное значение алгебраической кратности n .

Первое доказательство. Необходимость: пусть $A^k = 0$ и $Ax = \lambda x$, $x \neq 0$, тогда $\lambda^k x = 0 \Rightarrow \lambda = 0$. Достаточность: если A имеет нулевое собственное значение кратности n , то его характеристический многочлен имеет вид $f_A(\lambda) = (-\lambda)^n$ и по теореме Кэли–Гамильтона $A^n = 0$. $\square$

Второе доказательство. Здесь мы докажем достаточность, не используя теорему Кэли–Гамильтона. Пусть нуль — единственное собственное значение алгебраической кратности n . С помощью индукции по n покажем, что есть базис, в котором оператор A представляется верхней треугольной матрицей с нулевой главной диагональю. Пусть $e_1 \neq 0$ — собственный вектор для нулевого собственного значения. Тогда можно построить базис $e_1, e_2, \dots, e_n$, в котором оператор представляется матрицей вида

$$[A]_e = \begin{bmatrix} 0 & a_{12} & \dots & a_{1n} \\ 0 & & & A_1 \end{bmatrix}.$$

Подматрица A_1 имеет порядок $n - 1$ и нуль является ее собственным значением алгебраической кратности $n - 1$. Поэтому к ней можно применить индуктивное предположение $\Rightarrow$ для некоторой невырожденной матрицы P_1 матрица $B_1 := P_1^{-1} A_1 P_1$ является верхней треугольной с нулевой главной диагональю. Такой же вид будет иметь матрица

$$B := P^{-1} [A]_e P = \begin{bmatrix} 0 & [a_{12}, \dots, a_{1n}] P_1 \\ 0 & B_1 \end{bmatrix}, \quad \text{где} \quad P = \begin{bmatrix} 1 & 0 \\ 0 & P_1 \end{bmatrix}.$$

Непосредственно проверяется, что если верхняя треугольная матрица имеет k нулевых диагоналей начиная с главной и выше, то при умножении ее на B появляется еще одна нулевая диагональ над уже имеющимися $\Rightarrow B^n = 0 \Rightarrow A^n = 0$. $\square$

Теорема 5.9.1. *Любой линейный оператор на конечномерном пространстве является прямой суммой нильпотентного и обратимого операторов.*

Доказательство. Если A — обратимый оператор на n -мерном пространстве V , то в качестве нильпотентного можно взять нулевой оператор, т. е. теорема в этом случае тривиальна. Далее полагаем, что оператор A не является обратимым и, значит, имеет нетривиальное ядро. Рассмотрим цепочку ядер

$$0 \neq \ker A \subsetneq \ker A^2 \subsetneq \dots \subsetneq \ker A^k = \ker A^{k+1}.$$

В конечномерном пространстве размерности не могут расти бесконечно, поэтому равенство ядер k -й и $k+1$ -й степени в какой-то момент неизбежно — пусть оно впервые возникает для k -й степени. Докажем, что $\ker A^l = \ker A^{l+1}$ для всех $l \geq k$. Пусть уже установлено, что $\ker A^{l-1} = \ker A^l$. Пусть

$$x \in \ker A^{l+1} \Rightarrow A^{l+1}x = 0 \Rightarrow A^l(Ax) = 0 \Rightarrow$$

$$\Rightarrow Ax \in \ker A^l = \ker A^{l-1} \Rightarrow A^l x = 0 \Rightarrow x \in \ker A^l.$$

Включение $\ker A^l \subseteq \ker A^{l+1}$ очевидно. Следовательно, $\ker A^l = \ker A^{l+1}$.

Далее, сумма подпространств $\ker A^k$ и $\operatorname{im} A^k$ является прямой. В самом деле, пусть $x \in \ker A^k \cap \operatorname{im} A^k$. Тогда $A^k x = 0$ и $x = A^k y$ для какого-то вектора $y \Rightarrow A^{2k} y = 0 \Rightarrow x = A^k y = 0$. Учитывая, что $\dim \ker A^k + \dim \operatorname{im} A^k = n$, мы приходим к равенству

$$V = \ker A^k \oplus \operatorname{im} A^k.$$

Очевидно, что сужение оператора A на подпространство $\ker A^k$ является нильпотентным оператором индекса k . Обратимость сужения A на подпространство $\operatorname{im} A^k$ следует из тривиальности его ядра: если $A^k x = 0$ и $x \in \operatorname{im} A^k$, то $x = 0$. $\square$

Теорема 5.9.1 дает еще один способ вывести уже известное нам *корневое разложение* линейного оператора A с попарно различными собственными значениями $\lambda_1, \dots, \lambda_s$ и приведенным характеристическим многочленом вида $f(\lambda) = \prod_{i=1}^s (\lambda - \lambda_i)^{k_i}$.

Оператор $A - \lambda_1 I$ имеет нетривиальное ядро и, согласно теореме 5.9.1, мы получаем разложение $V = V_1 \oplus W_1$, в котором подпространства V_1 и W_1 инвариантны относительно $A - \lambda_1 I$ (а значит и относительно A) и при этом сужение оператора $A - \lambda_1 I$ на V_1 нильпотентно, а на W_1 обратимо. Отсюда вытекает, что оператор $A|_{V_1}$ имеет только одно (в общем случае кратное) собственное значение λ_1 и ни одно из собственных значений оператора $A|_{W_1}$ не равно λ_1 . Значит, $k_1 = \dim V_1$.

Если $s \geq 2$, то W_1 — нетривиальное подпространство размерности меньше n , на котором действует оператор $A|_{W_1}$ с характеристическим многочленом вида $f_1(\lambda) = \prod_{i=2}^s (\lambda - \lambda_i)^{k_i}$. Корневое разложение оператора A очевидным образом получается индукцией по n .

В приведенном ранее выводе корневого разложения теорема Кэли–Гамильтона была существенна. В новом рассуждении основной инструмент — это теорема 5.9.1 и лемма 5.9.1. Обратите внимание на второе доказательство леммы — в нем теорема Кэли–Гамильтона не используется. Более того, теперь сама теорема Кэли–Гамильтона может быть получена как следствие теоремы о корневом разложении. Для этого нужно сначала расширить основное поле так, чтобы оно содержало поле разложения характеристического многочлена $f(\lambda)$. Тогда $f(\lambda)$ можно записать в виде $f(\lambda) = \prod_{i=1}^s (\lambda_i - \lambda)^{k_i}$, где $\lambda_1, \dots, \lambda_s$ принадлежат расширенному полю. Далее, произвольный вектор $x \in V$ раскладывается по корневым подпространствам:

$$x = x_1 + \dots + x_s, \quad (A - \lambda_j I)^{k_j} x_j = 0, \quad 1 \leq j \leq s.$$

Для каждой компоненты этого разложения находим

$$\begin{aligned} f(A)x_j &= \prod_{i=1}^s (A - \lambda_i I)^{k_i} x_j = \\ &= \left(\prod_{1 \leq i \leq s, i \neq j} (A - \lambda_i I)^{k_i} \right) (A - \lambda_j I)^{k_j} x_j = 0 \Rightarrow f(A)x = 0. \end{aligned}$$

Задача 229. Линейный оператор A удовлетворяет равенству $A^2 = A$. Найдите его собственные значения и докажите, что он имеет простую структуру.

Задача 230. Докажите, что линейный оператор A является нильпотентным тогда и только тогда, когда $\text{tr } A^k = 0$ для всех $k \in \mathbb{N}$.

Задача 231. Линейные операторы A и B удовлетворяют равенству $AB - BA = A^{2015}$. Докажите, что A является нильпотентным.

5.10. Пространства Крылова и максимальное расщепление

Для заданного линейного оператора очень естественно поставить вопрос о выборе базиса, в котором его матрица получает наиболее простой вид. Чтобы искать решение, нужно, конечно, дать строгое определение понятию «простой вид». Давайте считать, что для заданного оператора это блочно диагональная матрица с максимально возможным числом блоков.

Задача о получении такого представления, очевидно, равносильна поиску расщепления оператора в прямую сумму максимально большого числа операторов, определенных на ненулевых подпространствах. Такое расщепление естественно называть *максимальным расщеплением*. В данном разделе мы дадим решение этой задачи для нильпотентного оператора.

Вообще поиск инвариантных пространств тесно связан с так называемыми *пространствами Крылова*. Эти пространства названы в честь русского морского инженера и математика, генерала флота и академика Алексея Николаевича Крылова, у которого они возникли в 1931 г. в связи с задачей о вычислении характеристического многочлена. *Пространствами Крылова* $L_k(A, x)$ для заданного оператора $A: V \rightarrow V$ и ненулевого заданного вектора $x \in V$ называются подпространства следующего вида:

$$L_k(A, x) := \langle x, Ax, \dots, A^{k-1}x \rangle, \quad k = 1, 2, \dots$$

Это линейные оболочки, натянутые на векторы $x, Ax, \dots, A^{k-1}x$, которые также называются *векторами Крылова*.

Согласно определению, $L_1(A, x) \subseteq L_2(A, x) \subseteq \dots$. Обозначим через d наименьшее натуральное число такое, что $L_d(A, x) = L_{d+1}(A, x)$. Очевидно, d — это наименьшее число, для которого вектор $A^d x$ оказывается линейной комбинацией векторов $x, Ax, \dots, A^{d-1}x$. При этом, конечно,

$$\dim L_k(A, x) = k \text{ при } 1 \leq k \leq d \text{ и } \dim L_k(A, x) = d \text{ при } k \geq d,$$

а пространство L_d является максимальным пространством Крылова, порожденным оператором A и вектором x . Для оператора A оно же, очевидно, является минимальным инвариантным пространством, содержащим вектор x .

Произвольное инвариантное пространство будем называть *нерасщепляемым*, если его нельзя представить в виде прямой суммы ненулевых инвариантных подпространств. Очевидно, каждое подпространство в искомом максимальном расщеплении обязано быть нерасщепляемым.

Лемма 5.10.1. *Для нильпотентного оператора A векторы $x, Ax, \dots, A^{k-1}x$ линейно независимы в том и только том случае, когда они отличны от нуля.*

Доказательство. Предположим, что заданные векторы Крылова ненулевые. Увеличив k (если потребуется), мы можем считать, что $A^k x = 0$. Допустим от противного, что векторы Крылова линейно зависимы и равная нулю нетривиальная линейная комбинация имеет вид

$$\alpha_l A^l x + \alpha_{l+1} A^{l+1} x + \dots + \alpha_{k-1} A^{k-1} x = 0, \quad \alpha_l \neq 0.$$

На обе части действуем оператором $A^{k-1-l} \Rightarrow \alpha_l A^{k-1} x = 0$. Мы получили то, чего быть не может, так как $\alpha_l \neq 0$ и $A^{k-1} x \neq 0$. Противоречие означает, что в случае нильпотентного оператора система ненулевых векторов Крылова линейно независима. $\square$

Лемма 5.10.2. *Для нильпотентного оператора любое максимальное пространство Крылова является нерасщепляемым инвариантным пространством.*

Доказательство. Пусть $L_d(A, x)$ — максимальное пространство Крылова, и пусть $L \subseteq L_d(A, x)$ — ненулевое инвариантное подпространство. Произвольный ненулевой вектор $y \in L$ можно записать в виде

$$y = \alpha_l A^l x + \alpha_{l+1} A^{l+1} x + \dots + \alpha_{d-1} A^{d-1} x, \quad \alpha_l \neq 0.$$

На обе части действуем оператором A^{d-1-l} . Тогда $\alpha_l A^{d-1} x = A^{d-1-l} y \in L \Rightarrow A^{d-1} x \in L$. Таким образом, любое ненулевое инвариантное подпространство содержит ненулевой вектор $A^{d-1} x \Rightarrow$ любая пара ненулевых инвариантных подпространств имеет ненулевое пересечение. $\square$

Лемма 5.10.3. *Пусть A — нильпотентный оператор и $L_{d_1}(A, x_1), \dots, L_{d_s}(A, x_s)$ — максимальные пространства Кры-*

лова. Для того чтобы их сумма была прямой, необходимо и достаточно, чтобы система векторов

$$A^{d_1-1}x_1, \dots, A^{d_s-1}x_s$$

была линейно независимой.

Доказательство. Необходимость очевидна, нетривиальной является только достаточность. Пусть $d = \max_{1 \leq i \leq s} d_i$. Если $d = 1$, то утверждение тривиально.

Проведем индукцию по d и рассмотрим равную нулю линейную комбинацию всех векторов Крылова, образующих данное пространство. Обозначим через $\alpha_1, \dots, \alpha_s$ коэффициенты при векторах $x_1, \dots, x_s$. Подействовав на данную линейную комбинацию оператором A^{d-1} , получаем

$$\alpha_1 A^{d-1}x_1 + \dots + \alpha_s A^{d-1}x_s = \sum_{i: d_i=d} \alpha_i A^{d-1}x_i = 0 \Rightarrow \Rightarrow \alpha_i = 0, \text{ если } d_i = d.$$

Здесь мы используем то, что векторы $A^{d-1}x_i$ из пространств Крылова размерности d образуют подсистему линейно независимой системы $A^{d_1-1}x_1, \dots, A^{d_s-1}x_s$.

Теперь рассмотрим новый набор пространств Крылова, включив в него пространства $L_{d_i}(A, x_i)$ при всех i таких, что $d_i < d$, и пространства $L_{d_i-1}(A, Ax_i)$ при всех i таких, что $d_i = d$. После удаления векторов x_i , для которых $d_i = d$, рассмотренная нами линейная комбинация редуцируется к равной нулю линейной комбинации векторов Крылова нового набора пространств. Это максимальные пространства Крылова, для которых максимальная размерность меньше или равна $d - 1$. Согласно индуктивному предположению они образуют прямую сумму, и поэтому все коэффициенты редуцированной, а значит и исходной, линейной комбинации должны быть нулями. $\square$

Теорема 5.10.1. Любой нильпотентный оператор A на конечномерном пространстве V расщепляется в прямую сумму операторов на максимальных пространствах Крылова и в любом таком расщеплении число n_d пространств размерности d не зависит от метода, которым получено расщепление, и равно

$$n_d = 2 \operatorname{def} A^d - \operatorname{def} A^{d+1} - \operatorname{def} A^{d-1}, \quad d = 1, 2, \dots$$

Доказательство. Пусть нильпотентный оператор A действует на пространстве V . Рассмотрим какие-либо максимальные пространства Крылова

$$L_1 := L_{d_1}(A, x_1), \dots, L_s := L_{d_s}(A, x_s),$$

дающие в сумме (не обязательно прямой!) пространство V . Чтобы получить такие пространства, в качестве начальных векторов $x_1, \dots, x_s$ можно взять, например, произвольный базис пространства V .

Если сумма $V = L_1 + \dots + L_s$ прямая, то нужное нам расщепление уже получено. Если нет, то согласно лемме 5.10.3 векторы $A^{d_1-1}x_1, \dots, A^{d_s-1}x_s$ линейно зависимы. Рассмотрим линейную комбинацию

$$\sum_{1 \leq i \leq s} \alpha_i A^{d_i-1} x_i = 0$$

и среди ее векторов с коэффициентами $\alpha_i \neq 0$ выберем вектор из пространства Крылова наименьшей размерности. Пусть это будет $A^{d_j-1}x_j$. Очевидно,

$$A^{d_j-1}x_j + \sum_{i \neq j, \alpha_i \neq 0} \frac{\alpha_i}{\alpha_j} A^{d_i-1} x_i = 0.$$

Заметим, что линейная оболочка не изменится, если какой-то из системы образующих ее векторов заменить суммой этого вектора и произвольной линейной комбинации остальных векторов системы. Учитывая это наблюдение и применяя его несколько раз, мы заменим векторы $x_j, Ax_j, \dots, A^{d_j-1}x_j$ соответственно на векторы

$$y_0 := x_j + \sum_{i \neq j, \alpha_i \neq 0} \frac{\alpha_i}{\alpha_j} A^{d_i-d_j} x_i,$$

$$y_1 := Ax_j + \sum_{i \neq j, \alpha_i \neq 0} \frac{\alpha_i}{\alpha_j} A^{d_i-d_j+1} x_i,$$

.....

$$y_{d_j-1} := A^{d_j-1}x_j + \sum_{i \neq j, \alpha_i \neq 0} \frac{\alpha_i}{\alpha_j} A^{d_i-d_j+(d_j-1)} x_i = 0$$

и заметим, что $y_0, y_1, \dots, y_{d_j-2}$ образуют последовательность векторов Крылова: $y_1 = Ay_0, y_2 = A^2y_0, \dots, y_{d_j-2} = A^{d_j-2}y_0$. Если $y_0 = 0$, то все они нулевые и пространство V есть сум-

ма меньшего числа максимальных пространств Крылова. Если $y_0 \neq 0$, то $V = L_1 + \dots + L_{j-1} + L'_j + L_{j+1} + \dots + L_s$, где $L'_j := L_d(A, y_0)$ — максимальное пространство Крылова размерности $d = \dim \langle y_0, \dots, y_{d_j-2} \rangle < d_j$. В любом случае мы получаем новое расщепление, в котором сумма размерностей максимальных пространств Крылова уменьшена. Таким образом, всякий раз, когда V представляется суммой максимальных пространств Крылова с суммой размерностей больше, чем $\dim V$, мы можем найти аналогичное расщепление с меньшей суммой размерностей. Очевидно, в какой-то момент сумма размерностей окажется равной $\dim V$. При этом условии сумма пространств будет, конечно, прямой.

Далее, пусть $V = L_{d_1}(A, x_1) \oplus \dots \oplus L_{d_s}(A, x_s)$ — прямая сумма максимальных пространств Крылова и среди них ровно m_d пространств имеют размерность $\geq d$. Докажем, что

$$m_d = \text{def } A^d - \text{def } A^{d-1}.$$

Для этого заметим, что множество $\{A^k x_i : d \leq k \leq d_i - 1, i = 1, \dots, s\}$ состоит из ненулевых векторов, образующих базис пространства $\text{im } A^d$. Число векторов в этом множестве равно

$$\begin{aligned} \text{rank } A^d &= \sum_{i=1}^s l_i, \quad l_i = \max(0, d_i - d) \Rightarrow \\ &\Rightarrow \text{def } A^d = \sum_{i=1}^s (d_i - l_i) \Rightarrow \ker A^d = \langle A^{l_1} x_1, A^{l_1+1} x_1, \dots \\ &\dots, A^{d_1-1} x_1, \dots, A^{l_s} x_s, A^{l_s+1} x_s, \dots, A^{d_s-1} x_s \rangle. \end{aligned}$$

Причина, по которой выполняется последнее равенство: число образующих векторов равно размерности ядра и все они принадлежат ядру оператора A^d . Действительно, если $l_j = d_j - d$, то $A^d A^{l_j} x_j = A^{d+d_j-d} x_j = 0$, а если $l_j = 0$, то это означает, что $d_j < d \Rightarrow A^d A^{l_j} x_j = A^d x_j = 0$. Среди образующих векторов все, кроме, возможно, первых векторов $A^{l_1} x_1, \dots, A^{l_s} x_s$ в последовательностях векторов Крылова, принадлежат пространству $\ker A^{d-1}$. А число тех из них, которые ему не принадлежат, как раз и равно числу пространств Крылова размерности $\geq d$. Пусть M_d — их линейная оболочка. Тогда $\dim M_d = m_d$, $\ker A^d = \ker A^{d-1} \oplus M_d \Rightarrow m_d = \text{def } A^d - \text{def } A^{d-1}$. Чтобы подсчитать, сколько имеется пространств размерности d , нужно из

числа пространств размерности $\geq d$ вычесть число пространств размерности $\geq d+1$:

$$\begin{aligned} n_d = m_d - m_{d+1} &= (\operatorname{def} A^d - \operatorname{def} A^{d-1}) - (\operatorname{def} A^{d+1} - \operatorname{def} A^d) = \\ &= 2 \operatorname{def} A^d - \operatorname{def} A^{d+1} - \operatorname{def} A^{d-1}. \quad \square \end{aligned}$$

Следствие 5.10.1. Для нильпотентного оператора на конечномерном пространстве расщепление в прямую сумму операторов является максимальным тогда и только тогда, когда операторы расщепления определены на максимальных пространствах Крылова.

Доказательство. Достаточно заметить, что если подпространство в прямой сумме не является максимальным пространством Крылова, то оно может быть разложено в нетривиальную прямую сумму таких пространств, а значит, исходное расщепление не было максимальным. Кроме того, число максимальных пространств Крылова в расщеплении не зависит от метода его получения и поэтому совпадает с числом подпространств любого максимального расщепления. $\square$

Задача 232. Пусть A — нильпотентный оператор и для некоторого натурального числа $d \geq 2$ и линейно независимых векторов $y_1, \dots, y_t$ имеет место соотношение

$$\ker A^d = \ker A^{d-1} \oplus \langle y_1, \dots, y_t \rangle.$$

Докажите, что система векторов

$$y_1, Ay_1, \dots, A^{d-1}y_1, \dots, y_t, Ay_t, \dots, A^{d-1}y_t$$

линейно независима.

Задача 233. Докажите, что нет ни одного нильпотентного оператора A на конечномерном пространстве, для которого выполнялись бы равенства

$$\operatorname{def} A = 2, \quad \operatorname{def} A^2 = 4, \quad \operatorname{def} A^3 = 6, \quad \operatorname{def} A^4 = 13.$$

Задача 234. Пусть A — нильпотентный оператор на n -мерном пространстве и $\operatorname{def} A = 1$. Докажите, что при $n \geq 2$ уравнение $X^2 = A$ не имеет решений.

5.11. Жорданова форма

Пусть $A : V \rightarrow V$ — нильпотентный оператор на n -мерном пространстве V . Согласно теореме 5.10.1, пространство V расщепляется в прямую сумму максимальных пространств Крылова

$$V = L_{d_1}(A, x_1) \oplus \dots \oplus L_{d_s}(A, x_s), \quad s = \text{def } A.$$

В базисе, составленном из произвольно выбранных базисов в пространствах Крылова, матрица для A является блочно диагональной. Однако в каждом пространстве Крылова имеется естественный базис, составленный из векторов Крылова:

$$e_1^{(i)} = x_i, \quad e_2^{(i)} = Ax_i, \quad \dots, \quad e_{d_i}^{(i)} = A^{d_i-1}x_i.$$

В таком базисе i -й блок приобретает очень специальный вид

$$B_{d_i} = \begin{bmatrix} 0 & & & \\ 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{bmatrix}_{d_i \times d_i},$$

а матрица для A будет, конечно, прямой суммой таких блоков.

Очевидно, любая перестановка векторов Крылова i -го пространства также дает базис. По традиции особой популярностью пользуется нумерация векторов в обратном порядке:

$$g_1^{(i)} = A^{d_i-1}x_i, \quad g_2^{(i)} = A^{d_i-2}x_i, \quad \dots, \quad g_{d_i-1}^{(i)} = Ax_i, \quad g_{d_i}^{(i)} = x_i.$$

В таком базисе матрица оператора A оказывается прямой суммой блоков вида

$$J_{d_i} = \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ & & & 0 \end{bmatrix} = B_{d_i}^\top.$$

Матрица J_{d_i} называется *жордановым блоком* (нередко также *жордановой клеткой* или *жордановым ящиком*).

Таким образом, мы только что доказали, что в некотором базисе нильпотентный оператор представляется прямой суммой жордановых блоков. Согласно теореме 5.10.1, число жордановых блоков заданного порядка не зависит от метода построения базиса.

Теперь предположим, что A — произвольный линейный оператор с приведенным характеристическим многочленом вида $f(\lambda) = \prod_{i=1}^s (\lambda - \lambda_i)^{k_i}$. Рассмотрим корневое разложение

$$A = A_1 \oplus \dots \oplus A_s, \quad A_i = A|_{V_i}, \quad V_i = \ker(A - \lambda_i I)^{k_i},$$

и заметим, что каждый оператор вида $B_i := (A - \lambda_i I)|_{V_i}$ является нильпотентным и поэтому в некотором базисе представляется прямой суммой жордановых блоков. В этом же базисе оператор $A_i = A|_{V_i}$ есть прямая сумма блоков вида

$$J_d(\lambda) = \begin{bmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \lambda & 1 \\ & & & \lambda \end{bmatrix}_{d \times d}, \quad \lambda = \lambda_i \quad (*)$$

для разных значений d , причем каких именно — зависит только от заданного оператора, но не от метода построения базиса.

Матрица вида $(*)$ также называется *жордановым блоком* или, более точно, *жордановым блоком для собственного значения λ* . Прямая сумма жордановых блоков называется *жордановой формой* или *жордановой матрицей*.

Теорема 5.11.1. Пусть A — произвольный линейный оператор на n -мерном пространстве над полем $\mathbb{P}$, которое содержит поле разложения характеристического многочлена для A . Пусть $\lambda_1, \dots, \lambda_s \in \mathbb{P}$ — все попарно различные собственные значения оператора A . Тогда в некотором базисе оператор A представляется жордановой матрицей и при любом выборе такого базиса число $n_d(\lambda_i)$ жордановых блоков порядка d для собственного значения λ_i равно

$$n_d(\lambda_i) = 2 \operatorname{def}(A - \lambda_i I)^d - \operatorname{def}(A - \lambda_i I)^{d+1} - \operatorname{def}(A - \lambda_i I)^{d-1},$$

$$d = 1, 2, \dots$$

Доказательство. Мы можем использовать базисы для нильпотентных операторов $(A - \lambda_i I)|_{V_i}$, где V_i — корневое подпространство для собственного значения λ_i . Таким образом, теорема с легкостью получается как следствие теоремы 5.8.1 о корневом разложении и теоремы 5.10.1 о расщеплении нильпотентного оператора в прямую сумму операторов на максимальных пространствах Крылова. $\square$

Базис, в котором матрица линейного оператора является прямой суммой жордановых блоков, называется *жордановым базисом*.

Задача 235. Найдите жорданову форму матрицы A^3 , где A — жорданов блок порядка n .

Задача 236. Матрица порядка n коммутирует с жордановым блоком. Докажите, что она не может иметь различных собственных значений.

Задача 237. Докажите, что матрица имеет конечное число инвариантных подпространств в том и только том случае, когда каждому собственному значению соответствует ровно одна жорданова клетка.

5.12. Блочная жорданова форма вещественной матрицы

Пусть A — вещественная матрица порядка n . Ее характеристический многочлен имеет, очевидно, вещественные коэффициенты, и если есть невещественное собственное значение $\lambda = \alpha + i\beta$, где $\alpha, \beta \in \mathbb{R}$ и $\beta \neq 0$, то комплексно сопряженное число $\bar{\lambda} = \alpha - i\beta$ также будет его корнем, а значит, еще одним собственным значением матрицы A , причем той же алгебраической кратности $\Rightarrow$ размерности корневых пространств $\mathcal{K}_\lambda$ и $\mathcal{K}_{\bar{\lambda}}$ соответственно для λ и $\bar{\lambda}$ совпадают, а сами пространства образуют прямую сумму. Кроме того, $\text{def}(A - \lambda I)^l = \text{def}(A - \bar{\lambda} I)^l \forall l \in \mathbb{N} \Rightarrow$ согласно теореме 5.11.1, число жордановых клеток заданного порядка для λ и $\bar{\lambda}$ одно и то же.

Если пространство $\mathcal{K}_\lambda$ имеет жорданов базис

$$x_1 = u_1 + i v_1, \dots, x_m = u_m + i v_m, \quad u_i, v_i \in \mathbb{R}^n,$$

то $\mathcal{K}_{\bar{\lambda}}$ получает жорданов базис из векторов

$$\bar{x}_1 = u_1 - i v_1, \dots, \bar{x}_m = u_m - i v_m.$$

Приравнивая вещественные и мнимые части, находим

$$A(u_i + i v_i) = (\alpha + i\beta)(u_i + i v_i) \Leftrightarrow A[u_1, v_1] = [u_1, v_1] \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix},$$

$$\begin{aligned}
A(u_i + \mathbf{i}v_i) &= (\alpha + \mathbf{i}\beta)(u_i + \mathbf{i}v_i) + (u_{i-1} + \mathbf{i}v_{i-1}) \Leftrightarrow \\
&\Leftrightarrow A[u_i, v_i] = [u_i, v_i] \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} + [u_{i-1}, v_{i-1}].
\end{aligned}$$

Предположим, что жорданова форма сужения оператора $A: x \rightarrow Ax$ на $\mathcal{K}_\lambda$ имеет вид

$$J(\lambda) = J_{m_1}(\lambda) \oplus \dots \oplus J_{m_s}(\lambda), \quad m_1 + \dots + m_s = m,$$

где $J_{m_i}(\lambda)$ — жорданова клетка порядка m_i . Тогда для сужения на $\mathcal{K}_{\bar{\lambda}}$ получаем жорданову форму вида

$$J(\bar{\lambda}) = J_{m_1}(\bar{\lambda}) \oplus \dots \oplus J_{m_s}(\bar{\lambda}).$$

Далее,

$$M := \mathcal{K}_\lambda \oplus \mathcal{K}_{\bar{\lambda}} = \langle x_1, \dots, x_m, \bar{x}_1, \dots, \bar{x}_m \rangle = \langle u_1, v_1, \dots, u_m, v_m \rangle$$

и в базисе $u_1, v_1, \dots, u_m, v_m$ матрица сужения оператора $A: x \rightarrow Ax$ на пространство M приобретает вид

$$\mathcal{J}(\lambda) = \mathcal{J}_{m_1}(\lambda) \oplus \dots \oplus \mathcal{J}_{m_s}(\lambda),$$

где, по определению, для $d = m_i$ матрица $\mathcal{J}_d(\lambda)$ — это *блочная жорданова клетка*, т. е. блочная матрица, составленная из $d \times d$ вещественных 2×2 -блоков:

$$\mathcal{J}_d(\lambda) = \begin{bmatrix} \Lambda & I_2 & & \\ & \ddots & \ddots & \\ & & \Lambda & I_2 \\ & & & \Lambda \end{bmatrix}, \quad \Lambda = \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix},$$

$$\lambda = \alpha + \mathbf{i}\beta, \quad \alpha, \beta \in \mathbb{R}, \quad \beta \neq 0.$$

Таким образом, мы доказали следующую теорему.

Теорема 5.12.1. *Любая вещественная квадратная матрица подобна прямой сумме жордановых клеток для вещественных собственных значений и блочных жордановых клеток для пар комплексно сопряженных не вещественных собственных значений.*

Прямую сумму, о которой идет речь в теореме, будем называть *блочной жордановой формой* вещественной матрицы.

Следствие 5.12.1. *Для любой вещественной нормальной матрицы A существует ортогональная матрица Q , такая что матрица $Q^{-1}AQ = Q^\top AQ$ является прямой суммой ве-*

вещественных блоков порядка 1 и 2 и каждый блок порядка 2 имеет вид $\begin{bmatrix} \alpha_k & \beta_k \\ -\beta_k & \alpha_k \end{bmatrix}$, где $\lambda_k = \alpha_k + i\beta_k$ — невещественное собственное значение матрицы A .

Доказательство. Пусть векторы $x_1, \dots, x_m$ образуют ортонормированный базис собственного подространства для невещественного собственного значения

$$\lambda_k = \alpha_k + i\beta_k.$$

Как и раньше, запишем $x_i = u_i + iv_i$, где $u_i, v_i \in \mathbb{R}^n$. Отсюда следует, что

$$u_i = \frac{1}{2}(x_i + \bar{x}_i), \quad v_i = \frac{1}{2i}(x_i - \bar{x}_i).$$

Поскольку $x_i \perp \bar{x}_i$, находим $(u_i + iv_i, u_i - iv_i) = ((u_i, u_i) - (v_i, v_i)) + 2i(u_i, v_i) = 0 \Rightarrow u_i \perp v_i$ и $\|u_i\| = \|v_i\|$. Кроме того, $u_i \perp u_j$, $v_i \perp v_j$ и $u_i \perp v_j$ при $i \neq j$. Следовательно, векторы

$$\frac{u_1}{\|u_1\|}, \frac{v_1}{\|v_1\|}, \dots, \frac{u_m}{\|u_m\|}, \frac{v_m}{\|v_m\|}$$

образуют ортонормированную систему и, поскольку $\|u_i\| = \|v_i\|$, получаем

$$A \left[\frac{u_i}{\|u_i\|}, \frac{v_i}{\|v_i\|} \right] = \left[\frac{u_i}{\|u_i\|}, \frac{v_i}{\|v_i\|} \right] \begin{bmatrix} \alpha_k & \beta_k \\ -\beta_k & \alpha_k \end{bmatrix}, \quad 1 \leq i \leq m. \quad \square$$

Пример. Пусть l_1 и l_2 — две пересекающиеся прямые в трехмерном геометрическом пространстве и задана декартова система координат, имеющая начало в точке их пересечения и ортонормированные базисные векторы e_1, e_2, e_3 . Пусть A_1 и A_2 — матрицы, представляющие в базисе e вращения вокруг l_1 и l_2 соответственно. Ясно, что это будут ортогональные матрицы с определителем 1. Значит, произведение $A = A_1 A_2$ также будет ортогональной матрицей с определителем 1. Легко доказывается, что все собственные значения ортогональной матрицы по модулю равны 1. Если A имеет три вещественных собственных значения, то либо все они равны 1, либо два из них равны -1 и одно 1. В первом случае A задает вращение на нулевой угол, во втором — вращение на угол π . Теперь предположим, что A имеет одно вещественное собственное значение γ и пару сопряженных невещественных собственных значений $\alpha + i\beta$ и $\alpha - i\beta$. Согласно следствию 5.12.1, имеется ортонормированный базис, в котором

оператор $A: x \rightarrow Ax$ будет представляться ортогональной матрицей вида

$$\begin{bmatrix} \gamma & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & -\beta & \alpha \end{bmatrix}, \quad \alpha^2 + \beta^2 = 1, \quad \gamma = \pm 1.$$

Определитель этой матрицы равен 1 $\Rightarrow \gamma = 1$. Очевидно также, что α и β можно представить в виде $\alpha = \cos \phi$, $\beta = \sin \phi$.

Мы получили еще одно доказательство утверждения о том, что композиция вращений относительно пересекающихся прямых представляет собой вращение относительно некоторой прямой, проходящей через точку пересечения данных прямых (см. раздел 2.9).

Задача 238. Матрица A называется кососимметричной, если $A = -A^T$. Какой вид имеет блочная жорданова форма вещественной кососимметричной матрицы?

5.13. Вычисление минимального многочлена

Пусть линейный оператор A имеет различные собственные значения $\lambda_1, \dots, \lambda_s$ и приведенный характеристический многочлен вида $f_A(\lambda) = \prod_{i=1}^s (\lambda - \lambda_i)^{k_i}$. Обозначим через ν_i индекс нильпотентности оператора $(A - \lambda_i I)|V_i$, где V_i — корневое подпространство для собственного значения λ_i .

Теорема 5.13.1. Максимальный порядок жордановых блоков для собственного значения λ_i оператора A равен индексу нильпотентности ν_i сужения оператора $A - \lambda_i I$ на корневое подпространство для λ_i . Минимальный многочлен оператора A имеет вид $\phi_A(\lambda) = \prod_{i=1}^s (\lambda - \lambda_i)^{\nu_i}$, где $\lambda_1, \dots, \lambda_s$ — все попарно различные собственные значения.

Доказательство. Число жордановых блоков порядка $\geq \nu_i + 1$ для собственного значения λ_i равно $\text{def}(A - \lambda_i I)^{\nu_i+1} - \text{def}(A - \lambda_i I)^{\nu_i} = 0$. В силу того что матрица $J_{\nu_i}(\lambda_i) - \lambda_i I_{\nu_i}$ имеет верхний треугольный вид и ее главная диагональ состоит из нулей, находим: $(J_{\nu_i}(\lambda_i) - \lambda_i I_{\nu_i})^{\nu_i} = 0 \Rightarrow \phi_A(J) = 0$, где $J = P^{-1}AP$ — жорданова форма оператора A и матрица P невырождена. Значит, $\phi_A(A) = \phi_A(PJP^{-1}) = P\phi_A(J)P^{-1} = 0$. Минимальный многочлен, пусть это будет $\phi(\lambda)$, является делителем любого

аннулирующего многочлена, в том числе и характеристического, и поэтому имеет вид $\phi(\lambda) = \prod_{i=1}^{l_i} (\lambda - \lambda_i)^{l_i}$, где $l_i \leq \nu_i$ для всех i . Если хотя бы для одного индекса неравенство строгое, например $l_j < \nu_j$, то $(J_{\nu_j} - \lambda_j I_{\nu_j})^{l_j} \neq 0$. В то же время при $i \neq j$ блок $(J_{\nu_j} - \lambda_i I_{\nu_j})^{l_i}$ есть верхняя треугольная матрица с ненулевой диагональю и поэтому невырожден. В итоге $\prod_{i=1}^s (J_{\nu_j} - \lambda_i I_{\nu_j})^{l_i} \neq 0$. $\square$

Теперь рассмотрим ситуацию, когда поле разложения многочлена $f_A(\lambda) \in \mathbb{P}[\lambda]$ не содержится в исходном поле $\mathbb{P}$. В доказательстве теоремы 5.13.1 минимальный многочлен $\phi_A(\lambda)$ строится над полем, содержащим все собственные значения. Можно ли утверждать, тем не менее, что $\phi_A(\lambda) \in \mathbb{P}[\lambda]$?

Лемма 5.13.1. Пусть A — линейный оператор на пространстве над произвольным полем, многочлены $f_1(\lambda)$ и $f_2(\lambda)$ над этим полем взаимно просты и являются минимальными для сужений $A_1 = A|_{L_1}$ и $A_2 = A|_{L_2}$, где $L_1 = \ker f_1(A)$ и $L_2 = \ker f_2(A)$. Тогда минимальный многочлен для прямой суммы $A_1 \oplus A_2$ есть произведение $f_1(\lambda)f_2(\lambda)$.

Доказательство. Не ограничивая общности, будем считать, что A действует на пространстве $L := L_1 \oplus L_2$. Как следствие взаимной простоты, $f_1(\lambda)g_1(\lambda) + f_2(\lambda)g_2(\lambda) = 1$ для некоторых многочленов g_1 и g_2 . Пусть $L \ni x = x_1 + x_2$ — разложение по подпространствам L_1 и L_2 . Тогда $f_1(A)f_2(A)x_1 = f_1(A)f_2(A)x_2 = 0 \Rightarrow f_1(A)f_2(A) = 0$. Если $\phi(\lambda)$ — произвольный многочлен, аннулирующий A , то он аннулирует также A_1 и A_2 и поэтому обязан делиться одновременно на $f_1(\lambda)$ и $f_2(\lambda)$, а значит, вследствие взаимной простоты, и на их произведение. $\square$

Теорема 5.13.2. Пусть A — линейный оператор на конечномерном пространстве над полем $\mathbb{P}$ и его характеристический многочлен $f(\lambda)$ записан в виде $f = f_1^{\mu_1} \dots f_t^{\mu_t}$, где многочлены $f_1, \dots, f_t$ неприводимы над полем $\mathbb{P}$ и $\mu_1, \dots, \mu_t$ — натуральные числа. Тогда произведение $\phi = f_1 \dots f_t$ есть минимальный многочлен оператора A .

Доказательство. Прежде всего покажем, что минимальный многочлен сужения A на ядро оператора $f_i^{\mu_i}(A)$ есть $f_i(\lambda)$. После этого доказательство сводится к последовательному применению леммы 5.13.1.

Итак, пусть $\phi_i(\lambda)$ — минимальный многочлен интересующего нас сужения. Тогда, как следствие теоремы об однозначном разложении на неприводимые множители, $f_i^{\mu_i} : \phi_i \Rightarrow f_i : \phi_i$. Поскольку f_i — неприводимый многочлен, он может отличаться от ϕ_i лишь ненулевым множителем. $\square$

Теорема 5.13.3. Пусть $A: V \rightarrow V$ — линейный оператор на пространстве V над полем $\mathbb{P}$ и степень его минимального многочлена над $\mathbb{P}$ равна m . Тогда любое максимальное пространство Крылова $L_d(A, x)$ имеет размерность $d \leq m$ и среди них есть пространство размерности $d = m$.

Доказательство. Очевидно, любые векторы вида $x, Ax, \dots, A^m x \in V$ линейно зависимы $\Rightarrow d \leq m$. Чтобы показать, что имеется пространство Крылова вида $L_m(A, x)$, начнем со случая, когда характеристический многочлен имеет вид $f = p^\mu$ для некоторого неприводимого многочлена p и натурального числа μ . Тогда, согласно теореме 5.13.2, $m = \deg p$. Всякое максимальное пространство Крылова L является инвариантным $\Rightarrow$ характеристический многочлен сужения $A|L$ является делителем p^μ и, поскольку его степень не может быть больше $m = \deg p$, она в точности равна m .

В общем случае рассмотрим разложение $f = f_1^{\mu_1} \dots f_t^{\mu_t}$ на неприводимые множители. Мы уже понимаем, что имеются максимальные пространства Крылова размерностей $m_i := \deg f_i$, $1 \leq i \leq t$. Наша задача — установить наличие максимального пространства Крылова размерности $m = m_1 + \dots + m_t$.

Для этого докажем следующее утверждение: прямая сумма максимальных пространств Крылова $L_1 = L_{d_1}(A, x_1)$, $L_2 = L_{d_2}(A, x_2)$ при условии взаимной простоты минимальных многочленов для сужений $A|L_1$ и $A|L_2$ является максимальным пространством Крылова. Положим $x = x_1 + x_2$ и установим линейную независимость векторов $x, Ax, \dots, A^{d_1+d_2-1}x$.

Эти векторы можно рассматривать также как векторы из линейного пространства над произвольным расширением исходного поля. Важно, что в конечномерном случае линейная независимость над более широким полем равносильна линейной независимости над исходным полем — ранг матрицы над некоторым полем очевидно совпадает с рангом той же матрицы над расширенным полем (минор отличен от нуля в том и только том случае, когда он отличен от нуля при переходе к более широкому полю). Пусть $f_1(\lambda)$ и $f_2(\lambda)$ — взаимно простые минимальные многочлены для

операторов $A|L_1$ и $A|L_2$. В качестве более широкого поля $\widehat{\mathbb{P}}$ возьмем поле, содержащее все корни произведения $f_1(\lambda)f_2(\lambda)$. Мы будем использовать разложение

$$f_1(\lambda) = \prod_{i=1}^{d_1} (\lambda - \lambda_i), \quad \lambda_1, \dots, \lambda_{d_1} \in \widehat{\mathbb{P}}.$$

Кроме этого, обратим внимание на легко проверяемый факт совпадения линейных оболочек

$$\langle x, Ax, \dots, A^{k-1}x \rangle = \langle x, B_1x, \dots, B_{k-1}x \rangle,$$

$$B_l := \prod_{i=1}^l (A - \alpha_l I), \quad 1 \leq l \leq k-1,$$

при произвольном выборе чисел $\alpha_1, \dots, \alpha_{k-1} \in \widehat{\mathbb{P}}$.

Теперь приступим собственно к доказательству линейной независимости. Из факта совпадения линейных оболочек следует

$$\langle x, Ax, \dots, A^{d_1+d_2-1}x \rangle = \langle B_0x, B_1x, \dots, B_{d_1+d_2-1}x \rangle,$$

$$B_0 := I, \quad B_k := \prod_{i=1}^k (A - \lambda_i I), \quad 1 \leq k \leq d_1,$$

$$B_{d_1+l} := A^l f_1(A), \quad 1 \leq l \leq d_2 - 1.$$

Здесь нужно обратить внимание на то, что $B_{d_1} = f_1(A)$. Будем доказывать линейную независимость векторов $B^0x, \dots, B^{d_1+d_2-1}x$:

$$\sum_{i=1}^{d_1+d_2} \alpha_i B_{i-1}x = 0, \quad \alpha_i \in \mathbb{P} \Rightarrow \sum_{i=1}^{d_1+d_2} \alpha_i B_{i-1}x_1 = \sum_{i=1}^{d_1+d_2} \alpha_i B_{i-1}x_2 = 0.$$

Заметим, что $B_{i-1}x_1 = 0$ при $d_1 + 1 \leq i \leq d_2$. Следовательно, $\sum_{i=1}^{d_1} \alpha_i B_{i-1}x_1 = 0$ и при этом $\langle x_1, Ax_1, \dots, A^{d_1-1}x_1 \rangle = \langle B_0x_1, B_1x_1, \dots, B_{d_1-1}x_1 \rangle$. Значит, $\alpha_1 = \dots = \alpha_{d_1} = 0$. Теперь мы получаем равенство

$$\sum_{i=d_1+1}^{d_1+d_2} \alpha_i A^{i-d_1-1} f_1(A) x_2 = 0 \Rightarrow f_1(A) \left(\sum_{i=d_1+1}^{d_1+d_2} \alpha_i A^{i-d_1-1} x_2 \right) = 0$$

и, учитывая обратимость оператора $f_1(A)|_{L_2}$, находим

$$\sum_{i=d_1+1}^{d_1+d_2} \alpha_i A^{i-d_1-1} x_2 = 0 \Rightarrow \alpha_i = 0 \text{ при } d_1 + 1 \leq i \leq d_1 + d_2. \quad \square$$

Следствие 5.13.1. Коэффициенты многочлена $\phi_A(\lambda)$ из теоремы 5.13.1 принадлежат исходному полю $\mathbb{P}$.

Доказательство. Пусть $\phi(\lambda) \in \mathbb{P}[\lambda] \subseteq \widehat{\mathbb{P}}[\lambda]$ — минимальный многочлен для оператора A над исходным полем $\mathbb{P}$. По построению, $\phi_A(\lambda) \in \widehat{\mathbb{P}}[\lambda]$, где поле $\widehat{\mathbb{P}}$ содержит собственные значения. Над расширенным полем $\phi(\lambda)$ делится на $\phi_A(\lambda) \Rightarrow \deg \phi(\lambda) \geq \deg \phi_A(\lambda)$. В то же время, согласно теореме 5.13.3, имеется максимальное пространство Крылова размерности $\deg \phi(\lambda)$ и при этом его размерность не может быть больше $\deg \phi_A(\lambda) \Rightarrow \deg \phi(\lambda) \leq \deg \phi_A(\lambda)$. Поэтому $\deg \phi(\lambda) = \deg \phi_A(\lambda)$ и, поскольку один из многочленов делится на другой, они могут отличаться лишь ненулевым множителем. $\square$

Задача 239. Найдите минимальный многочлен $n \times n$ -матрицы

$$A = \begin{bmatrix} a_{n-1} & a_{n-2} & \dots & a_0 \\ 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{bmatrix}.$$

Задача 240. Придумайте, как установить или опровергнуть диагонализуемость матрицы за конечное число арифметических операций над ее элементами.

5.14. Резольвенты Лагранжа

Пусть $A: V \rightarrow V$ — линейный оператор и его минимальный многочлен имеет вид

$$f(\lambda) = \prod_{i=1}^n (\lambda - \lambda_i),$$

где $\lambda_1, \dots, \lambda_n$ — попарно различные числа. Как обычно, $f'(\lambda)$ — это производная многочлена $f(\lambda)$. Многочлены вида

$$f_i(\lambda) := \frac{f(\lambda)}{(\lambda - \lambda_i)f'(\lambda_i)} = \prod_{1 \leq j \leq n, j \neq i} \frac{\lambda - \lambda_j}{\lambda_i - \lambda_j}$$

называются *элементарными многочленами Лагранжа*. С их помощью легко решается *задача полиномиальной интерполяции*: построить многочлен, принимающий заданные значения в точках $\lambda_1, \dots, \lambda_n$.

Утверждение 5.14.1. Для произвольного многочлена $g(\lambda)$ степени не выше $n - 1$ имеет место формула

$$g(\lambda) = \sum_{i=1}^n g(\lambda_i) f_i(\lambda).$$

Доказательство. Достаточно заметить, что многочлен степени не выше $n - 1$ однозначно определяется по своим значениям в n различных точках, правая часть является многочленом степени не выше $n - 1$ и для элементарных многочленов Лагранжа справедливы равенства

$$f_i(\lambda_i) = 1, \quad f_i(\lambda_j) = 0 \quad \text{при} \quad i \neq j. \quad \square$$

Следствие 5.14.1. Операторы $f_1(A), \dots, f_n(A)$ удовлетворяют следующим соотношениям:

$$\sum_{i=1}^n f_i(A) = I, \quad (1)$$

$$f_i(A)f_j(A) = 0 \quad \text{при} \quad i \neq j, \quad (f_i(A))^2 = f_i(A), \quad (2)$$

$$Af_j(A) = \lambda_j f_j(A), \quad 1 \leq j \leq n. \quad (3)$$

Доказательство. Согласно утверждению 5.14.1, находим

$$1 = \sum_{i=1}^n f_i(\lambda) \Rightarrow (1).$$

Если $i \neq j$, то $f_i(\lambda)f_j(\lambda) : f(\lambda) \Rightarrow f_i(A)f_j(A) = 0$. Учитывая это равенство при умножении обеих частей равенства (1) на $f_j(A)$, получаем $(f_j(A))^2 = f_j(A)$. Еще одно применение утверждения 5.14.1 дает равенство

$$\lambda = \sum_{i=1}^n \lambda_i f_i(\lambda) \Rightarrow A = \sum_{i=1}^n \lambda_i f_i(A).$$

После умножения обеих частей на $f_j(A)$ получаем (3). $\square$

Следствие 5.14.2. Для любого вектора $x \in V$ имеет место расщепление

$$x = x_1 + \dots + x_n, \quad x_i = f_i(A)x,$$

в котором каждый ненулевой вектор x_i является собственным вектором для собственного значения λ_i .

Многочлены $f_i(A)$ называются *резольвентами Лагранжа* для линейного оператора A . При их определении предполагается, что минимальный многочлен оператора A имеет только простые корни. Лагранж использовал их для некоторых специальных операторов, связанных с проблемой поиска формул для корней многочленов степени n . Они действительно дают общий, внушающий надежду метод, который, однако, приводит к успеху только в частных случаях, а именно для $n = 2, 3, 4$.

В данной задаче в качестве линейного пространства V рассматривается кольцо $\mathbb{C}[x_1, \dots, x_n]$. Здесь естественным образом определяется также операция умножения элемента кольца на число. Вместе с операцией сложения она превращает V в линейное пространство.

В общем случае, пусть V — ассоциативное кольцо с единицей и одновременно линейное пространство над полем $\mathbb{P}$ с условием ¹⁾

$$\alpha(ab) = (\alpha a)b = a(\alpha b) \quad \forall a, b \in V, \quad \forall \alpha \in \mathbb{P}. \quad (*)$$

Тогда V называется *алгеброй* над полем $\mathbb{P}$. Если кольцо коммутативно, то V называется *коммутативной алгеброй*. Если пространство V конечномерно, то алгебра называется *конечномерной* и размерность пространства называется *размерностью алгебры*.

Итак, пусть V — алгебра комплексных многочленов от переменных $x_1, \dots, x_n$. Любая подстановка $\sigma \in S_n$ естественным образом задает отображение

$$p(x_1, \dots, x_n) \rightarrow p(x_{\sigma(1)}, \dots, x_{\sigma(n)}),$$

которое, очевидно, является линейным оператором на V . Мы полагаем, что переменные $x_1, \dots, x_n$ суть корни уравнения

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0.$$

¹⁾ Условие $(*)$ означает, что функция $\phi(a, b) := ab$ является *билинейной*, т. е. линейной по каждому аргументу.

Это означает, что $a_{n-i} = (-1)^i E_i(x_1, \dots, x_n)$, где $E_i(x_1, \dots, x_n)$ — элементарный симметрический многочлен степени i . Все симметрические многочлены образуют в V подпространство, которое состоит из *неподвижных точек* при всех подстановках степени n :

$$V_0 = \{p \in V : \sigma p = p \ \forall \sigma \in S_n\}.$$

Лагранж строил свои резольвенты для многочлена $f(\lambda) = \lambda^N - 1$. Его корни — это корни степени N из единицы:

$$\lambda_i = \varepsilon^i, \quad \varepsilon = \cos\left(\frac{2\pi}{N}\right) + i \sin\left(\frac{2\pi}{N}\right).$$

Многочлен $f(\lambda)$ является минимальным для подстановки σ , представляющей собой цикл длины N . Согласно определению

$$\begin{aligned} f_i(\lambda) &= \frac{\lambda^N - 1}{N\lambda_i^{N-1}(\lambda - \lambda_i)} = \frac{\lambda^N - \lambda_i^N}{N\lambda_i^{N-1}(\lambda - \lambda_i)} = \\ &= \frac{1}{N} (\lambda_i \lambda^{N-1} + \lambda_i^2 \lambda^{N-2} + \dots + \lambda_i^N). \end{aligned}$$

Таким образом, резольвенты Лагранжа имеют вид

$$f_i(\sigma) = \frac{1}{N} (\lambda_i \sigma^{N-1} + \lambda_i^2 \sigma^{N-2} + \dots + \lambda_i^{N-1} \sigma + e), \quad 1 \leq i \leq N.$$

Согласно следствию 5.14.2 любой элемент $x \in V$, в том числе и $x = x_1$, допускает разложение

$$\begin{aligned} x_1 &= y_1 + \dots + y_N, \quad y_i = f_i(\sigma)x_1, \quad \sigma y_i = \lambda_i y_i \Rightarrow \\ &\Rightarrow \sigma y_i^N = (\sigma y_i)^N = \lambda_i^N y_i^N = y_i^N. \end{aligned}$$

Здесь возникает ключевое наблюдение: многочлен y_i^N остается неподвижным при действии на него подстановкой σ , а значит, и любой степенью подстановки σ . Обозначим через $H = \langle \sigma \rangle$ циклическую группу, порожденную подстановкой σ . Тогда

$$h y_i^N = y_i^N \quad \forall h \in H.$$

Элемент y_i называется *радикалом N -й степени* от y_i^N , т.е. в данном случае от элемента из множества

$$V^H := \{p \in V : h p = p \ \forall h \in H\}.$$

Множество V^H состоит из всех неподвижных точек при действии группы H . Как легко видеть, оно является алгеброй и некоторым подпространством в исходном пространстве V .

Общая идея заключается в следующем. Попробуем найти цепочку подпространств и одновременно алгебр

$$V_0 \subset V_1 \subset \dots \subset V_s = V,$$

неподвижных (каждая точка остается на месте) относительно подстановок из группы с тем же индексом в цепочке

$$S_n = G_0 \triangleright G_1 \triangleright \dots \triangleright G_s = \{e\},$$

которая начинается с симметрической группы степени n , заканчивается единичной группой и подчиняется следующим требованиям: *если $1 \leq i \leq s$, то G_i — нормальная подгруппа группы G_{i-1} и фактор-группа G_{i-1}/G_i является циклической*. Мы сейчас увидим, что если цепочки пространств и групп с такими свойствами существуют, то x_1 можно *выразить в радикалах* через $a_0, \dots, a_{n-1}$. Другими словами, от многочленов $a_0, \dots, a_{n-1}$ к x_1 можно перейти с помощью конечной последовательности арифметических операций и переходов вида $a^N \rightarrow a$.

По ходу дела мы, конечно, разберемся, откуда берутся требования нормальности подгрупп и цикличности фактор-групп. Пространства и группы связаны условием

$$V_i = V^{G_i}, \quad 0 \leq i \leq s.$$

Таким образом,

$$p \in V_i \Leftrightarrow g_i p = p \quad \forall g_i \in G_i.$$

Нормальность подгруппы $G_i \triangleleft G_{i-1}$ означает *инвариантность пространства V_i относительно подстановок подгруппы G_{i-1}* :

$$\begin{aligned} g_{i-1}^{-1} g_i g_{i-1} \in G_i \quad \forall g_i \in G_i, \quad \forall g_{i-1} \in G_{i-1} &\Leftrightarrow \\ \Leftrightarrow g_i(g_{i-1}p) = g_{i-1}p \quad \forall g_i \in G_i, \quad \forall g_{i-1} \in G_{i-1}, \quad \forall p \in V_i &\Leftrightarrow \\ \Leftrightarrow g_{i-1}p \in V_i \quad \forall g_{i-1} \in G_{i-1}, \quad \forall p \in V_i. \end{aligned}$$

Согласно определению, циклическая фактор-группа $H_i := G_{i-1}/G_i$ порядка $N_i := |G_{i-1}/G_i|$ состоит из смежных классов вида

$$G_i, \quad \sigma_i G_i, \quad \dots, \quad \sigma_i^{N_i-1} G_i, \quad \sigma^{N_i} = e, \quad \sigma_i \in G_{i-1}.$$

Возьмем произвольный многочлен $p \in V_i$. Поскольку пространство V_i инвариантно относительно оператора $\sigma_i \in G_{i-1}$, мы можем рассматривать подстановку $\sigma_i: V \rightarrow V$ как оператор

на пространстве V_i . Его минимальный многочлен имеет вид $f(\lambda) = \lambda^{N_i} - 1$ и, применяя резольвенты Лагранжа, находим

$$p = \sum_{k=1}^{N_i} p_j, \quad p_j = f_j(\sigma_i)p, \quad \sigma_i p_j^{N_i} = p_j^{N_i} \Leftrightarrow p_j^{N_i} \in V_{i-1}.$$

В результате мы видим, что каждый многочлен $p \in V_i$ есть сумма многочленов p_j таких, что $p_j^{N_i} \in V_{i-1}$.

Случай $n = 2$. Дано уравнение $x^2 + a_1x + a_0 = 0$, $a_1 = -(x_1 + x_2)$, $a_0 = x_1x_2$. Симметрическая группа S_2 состоит всего из двух подстановок, цепочки получаются очевидным образом:

$$V_0 \subset V_1 = V, \quad G_0 = S_2 \triangleright G_1 = \{e\}.$$

В данном случае $H_1 = G_1/G_0 = \langle \sigma_1 \rangle$, где $\sigma_1 = (1, 2)$ — транспозиция. Минимальный многочлен для σ_1 имеет вид $\lambda^2 - 1$ и корни $\lambda_1 = 1$, $\lambda_2 = -1$. Вот резольвенты Лагранжа:

$$f_1(\sigma_1) = \frac{1}{2}(\sigma_1 + e), \quad f_2(\sigma_1) = \frac{1}{2}(-\sigma_1 + e).$$

Следовательно, $x_1 = y_1 + y_2$, где

$$y_1 = \frac{1}{2}(\sigma_1 + e)x_1 = \frac{1}{2}(x_2 + x_1) = -\frac{a_1}{2} \in V_0,$$

$$y_2 = \frac{1}{2}(-\sigma_1 + e)x_1 = \frac{1}{2}(-x_2 + x_1),$$

$$y_2^2 = \frac{1}{4}(x_2 - x_1)^2 = \frac{1}{4}((x_1 + x_2)^2 - 4x_1x_2) = \frac{1}{4}(a_1^2 - 4a_0) \in V_0.$$

Очевидно, что у нас получилась известная формула школьной математики

$$x_{1,2} = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2}.$$

Случай $n = 3$. Дано уравнение $x^3 + a_2x^2 + a_1x + a_0 = 0$, $a_2 = -(x_1 + x_2 + x_3)$, $a_1 = x_1x_2 + x_2x_3 + x_1x_3$, $a_0 = -x_1x_2x_3$. Симметрическая группа S_3 содержит 6 подстановок, подгруппа четных подстановок (так называемая *знакопеременная группа*) A_3 является нормальной, причем фактор-группа S_3/A_3 имеет порядок 2 и поэтому очевидно является циклической. Группа A_3 имеет порядок 3 и поэтому также является циклической. Вот нужные нам цепочки:

$$V_0 \subset V_1 \subset V_2 = V, \quad G_0 = S_3 \triangleright G_1 = A_3 \triangleright G_2 = \{e\},$$

$$H_1 = S_3/A_3 = \langle \sigma_1 A_3 \rangle, \quad H_2 = A_3/\{e\} = \langle \sigma_2 \rangle,$$

$$\sigma_1 = (2, 3), \quad \sigma_2 = (1, 2, 3).$$

Сначала получаем разложение $x_1 = y_1 + y_2 + y_3$, где $y_1^3, y_2^3, y_3^3 \in V_1$. Минимальный многочлен для σ_2 имеет вид $\lambda^3 - 1$ и корни

$$\lambda_1 = 1, \quad \lambda_2 = \varepsilon, \quad \lambda_3 = \varepsilon^2, \quad \varepsilon = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right).$$

Вот резольвенты Лагранжа:

$$f_1(\sigma_2) = \frac{1}{3}(\sigma_2^2 + \sigma_2 + e), \quad f_2(\sigma_2) = \frac{1}{3}(\varepsilon\sigma_2^2 + \varepsilon^2\sigma_2 + e),$$

$$f_3(\sigma_2) = \frac{1}{3}(\varepsilon^2\sigma_2^2 + \varepsilon\sigma_2 + e).$$

Следовательно,

$$y_1 = \frac{1}{3}(x_3 + x_2 + x_1) = -\frac{1}{3}a_2 \in V_0,$$

$$y_2 = \frac{1}{3}(\varepsilon x_3 + \varepsilon^2 x_2 + x_1), \quad y_3 = \frac{1}{3}(\varepsilon^2 x_3 + \varepsilon x_2 + x_1), \quad y_2^3, y_3^3 \in V_1.$$

Теперь нужно найти $u := y_2^3$ и $v := y_3^3$. У нас уже был опыт применения резольвент Лагранжа для транспозиции. Опираясь на него, можно утверждать, что многочлены $u + v$ и $(u - v)^2$ принадлежат V_0 , т. е. являются симметрическими и поэтому выражаются через a_0, a_1, a_2 .

Читатель может проявить настойчивость и завершить выкладки. Мы же заметим, что есть возможность упрощения. Заменив x на $z - a_2/3$, мы получаем уравнение для z вида $z^3 + pz + q = 0$ (исчезает коэффициент при z^2). Далее, записав $z = u + v$, находим

$$(u + v)^3 + p(u + v) + q = (u^3 + v^3 + q) + (u + v)(3uv + p) = 0.$$

Очевидно, что z будет корнем, если u и v удовлетворяют системе уравнений

$$u^3 + v^3 = -q, \quad uv = -\frac{p}{3}$$

и, следовательно, u^3 и v^3 являются корнями квадратного уравнения

$$X^2 + qX - \frac{p^3}{27} = 0.$$

В итоге получается известная *формула Кардано*¹⁾:

$$z = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Случай $n = 4$. Дано уравнение $x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$. Здесь можно обнаружить такую цепочку подгрупп:

$$S_4 \triangleright A_4 \triangleright K_4 \triangleright H \triangleright \{e\}, \quad H = \langle (1, 2)(3, 4) \rangle,$$

A_4 — знакопеременная группа и K_4 — *четверная группа Клейна*, состоящая из подстановок $\{e, (1, 2)(3, 4), (1, 3)(2, 4), (2, 3)(1, 4)\}$. Все фактор-группы имеют простой порядок и поэтому являются циклическими группами.

В случае $n \geq 5$ метод не работает, так как нет ни одной цепочки подгрупп с нужными нам свойствами. Причина в том, что при $n \geq 5$ подгруппа четных подстановок A_n является единственной нетривиальной нормальной подгруппой в симметрической группе S_n и сама она не имеет нетривиальных нормальных подгрупп.

Итак, при $n \geq 5$ метод резольвент Лагранжа не работает. Но это еще не доказывает того, что корни многочленов степени 5 и выше нельзя выразить в радикалах. Пока что мы убедились только в том, что наличие цепочки подгрупп с описанными выше свойствами для разрешимости в радикалах является условием достаточным.

В действительности оно является также необходимым условием. Но доказательство этого факта требует развития специальной теории, ей посвящается гл. 7 этой книги.

Задача 241. Докажите, что для любой коммутативной алгебры линейных операторов на пространстве $\mathbb{C}^n$ существует базис, в котором каждый оператор представляется верхней треугольной матрицей.

Задача 242. Известно, что квадрат любой матрицы из некоторой коммутативной алгебры $n \times n$ -матриц равен нулю. Докажите, что размерность этой алгебры не выше $n^2/4$ ²⁾.

¹⁾ Кардано впервые опубликовал эту формулу, сообщив при этом, что она получена другим итальянским математиком. Применение формулы требует осторожности, так как есть несколько значений для корней из единицы и нужно специально заботиться о том, чтобы обеспечить равенство $uv = -p/3$.

²⁾ Задача связана с теоремой Шура из теории коммутативных матричных алгебр, которая утверждает, что максимальное количество попарно коммутирующих линейно независимых матриц порядка n равно $\lfloor n^2/4 \rfloor + 1$.

Глава 6

НОРМЫ И НЕРАВЕНСТВА

6.1. Расстояния, нормы, длины

В совершенно абстрактном непустом множестве M можно ввести понятие *расстояния* $\rho(x, y)$ между его элементами x и y . Функция $\rho(x, y)$ должна быть определена для всех $x, y \in M$, принимать вещественные значения и обладать следующими свойствами:

- $\rho(x, y) \geq 0$ для всех $x, y \in M$ и $\rho(x, y) = 0 \Leftrightarrow x = y$;
- $\rho(x, y) = \rho(y, x)$ для всех $x, y \in M$ (симметрия);
- $\rho(x, z) \leq \rho(x, y) + \rho(y, z)$ для всех $x, y, z \in M$ (неравенство треугольника).

Множество M , снабженное расстоянием (иногда говорят — *метрикой*) $\rho(x, y)$, называется *метрическим пространством*. На одном и том же множестве расстояния можно вводить разными способами, при этом будут возникать разные метрические пространства с одним и тем же множеством элементов.

Пример 1. M — произвольное непустое подмножество вещественных чисел и $\rho(x, y) = |x - y|$.

Пример 2. M — произвольное непустое множество и $\rho(x, y) = 1$ при $x \neq y$ и $\rho(x, y) = 0$ при $x = y$.

Если на множестве M определены какие-то операции, то полезно требовать, чтобы расстояние имело связь с этими операциями. Пусть V — комплексное или вещественное линейное пространство. Тогда от расстояния принято требовать таких дополнительных свойств:

- $\rho(x + z, y + z) = \rho(x, y)$ для любых векторов $x, y, z \in V$;
- $\rho(\alpha x, \alpha y) = |\alpha| \rho(x, y)$ для любого числа α и любых векторов $x, y \in V$.

В таких случаях величина $\rho(0, x)$ называется *нормой* вектора x и обозначается $\|x\|$. Нетрудно проверить, что норма обладает следующими свойствами:

- $\|x\| \geq 0$ для всех $x \in V$ и $\|x\| = 0 \Leftrightarrow x = 0$;
- $\|\alpha x\| = |\alpha| \|x\|$ для всех чисел α и всех векторов x ;
- $\|x + y\| \leq \|x\| + \|y\|$ для всех $x, y \in V$ (неравенство треугольника).

Комплексное или вещественное пространство V называется *нормированным*, если на нем имеется функция $x \rightarrow \|x\|$ с данными тремя свойствами. В нормированном пространстве расстояние всегда вводится через норму: $\rho(x, y) = \|x - y\|$.

Пример 3. Пусть $c_1, \dots, c_n$ — произвольные положительные числа и V — комплексное пространство с базисом $e_1, \dots, e_n$. Любой вектор $x \in V$ имеет однозначно определенное разложение $x = \sum_{i=1}^n x_i e_i$, и функция $x \rightarrow \sum_{i=1}^n c_i |x_i|$ задает норму на V .

Пример показывает, что любое конечномерное комплексное пространство можно сделать нормированным. Можно ли ввести норму в *произвольном* бесконечномерном пространстве — совсем не очевидно. Здесь мы имеем пример неконструктивной теоремы существования: норму ввести можно, но метода вычисления в общем случае у нас нет.

Утверждение 6.1.1. *Любое комплексное или вещественное пространство можно сделать нормированным.*

Доказательство. Несколько позже мы докажем (см. раздел 8.8 и теорему 8.8.3), что в любом линейном пространстве V существует *базис Гамеля*: так называется любое подмножество $E \subseteq V$, такое что: (1) любой вектор из V представляется линейной комбинацией какой-то конечной системы векторов из E ; (2) любая конечная система векторов из E линейно независима. Таким образом, для вектора $x \in V$ существует зависящая от x система векторов $e_1(x), \dots, e_{n(x)}(x) \in E$, такая

что $x = \sum_{i=1}^{n(x)} \alpha_i(x) e_i(x)$. Несложно проверяется, что функция $x \rightarrow \sum_{i=1}^{n(x)} |\alpha_i(x)|$ является нормой на V . □

Теперь рассмотрим произвольное пространство V со скалярным произведением. В вещественном случае такое пространство

называется *евклидовым*, в комплексном случае — *унитарным*. Мы уже знаем, что величина $\sqrt{(x, x)}$ называется *длиной* вектора x . Ясно, что длина обладает первыми двумя свойствами нормы. Из аксиом скалярного произведения выводится неравенство Коши–Буняковского–Шварца $|(x, y)|^2 \leq (x, x)(y, y)$ ¹⁾, а из него нетрудно получить также и неравенство треугольника. Таким образом, длина всегда является нормой. В пространстве со скалярным произведением норма определяется как длина, порожденная скалярным произведением: $\|x\| := \sqrt{(x, x)}$.

Характеристическим свойством длины является *тождество параллелограмма*:

$$\|x + y\|^2 + \|x - y\|^2 = 2\|x\|^2 + 2\|y\|^2 \quad \forall x, y \in V.$$

Теорема 6.1.1. *Норма является длиной, порожденной некоторым скалярным произведением, в том и только том случае, когда для нее имеет место тождество параллелограмма.*

Доказательство. Если норма является длиной, то тождество параллелограмма получается совсем просто:

$$\begin{aligned} (x + y, x + y) &= (x, x) + (x, y) + (y, x) + (y, y), \\ (x - y, x - y) &= (x, x) - (x, y) - (y, x) + (y, y) \Rightarrow \\ &\Rightarrow (x + y, x + y) + (x - y, x - y) = 2(x, x) + 2(y, y). \end{aligned}$$

Кроме того, в этом случае скалярное произведение (x, y) можно выразить через длины векторов x , y , $x + y$, $x + iy$. Обозначим через $f(x, y)$ и $g(x, y)$ вещественную и мнимую части числа $(x, y) = f(x, y) + ig(x, y)$. Тогда

$$\begin{aligned} (x + y, x + y) &= (x, x) + (y, y) + 2f(x, y), \\ (x + iy, x + iy) &= (x, x) + (y, y) + 2g(x, y) \Rightarrow \\ &\Rightarrow f(x, y) = \frac{1}{2} (\|x + y\|^2 - \|x\|^2 - \|y\|^2), \\ g(x, y) &= \frac{1}{2} (\|x + iy\|^2 - \|x\|^2 - \|y\|^2). \end{aligned}$$

¹⁾ В разделе 1.12 приведено доказательство для вещественного случая. Для комплексного пространства в случае $(x, y) \neq 0$ надо рассмотреть квадратный трехчлен $f(t) = (x + t\zeta y, x + t\zeta y) \geq 0$ при вещественных t , выбрав $\zeta = (x, y)/|(x, y)|$, и выписать условие неположительности дискриминанта.

Теперь предположим, что для нормы выполняется тождество параллелограмма, и докажем, что функция $S(x, y) := f(x, y) + ig(x, y)$ удовлетворяет всем аксиомам скалярного произведения.

Прежде всего заметим, что $f(x, x) = \|x\|^2$ и $g(x, x) = 0 \Rightarrow S(x, x) = \|x\|^2$. Далее, нетрудно проверить, что $f(x, y) = f(y, x)$ и $g(x, y) = -g(y, x) \Rightarrow S(x, y) = \overline{S(y, x)}$. Остается установить, что функция $S(x, y)$ линейна по первому аргументу. Для этого достаточно доказать, что этим свойством обладает каждая из функций $f(x, y)$ и $g(x, y)$. Докажем сначала, что для любых векторов x, y, z выполняется равенство

$$\begin{aligned} f(x+y, z) &= f(x, z) + f(y, z) \Leftrightarrow \\ \Leftrightarrow \|x+y+z\|^2 - \|x+y\|^2 - \|z\|^2 &= (\|x+z\|^2 - \|x\|^2 - \|z\|^2) + \\ &+ (\|y+z\|^2 - \|y\|^2 - \|z\|^2) \Leftrightarrow \\ \Leftrightarrow \|x+y+z\|^2 + \|x\|^2 + \|y\|^2 + \|z\|^2 &= \|x+y\|^2 + \|x+z\|^2 + \\ &+ \|y+z\|^2. \quad (*) \end{aligned}$$

Чтобы применить тождество параллелограмма, запишем

$$\begin{aligned} x+y+z &= u+v, \quad x=u-v \Rightarrow u = x + \frac{1}{2}(y+z), \quad v = \frac{1}{2}(y+z), \\ x+y &= p+q, \quad x+z = p-q \Rightarrow p = x + \frac{1}{2}(y+z), \quad q = \frac{1}{2}(y-z). \end{aligned}$$

Используя равенства

$$\begin{aligned} \|u+v\|^2 + \|u-v\|^2 &= 2\|u\|^2 + 2\|v\|^2, \\ \|p+q\|^2 + \|p-q\|^2 &= 2\|p\|^2 + 2\|q\|^2, \end{aligned}$$

преобразуем (*) к равносильному равенству

$$\begin{aligned} 2\|x + \frac{1}{2}(y+z)\|^2 + 2\|\frac{1}{2}(y+z)\|^2 + \|y\|^2 + \|z\|^2 &= \\ = 2\|x + \frac{1}{2}(y+z)\|^2 + 2\|\frac{1}{2}(y-z)\|^2 + \|y+z\|^2 &\Leftrightarrow \\ \Leftrightarrow \|y+z\|^2 + \|y-z\|^2 &= 2\|y\|^2 + 2\|z\|^2. \end{aligned}$$

Остается доказать равенство $f(\alpha x, y) = \alpha f(x, y)$. Из уже доказанного тождества $f(x+y, z) = f(x, z) + f(y, z)$ оно довольно очевидным образом выводится для натуральных чисел α , а затем

и для всех рациональных чисел α . Далее нужно заметить, что функция $F(\alpha) := f(\alpha x, y)$ является непрерывной функцией от α , а любое вещественное число есть предел последовательности рациональных чисел. Переходом к пределу нужное нам равенство устанавливается уже для всех вещественных чисел α . Остается проверить, что оно верно, когда α равно мнимой единице.

Линейность функции $g(x, y)$ по первому аргументу доказывается аналогично. $\square$

Задача 243. *Норма вектора определяется как сумма модулей его координат по фиксированному базису. Докажите, что эта норма не порождается никаким скалярным произведением.*

Задача 244. *Докажите, что в произвольном комплексном линейном пространстве можно ввести скалярное произведение.*

6.2. Сходимость, полнота, пополнение

В произвольном метрическом пространстве M последовательность элементов $x_n \in M$ называется *сходящейся к элементу* $x \in M$, если $\rho(x_n, x) \rightarrow 0$ при $n \rightarrow \infty$. При этом x называется *пределом* последовательности x_n и мы пишем: $x_n \rightarrow x$ или $x = \lim_{n \rightarrow \infty} x_n$. Двух разных пределов у одной последовательности быть не может: если $x_n \rightarrow x'$ и $x_n \rightarrow x''$, то в силу неравенства треугольника

$$\rho(x', x'') \leq \rho(x', x_n) + \rho(x_n, x'') \rightarrow 0 \Rightarrow \rho(x', x'') = 0 \Rightarrow x' = x''.$$

Поэтому мы имеем право говорить о *сходящейся последовательности*, не уточняя, к какому именно элементу она сходится. Важно только то, что этот элемент принадлежит тому же метрическому пространству M .

Последовательность $x_n \in M$ называется *фундаментальной* или *сходящейся в себе* (иногда также *последовательностью Коши*), если для любого $\varepsilon > 0$ существует натуральное число $N = N(\varepsilon)$, такое что для всех $m, n \geq N$ выполняется неравенство $\rho(x_m, x_n) < \varepsilon$.

Утверждение 6.2.1. *Любая сходящаяся последовательность является фундаментальной.*

Доказательство. Если $x_n \rightarrow x$, то для любого $\varepsilon > 0$ существует натуральное число $N = N(\varepsilon)$, такое что $\rho(x_n, x) < \frac{\varepsilon}{2}$ при всех $n \geq N = N(\varepsilon)$. Для любых номеров $m, n \geq N$ получаем $\rho(x_m, x_n) \leq \rho(x_m, x) + \rho(x, x_n) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$. $\square$

Метрическое пространство называется *полным*, если в нем любая фундаментальная последовательность сходится. Полное нормированное пространство называется *банаховым*, а полное пространство со скалярным произведением называется *гильбертовым пространством*¹⁾.

Пример 1. Пусть $M_1 := \mathbb{R}$, $M_2 := \{x \in \mathbb{R} : x > 0\}$, $\rho(x, y) := |x - y|$. Тогда пространство M_1 полное, а M_2 неполное: последовательность $x_n = \frac{1}{n} \in M_2$ фундаментальна, но не сходится в M_2 (ее пределом должно было бы быть число 0, но оно не принадлежит пространству M_2).

Пример 2. Пусть $x = (x_1, x_2, \dots)$ и $y = (y_1, y_2, \dots)$ — комплексные (вещественные) последовательности, и пусть существуют пределы $\sum_{i=1}^{\infty} |x_i|^2 := \lim_{N \rightarrow \infty} \sum_{i=1}^N |x_i|^2$ и $\sum_{i=1}^{\infty} |y_i|^2 := \lim_{N \rightarrow \infty} \sum_{i=1}^N |y_i|^2 \Rightarrow$ существует предел $(x, y) := \sum_{i=1}^{\infty} x_i \bar{y}_i = \lim_{N \rightarrow \infty} \sum_{i=1}^N x_i \bar{y}_i$. Множество всех таких последовательностей с почленными операциями сложения и умножения на число и скалярным произведением указанного вида обозначается $l_2(\mathbb{C})$ в комплексном случае и $l_2(\mathbb{R})$ в вещественном случае (или просто l_2 , если ясно, о каком поле идет речь). По-видимому, это исторически первые примеры бесконечномерных гильбертовых пространств.

Утверждение 6.2.2. Пространства $l_2(\mathbb{C})$ и $l_2(\mathbb{R})$ полные.

Доказательство. Если последовательность

$$x^{(n)} = (x_1^{(n)}, x_2^{(n)}, \dots), \quad n = 1, 2, \dots,$$

фундаментальна, то для каждого фиксированного i последовательность комплексных чисел $x_i^{(n)}$, $n = 1, 2, \dots$, также фундаментальна и поэтому сходится к некоторому пределу, обозначим

¹⁾ В честь Стефана Банаха и Давида Гильберта.

его через x_i ¹⁾. Несложно проверяется, что $x := (x_1, x_2, \dots) \in l_2$. Далее, для любого $\varepsilon > 0$ найдется $m \in \mathbb{N}$, такое что $\sum_{i=1}^{\infty} |x_i^{(n)} - x_i^m|^2 < \varepsilon$ при всех $n \geq m \Rightarrow \sum_{i=N+1}^{\infty} |x_i^{(n)}|^2 < 2\varepsilon + 2 \sum_{i=N+1}^{\infty} |x_i^m|^2$ для любого $n \geq m$ и любого $N \in \mathbb{N}$.

При достаточно большом N правая часть будет меньше 4ε и одновременно будет справедливо неравенство $\sum_{i=N+1}^{\infty} |x_i|^2 < \varepsilon \Rightarrow \sum_{i=N+1}^{\infty} |x_i^{(n)}|^2 < 4\varepsilon$ для всех достаточно больших $n \Rightarrow \sum_{i=1}^{\infty} |x_i^{(n)} - x_i|^2 \leq 2 \sum_{i=1}^N |x_i^{(n)} - x_i|^2 + 10\varepsilon \leq 12\varepsilon$ при всех достаточно больших n . $\square$

Причина неполноты заключается в том, что в метрическом пространстве M может не оказаться элементов, которые должны быть пределами фундаментальных последовательностей. В духе конструкций алгебры находится идея *пополнения*: добавить недостающие пределы и тем самым расширить M до полного метрического пространства $\widehat{M}$.

Для реализации идеи пополнения рассмотрим всевозможные фундаментальные последовательности элементов из M и объявим, что последовательность x_n эквивалентна последовательности y_n , если $\rho(x_n, y_n) \rightarrow 0$ при $n \rightarrow \infty$. В случае эквивалентности будем писать: $\{x_n\} \sim \{y_n\}$. Таким образом на множестве всевозможных фундаментальных последовательностей элементов пространства M возникает бинарное отношение эквивалентности и, следовательно, все это множество разбивается на *классы эквивалентности* — они и будут элементами множества $\widehat{M}$.

Расстояние между классами $A, B \in \widehat{M}$ определим так: если $\{x_n\} \in A$ и $\{y_n\} \in B$, то $\rho(A, B) := \lim_{n \rightarrow \infty} \rho(x_n, y_n)$. Нужно проверить, что предел существует для любых фундаментальных последовательностей: $\rho(x_n, y_n) \leq \rho(x_n, x_m) + \rho(x_m, y_m) + \rho(y_m, y_n) \Rightarrow |\rho(x_n, y_n) - \rho(x_m, y_m)| \leq \rho(x_n, x_m) + \rho(y_m, y_n) \Rightarrow$ вещественная последовательность $\rho(x_n, y_n)$ фундаментальна и поэтому сходится. Кроме того, нужно показать, что если $\{x_n\} \sim \{x'_n\}$ и $\{y_n\} \sim \{y'_n\}$, то $\lim_{n \rightarrow \infty} \rho(x_n, y_n) = \lim_{n \rightarrow \infty} \rho(x'_n, y'_n)$. Далее читатель

¹⁾ Здесь мы опираемся на полноту пространств $\mathbb{C}$ и $\mathbb{R}$ с расстоянием $\rho(x, y) = |x - y|$.

должен проверить, что функция $\rho(A, B)$ действительно является расстоянием.

Будем говорить, что последовательность x_n ассоциирована с элементом $x \in M$, если $x_n = x$ для всех достаточно больших n . Все последовательности, ассоциированные с x , образуют класс эквивалентности, который естественным образом можно отождествить с элементом x — мы получаем право считать, что M вложено в $\widehat{M}$.

Утверждение 6.2.3. *Метрическое пространство $\widehat{M}$ является полным.*

Доказательство. Пусть классы $A_1, A_2, \dots$ принадлежат $\widehat{M}$ и образуют фундаментальную последовательность. Каждый класс эквивалентности определяется любым своим представителем, пусть $\{x_n^{(k)}\} \in A_k$. В силу фундаментальности для любого $\varepsilon > 0$ при всех достаточно больших k и l справедливо неравенство

$$\rho(A_k, A_l) = \lim_{n \rightarrow \infty} \rho(x_n^{(k)}, x_n^{(l)}) < \frac{\varepsilon}{2}.$$

Отсюда следует, что при всех достаточно больших k для всех достаточно больших n выполняется неравенство

$$\rho(x_n^{(k)}, x_n^{(n)}) < \varepsilon.$$

Докажем, что последовательность $z_n := x_n^{(n)}$ является фундаментальной:

$$\rho(z_m, z_n) \leq \rho(x_m^{(m)}, x_m^{(k)}) + \rho(x_m^{(k)}, x_n^{(k)}) + \rho(x_n^{(k)}, x_n^{(n)}).$$

При всех достаточно больших k для всех достаточно больших m и n находим

$$\rho(z_m, z_n) < 2\varepsilon + \rho(x_m^{(k)}, x_n^{(k)}) < 3\varepsilon.$$

Итак, последовательность $\{z_n\}$ фундаментальна. Пусть она порождает класс $A \in \widehat{M}$. Тогда при всех достаточно больших k

$$\rho(A_k, A) = \lim_{n \rightarrow \infty} \rho(x_n^{(k)}, z_n) \leq \varepsilon \Rightarrow \lim_{k \rightarrow \infty} \rho(A_k, A) = 0. \quad \square$$

Задача 245. Докажите полноту пространства $\mathbb{C}$ с расстоянием $\rho(x, y) = |x - y|$.

Задача 246. Пусть $V = C[0, 1]$ — линейное пространство вещественных функций, непрерывных на отрезке $[0, 1]$. Докажите, что формула $(f, g) := \int_0^1 f(x)g(x)dx$ задает скалярное произведение на V и при этом пространство V не является полным.

Задача 247. Пусть V — линейное пространство вещественных многочленов. Докажите, что формула $\|f\| := \max_{0 \leq x \leq 1} |f(x)|$ задает некоторую норму на V ¹⁾. Докажите, что эта норма не порождается никаким скалярным произведением. Является ли пространство V полным?

6.3. Ограниченность, замкнутость, компактность

Пусть M — произвольное метрическое пространство. Множество $S \subseteq M$ называется *ограниченным*, если существуют точка $a \in M$ и вещественное число $R > 0$ такие, что $\rho(a, x) < R$ для любой точки $x \in S$. Другими словами,

$$S \subseteq B(a, R) := \{x \in M : \rho(a, x) < R\} \subseteq \bar{B}(a, R) := \{x \in M : \rho(a, x) \leq R\}.$$

Множества $B(a, R)$ и $\bar{B}(a, R)$ называются соответственно *открытым* и *замкнутым шаром радиуса R с центром в точке a* . Последовательность называется *ограниченной*, если множество ее элементов ограничено.

Замыканием множества S называется множество $\bar{S}$ всех точек из M , которые являются пределами последовательностей точек, принадлежащих множеству S . Если множество совпадает со своим замыканием, то оно называется *замкнутым*. Множество называется *открытым*, если вместе с каждой точкой в нем находятся все точки некоторого открытого шара, содержащего эту точку. Замкнутое множество называется *компактным*, если из любой последовательности его точек можно выделить сходящуюся подпоследовательность.

¹⁾ Эта норма часто называется равномерной или чебышевской — в честь русского математика Пафнутия Львовича Чебышева.

Утверждение 6.3.1. *Любая фундаментальная последовательность является ограниченной.*

Доказательство. Фиксируем $\varepsilon > 0$ и натуральное число N такое, что при всех $m, n \geq N$ выполняется неравенство $\rho(x_m, x_n) < \varepsilon$. Применяя неравенство треугольника, для всех n находим

$$\rho(x_1, x_n) < R := \varepsilon + \max \{\rho(x_1, x_2), \rho(x_1, x_3), \dots, \rho(x_1, x_N)\}. \quad \square$$

Следствие 6.3.1. *Любое компактное множество является ограниченным.*

Доказательство. Предположим, что множество S неограничено. Тогда можно построить последовательность точек $x_n \in S$ такую, что $\rho(x_1, x_n) \geq n$ для всех n . Любая ее подпоследовательность будет неограниченной: если для какой-то точки $a \in M$ и какого-то числа $R > 0$ справедливы неравенства $\rho(a, x_{n_k}) < R$, то, согласно неравенству треугольника,

$$k \leq n_k \leq \rho(x_1, x_{n_k}) \leq \rho(x_1, a) + \rho(a, x_{n_k}) < \rho(x_1, a) + R,$$

что невозможно при достаточно больших номерах k . Таким образом, нет ни одной сходящейся подпоследовательности. $\square$

Вещественная функция $f(x)$ на метрическом пространстве M называется *непрерывной в точке $x \in M$* , если для любой последовательности x_n , сходящейся к x , имеет место сходимости последовательности значений $f(x_n)$ к $f(x)$.

Теорема 6.3.1 (ТЕОРЕМА ВЕЙЕРШТРАССА). *Вещественная функция $f(x)$, непрерывная в каждой точке компактного множества S , достигает на S своих максимального и минимального значений, т. е. существуют точки $a, b \in S$ такие, что $f(a) \leq f(x) \leq f(b)$ для всех $x \in S$.*

Доказательство. Докажем, что множество всех вещественных чисел $f(x)$ при $x \in S$ ограничено сверху и снизу. Неограниченность сверху означала бы существование последовательности точек $x_n \in S$, для которых $f(x_n) \geq n$. В силу компактности, должна быть сходящаяся подпоследовательность $x_{n_k} \rightarrow x \in S$, а в силу непрерывности функции $f(x)$ получаем $f(x_{n_k}) \rightarrow f(x)$. Последнее невозможно, поскольку в данном случае любая подпоследовательность, в том числе $f(x_{n_k})$, является неограниченной. Аналогично доказывается ограниченность снизу.

Обозначим через β точную верхнюю грань множества значений $f(x)$ при $x \in S$. Согласно определению точной верхней грани,

найдется последовательность $x_n \in S$ такая, что $\beta - \frac{1}{n} \leq f(x_n) \leq \beta$. Компактность множества S означает, что есть сходящаяся подпоследовательность $x_{n_k} \rightarrow b \in S$. Переходя к пределу в неравенствах, находим

$$\beta - \frac{1}{n} \leq \beta - \frac{1}{n_k} \leq f(x_{n_k}) \leq \beta \Rightarrow \lim_{k \rightarrow \infty} f(x_{n_k}) = f(b) = \beta.$$

Достижимость точной нижней грани доказывается аналогично. $\square$

Наша цель — доказать, что в конечномерном нормированном пространстве компактность множества равносильна его замкнутости и ограниченности. Для этого нам понадобится понятие эквивалентных норм и следующий частный пример компактного множества в специальном нормированном пространстве.

Лемма 6.3.1. Пусть V — конечномерное пространство, $e_1, \dots, e_n$ — его базис и норма вектора $x = \sum_{i=1}^n x_i e_i$ определяется формулой $\|x\| := \sum_{i=1}^n |x_i|$. Тогда единичная сфера $S = \{x \in V : \|x\| = 1\}$ является компактным множеством.

Доказательство. Рассмотрим произвольную последовательность $x^{(k)} = \sum_{i=1}^n x_i^{(k)} e_i$. Обозначим через s максимальное натуральное число, такое что существует подпоследовательность $x^{(k_l)}$, в которой последовательности первых s координат сходятся к каким-то пределам:

$$\lim_{l \rightarrow \infty} x_i^{(k_l)} = x_i, \quad 1 \leq i \leq s.$$

Поскольку последовательность первых координат $x_1^{(k)}$ ограничена, из нее можно выделить сходящуюся подпоследовательность $x_1^{(k_l)} \rightarrow x_1$. Следовательно, $s \geq 1$.

Докажем, что $s = n$. От противного, если $1 \leq s < n$, то последовательность $x_{s+1}^{(k_l)}$ является ограниченной и поэтому из нее можно выделить сходящуюся подпоследовательность, пусть $\lim_{m \rightarrow \infty} x_{s+1}^{(k_{l_m})} = x_{s+1}$. Таким образом,

$$\lim_{m \rightarrow \infty} x_i^{(k_{l_m})} = x_i, \quad 1 \leq i \leq s+1,$$

и возникает противоречие с максимальной s . $\square$

На одном и том же линейном пространстве V можно рассматривать разные нормы. Нормы $\|x\|_*$ и $\|x\|_\#$ называются *эквивалентными*, если существуют константы $c_1, c_2 > 0$, такие что

$$c_1 \|x\|_\# \leq \|x\|_* \leq c_2 \|x\|_\# \quad \forall x \in V.$$

Теорема 6.3.2. *Любые две нормы на одном и том же конечномерном линейном пространстве эквивалентны.*

Доказательство. Пусть $e_1, \dots, e_n$ — базис линейного пространства V и норма вектора $x = \sum_{i=1}^n x_i e_i$ определена формулой

$\|x\| = \sum_{i=1}^n |x_i|$. Докажем, что любая норма $\|x\|_*$ эквивалентна данной специальной норме $\|x\|$. Для этого заметим, что функция $f(x) := \|x\|_*$ является непрерывной на пространстве V , в котором для определения сходимости используется введенная нами специальная норма. В силу теоремы Вейерштрасса, на компактном множестве $S = \{x \in V : \|x\| = 1\}$ найдутся точки $a, b \in S$ такие, что $f(a) \leq f(x) \leq f(b)$ для всех $x \in S$. Положим $c_1 = f(a)$ и $c_2 = f(b)$. Тогда

$$c_1 \leq \|x\|_* \leq c_2 \quad \forall x \in S \Rightarrow c_1 \|x\| \leq \|x\|_* \leq c_2 \|x\| \quad \forall x \in V.$$

Заметим, что $\|a\| = 1 \Rightarrow a \neq 0 \Rightarrow c_1 = \|a\|_* > 0$. Если каждая из двух норм эквивалентна какой-то третьей норме, то эти две нормы эквивалентны. $\square$

Теорема 6.3.3. *В произвольном конечномерном нормированном пространстве компактность множества равносильна его замкнутости и ограниченности.*

Доказательство. Мы уже знаем, что компактное множество обязано быть замкнутым и ограниченным. Теперь рассмотрим произвольное замкнутое ограниченное множество S , фиксируем какой-либо базис $e_1, \dots, e_n$ и введем специальную норму $\|x\|$ как сумму модулей координат по данному базису. В силу эквивалентности норм в конечномерном пространстве для некоторого $R > 0$ имеем: $\|x\| \leq R$ для всех $x \in S$. Поэтому координаты каждого вектора $x \in S$ ограничены и мы можем повторить рассуждение из доказательства леммы 6.3.1. $\square$

Следствие 6.3.2. *Любое конечномерное нормированное пространство является полным.*

Доказательство. Фундаментальная последовательность x_n обязана быть ограниченной и поэтому принадлежит некоторому замкнутому шару, который является компактным множеством в конечномерном пространстве. Следовательно, имеется подпоследовательность x_{n_k} , которая сходится к какому-то элементу x данного шара. Далее, для любого $\varepsilon > 0$ при всех достаточно больших k получаем $\|x_k - x_{n_k}\| < \frac{\varepsilon}{2}$ (фундаментальность исходной последовательности) и $\|x_{n_k} - x\| < \frac{\varepsilon}{2}$ (сходимость подпоследовательности). Согласно неравенству треугольника, $\|x_k - x\| \leq \|x_k - x_{n_k}\| + \|x_{n_k} - x\| < \varepsilon$. $\square$

Пусть M — произвольное метрическое пространство и L — его непустое подмножество, элементы которого используются для приближения элементов $x \in M$. Элемент $z \in L$ называется *элементом наилучшего приближения* элемента x на множестве L , если $\rho(x, z) \leq \rho(x, y)$ для всех $y \in L$.

Теорема 6.3.4. *Пусть V — произвольное нормированное пространство и L — его конечномерное подпространство. Тогда для любого элемента $x \in V$ существует элемент $z \in L$ такой, что $\|x - z\| \leq \|x - y\|$ для всех $y \in L$.*

Доказательство. Пусть $\gamma = \inf_{y \in L} \|x - y\|$. Согласно определению точной нижней грани для некоторой последовательности точек $y_n \in L$ выполняются неравенства $\gamma \leq \|x - y_n\| \leq \gamma + \frac{1}{n}$. Очевидно, $\|y_n - y_1\| \leq \|x - y_1\| + \gamma + 1$ для всех $n \Rightarrow$ элементы y_n принадлежат замкнутому шару в конечномерном пространстве $L \Rightarrow$ существует подпоследовательность y_{n_k} , сходящаяся к некоторому элементу $z \in L$. При этом выполняются неравенства $\gamma \leq \|x - y_{n_k}\| \leq \gamma + \frac{1}{n_k} \leq \gamma + \frac{1}{k}$. Переходя к пределу, находим $\|x - z\| = \gamma$. $\square$

Пример. Пусть $V = C[-1, 1]$ — линейное пространство непрерывных вещественных функций на отрезке $[-1, 1]$ с чебышевской нормой $\|f(x)\| := \max_{-1 \leq x \leq 1} |f(x)|$, и пусть L — подпространство многочленов степени не выше чем n . Из теоремы 6.3.4 вытекает, что для любой непрерывной функции $f(x)$ на отрезке $[-1, 1]$ существует *многочлен наилучшего приближения* на L .

Можно также доказать его единственность¹⁾. Известно (и не очень сложно доказывается), что для функции $f(x) = x^{n+1}$ этот многочлен имеет вид

$$g(x) = x^{n+1} - 2^{-n} T_{n+1}(x), \quad \text{где } T_{n+1}(x) = \cos((n+1) \arccos x).$$

Нетрудно проверить, что для $n = 0, 1, \dots$ функция $T_n(x) = \cos(n \arccos x)$, определенная для всех x на отрезке $-1 \leq x \leq 1$, является многочленом со старшим коэффициентом 2^{n-1} — это знаменитые *многочлены Чебышева*.

Следствие 6.3.3. *Единичная сфера $S = \{x \in V : \|x\| = 1\}$ в нормированном пространстве V является компактным множеством в том и только том случае, когда пространство V конечномерно.*

Доказательство. Предположим, что пространство V бесконечномерно, и построим последовательность векторов e_n , принадлежащих сфере S и таких, что $\|e_i - e_j\| \geq 1$ при $i \neq j$. Данная последовательность не имеет ни одной фундаментальной подпоследовательности, а значит и ни одной сходящейся подпоследовательности. Поэтому множество S некомпактно.

В качестве e_1 возьмем произвольный вектор из S . По индукции, пусть уже построены векторы $e_1, \dots, e_n$, для которых $\|e_i - e_j\| \geq 1$ при $i \neq j$. Поскольку пространство V бесконечномерно, в нем имеется вектор x_{n+1} , не принадлежащий линейной оболочке L_n векторов $e_1, \dots, e_n$. Обозначим через z_{n+1} элемент наилучшего приближения элемента x_{n+1} на подпространстве L_n и положим

$$e_{n+1} := \frac{x_{n+1} - z_{n+1}}{\gamma_{n+1}}, \quad \gamma_{n+1} := \|x_{n+1} - z_{n+1}\|.$$

Тогда при $1 \leq i \leq n$ получаем

$$\|e_{n+1} - e_i\| = \frac{1}{\gamma_{n+1}} \|x_{n+1} - (z_{n+1} + \gamma_{n+1} e_i)\| \geq \frac{1}{\gamma_{n+1}} \gamma_{n+1} = 1. \quad \square$$

Задача 248. *Докажите, что конечномерное подпространство нормированного пространства является замкнутым, и приведите пример бесконечномерного подпространства, которое не является замкнутым.*

¹⁾ Для этого нужна *теорема Чебышева об альтернансе* — один из основных результатов теории равномерных приближений, включаемый в стандартные курсы вычислительных методов и численного анализа.

Задача 249. Всегда ли замыкание открытого шара совпадает с замкнутым шаром с тем же центром и того же радиуса?

Задача 250. В полном метрическом пространстве дана последовательность замкнутых шаров, в которой каждый шар вложен в предыдущий и радиусы шаров стремятся к нулю. Докажите, что все эти шары имеют ровно одну общую точку. Покажите также, что общей точки у вложенных шаров может не быть, если их радиусы не стремятся к нулю.

6.4. Нормы линейных операторов

Пусть M_1 и M_2 — метрические пространства. Отображение $f: M_1 \rightarrow M_2$ называется *непрерывным в точке* $x_0 \in M_1$, если для любой последовательности $x_n \in M_1$ из сходимости $x_n \rightarrow x_0$ следует $f(x_n) \rightarrow f(x_0)$. Если отображение непрерывно в каждой точке множества M , то оно называется *непрерывным на M* или просто *непрерывным*, если ясно, о каком множестве идет речь.

Пусть V и W — пространства с нормами $\|\cdot\|_V$ и $\|\cdot\|_W$. Если $A: V \rightarrow W$ — линейный оператор, то из его непрерывности в какой-то одной точке $x_0 \in V$ вытекает непрерывность на всем пространстве V .

Линейный оператор $A: V \rightarrow W$ называется *ограниченным*, если существует константа $c > 0$, для которой $\|Ax\|_W \leq c\|x\|_V$ для всех $x \in V$.

Теорема 6.4.1. *Непрерывность линейного оператора равносильна его ограниченности.*

Доказательство. Из ограниченности непрерывность в точке 0 выводится тривиальным образом, а из линейности следует непрерывность в любой точке. Теперь предположим, что линейный оператор $A: V \rightarrow W$ непрерывен. Если допустить его неограниченность, то найдется последовательность $x_n \in V$, такая что $\|Ax_n\|_W \geq n\|x_n\|_V$. Не ограничивая общности можно считать, что $\|x_n\|_V = 1 \Rightarrow y_n := x_n/\|Ax_n\|_W \rightarrow 0$, но $\|Ay_n\|_W = 1 \Rightarrow$ последовательность Ay_n не стремится к 0. $\square$

Пример неограниченного оператора. Пусть $a < b$ и $V = C^1[a, b]$ — линейное пространство вещественных функций, непрерывно дифференцируемых на отрезке $[a, b]$, а $W = C[a, b]$ — пространство непрерывных функций на $[a, b]$. Пусть на V и W

используется чебышевская норма $\|f\| = \max_{a \leq x \leq b} |f(x)|$. Тогда оператор дифференцирования $f(x) \rightarrow f'(x)$ линейный, но не будет ограниченным и поэтому не является непрерывным: для функций $f_n(x) := \sin(nx)$ при всех достаточно больших n находим $\|f_n\| = 1$ и $\|f'_n\| = n$.

Множество всех ограниченных линейных операторов $A: V \rightarrow W$ для фиксированных нормированных пространств V и W является линейным пространством, на котором для каждого оператора определена следующая *операторная норма*:

$$\|A\| := \sup_{0 \neq x \in V} \frac{\|Ax\|_W}{\|x\|_V} = \sup_{\|x\|_V=1} \|Ax\|_W.$$

Говорят, что норма $\|A\|$ *подчинена векторным нормам* $\|\cdot\|_V$ и $\|\cdot\|_W$.

Для комплексного (вещественного) нормированного пространства V линейное пространство непрерывных линейных функционалов с комплексными (вещественными) значениями называется *сопряженным пространством* и обозначается V^* . Норма для функционала $f \in V^*$ определяется как операторная норма вида

$$\|f\| := \sup_{0 \neq x \in V} \frac{|f(x)|}{\|x\|}$$

и называется *дуальной* к норме $\|x\|$.

Утверждение 6.4.1. *Операторная норма является нормой.*

Доказательство проводится очевидным образом и предоставляется читателю.

Утверждение 6.4.2. *Пусть V, W — нормированные пространства. Если V конечномерно, то любой линейный оператор $A: V \rightarrow W$ является ограниченным и его операторная норма достигается на векторе единичной сферы пространства V : $\|A\| = \|Ax_0\|_W$ и $\|x_0\|_V = 1$ для некоторого зависящего от A вектора x_0 .*

Доказательство. Функция $f(x) := \|Ax\|_W$ непрерывна на единичной сфере $S = \{x \in V: \|x\|_V = 1\}$. Если V конечномерно, то множество S компактно и мы можем применить теорему Вейерштрасса. $\square$

Пусть $A = [a_{ij}]$ — комплексная матрица размера $m \times n$. Тогда правило $x \rightarrow Ax$ определяет линейный оператор $A: \mathbb{C}^n \rightarrow \mathbb{C}^m$

умножения векторов на матрицу A . Наиболее популярные нормы для векторов $x = [x_1, \dots, x_n]^T$ имеют вид

$$\|x\|_2 := \sqrt{\sum_{i=1}^n |x_i|^2}, \quad \|x\|_1 := \sum_{i=1}^n |x_i|, \quad \|x\|_\infty := \max_{1 \leq i \leq n} |x_i|$$

и порождают операторные нормы

$$\|A\|_2 = \max_{x \neq 0} \frac{\|Ax\|_2}{\|x\|_2}, \quad \|A\|_1 = \max_{x \neq 0} \frac{\|Ax\|_1}{\|x\|_1}, \quad \|A\|_\infty = \max_{x \neq 0} \frac{\|Ax\|_\infty}{\|x\|_\infty}.$$

Напомним, что величина $\|A\|_2$ называется *спектральной нормой* и равна старшему сингулярному числу матрицы A (см. раздел 5.7).

Иногда нормы для операторов вводятся без какой-либо связи с векторными нормами. Наиболее важный пример — *евклидова*, или *фробениусова*, *норма* матрицы, определяемая как корень квадратный из суммы квадратов модулей ее элементов. Обозначение: $\|A\|_F$.

Удобно, когда для норм на пространствах $\mathbb{C}^{m \times n}$ при всех $m, n \in \mathbb{N}$ выполнено следующее *свойство мультипликативности*: $\|AB\| \leq \|A\| \|B\|$ для любых матриц A и B , которые можно перемножить. Термин *матричная норма* употребляется именно для таких случаев.

Задача 251. Пусть M_1 и M_2 — метрические пространства. Докажите, что для непрерывности отображения $f: M_1 \rightarrow M_2$ необходимо и достаточно, чтобы полным прообразом каждого открытого множества в M_2 было открытое множество в M_1 .

Задача 252. Пусть $A = [a_{ij}] \in \mathbb{C}^{m \times n}$. Докажите, что

$$\|A\|_1 = \max_{1 \leq j \leq n} \sum_{i=1}^m |a_{ij}|, \quad \|A\|_\infty = \max_{1 \leq i \leq m} \sum_{j=1}^n |a_{ij}|.$$

Задача 253. Докажите, что фробениусова норма матрицы является матричной нормой, т.е. нормой со свойством мультипликативности.

Задача 254. Докажите, что фробениусова норма матрицы не подчинена векторным нормам.

6.5. Выпуклые множества и выпуклые функции

Для дальнейшего изучения норм и неравенств нам нужен целый ряд фактов и построений геометрического характера, связанных с понятием выпуклости.

Пусть V — произвольное линейное пространство над полем вещественных чисел. Геометрические построения обычно используют точки, прямые, отрезки и т. д.

В этой связи будем считать, что точки отождествляются с векторами — при этом точка, определенная нулевым вектором, не имеет какого-либо особого геометрического смысла. Каждая упорядоченная пара точек a, b естественным образом определяет вектор $b - a$.

Если L — линейное подпространство пространства V и a — точка пространства V , то множество $A = a + L$ называется *плоскостью*, проходящей через точку a . Подпространство L называется *направляющим подпространством* данной плоскости. Легко видеть, что L совпадает с множеством разностей векторов, принадлежащих A , и поэтому определяется по A однозначно. Под *размерностью плоскости* понимается размерность ее направляющего подпространства.

Утверждение 6.5.1. *Пересечение произвольного числа плоскостей является либо пустым множеством, либо плоскостью, для которой направляющее подпространство есть пересечение направляющих подпространств заданных плоскостей.*

Пусть M — произвольное непустое множество точек. Пересечение всех плоскостей, содержащих M , называется *аффинной оболочкой* множества M и является наименьшей плоскостью, в которую вложено множество M . Линейная комбинация векторов называется *аффинной* или *барицентрической* комбинацией, если все ее коэффициенты вещественны и их сумма равна 1.

Утверждение 6.5.2. *Аффинная оболочка множества M совпадает с множеством всевозможных барицентрических комбинаций конечных систем векторов, принадлежащих множеству M .*

Доказательство. Пусть A — аффинная оболочка множества M . Если $a_1, \dots, a_n \in M$, то A можно представить в виде $A = a_1 + L$, где L — направляющее подпространство плоскости A .

Следовательно, $a_i - a_1 \in L$, и для произвольных вещественных α_i при $2 \leq i \leq n$ находим

$$a_1 + \sum_{i=2}^n \alpha_i (a_i - a_1) = \sum_{i=1}^n \alpha_i a_i \in A, \quad \alpha_1 := 1 - \sum_{i=2}^n \alpha_i, \quad \sum_{i=1}^n \alpha_i = 1.$$

Таким образом, все барицентрические комбинации векторов из M принадлежат A . Остается доказать, что множество всевозможных барицентрических комбинаций является плоскостью. Обозначим это множество через B . Легко проверяется, что множество разностей векторов из B , обозначим его L , образует подпространство, и в итоге $B = a + L$, где a — произвольно выбранный вектор из B . $\square$

Барицентрическая комбинация векторов $a_1, \dots, a_n$, в которой все коэффициенты неотрицательны, называется *выпуклой комбинацией*. Пусть a и b — произвольные векторы. Множество всех выпуклых комбинаций векторов (точек) a и b называется *отрезком с граничными точками a и b* и обозначается $[a, b]$. Мы говорим также, что отрезок $[a, b]$ *соединяет точки a и b* . Любая точка отрезка, отличная от граничных, называется *внутренней точкой*. Множество $M \subseteq V$ называется *выпуклым*, если вместе с любыми двумя точками оно содержит и все точки соединяющего их отрезка.

Пример 1. Любой шар.

Пример 2. Пусть заданы вещественные числа a_{ij} и b_i . Если множество вещественных арифметических векторов $(x_1, \dots, x_n)$, удовлетворяющих системе неравенств

$$\begin{array}{ccccccc} a_{11}x_1 + \dots + a_{1n}x_n & \leq & b_1, \\ & \dots & \dots & \dots & \\ a_{m1}x_1 + \dots + a_{mn}x_n & \leq & b_m, \end{array}$$

непусто, то оно является выпуклым.

Пример 3. Вещественная квадратная матрица A называется *двоякостохастической*, если все ее элементы неотрицательны и суммы элементов в любой ее строке и в любом ее столбце одинаковы и равны 1. Множество всех двоякостохастических матриц порядка n является выпуклым.

Утверждение 6.5.3. *Пересечение любого числа выпуклых множеств либо пусто, либо является выпуклым множеством.*

Пересечение всех выпуклых множеств, содержащих заданное непустое множество M , называется *выпуклой оболочкой* множества M и является наименьшим выпуклым множеством, в которое вложено множество M . Обозначение: $\text{conv}(M)$.

Утверждение 6.5.4. *Выпуклая оболочка множества M совпадает с множеством всевозможных выпуклых комбинаций конечных систем векторов, принадлежащих множеству M .*

Выпуклая оболочка конечного числа точек называется *выпуклым многогранником*. Если число точек равно $n + 1$, а размерность их аффинной оболочки равна n , то говорят, что точки находятся *в общем положении*. Выпуклая оболочка таких точек называется *n -мерным симплексом*. Множество линейных комбинаций заданных векторов $a_1, \dots, a_n$ с произвольными неотрицательными коэффициентами называется *конечнопорожденным конусом*. Обозначение: $\text{con}(a_1, \dots, a_n)$.

Теорема 6.5.1. *Конечнопорожденный конус является замкнутым множеством.*

Доказательство. Пусть $K_n = \text{con}(a_1, \dots, a_n)$. При $n = 1$ утверждение тривиально. По индукции, пусть $n > 1$ и пусть

$$\lim_{k \rightarrow \infty} \sum_{i=1}^n \alpha_i^{(k)} a_i = a, \quad \alpha_i^{(k)} \geq 0, \quad 1 \leq i \leq n, \quad k = 1, 2, \dots$$

Нам нужно доказать, что $a \in K_n$. Предположим, что для какого-то i координатная последовательность $\alpha_i^{(k)}$ при $k \rightarrow \infty$ не стремится к бесконечности и, значит, обладает ограниченной подпоследовательностью. Для определенности пусть $i = n$. Тогда можно выделить сходящуюся подпоследовательность $\alpha_n^{(k_l)} \rightarrow \alpha_n$ и имеет место равенство $\lim_{l \rightarrow \infty} \sum_{i=1}^{n-1} \alpha_i^{(k_l)} a_i = a - \alpha_n a_n$. Очевидно, $\alpha_n \geq 0$ и, по индуктивному предположению, $a - \alpha_n a_n \in K_{n-1} \Rightarrow a \in K_n$. Теперь рассмотрим случай, когда каждая координатная последовательность стремится к бесконечности. Тогда

$$\lim_{k \rightarrow \infty} \sum_{1 \leq i \leq n, i \neq j} \frac{\alpha_i^{(k)}}{\alpha_j^{(k)}} a_i = -a_j, \quad 1 \leq j \leq n.$$

По индуктивному предположению, $-a_j \in K_{n-1} \subseteq K_n$. Таким образом, для каждого j оба вектора a_j и $-a_j$ принадлежат $K_n \Rightarrow$ множество K_n является конечномерным подпространством и поэтому замкнуто. $\square$

Вещественная функция $f(x)$, определенная на выпуклом множестве M , называется *выпуклой*, если для любых точек $a, b \in M$ и любой их выпуклой комбинации выполняется неравенство

$$f(\alpha a + \beta b) \leq \alpha f(a) + \beta f(b), \quad \alpha, \beta \geq 0, \quad \alpha + \beta = 1.$$

Из определения вытекает, что для любых точек $a_1, \dots, a_n \in V$ и любой их выпуклой комбинации выполняется неравенство

$$f\left(\sum_{i=1}^n \alpha_i a_i\right) \leq \sum_{i=1}^n \alpha_i f(a_i), \quad \alpha_1, \dots, \alpha_n \geq 0, \quad \sum_{i=1}^n \alpha_i = 1.$$

Функция $f(x)$ называется *вогнутой*, если функция $\phi(x) := -f(x)$ выпукла.

Утверждение 6.5.5. Пусть $M \subseteq \mathbb{R}$ — выпуклое множество, вещественная функция $f(x)$ дважды дифференцируема в любой его точке и вторая производная неотрицательна, т.е. $f''(x) \geq 0$ для всех $x \in M$. Тогда функция $f(x)$ выпукла на множестве M .

Доказательство. Пусть $a, b \in M$ и $a < c < b$. Согласно теореме Лагранжа из анализа, имеем равенства

$$\begin{aligned} f(c) - f(a) &= f'(\theta)(c - a), \quad a < \theta < c, \\ f(b) - f(c) &= f'(\tau)(b - c), \quad c < \tau < b, \\ f'(\tau) - f'(\theta) &= f''(\xi)(\tau - \theta), \quad \theta < \xi < \tau. \end{aligned}$$

Отсюда

$$\begin{aligned} 0 \leq f''(\xi) &= \frac{1}{\tau - \theta} \left(\frac{f(b) - f(c)}{b - c} - \frac{f(c) - f(a)}{c - a} \right) \Rightarrow \\ \Rightarrow f(c) &\leq \frac{b - c}{b - a} f(a) + \frac{c - a}{b - a} f(b), \quad c = \frac{b - c}{b - a} a + \frac{c - a}{b - a} b. \quad \square \end{aligned}$$

Следствие 6.5.1. Функция $F(x) = -\ln x$ выпукла на множестве $\{x \in \mathbb{R}: x > 0\}$.

Следствие 6.5.2. Для любых неотрицательных чисел $x_1, \dots, x_n$ справедливо неравенство ¹⁾

$$(x_1 \dots x_n)^{1/n} \leq \frac{x_1 + \dots + x_n}{n}.$$

Доказательство. Если хотя бы одно из чисел $x_1, \dots, x_n$ равно нулю, то неравенство очевидно. Пусть все они отличны от нуля. Тогда, используя выпуклость функции $F(x) = -\ln x$, находим

$$\begin{aligned} F\left(\frac{1}{n}x_1 + \dots + \frac{1}{n}x_n\right) &\leq \frac{1}{n}F(x_1) + \dots + \frac{1}{n}F(x_n) \Rightarrow \\ &\Rightarrow \ln(x_1 \dots x_n)^{1/n} \leq \ln\left(\frac{x_1 + \dots + x_n}{n}\right). \quad \square \end{aligned}$$

Ниже под *окрестностью* точки x понимается любой содержащий ее открытый шар. Точка x называется *внутренней точкой* множества M , если все точки некоторой ее окрестности принадлежат M . Точка x называется *граничной точкой* множества M , если в любой ее окрестности есть точки как из M , так и внешние для M , при этом x может и не быть точкой множества M . Точка $x \in M$ называется *угловой* или *крайней точкой* множества M , если нет ни одного принадлежащего M отрезка, для которого она является внутренней точкой. Для разных норм множества окрестностей будут, вообще говоря, разные, но очевидно, что при переходе к любой эквивалентной норме внутренние и граничные точки множества M будут те же.

Очевидно, что любая внутренняя точка $x \in M$ является также *линейно внутренней* — это значит, что для любой проходящей через нее прямой точка x является внутренней точкой отрезка данной прямой, все точки которого принадлежат M . Понятие линейно внутренней точки вообще не зависит от нормы. Выпуклое множество, обладающее хотя бы одной линейно внутренней точкой, называется *выпуклым телом*. В конечномерном пространстве, конечно, любая линейно внутренняя точка будет также внутренней точкой по отношению к любой

¹⁾ Левая часть неравенства известна как среднее геометрическое, а правая часть — как среднее арифметическое чисел $x_1, \dots, x_n$.

норме. В бесконечномерном нормированном пространстве все сложнее ¹⁾, но граничные точки и замыкание выпуклого тела, обладающего внутренней точкой, имеют, тем не менее, очень специальное строение.

Утверждение 6.5.6. Пусть M — выпуклое тело в нормированном пространстве и a — его внутренняя точка. Точка b является граничной для M в том и только том случае, когда $a + t(b - a) \in M$ при $0 \leq t < 1$ и $a + t(b - a) \notin M$ при $t > 1$.

Доказательство. Если $c \in M$, то все точки отрезка $[a, c]$ будут внутренними, кроме, возможно, точки c : для некоторого $r > 0$ имеется шар $W := B(a, r) \subset M$ и отсюда легко вывести, что для любой внутренней точки d отрезка $[a, c]$ выпуклая оболочка множества $\{c\} \cup W$ будет содержать шар с центром в точке d , целиком принадлежащий M . Если b — граничная точка для M , то найдется последовательность $b_n \in M$, сходящаяся к b . Если $c = a + t(b - a) \in M$ при каком-то $t > 1$, то точка b будет внутренней для отрезка $[a, c]$, а значит и внутренней для множества M . Далее, взяв точку $c = a + t(b - a)$ при $0 < t < 1$, мы можем заметить, что при достаточно большом n точка b_n будет настолько близка к точке b , что c попадет во внутренность выпуклой оболочки множества $\{b_n\} \cup W$. $\square$

В заключение заметим, что понятие выпуклого множества имеет смысл и в комплексных линейных пространствах. Так, нетрудно показать, что единичный замкнутый шар B в *любом* нормированном пространстве является ограниченным замкнутым выпуклым телом с внутренней точкой 0 и следующим свойством симметрии: если $x \in B$, то $\alpha x \in B$ для всех чисел α , таких что $|\alpha| \leq 1$ (в комплексном случае $\alpha \in \mathbb{C}$). Более того, можно доказать, что любое множество B с перечисленными выше свойствами является единичным шаром для нормы, которая задается следующим функционалом Минковского:

$$f(x) := \inf \left\{ \alpha > 0: \frac{1}{\alpha} x \in B \right\}.$$

¹⁾ Линейно внутренняя точка может не быть внутренней. Например, пусть V — линейное пространство непрерывно дифференцируемых функций на отрезке $[0, 1]$ с нормой $\|f\|_C = \max_{0 \leq x \leq 1} |f(x)|$. Тогда множество $M := \{f \in V: \|f\|_C + \|f'\|_C \leq 1\}$ выпукло, точка $f = 0$ является для него линейно внутренней, но $f_n(x) := \frac{\sin(nx)}{\sqrt{n}} \notin M$ при всех достаточно больших n и $f_n(x) \rightarrow 0$ при $n \rightarrow \infty$.

Задача 255. Докажите, что угловыми точками множества двоякостохастических матриц порядка n являются матрицы перестановки и только они. Что представляют собой граничные точки этого множества?

Задача 256. Докажите, что множество всех внутренних точек выпуклого тела и замыкание любого выпуклого множества являются выпуклыми множествами.

Задача 257. Пусть M — выпуклое множество, обладающее внутренней точкой, и $\bar{M}$ — его замыкание. Докажите, что ни одна точка множества $\bar{M} \setminus M$ не является внутренней точкой множества $\bar{M}$.

Задача 258. Пусть V — нормированное пространство и B — замкнутое ограниченное выпуклое тело, для которого нуль является внутренней точкой и вместе с любой точкой $x \in B$ множество B содержит все точки вида αx при $|\alpha| \leq 1$. Докажите, что функционал Минковского задает некоторую, возможно другую, норму на пространстве V , для которой множество B является единичным шаром.

Задача 259. В гильбертовом пространстве $l_2(\mathbb{R})$ рассматривается «гильбертов кирпич» — множество вида

$$M := \left\{ (x_1, x_2, \dots) \in l_2(\mathbb{R}) : |x_k| \leq \frac{1}{k}, \quad k = 1, 2, \dots \right\}.$$

Докажите, что множество M выпукло, замыкание его аффинной оболочки совпадает с $l_2(\mathbb{R})$ и в то же время M не имеет ни одной внутренней точки.

6.6. Неравенства Гёльдера и Минковского

На пространстве $\mathbb{C}^n$ популярны так называемые p -нормы Гёльдера, определяемые для любого $p \geq 1$ следующим образом:

$$\|x\|_p := \left(\sum_{i=1}^n |x_i|^p \right)^{1/p}, \quad x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

При проверке свойств нормы для p -норм затруднение вызывает лишь неравенство треугольника

$$\|x + y\|_p \leq \|x\|_p + \|y\|_p, \quad x, y \in \mathbb{C}^n,$$

которое в данном случае называется *неравенством Минковского*. Чтобы его доказать, нам понадобится ряд вспомогательных неравенств, имеющих также самостоятельную ценность.

Пара положительных чисел p, q называется *парой Гёльдера*, если $\frac{1}{p} + \frac{1}{q} = 1$.

Лемма 6.6.1. Для любой пары Гёльдера p, q и любых $a, b \geq 0$ справедливо неравенство

$$ab \leq \frac{a^p}{p} + \frac{b^q}{q}.$$

Доказательство. Используем выпуклость функции $F(x) = -\ln x$:

$$\begin{aligned} F\left(\frac{1}{p} a^p + \frac{1}{q} b^q\right) &\leq \frac{1}{p} F(a^p) + \frac{1}{q} F(b^q) \Rightarrow \\ \Rightarrow \ln(ab) &= \frac{1}{p} \ln a^p + \frac{1}{q} \ln b^q \leq \ln\left(\frac{1}{p} a^p + \frac{1}{q} b^q\right). \quad \square \end{aligned}$$

Теорема 6.6.1 (неравенство Гёльдера). Для любой пары Гёльдера p, q и произвольных неотрицательных чисел $x_1, \dots, x_n$ и $y_1, \dots, y_n$ имеет место неравенство

$$\sum_{i=1}^n x_i y_i \leq \left(\sum_{i=1}^n x_i^p\right)^{1/p} \left(\sum_{i=1}^n y_i^q\right)^{1/q}.$$

Доказательство. Положим $A = \left(\sum_{i=1}^n x_i^p\right)^{1/p}$, $B = \left(\sum_{i=1}^n y_i^q\right)^{1/q}$.

Если $A = 0$ или $B = 0$, то неравенство тривиально. В случае ненулевых A, B для каждого $1 \leq i \leq n$ запишем, а затем сложим следующие равенства:

$$\left(\frac{x_i}{A}\right) \left(\frac{y_i}{B}\right) \leq \frac{x_i^p}{p A^p} + \frac{y_i^q}{q B^q} \Rightarrow \frac{\sum_{i=1}^n x_i y_i}{AB} \leq \frac{1}{p} + \frac{1}{q} = 1. \quad \square$$

Теорема 6.6.2 (неравенство Минковского). Для любого $p \geq 1$ и любых векторов $x, y \in \mathbb{C}^n$ выполняется неравенство $\|x + y\|_p \leq \|x\|_p + \|y\|_p$.

Доказательство. В случае $p = 1$ неравенство Минковского сразу же следует из неравенств треугольника для модуля ком-

плексных чисел: $|x_i + y_i| \leq |x_i| + |y_i|$. Пусть $p > 1$ и числа p, q образуют пару Гёльдера. Теперь получаем

$$\|x + y\|_p^p = \sum_{i=1}^n |x_i + y_i| |x_i + y_i|^{p-1} \leq A + B,$$

$$A = \sum_{i=1}^n |x_i| |x_i + y_i|^{p-1}, \quad B = \sum_{i=1}^n |y_i| |x_i + y_i|^{p-1}.$$

Для величин A и B запишем неравенство Гёльдера:

$$A \leq \|x\|_p C, \quad B \leq \|y\|_p C, \quad C = \left(\sum_{i=1}^n |x_i + y_i|^{(p-1)q} \right)^{1/q}.$$

Заметим, что $(p-1)q = p \Rightarrow C = \|x + y\|_p^{p/q} \Rightarrow \|x + y\|_p^p / C = \|x + y\|_p$. $\square$

Задача 260. Пусть $x = [x_1, \dots, x_n]^\top \in \mathbb{C}^n$. Докажите, что

$$\lim_{p \rightarrow +\infty} \|x\|_p = \|x\|_\infty := \max_{1 \leq i \leq n} |x_i|.$$

Задача 261. Числа $p, q > 1$ образуют пару Гёльдера, т. е. $\frac{1}{p} + \frac{1}{q} = 1$. Докажите, что $\max_{\|x\|_p=1} |y^* x| = \|y\|_q$, $x, y \in \mathbb{C}^n$.

Задача 262. Найдите все угловые точки единичных шаров

$$B_p = \{x \in \mathbb{R}^n : \|x\|_p \leq 1\}, \quad 1 \leq p \leq \infty.$$

6.7. Наилучшие приближения на выпуклых множествах

Теорема 6.7.1. Пусть V — полное пространство со скалярным произведением и $M \subset V$ — замкнутое выпуклое множество. Тогда для любого вектора $x \in V$ существует и притом единственный вектор $z \in M$, такой что $\|x - z\| \leq \|x - y\|$ для всех $y \in M$. Кроме того, в вещественном случае $(x - z, y - z) \leq 0$ для всех $y \in M$.

Доказательство. Пусть $\gamma = \inf_{y \in M} \|x - y\|$ и последовательность $y_n \in M$ обеспечивает неравенства $\gamma^2 \leq \|x - y_n\|^2 \leq \gamma^2 + \frac{1}{n}$. Согласно тождеству параллелограмма

$$\|x - y_m\|^2 + \|x - y_n\|^2 = 2\|x - \frac{1}{2}(y_m + y_n)\|^2 + 2\|\frac{1}{2}(y_m - y_n)\|^2.$$

Выпуклость нужна лишь для того, чтобы утверждать, что $\frac{1}{2}(y_m + y_n) \in M \Rightarrow \|x - \frac{1}{2}(y_m + y_n)\| \geq \gamma$. Используя последнее неравенство, находим

$$\|y_m - y_n\|^2 \leq 2\left(\gamma^2 + \frac{1}{m}\right) + 2\left(\gamma^2 + \frac{1}{n}\right) - 4\gamma^2 \leq 2\left(\frac{1}{m} + \frac{1}{n}\right).$$

Таким образом, последовательность y_n фундаментальна и в силу полноты пространства V сходится к некоторому элементу $z \in V$. Множество M замкнуто, поэтому $z \in M$. Пусть z_1 и z_2 — два элемента наилучшего приближения для x . Тогда $\frac{1}{2}(z_1 + z_2) \in M$ и поэтому

$$\begin{aligned} \|z_1 - z_2\|^2 &\leq 2\|x - z_1\|^2 + 2\|x - z_2\|^2 - \\ &\quad - 4\left\|x - \frac{1}{2}(z_1 + z_2)\right\|^2 \leq 0 \Rightarrow z_1 = z_2. \end{aligned}$$

Теперь предположим, что V — вещественное пространство. Пусть y — произвольный вектор из M . Тогда при всех $0 < \varepsilon < 1$ вектор $z + \varepsilon(y - z)$ принадлежит M . Значит,

$$\begin{aligned} \gamma^2 &\leq \|x - z - \varepsilon(y - z)\|^2 = \\ &= \|x - z\|^2 - 2\varepsilon(x - z, y - z) + \varepsilon^2\|y - z\|^2 \Rightarrow \\ &\Rightarrow (x - z, y - z) \leq \frac{\varepsilon}{2}\|y - z\|^2 \quad \forall 0 < \varepsilon < 1 \Rightarrow \\ &\Rightarrow (x - z, y - z) \leq 0. \quad \square \end{aligned}$$

Следствие 6.7.1. Пусть V — вещественное полное пространство со скалярным произведением и L — его замкнутое подпространство. Тогда для любого вектора $x \in V$ существует и притом единственное разложение

$$x = z + h, \quad z \in L, \quad h \perp L.$$

Доказательство. Любое подпространство является выпуклым множеством. В силу теоремы 6.7.1 для любого вектора $x \in V$ существует элемент наилучшего приближения $z \in L$. Для вектора $h = x - z$ находим $(h, y - z) \leq 0 \quad \forall y \in L \Rightarrow (h, y) \leq 0 \quad \forall y \in L \Rightarrow (h, y) = 0 \quad \forall y \in L \Leftrightarrow h \perp L$. Далее, если $x = z + h = z' + h'$ и при этом $z, z' \in L$ и $h, h' \perp L$, то вектор $z - z' = h' - h$ принадлежит L и одновременно ортогонален L и поэтому равен нулю. $\square$

В качестве еще одного следствия получается очень полезная теорема о представлении непрерывных линейных функционалов.

Теорема 6.7.2 (ТЕОРЕМА РИССА). Пусть V — полное пространство со скалярным произведением и $f(x)$ — непрерывный линейный функционал на V . Тогда существует и притом единственный вектор $h \in V$, для которого $f(x) = (x, h)$ для всех $x \in V$.

Доказательство. Множество $H := \{x \in V : f(x) = 0\}$ является линейным подпространством и в силу непрерывности $f(x)$ замкнуто. Если $H = V$, то можно взять $h = 0$. Если $H \neq V$, то существует ненулевой вектор $x_0 \notin H$ и его можно представить в виде $x_0 = z_0 + h_0$, где $z_0 \in H$ и $h_0 \perp H$. Ясно, что $f(h_0) \neq 0$.

Для произвольного вектора $x \in V$ рассмотрим уравнение $f(x - \alpha h_0) = 0$ относительно α . Оно имеет единственное решение $\alpha = \alpha(x) = f(x)/f(h_0)$, и при этом $z(x) := x - \alpha(x)h_0 \in H$. Таким образом, для произвольного вектора $x \in V$ получаем

$$\begin{aligned} x &= z(x) + \alpha(x)h_0, & z(x) &\in H, & h_0 &\perp H \Rightarrow \\ &\Rightarrow (x, h_0) = \alpha(x)\|h_0\|^2 \Rightarrow \\ &\Rightarrow f(x) = \alpha(x)f(h_0) = \frac{(x, h_0)}{\|h_0\|^2} f(h_0) = (x, h), & h &:= \frac{\overline{f(h_0)}}{\|h_0\|^2} h_0. \end{aligned}$$

Вектор h определен однозначно: пусть $(x, h_1) = (x, h_2) \forall x \in V \Rightarrow (x, h_1 - h_2) = 0$ при $x = h_1 - h_2 \Rightarrow h_1 - h_2 = 0$. $\square$

Задача 263. Пусть V — гильбертово пространство и V^* — его сопряженное пространство. Докажите, что существует изоморфизм $\phi: V \rightarrow (V^*)^*$, сохраняющий не только операции, но и норму, т.е. $\|\phi(x)\| = \|x\|$ для всех $x \in V$. Изоморфны ли пространства V и V^* ?

6.8. Разделяющие и опорные гиперплоскости

Обсудим геометрический смысл следующей теоремы, непосредственно вытекающей из теоремы 6.7.1.

Теорема 6.8.1. Пусть M — произвольное замкнутое выпуклое множество в вещественном полном пространстве со скалярным произведением. Тогда для любого вектора $x \notin M$ существует вектор $h \neq 0$, такой что $(h, y) \leq (h, x) - \|h\|^2$ для всех $y \in M$.

Доказательство. Используя обозначения теоремы 6.7.1, положим $h := x - z \Rightarrow (h, y - z) = (h, y) - (h, x) + (h, h) \leq 0 \forall y \in M$. $\square$

Пусть V — вещественное пространство и на нем задана непостоянная *аффинная функция*, т. е. функция вида $f(\xi) = \phi(\xi) - c$, где $\phi(x)$ — линейный функционал, не равный нулю тождественно, и c — вещественное число. Множество $V_0 = \{\xi \in V: f(\xi) = 0\}$ нулей аффинной функции $f(\xi)$ представляет собой *гиперплоскость*. Говорят, что точки ξ_1 и ξ_2 расположены *по разные стороны* от гиперплоскости, если отрезок $[\xi_1, \xi_2]$ пересекается с гиперплоскостью в какой-то одной внутренней точке. В противном случае точки ξ_1 и ξ_2 считаются расположенными *по одну сторону* от гиперплоскости.

Утверждение 6.8.1. Точки ξ_1 и ξ_2 лежат по разные стороны от гиперплоскости $f(\xi) = 0$ в том и только том случае, когда значения $f(\xi_1)$ и $f(\xi_2)$ отличны от нуля и имеют разные знаки.

Гиперплоскость V_0 совпадает с пересечением множеств

$$V_+ = \{\xi: f(\xi) \geq 0\}, \quad V_- = \{\xi: f(\xi) \leq 0\},$$

которые называются *полупространствами*. Множества $V_+ \setminus V_0$ и $V_- \setminus V_0$ называются соответствующими *открытыми полупространствами*. В вещественном пространстве со скалярным произведением функция $f(\xi) := (h, \xi) - c$, $h \neq 0$, является, очевидно, непостоянной аффинной функцией. Теорема 6.8.1 утверждает, что имеется гиперплоскость, относительно которой точка x и все точки замкнутого выпуклого множества M расположены в разных полупространствах. Такая гиперплоскость называется *строго разделяющей* точку $x \notin M$ и множество M .

Любая гиперплоскость, проходящая через граничную точку выпуклого множества M и такая, что все точки множества M лежат по одну сторону от нее, называется *опорной гиперплоскостью* множества M . Из теоремы 6.8.1 вытекает, что в полном пространстве со скалярным произведением для любой точки x , лежащей вне замкнутого выпуклого множества M , существует опорная гиперплоскость множества M , строго разделяющая x и M .

Теорема 6.8.2. Через любую граничную точку замкнутого выпуклого множества в конечномерном вещественном про-

пространстве проходит хотя бы одна опорная гиперплоскость данного множества.

Доказательство. Пусть x — граничная точка замкнутого выпуклого множества M . Тогда имеется последовательность точек $x_n \notin M$, сходящаяся к x . Обозначим через $z_n \in M$ однозначно определенный элемент наилучшего приближения точки x_n . Тогда

$$(h_n, y) < (h_n, x_n) \quad \forall y \in M, \quad h_n := \frac{x_n - z_n}{\|x_n - z_n\|}.$$

В силу компактности единичной сферы в конечномерном пространстве существует сходящаяся подпоследовательность $h_{n_k} \rightarrow h$, $\|h\| = 1$. После перехода к пределу в неравенствах $(h_{n_k}, y) < (h_{n_k}, x_{n_k})$ получаем $(h, y) \leq (h, x)$. Искомая опорная гиперплоскость есть множество нулей аффинной функции $f(\xi) := (h, \xi) - (h, x)$. $\square$

Вот одно из применений теоремы об опорной гиперплоскости.

Теорема 6.8.3. *Любая точка компактного выпуклого множества в конечномерном пространстве является выпуклой комбинацией каких-то угловых точек этого множества.*

Доказательство. Рассмотрим произвольное компактное выпуклое множество M , расположенное в n -мерной плоскости, и проведем индукцию по n . Предположим, что точка $x \in M$ является внутренней для M . Тогда любая прямая, проходящая через x , содержит ровно две граничные точки множества M . Обозначим их через a и b . Пусть P_a и P_b — опорные гиперплоскости, проходящие через точки a и b соответственно. Множества $P_a \cap M$ и $P_b \cap M$ будут компактными выпуклыми множествами, принадлежащими плоскости размерности $n - 1$, и несложно проверяется, что каждая угловая точка для них будет одновременно угловой точкой множества M . Далее, в силу индуктивного предположения, каждая из точек a и b будет выпуклой комбинацией каких-то угловых точек и в то же время x есть выпуклая комбинация точек a и b . Если x — граничная точка, то индуктивное предположение применяется к множеству $P_x \cap M$, где P_x — опорная гиперплоскость, проходящая через точку x . $\square$

Следствие 6.8.1 (ТЕОРЕМА БИРКГОФФА). *Любая двоякостохастическая матрица является выпуклой комбинацией каких-то матриц перестановки.*

Задача 264. A — выпуклое тело, B — выпуклое множество. Докажите, что множество $A + B := \{a + b: a \in A, b \in B\}$ является выпуклым телом.

Задача 265. Множество $M \subset \mathbb{R}^n$ выпукло, но не замкнуто. Докажите, что любая граничная точка для M обладает опорной гиперплоскостью.

Задача 266. Докажите, что произвольную двоякостochasticкую матрицу порядка n можно выразить в виде выпуклой комбинации матриц перестановки, число которых не превышает n^2 .

Задача 267. Приведите пример замкнутого выпуклого множества в бесконечномерном пространстве, в котором для граничной точки нет ни одной опорной гиперплоскости.

6.9. Продолжение линейных функционалов

Часто бывает так, что линейный функционал обладает интересными для нас свойствами, но определен лишь на некотором подпространстве. Можно ли доопределить (говорят также — *продолжить*) его на все пространство с сохранением тех же самых свойств? Этот вопрос удивительным образом связан с получением разделяющей гиперплоскости.

Пусть V — вещественное линейное пространство и на нем задан функционал $p(x)$, принимающий вещественные значения и такой, что $p(\alpha x) = \alpha p(x)$ для всех $\alpha \geq 0$ и $p(x + y) \leq p(x) + p(y)$ для всех $x, y \in V$. В таких случаях $p(x)$ называется *квазинормой*.

Теорема 6.9.1 (ТЕОРЕМА ХАНА–БАНАХА). Пусть V — вещественное линейное пространство с квазинормой $p(x)$, и пусть $f(x)$ — линейный функционал, заданный на подпространстве $L \subset V$ и удовлетворяющий неравенству $f(x) \leq p(x)$ для всех $x \in L$. Тогда $f(x)$ можно продолжить на V с сохранением данного неравенства для всех $x \in V$.

Доказательство. Возьмем точку $x_0 \notin L$ и докажем, что $f(x)$ можно продолжить на подпространство $M := L + \langle x_0 \rangle$. Для этого нужно найти подходящее значение $c = f(x_0) \in \mathbb{R}$ таким образом, чтобы выполнялось неравенство

$$f(x + \alpha x_0) = f(x) + \alpha c \leq p(x + \alpha x_0) \quad \forall x \in L, \forall \alpha \in \mathbb{R}.$$

При $\alpha = 0$ неравенство выполняется при любом c . В случаях $\alpha = \pm\beta$, $\beta > 0$, неравенство принимает такие формы:

$$f(x) + \beta c \leq p(x + \beta x_0) \Leftrightarrow f(u) + c \leq p(u + x_0), \quad u = \frac{1}{\beta} x,$$

$$f(x) - \beta c \leq p(x - \beta x_0) \Leftrightarrow f(v) - c \leq p(v - x_0), \quad v = \frac{1}{\beta} x.$$

Таким образом, подходит любое значение c , удовлетворяющее неравенствам

$$f(v) - p(v - x_0) \leq c \leq p(u + x_0) - f(u), \quad \forall u, v \in L.$$

Такое число c заведомо существует, если правая часть при всех $u \in L$ не больше левой части при всех $v \in L$. Чтобы это доказать, нужно использовать свойства квазинормы:

$$\begin{aligned} f(u) + f(v) = f(u + v) &\leq p(u + v) = p((u + x_0) + (v - x_0)) \leq \\ &\leq p(u + x_0) + p(v - x_0) \Rightarrow f(v) - p(v - x_0) \leq \\ &\leq p(u + x_0) - f(u) \quad \forall u, v \in L. \end{aligned}$$

Доказательство завершается применением леммы Цорна, которая появится у нас позже (см. раздел 8.8)¹⁾. $\square$

Следствие 6.9.1. Пусть V — вещественное нормированное пространство и линейный функционал $f(x)$ определен на подпространстве $L \subset V$ и при некотором $c > 0$ удовлетворяет неравенству $|f(x)| \leq c\|x\|$ для всех $x \in L$. Тогда $f(x)$ можно продолжить на все пространство V с сохранением данного неравенства для всех $x \in V$.

Доказательство. Функционал $p(x) := c\|x\|$ является квазинормой и $f(x) \leq p(x)$ для всех $x \in L$. Согласно теореме Хана–Банаха, можно считать, что $f(x)$ определен при всех $x \in V$ и удовлетворяет тому же неравенству. Если $f(x) \geq 0$, то

¹⁾ На множестве подпространств вводим частичный порядок: считаем, что $L_1 \leq L_2$, если $L \subseteq L_1 \subseteq L_2$ и существуют линейные функционалы $f_1(x)$ на L_1 и $f_2(x)$ на L_2 , такие что каждый не превосходит $p(x)$ на своей области определения, каждый является продолжением исходного функционала $f(x)$ и при этом $f_1(x) = f_2(x)$ для всех $x \in L_1$. Совсем легко проверяется, что любая цепь подпространств имеет верхнюю границу, и значит, согласно лемме Цорна, существует подпространство M со свойством $Z \leq M$ для любого сравнимого с ним подпространства Z . Если $Z \neq V$, то предыдущее рассуждение показывает, что исходный функционал можно продолжить на более широкое подпространство, а это будет противоречить максимальности подпространства M .

$|f(x)| = f(x) \leq c\|x\|$. Если $f(x) < 0$, то $|f(x)| = f(-x) \leq c\|-x\| = c\|x\|$. $\square$

Утверждение 6.9.1. Пусть x_0 — линейно внутренняя точка выпуклого тела M в вещественном пространстве V . Тогда $M \subseteq \{x \in V : p(x - x_0) \leq 1\}$, где $p(u)$ — некоторая квазинорма на пространстве V .

Доказательство. Искомой квазинормой является функционал Минковского $p(u) := \inf \{\alpha > 0 : x_0 + \frac{1}{\alpha} u \in M\}$. $\square$

Следствие 6.9.2. Пусть M — выпуклое тело в вещественном пространстве V и точка $z \in V$ не является линейно внутренней для M . Тогда существует аффинная функция $f(x)$, такая что $f(x) \leq f(z)$ для всех $x \in M$.

Доказательство. Пусть x_0 — линейно внутренняя точка для M и $p(u)$ — квазинорма из утверждения 6.9.1. Положим $u_0 := z - x_0$ и на подпространстве $L = \langle u_0 \rangle$ определим линейный функционал $\phi(\alpha u_0) := \alpha p(u_0)$. При $\alpha \geq 0$ получаем: $\phi(\alpha u_0) = p(\alpha u_0)$, $\phi(-\alpha u_0) = -\alpha p(u_0)$ и $0 = p(0) = p(-\alpha u_0 + \alpha u_0) \leq p(-\alpha u_0) + \alpha p(u_0)$. Следовательно, $-\alpha p(u_0) \leq p(-\alpha u_0) \Rightarrow \phi(\alpha u_0) \leq p(\alpha u_0) \forall \alpha \in \mathbb{R}$. Согласно теореме Хана-Банаха можно считать, что функционал $\phi(u)$ определен при всех $u \in V$ и удовлетворяет неравенству $\phi(u) \leq p(u)$. Искомая аффинная функция имеет вид $f(x) = \phi(x) - \phi(x_0)$. Действительно, $x \in M \Rightarrow p(x - x_0) \leq 1 \leq p(z - x_0) = f(z)$ и $f(x) \leq p(x - x_0)$, и значит, если $p(x - x_0) \leq 1$, то $f(x) \leq f(z)$. $\square$

Теорема 6.9.2. Пусть V — комплексное нормированное пространство и линейный функционал $f(x)$ определен на подпространстве $L \subset V$ и удовлетворяет неравенству $|f(x)| \leq c\|x\|$ для всех $x \in L$. Тогда $f(x)$ можно продолжить на V с сохранением того же неравенства для всех $x \in V$.

Доказательство. Обозначим через V' вещественное линейное пространство с множеством векторов V и через L' — его подпространство с множеством векторов L . Запишем $f(x) = g(x) + ih(x)$, где $g(x), h(x) \in \mathbb{R}$. Тогда $g(x)$ и $h(x)$ — это вещественные линейные функционалы на вещественном пространстве L' и при этом $h(x) = -g(ix)$. Продолжим $g(x)$ на V' с сохранением неравенства $|g(x)| \leq c\|x\|$ для всех $x \in V'$ и заметим, что функционал $f(x) := g(x) - ig(ix)$ совпадает с исходным функционалом при всех $x \in L$. Пусть $|f(x)| = \xi f(x) \Rightarrow \xi f(x) = f(\xi x) = g(\xi x) \Rightarrow \Rightarrow |f(x)| \leq c\|x\| \forall x \in V$. $\square$

Задача 268. Пусть A — выпуклое тело и B — выпуклое множество. Докажите, что если ни одна линейно внутренняя точка множества A не принадлежит B , то существует аффинная функция $f(x)$, такая что $f(x) \leq f(y)$ для любых $x \in A$ и любых $y \in B$.

Задача 269. Для произвольной нормы $\|x\|$ на $\mathbb{C}^n$ функция $y \rightarrow \|y\|' := \max_{\|x\|=1} |y^*x|$ называется нормой, дуальной к норме $\|x\|$. Докажите, что дуальная норма является нормой и норма, дуальная к дуальной норме, совпадает с исходной нормой.

6.10. Системы линейных неравенств

Мы готовы к получению некоторых содержательных результатов о системах линейных неравенств

$$\begin{aligned} a_{11}x_1 + \dots + a_{1n}x_n &\leq b_1, \\ &\dots \dots \dots \\ a_{m1}x_1 + \dots + a_{mn}x_n &\leq b_m \end{aligned}$$

с заданными вещественными коэффициентами a_{ij} и вещественными правыми частями b_i . Используя естественное скалярное произведение в вещественном арифметическом пространстве, запишем систему в виде

$$\begin{aligned} (a_1, x) &\leq b_1, \dots, (a_m, x) \leq b_m, \\ a_i &= (a_{i1}, \dots, a_{in}), \quad 1 \leq i \leq m, \quad x = (x_1, \dots, x_n). \end{aligned} \quad (1)$$

Рассмотрим еще одно неравенство такого же типа:

$$(c, x) \leq d, \quad c = (c_1, \dots, c_n). \quad (2)$$

Теорема 6.10.1 (ТЕОРЕМА ФАРКАША). Пусть система неравенств (1) совместна. Тогда неравенство (2) является следствием неравенств (1) в том и только том случае, когда существуют неотрицательные числа $\alpha_1, \dots, \alpha_n$, такие что

$$c = \sum_{i=1}^m \alpha_i a_i, \quad \sum_{i=1}^m \alpha_i b_i \leq d. \quad (3)$$

Доказательство. Пусть система неравенств (1) совместна. Умножив отдельные неравенства на неотрицательные числа α_i и сложив неравенства, при выполнении соотношений (3) находим

$(c, x) \leq \sum_{i=1}^m \alpha_i b_i \leq d \Rightarrow (c, x) \leq d$. Таким образом, соотношения (3) гарантируют, что для любого вектора x , удовлетворяющего системе неравенств (1), будет выполнено также и неравенство (2).

Теперь предположим, что (2) является следствием (1). Введем векторы

$$\hat{a}_i = (-b_i, a_{i1}, \dots, a_{in}), \quad 1 \leq i \leq m,$$

$$\hat{a}_0 = (-1, 0, \dots, 0), \quad \hat{c} = (-d, c_1, \dots, c_n).$$

Тогда соотношения (3) означают, что $\hat{c} \in K := \text{con}(\hat{a}_0, \hat{a}_1, \dots, \hat{a}_m)$. От противного, допустим, что $\hat{c} \notin K$. Мы уже знаем, что конечнопорожденный конус является замкнутым выпуклым множеством, поэтому теорема 6.7.1 гарантирует существование и единственность принадлежащего множеству K элемента $\hat{z}$ наилучшего приближения элемента $\hat{c} \notin K$. Пусть $\hat{h} = (h_0, h_1, \dots, h_n) := \hat{c} - \hat{z}$. Тогда согласно теореме 6.8.1

$$(\hat{h}, \hat{y}) \leq (\hat{h}, \hat{z}) = (\hat{h}, \hat{c}) - \|\hat{h}\|^2 \quad \forall \hat{y} \in K.$$

Точка $\hat{y} = 0$ принадлежит $K \Rightarrow (\hat{h}, \hat{z}) \geq 0$. Однако если $(\hat{h}, \hat{z}) > 0$, то при некотором α длина вектора $\hat{c} - \alpha \hat{z}$ будет строго меньше длины вектора $\hat{h}$ и возникнет противоречие с тем, что $\hat{z}$ — элемент наилучшего приближения. Значит, $(\hat{h}, \hat{z}) = 0$ и выполняются следующие неравенства:

$$(\hat{a}_i, \hat{h}) \leq 0, \quad 0 \leq i \leq m, \quad (\hat{c}, \hat{h}) > 0.$$

Неравенство $(\hat{a}_0, \hat{h}) \leq 0$ равносильно неравенству $h_0 \geq 0$.

Положим $h = (h_1, \dots, h_n)$. Если $h_0 > 0$, то для вектора $p := \frac{1}{h_0} h$ выполняются неравенства (1), но нарушается неравенство (2): $(a_i, p) \leq b_i$ при $1 \leq i \leq m$ и $(c, p) > d$. Следовательно, $h_0 = 0$. По условию теоремы система неравенств (1) совместна. Если $(a_i, x) \leq b_i$ при $1 \leq i \leq m$, то для вектора $q = x + \alpha h$ получаем: $(a_i, q) \leq b_i$ при всех $\alpha \geq 0$ для всех $1 \leq i \leq m$ и $(c, q) > d$ при всех достаточно больших $\alpha > 0$. Опять возникает противоречие с тем, что неравенство (2) является следствием системы неравенств (1). $\square$

Следствие 6.10.1. Система неравенств (1) несовместна в том и только том случае, когда существуют неотрицательные числа $\alpha_1, \dots, \alpha_n$, такие что

$$\sum_{i=1}^m \alpha_i a_i = 0, \quad \sum_{i=1}^m \alpha_i b_i = -1.$$

Доказательство. Введем векторы $\hat{a}_i = (-b_i, a_{1i}, \dots, a_{in})$, $\hat{x} = (x_0, x_1, \dots, x_n)$, $\hat{c} = (1, 0, \dots, 0)$. Система неравенств $(\hat{a}_i, \hat{x}) \leq 0$, очевидно, совместна, и любое ее решение должно удовлетворять неравенству $x_0 = (\hat{c}, \hat{x}) \leq 0$. В противном случае $x_0 > 0$ и вектор $\frac{1}{x_0} \hat{x}$ будет решением системы неравенств (1). В силу теоремы 6.10.1, $\hat{c} = \sum_{i=1}^m \alpha_i \hat{a}_i$ для некоторых $\alpha_1, \dots, \alpha_m \geq 0$. $\square$

Пересечение конечного числа полупространств называется *полиэдром*. Таким образом, множество решений системы неравенств (1) задает некоторый полиэдр. Само пространство также считается полиэдром (и действительно является пересечением полупространств пространства более высокой размерности), в этом случае полиэдр совпадает со своей аффинной оболочкой и мы будем называть его *тривиальным*.

Полученные нами результаты имеют большое значение для задач *линейного программирования*, т.е. задач о поиске минимальных или максимальных значений линейных функционалов на полиэдрах. Пусть $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$, $c \in \mathbb{R}^n$, $x \in \mathbb{R}^n$, $y \in \mathbb{R}^m$, и пусть символы $\leq$, $<$, $\geq$, $>$ между матрицами одинакового размера означают поэлементные неравенства. Вот стандартные *двойственные друг другу* задачи линейного программирования:

(P) Найти максимум функционала (c, x) на полиэдре

$$P = \{x: Ax \leq b, x \geq 0\};$$

(Q) Найти минимум функционала (b, y) на полиэдре

$$Q = \{y: A^T y \geq c, y \geq 0\}.$$

Лемма 6.10.1. Если линейный функционал на непустом полиэдре ограничен сверху (снизу), то его максимальное (минимальное) значение достигается в некоторой граничной точке полиэдра.

Доказательство. Пусть функционал $f(x) = (c, x)$ ограничен сверху для всех x , принадлежащих непустому полиэдру P ,

γ — его точная верхняя грань и M — гиперплоскость, заданная уравнением $(c, x) = \gamma$. Тогда существует последовательность точек $x_k \in P$, такая что $\rho(x_k, M) = \min_{y \in M} \|x_k - y\| \rightarrow 0$. Нужно доказать, что $P \cap M \neq \emptyset$.

Для проведения индукции по n сформируем следующее предположение: если плоскость M размерности $n - 1$ и полиэдр P содержатся в некоторой плоскости Π размерности n и при этом $\inf_{x \in P} \rho(x, M) = 0$, то $P \cap M \neq \emptyset$. Случай $n = 1$ очевиден. Пусть $n > 1$ и P задается неравенствами $(a_1, x) \leq b_1, \dots, (a_m, x) \leq b_m$. Если $P \subseteq M$, то все доказано. В противном случае рассмотрим последовательность точек $x_k \in P$ таких, что $\rho(x_k, M) \rightarrow 0$. Нетрудно понять, что должна быть подпоследовательность x_{k_l} , принадлежащая какой-то одной граничной плоскости $\Pi' := \{x \in \Pi: (a_i, x) = b_i\}$. Множество $P' := P \cap \Pi'$ является полиэдром на плоскости Π' . Если $\Pi' = M$, то доказывать уже нечего. В противном случае $M' := M \cap \Pi'$ — это плоскость размерности $n - 2$ (здесь нужно применить теорему Грассмана). При этом P' и M' содержатся в плоскости Π' размерности $n - 1$, и можно показать, что $\rho(x_{k_l}, M') \rightarrow 0 \Rightarrow \rho(P', M') = 0$. Теперь можно применить индуктивное предположение. $\square$

Теорема 6.10.2. Если одна из задача, (P) или (Q) , имеет решение, то двойственная ей задача также имеет решение и при этом

$$\max_{x \in P} (c, x) = \min_{y \in Q} (b, y).$$

Доказательство. Предположим, что задача (P) имеет решение и максимум достигается в точке x_0 . Пусть $\gamma := (c, x_0) = \max_{x \in P} (c, x)$. Это означает, что неравенство $(c, x) \leq \gamma$ является следствием неравенств $Ax \leq b, x \geq 0$. Согласно теореме 6.10.1, существуют векторы $y_0 \in \mathbb{R}^m$ и $z_0 \in \mathbb{R}^n$ такие, что

$$y_0^\top A - z_0^\top = c^\top, \quad y_0^\top b \leq \gamma, \quad y_0 \geq 0, \quad z_0 \geq 0.$$

Полиэдр Q непуст, так как $y_0 \in Q$. Далее, для произвольного вектора $y \in Q$ находим $\gamma = c^\top x_0 \leq y^\top A x_0 \leq y^\top b$. Таким образом, функционал (b, y) ограничен снизу на полиэдре Q числом γ и отсюда вытекает, что задача (Q) имеет решение и при этом $\gamma = (c, x_0) = (b, y_0)$. $\square$

Задача 270. Пусть A и B — компактные выпуклые множества в пространстве $\mathbb{R}^n$ и для любого вектора $x \in A$ существует вектор $y(x) \in B$, такой что $(x, y(x)) \geq 0$. Докажите, что существует вектор $y_0 \in B$, такой что $(x, y_0) \geq 0$ для всех $x \in A$.

6.11. Грани полиэдра и выпуклые многогранники

Размерностью полиэдра P называется размерность его аффинной оболочки. Обозначение: $\dim P$. Если полиэдр $P \subsetneq \mathbb{R}^n$ задан неравенствами $(a_i, x) \leq b_i$, $1 \leq i \leq m$, то гиперплоскости $P_i := \{x \in \mathbb{R}^n : (a_i, x) = b_i\}$ будем называть *граничными*. Легко проверяется, что точка $x \in P$ является внутренней тогда и только тогда, когда она не принадлежит ни одной граничной гиперплоскости, и размерность P равна n в том и только том случае, когда P обладает внутренней точкой.

Гранью $\Gamma(x)$ точки $x \in P$ называется пересечение полиэдра P со всеми граничными гиперплоскостями, содержащими точку x . По определению, для внутренней точки $\Gamma(x) := P$. Грань размерности 0 называется *вершиной*, а размерности 1 — *ребром*.

Точку x множества M будем называть *локально внутренней* для M , если имеется содержащий ее открытый шар, пересечение которого с аффинной оболочкой множества M целиком принадлежит M . Очевидно, что грань точки x — это полиэдр, для которого точка x является локально внутренней, и для любой локально внутренней точки $y \in \Gamma(x)$ имеет место равенство $\Gamma(x) = \Gamma(y)$.

Теорема 6.11.1 (ТЕОРЕМА ФАНЬ ЦЗЫ). Пусть $P \subsetneq \mathbb{R}^n$ — полиэдр размерности d и r — размерность линейной оболочки векторов $a_1, \dots, a_m$. Тогда P обладает гранью размерности s в том и только том случае, когда $n - r \leq s \leq d$, и при каждом $n - r < s \leq d$ любая грань размерности s содержит грань размерности $s - 1$.

Доказательство. Грань размерности d — это сам полиэдр P . Пусть $\Gamma = \Gamma(x_0)$ — грань размерности s . Для определенности будем считать, что

$$(a_1, x_0) < b_1, \dots, (a_k, x_0) < b_k, \\ (a_{k+1}, x_0) = b_{k+1}, \dots, (a_m, x_0) = b_m.$$

Таким образом, x_0 принадлежит плоскости Π , которая является пересечением граничных гиперплоскостей $(a_i, x) = b_i$ при $k+1 \leq i \leq m$. Точка x_0 является локально внутренней для Γ , поэтому Π совпадает с аффинной оболочкой грани $\Gamma \Rightarrow s = \dim \Gamma = \dim \Pi = n - \dim \langle a_{k+1}, \dots, a_m \rangle \geq n - r$.

Теперь предположим, что $n - r < s \leq d$. Пусть L — направляющее подпространство плоскости Π и $g_1, \dots, g_s$ — его базис.

Тогда каждая точка плоскости Π имеет вид $x_0 + \sum_{i=1}^s z_i g_i$ и однозначно определяется вектором $z = [z_1, \dots, z_s]^T \in \mathbb{R}^s$, а грань Γ задается неравенствами вида $(h_1, z) \leq \beta_1, \dots, (h_k, z) \leq \beta_k$, где $z, h_1, \dots, h_k \in \mathbb{R}^s$ и $\beta_1, \dots, \beta_k \in \mathbb{R}$. Если $h_1 = \dots = h_k = 0$, то $a_1, \dots, a_k \perp L \Rightarrow \langle a_1, \dots, a_k \rangle \subseteq \langle a_{k+1}, \dots, a_m \rangle \Rightarrow s = n - r$. Значит, ненулевые h_i присутствуют. Для определенности будем считать, что $h_i \neq 0$ при $1 \leq i \leq l$. В этом случае Γ определяется полиэдром $Q \subsetneq \mathbb{R}^s$ с граничными гиперплоскостями $\Pi_i := \{z \in \mathbb{R}^s : (h_i, z) = \beta_i\}$, $1 \leq i \leq l$.

Точка $0 \in \mathbb{R}^s$ соответствует точке $x_0 \in \mathbb{R}^n$ и является внутренней для Q . Множество точек полиэдра Q , равноудаленных от Π_i и Π_j при фиксированных $i \neq j$, принадлежит плоскости размерности $s - 1$. Ясно, что шар в $\mathbb{R}^s$ нельзя накрыть конечным объединением плоскостей размерности меньше $s \Rightarrow$ найдется точка $z_0 \in Q$, для которой расстояния $\rho(Q, \Pi_1), \dots, \rho(Q, \Pi_l)$ попарно различны. Не ограничивая общности, можно считать, что $\rho(Q, \Pi_1)$ — наименьшее из них. Пусть $z_1 \in \Pi_1$ — точка, ближайшая к точке z_0 среди всех точек Π_1 . Несложно показать, что $z_1 \in \Pi_1 \cap Q$ и $z_1 \notin \Pi_i \cap Q$ при $2 \leq i \leq l \Rightarrow$ полиэдр $\Pi_1 \cap Q$ является гранью точки z_1 , имеет размерность $s - 1$ и определяет грань той же размерности для полиэдра Γ . $\square$

Следствие 6.11.1. Пусть размерность линейной оболочки векторов $a_1, \dots, a_m$ из $\mathbb{R}^n$ равна n и непустой полиэдр задан неравенствами $(a_1, x) \leq b_1, \dots, (a_m, x) \leq b_m$. Тогда он имеет хотя бы одну вершину.

Следующий факт может показаться геометрически очевидным, но строгое обоснование вряд ли покажется очень простым.

Теорема 6.11.2 (Г. Вейль). Конечнопорожденный конус является полиэдром.

Доказательство. Не ограничивая общности, будем считать, что размерность аффинной оболочки конуса $K = \text{con}(a_1, \dots, a_m)$,

порожденного n -мерными векторами, равна $n \Rightarrow \dim \langle a_1, \dots, a_m \rangle = n$. Мы докажем, что для любой внешней точки $a \notin K$ найдется гиперплоскость $(h, x) = 0$, строго разделяющая точку a и конус K и такая, что вектор h ортогонален некоторым линейно независимым векторам $a_{i_1}, \dots, a_{i_{n-1}}$, выбор которых зависит от a . Пересечение соответствующих полупространств для всех внешних точек a будет совпадать с K и, очевидно, имеется лишь конечное число полупространств такого вида.

Итак, пусть a — произвольная внешняя точка для K . Согласно теореме Фаркаша, найдется вектор b такой, что $(a_1, b) \leq 0, \dots, (a_m, b) \leq 0$ и $(a, b) > 0$. Рассмотрим полиэдр P , заданный неравенствами $(a_1, x) \leq 0, \dots, (a_m, x) \leq 0$ и $(a, x) \geq (a, b)$. Ясно, что $b \in P$, т. е. полиэдр непуст. Согласно теореме Фань Цзы в нашем случае полиэдр имеет хотя бы одну вершину. Обозначим ее через h . Эта вершина, как и любая вершина, является единственной точкой пересечения каких-то n граничных гиперплоскостей, для которых нормальные векторы линейно независимы. Если эти гиперплоскости имеют вид $(a_{i_1}, x) = 0, \dots, (a_{i_n}, x) = 0$, то их единственной общей точкой будет $x = 0$. Но, очевидно, $0 \notin P$. Значит, вершина h является единственным решением системы уравнений вида

$$(a_{i_1}, h) = 0, \dots, (a_{i_{n-1}}, h) = 0, \quad (a, h) = (a, b).$$

При этом $h \in P \Rightarrow (h, x) \leq 0 \forall x \in K$ и $(h, a) > 0$. □

Следствие 6.11.2. *Выпуклый многогранник является полиэдром.*

Доказательство. Рассмотрим $M = \text{conv}(a_1, \dots, a_m)$ как множество на гиперплоскости пространства $\mathbb{R}^{n+1}$, определенной уравнением $(h, x) = 1$ для $h = (0, \dots, 0, 1)$. Тогда M будет пересечением гиперплоскости $(h, x) = 1$ и конуса $\text{con}(a_1, \dots, a_m)$. □

Задача 271. *Аффинная функция неотрицательна на непустом полиэдре и принимает нулевое значение в его локально внутренней точке. Докажите, что на этом полиэдре функция тождественно равна нулю.*

Задача 272. *Докажите, что вершины полиэдра и только они являются его угловыми точками.*

6.12. Сопряженный оператор и нормальные операторы

Пусть V и W — комплексные пространства, снабженные скалярными произведениями $(\cdot, \cdot)_V$ и $(\cdot, \cdot)_W$, и пусть $A: V \rightarrow W$ — произвольный оператор. Оператор $B: W \rightarrow V$ называется *сопряженным оператору A в заданных скалярных произведениях*, если

$$(Ax, y)_W = (x, By)_V \quad \forall x \in V, \quad \forall y \in W.$$

Утверждение 6.12.1. *Если оператор обладает сопряженным оператором, то он сам и его сопряженный оператор являются линейными операторами.*

Доказательство. Пусть $u, v \in V$ — произвольные векторы и α, β — произвольные числа. Тогда

$$\begin{aligned} (A(\alpha u + \beta v), y)_W &= (\alpha u + \beta v, By)_V = \alpha(u, By)_V + \beta(v, By)_V = \\ &= \alpha(Au, y)_W + \beta(Av, y)_W = (\alpha Au + \beta Av, y)_W \quad \forall y \in W. \end{aligned}$$

Взяв $y := A(\alpha u + \beta v) - \alpha Au - \beta Av$, находим $(y, y)_W = 0 \Rightarrow y = 0$. $\square$

Теперь предположим, что пространства V и W конечномерны, и выберем в них ортонормированные базисы. Напомним, что через $[x]$ обозначается вектор-столбец из коэффициентов разложения вектора x по фиксированному базису. Тогда для любых векторов $u, v \in V$ и любых векторов $p, q \in W$ имеем

$$(u, v)_V = ([u], [v]) := [v]^*[u], \quad (p, q)_W = ([p], [q]) := [q]^*[p].$$

Утверждение 6.12.2. *Пусть V и W — конечномерные комплексные пространства, снабженные скалярными произведениями. Тогда для любого линейного оператора $A: V \rightarrow W$ сопряженный оператор существует и единствен.*

Доказательство. Пусть в V и W выбраны ортонормированные базисы. Тогда

$$(Ax, y)_W = (x, By)_V \Leftrightarrow ([Ax], [y]) = ([x], [By]).$$

С учетом равенств $[Ax] = [A][x]$, $[By] = [B][y]$ находим

$$[y]^*[A][x] = [y]^*[B]^*[x] \Leftrightarrow [A] = [B]^* \Leftrightarrow [B] = [A]^*.$$

Таким образом, при использовании ортонормированных базисов линейный оператор B удовлетворяет условиям на сопряженный оператор в том и только том случае, когда он задается сопряженной матрицей $[A]$ матрицей $[B] = [A]^*$. $\square$

Обозначение для сопряженного оператора: $B = A^*$. В случае $V = W$ линейный оператор $A: V \rightarrow V$ называется *нормальным* в данном скалярном произведении, если $A^*A = AA^*$. В заданном скалярном произведении линейный оператор A называется *эрмитовым*, если $A = A^*$, и *унитарным*, если он обратим и $A^{-1} = A^*$. Очевидно, что эрмитовы и унитарные операторы являются нормальными.

При выборе ортонормированного базиса сопряженный оператор определяется сопряженной матрицей, поэтому *условие нормальности оператора A равносильно условию нормальности его матрицы в ортонормированном базисе*: $[A]^*[A] = [A][A]^*$.

Теорема 6.12.1. *Линейный оператор на комплексном конечномерном пространстве со скалярным произведением является нормальным относительно данного скалярного произведения тогда и только тогда, когда он обладает ортонормированным в заданном скалярном произведении базисом из собственных векторов.*

Доказательство сразу же получается из полученного ранее критерия нормальности матрицы (см. раздел 5.6).

Следствие 6.12.1. *Нормальный оператор обязан быть диагонализуемым.*

Утверждение 6.12.3. *Нормальный оператор является эрмитовым (унитарным) тогда и только тогда, когда все его собственные значения вещественны (по модулю равны единице).*

Линейный оператор A , действующий на комплексном пространстве V со скалярным произведением, называется *неотрицательно определенным* в данном скалярном произведении, если $(Ax, x) \geq 0$ для всех $x \in V$, и *положительно определенным*, если $(Ax, x) > 0$ для всех $0 \neq x \in V$. Обозначение для факта неотрицательной (положительной) определенности: $A \geq 0$ ($A > 0$).

Подчеркнем, что понятие сопряженного оператора существенно зависит от того, какие именно скалярные произведения введены в пространствах V и W , и нужно иметь в виду, что свойства нормальности, эрмитовости, унитарности, положительной или неотрицательной определенности оператора *зависят от скалярного произведения*.

Пример. Пусть A и B — эрмитовы матрицы порядка n и $B > 0$. Тогда оператор умножения на матрицу $C := AB$ в общем случае не является эрмитовым в естественном скалярном произведении пространства $\mathbb{C}^n$, но он становится эрмитовым в скалярном произведении $(x, y)_B := (Bx, y)$:

$$(ABx, y)_B = (BABx, y) = (Bx, ABu) = (x, ABu)_B \quad \forall x, y \in \mathbb{C}^n.$$

Утверждение 6.12.4. Если линейный оператор неотрицательно определен в каком-либо скалярном произведении, то он является эрмитовым в данном скалярном произведении.

Доказательство. Запишем A в виде $A = H_1 + iH_2$, где $H_1 = \frac{1}{2}(A + A^*)$ и $H_2 = \frac{1}{2i}(A - A^*)$. Заметим, что $H_1 = H_1^*$, $H_2 = H_2^*$ и значения (H_1x, x) , (H_2x, x) вещественны для любого $x \in V$. По условию утверждения число $(Ax, x) = (H_1x, x) + i(H_2x, x)$ вещественно для всех $x \in V \Rightarrow (H_2x, x) = 0$ для всех $x \in V$. Оператор H_2 , как и любой нормальный оператор, обладает ортонормированным базисом из собственных векторов $z_1, \dots, z_n$. Пусть они соответствуют собственным значениям $\lambda_1, \dots, \lambda_n \Rightarrow H_2z_i = \lambda_i z_i \Rightarrow (H_2z_i, z_i) = \lambda_i(z_i, z_i) = 0 \Rightarrow \lambda_i = 0$. Значит, все собственные значения эрмитова оператора H_2 равны нулю $\Rightarrow H_2 = 0$. $\square$

Утверждение 6.12.5. Эрмитов оператор является неотрицательно определенным (положительно определенным) тогда и только тогда, когда все его собственные значения неотрицательны (положительны).

Доказательство. Пусть A — эрмитов оператор на n -мерном пространстве V , и пусть $z_1, \dots, z_n$ — ортонормированный базис, составленный из его собственных векторов, и $\lambda_1, \dots, \lambda_n$ — соответствующие им собственные значения. Все они вещественны: $(Ax, x) = (x, Ax) = \overline{(Ax, x)} \in \mathbb{R} \quad \forall x \in V \Rightarrow$ из равенства $Az_i = \lambda_i z_i$ следует

$$\lambda_i = \frac{(Az_i, z_i)}{(z_i, z_i)} \in \mathbb{R}.$$

Далее, если $A \geq 0$, то $(Az_i, z_i) \geq 0 \Rightarrow \lambda_i \geq 0$. Аналогично, если $A > 0$, то $\lambda_i > 0$ при всех $1 \leq i \leq n$. Теперь выведем неотрицательную определенность из неотрицательности собственных значений. Для произвольного вектора $x = \sum_{i=1}^n \xi_i z_i$ получаем

$Ax = \sum_{i=1}^n \lambda_i \xi_i z_i \Rightarrow (Ax, x) = \sum_{i=1}^n \lambda_i |\xi_i|^2 \geq 0$. Если все собственные значения положительны и $x \neq 0$, то $(Ax, x) > 0$. $\square$

Теорема 6.12.2. Пусть V и W — комплексные пространства размерностей n и m , снабженные какими-то скалярными произведениями, и $A: V \rightarrow W$ — произвольный линейный оператор. Тогда существуют ортонормированные базисы $u_1, \dots, u_n \in V$ и $v_1, \dots, v_m \in W$, в которых матрица линейного оператора имеет вид

$$[A] = \begin{bmatrix} \Sigma_r & 0_{r \times (n-r)} \\ 0_{(m-r) \times r} & 0_{(m-r) \times (n-r)} \end{bmatrix}, \quad \Sigma_r = \begin{bmatrix} \sigma_1 & & \\ & \ddots & \\ & & \sigma_r \end{bmatrix},$$

$$\sigma_1, \dots, \sigma_r \geq 0.$$

Доказательство. Оператор A^*A эрмитов и, как любой нормальный оператор, обладает ортонормированным базисом из собственных векторов. Обозначим его через $u_1, \dots, u_n$. Пусть λ — произвольное собственное значение оператора A^*A и x — его собственный вектор $\Rightarrow A^*Ax = \lambda x \Rightarrow \lambda(x, x) = (A^*Ax, x) = (Ax, Ax) \Rightarrow \lambda \geq 0$. Таким образом, все собственные значения оператора A^*A неотрицательны и с учетом кратностей образуют набор $\sigma_1^2, \dots, \sigma_n^2$, где $\sigma_1, \dots, \sigma_n \geq 0$. Будем считать, что $A \neq 0$ и $\sigma_i > 0$ при $1 \leq i \leq r$ и $\sigma_i = 0$ при $r+1 \leq i \leq n$. Положим $v_i := \frac{1}{\sigma_i} Au_i$ при $1 \leq i \leq r$, а в случае $r+1 \leq i \leq n$ заметим, что если $A^*Au_i = 0$, то $(A^*Au_i, u_i) = (Au_i, Au_i) = 0 \Rightarrow Au_i = 0$. Следовательно,

$$Au_i = \begin{cases} \sigma_i v_i, & 1 \leq i \leq r, \\ 0, & r+1 \leq i \leq n. \end{cases}$$

Заметим, что векторы $v_1, \dots, v_r$ образуют ортонормированную систему:

$$(v_i, v_j) = \left(\frac{1}{\sigma_i} Au_i, \frac{1}{\sigma_j} Au_j \right) = \frac{1}{\sigma_i \sigma_j} (A^*Au_i, u_j) = \frac{\sigma_i}{\sigma_j} (u_i, u_j).$$

Дополнив систему $v_1, \dots, v_r$ до ортонормированного базиса $v_1, \dots, v_m$, получаем

$$Au_i = \begin{cases} \sigma_i v_i, & 1 \leq i \leq r, \\ 0 \cdot v_i, & r+1 \leq i \leq n. \end{cases} \quad \square$$

При выборе ортонормированных базисов доказанная теорема дает нам сингулярное разложение матрицы линейного оператора в этих базисах (см. раздел 5.7).

Задача 273. Докажите, что любой диагонализуемый линейный оператор на конечномерном пространстве можно сделать нормальным в некотором скалярном произведении.

Задача 274. Приведите пример неотрицательно определенного оператора, который теряет это свойство в некотором другом скалярном произведении.

Задача 275. Докажите, что минимальный по модулю элемент унитарной матрицы порядка n не превосходит $1/\sqrt{n}$. Для каждого n приведите пример унитарной матрицы, в которой все элементы по модулю равны $1/\sqrt{n}$.

Задача 276. Пусть A и B — эрмитовы матрицы порядка n и хотя бы одна из них положительно определена. Докажите, что все собственные значения матрицы AB вещественны.

Задача 277. Пусть V, W — конечномерные комплексные пространства со скалярными произведениями и $A: V \rightarrow W$ — произвольный линейный оператор. Докажите, что $\ker A \oplus \operatorname{im} A^* = V$, $\ker A^* \oplus \operatorname{im} A = W$ и при этом подпространства в суммах ортогональны.

Задача 278. Пусть $A, B \in \mathbb{C}^{n \times n}$. Докажите, что если хотя бы одна из матриц нормальна, то выполняется неравенство $\|AB - BA\|_F \leq \sqrt{2} \|A\|_F \|B\|_F$.

6.13. Собственные значения эрмитовых матриц

Мы уже знаем, что собственные значения любой эрмитовой матрицы вещественны. Для матрицы A порядка n обозначим их через $\lambda_k(A)$ и будем упорядочивать по невозрастанию: $\lambda_1(A) \geq \dots \geq \lambda_n(A)$. Функция $f(x) := \frac{(Ax, x)}{(x, x)}$ определена для всех ненулевых векторов $x \in \mathbb{C}^n$ и называется *отношением Рэля*.

Лемма 6.13.1. В любом подпространстве пространства $\mathbb{C}^n$ существуют векторы, на которых отношение Рэля для эрмитовой матрицы порядка n достигает своих максимального и минимального значений на данном подпространстве.

Теорема 6.13.1 (ТЕОРЕМА КУРАНТА–ФИШЕРА). Пусть A — эрмитова матрица порядка n с собственными значениями $\lambda_1(A) \geq \dots \geq \lambda_n(A)$. Тогда

$$\lambda_k = \max_{\dim L=k} \min_{0 \neq x \in L} \frac{(Ax, x)}{(x, x)}, \quad 1 \leq k \leq n.$$

Доказательство. Пусть $z_1, \dots, z_n$ — ортонормированный базис из собственных векторов: $Az_i = \lambda_i(A)z_i$, $1 \leq i \leq n$. Пусть $L \subseteq \mathbb{C}^n$ — произвольное k -мерное подпространство и $M = \langle z_k, z_{k+1}, \dots, z_n \rangle$. Согласно теореме Грассмана

$$\begin{aligned} \dim L \cap M &= \dim L + \dim M - \dim(L + M) \geq \\ &\geq k + (n - k + 1) - n = 1 \Rightarrow \exists 0 \neq y \in L \cap M \Rightarrow \\ &\Rightarrow \min_{0 \neq x \in L} \frac{(Ax, x)}{(x, x)} \leq \frac{(Ay, y)}{(y, y)} \leq \max_{0 \neq x \in M} \frac{(Ax, x)}{(x, x)} = \lambda_k(A). \end{aligned}$$

Докажем последнее равенство. Используя ортонормированность системы $z_k, \dots, z_n$, находим

$$0 \neq x \in M \Rightarrow x = \sum_{k \leq i \leq n} \xi_i z_i \Rightarrow \frac{(Ax, x)}{(x, x)} = \frac{\sum_{i=1}^n \lambda_i(A) |\xi_i|^2}{\sum_{i=1}^n |\xi_i|^2} \leq \lambda_k(A),$$

и очевидно, что при $x = z_k$ получается равенство. Кроме того, вполне аналогичная выкладка показывает, что если $L := \langle z_1, \dots, z_k \rangle$, то $\min_{0 \neq x \in L} \frac{(Ax, x)}{(x, x)} = \lambda_k(A)$. $\square$

Следствие 6.13.1.

$$\begin{aligned} \lambda_k(A) &= \min_{\dim L=k} \max_{0 \neq x \perp L} \frac{(Ax, x)}{(x, x)} = \min_{\dim L=n-k+1} \max_{0 \neq x \in L} \frac{(Ax, x)}{(x, x)}, \\ &1 \leq k \leq n. \end{aligned}$$

Доказательство. Матрица $B := A$ также эрмитова, а ее собственные значения в порядке невозрастания имеют вид $\lambda_k(B) = -\lambda_{n-k+1}(A)$. В силу теоремы Куранта–Фишера

$$\begin{aligned} -\lambda_k(A) &= \lambda_{n-k+1}(B) = \max_{\dim L=n-k+1} \min_{0 \neq x \in L} \frac{(Bx, x)}{(x, x)} = \\ &= - \min_{\dim L=n-k+1} \left(- \min_{0 \neq x \in L} \frac{(Bx, x)}{(x, x)} \right) = \end{aligned}$$

$$\begin{aligned}
 &= - \min_{\dim L = n-k+1} \max_{0 \neq x \in L} \left(- \frac{(Bx, x)}{(x, x)} \right) = \\
 &= - \min_{\dim L = n-k+1} \max_{0 \neq x \in L} \frac{(Ax, x)}{(x, x)}. \quad \square
 \end{aligned}$$

Следствие 6.13.2. $\lambda_1(A) = \max_{0 \neq x} \frac{(Ax, x)}{(x, x)}$, $\lambda_n(A) = \min_{0 \neq x} \frac{(Ax, x)}{(x, x)}$.

Следствие 6.13.3. Пусть A — комплексная матрица размера $m \times n$ с сингулярными числами $\sigma_1(A) \geq \dots \geq \sigma_n(A) \geq 0$. Тогда

$$\begin{aligned}
 \sigma_k(A) &= \max_{\substack{L \subseteq \mathbb{C}^n \\ \dim L = k}} \min_{0 \neq x \in L} \frac{\|Ax\|_2}{\|x\|_2} = \min_{\substack{L \subseteq \mathbb{C}^n \\ \dim L = n-k+1}} \max_{0 \neq x \in L} \frac{\|Ax\|_2}{\|x\|_2}, \\
 1 &\leq k \leq n.
 \end{aligned}$$

Чудесным следствием теоремы Куранта–Фишера являются *соотношения разделения* для собственных значений эрмитовых матриц и их главных подматриц, а также для сингулярных чисел произвольных матриц и их *максимальных подматриц* (нерасширяемых подматриц, составленных из полных строк либо полных столбцов исходной матрицы). Напомним, что квадратная подматрица называется *главной*, если она расположена на строках и столбцах с одинаковыми номерами. В частности, в матрице порядка n имеется ровно n разных главных подматриц порядка $n-1$. Главная подматрица, расположенная в левом верхнем углу матрицы, называется *ведущей подматрицей*. Миноры главных и ведущих подматриц называются соответственно *главными* и *ведущими*. Очевидно, что любая главная подматрица эрмитовой матрицы сохраняет эрмитовость.

Теорема 6.13.2. Пусть A — эрмитова матрица порядка n и B — ее главная подматрица порядка $n-1$. Тогда для их собственных значений $\lambda_1(A) \geq \dots \geq \lambda_n(A)$ и $\lambda_1(B) \geq \dots \geq \lambda_{n-1}(B)$ выполняются *соотношения разделения*

$$\lambda_k(A) \geq \lambda_k(B) \geq \lambda_{k+1}(A), \quad 1 \leq k \leq n-1.$$

Доказательство. Для определенности в качестве B возьмем ведущую подматрицу:

$$A = \begin{bmatrix} B & p \\ p^* & \alpha \end{bmatrix}, \quad p \in \mathbb{C}^{n-1}, \quad \alpha = \bar{\alpha} \in \mathbb{R}.$$

Обозначим через M подпространство векторов $x = [x_1, \dots, \dots, x_n]^\top \in \mathbb{C}^n$, для которых $x_n = 0$. Поскольку максимум на подмножестве не может быть больше, чем максимум на множестве, находим

$$\begin{aligned} \lambda_k(A) &= \max_{\substack{L \subseteq \mathbb{C}^n \\ \dim L = k}} \min_{0 \neq x \in L} \frac{(Ax, x)}{(x, x)} \geq \max_{\substack{L \subseteq M \\ \dim L = k}} \min_{0 \neq x \in L} \frac{(Ax, x)}{(x, x)} = \\ &= \max_{\substack{Z \subseteq \mathbb{C}^{n-1} \\ \dim Z = k}} \min_{0 \neq z \in Z} \frac{(Bz, z)}{(z, z)} = \lambda_k(B). \end{aligned}$$

Для эрмитовой матрицы $\tilde{A} := -A$ и ее главной подматрицы $\tilde{B} := -B$ при той же упорядоченности по невозрастанию получаем: $\lambda_{n-k}(\tilde{A}) = -\lambda_{k+1}(A)$ и $\lambda_{n-k}(\tilde{B}) = -\lambda_k(B)$. По уже доказанному, $\lambda_{n-k}(\tilde{A}) \geq \lambda_{n-k}(\tilde{B}) \Rightarrow \lambda_k(B) \geq \lambda_{k+1}(A)$. $\square$

Следствие 6.13.4. Для собственных значений эрмитовой матрицы A порядка n и ее главной подматрицы порядка s имеют место соотношения

$$\lambda_k(A) \geq \lambda_k(B) \geq \lambda_{n-s+k}(A), \quad 1 \leq k \leq m.$$

Теорема 6.13.3 (КРИТЕРИЙ СИЛЬВЕСТРА). Эрмитова матрица является положительно определенной в том и только том случае, когда все ее ведущие миноры положительны.

Доказательство. Пусть A — эрмитова матрица порядка n , A_k — ее ведущая подматрица порядка n и $\lambda_1^{(k)} \geq \dots \geq \lambda_k^{(k)}$ — ее собственные значения. Предположим, что $|A_k| = \prod_{i=1}^n \lambda_i^{(k)} > 0$, $1 \leq k \leq n$. Для A_2 и A_1 запишем соотношения разделения:

$$\begin{aligned} \lambda_1^{(2)} \geq \lambda_1^{(1)} \geq \lambda_2^{(2)}, \quad \lambda_1^{(1)} > 0, \quad |A_2| = \lambda_1^{(2)} \lambda_2^{(2)} > 0 \Rightarrow \\ \Rightarrow \lambda_1^{(2)} \geq \lambda_2^{(2)} > 0. \end{aligned}$$

Теперь предположим, что уже доказаны неравенства $\lambda_1^{(k-1)} \geq \dots \geq \lambda_{k-1}^{(k-1)} > 0$. Тогда из соотношений разделения для ведущих подматриц A_k и A_{k-1} получаем

$$\begin{aligned} \lambda_i^{(k)} \geq \lambda_i^{(k-1)} > 0 \text{ при } 1 \leq i \leq k-1, \quad |A_k| = \prod_{i=1}^k \lambda_i^{(k)} > 0 \Rightarrow \\ \Rightarrow \lambda_1^{(k)} \geq \dots \geq \lambda_k^{(k)} > 0. \end{aligned}$$

Итак, мы доказали, что все собственные значения эрмитовой матрицы $A = A_n$ положительны $\Rightarrow A > 0$. Теперь предположим, что $A > 0 \Rightarrow (Ax, x) > 0 \forall x \in \mathbb{C}^n \Rightarrow (A_k y, y) > 0 \forall y \in \mathbb{C}^k \Rightarrow A_k > 0 \Rightarrow |A_k| > 0$. $\square$

Теорема 6.13.4 (ТЕОРЕМА ЛИДСКОГО). Пусть A и B — эрмитовы $n \times n$ -матрицы, $\lambda_1(A) \geq \dots \geq \lambda_n(A)$, $\lambda_1(B) \geq \dots \geq \lambda_n(B)$, $\lambda_1(A+B) \geq \dots \geq \lambda_n(A+B)$ — собственные значения матриц A , B и $A+B$. Тогда для любого непустого множества $I \subseteq \{1, \dots, n\}$, содержащего k элементов, выполняется неравенство

$$\sum_{i \in I} \lambda_i(A+B) \leq \sum_{i \in I} \lambda_i(A) + \sum_{i=1}^k \lambda_i(B).$$

Доказательство. Случай $k = n$ очевидным образом дает равенство: сумма в левой части — это след матрицы $A+B$, а в правой части — сумма следов матриц A и B . Далее полагаем, что $k < n$, и предположим, что теорема уже доказана для матриц порядка $n-1$.

Пусть $1 \leq s \leq n$ и $s \notin I$. Запишем $I = L \cup M$, где подмножества L и M содержат индексы строго меньше и строго больше s соответственно. Пусть $u_1, \dots, u_n$ и $v_1, \dots, v_n$ — ортонормированные базисы из собственных векторов матриц $A+B$ и A . Рассмотрим линейную оболочку, натянутую на векторы $u_1, \dots, u_{s-1}, v_{s+1}, \dots, v_n$, и вложим ее в некоторое подпространство $V \subsetneq \mathbb{C}^n$ размерности $n-1$. Теперь выберем в V ортонормированный базис и из его векторов составим матрицу $Q \in \mathbb{C}^{n \times (n-1)}$. Очевидно, $A_1 := Q^* A Q$ и $B_1 := Q^* B Q$ — эрмитовы матрицы порядка $n-1$. Согласно построению любой вектор u_l для $l \in L$ имеет вид $u_l = Q \hat{u}_l$ для некоторого $\hat{u}_l \in \mathbb{C}^{n-1} \Rightarrow \hat{u}_l = Q^* u_l \Rightarrow (A_1 + B_1) \hat{u}_l = Q^* (A+B) Q \hat{u}_l = Q^* (\lambda_l(A+B) u_l) = \lambda_l(A+B) \hat{u}_l$. Таким образом, в списке собственных значений матрицы $A_1 + B_1$ с учетом кратностей присутствуют все собственные значения $\lambda_l(A+B)$ при $1 \leq l \leq s-1$. Аналогично, среди собственных значений матрицы A_1 имеются все собственные значения $\lambda_m(A)$ при $s+1 \leq m \leq n$.

Пусть P — унитарная матрица порядка n , в которой первые $n-1$ столбцов совпадают со столбцами матрицы Q . Тогда A_1 и B_1 — это главные подматрицы порядка $n-1$ в эрмитовых матрицах $P^* A P$ и $P^* B P$, имеющих те же собственные значения, что и матрицы A и B соответственно. В силу соотношений

разделения числа $\lambda_1(A+B) \geq \dots \geq \lambda_{s-1}(A+B)$ представляют собой в точности $s-1$ старших собственных значений матрицы A_1+B_1 , а числа $\lambda_{s+1}(A) \geq \dots \geq \lambda_n(A)$ — это $n-s$ младших собственных значений матрицы A_1 . Значит,

$$\sum_{l \in L} \lambda_l(A_1+B_1) = \sum_{l \in L} \lambda_l(A+B),$$

$$\sum_{m+1 \in M} \lambda_m(A_1) = \sum_{m \in M} \lambda_m(A).$$

Далее, согласно индуктивному предположению, для матриц A_1 и B_1 справедливо неравенство

$$\begin{aligned} \sum_{l \in L} \lambda_l(A_1+B_1) + \sum_{m+1 \in M} \lambda_m(A_1+B_1) &\leq \\ &\leq \sum_{l \in L} \lambda_l(A_1) + \sum_{m+1 \in M} \lambda_m(A_1) + \sum_{i=1}^k \lambda_i(B_1), \end{aligned}$$

и, в силу тех же соотношений разделения,

$$\sum_{i=1}^k \lambda_i(B_1) \leq \sum_{i=1}^k \lambda_i(B), \quad \sum_{l \in L} \lambda_l(A_1) \leq \sum_{l \in L} \lambda_l(A),$$

$$\sum_{m \in M} \lambda_m(A+B) = \sum_{m+1 \in M} \lambda_{m+1}(A+B) \leq \sum_{m+1 \in M} \lambda_m(A_1+B_1).$$

□

Следствие 6.13.5. В условиях теоремы Лидского справедливо также неравенство

$$\sum_{i \in I} \lambda_i(A) + \sum_{i=n-k+1}^n \lambda_i(B) \leq \sum_{i \in I} \lambda_i(A+B).$$

Для доказательства нужно перейти к матрицам $-A$ и $-B$, а затем применить уже доказанную теорему Лидского.

Задача 279. Докажите, что в любом подпространстве пространства $\mathbb{C}^n$ существуют векторы, на которых отношение Рэлея для эрмитовой матрицы порядка n достигает

своих максимального и минимального значений на данном подпространстве.

Задача 280. Пусть B — произвольная главная подматрица порядка k в эрмитовой положительно определенной матрице A порядка n . Докажите, что след и определитель матрицы B не больше, чем соответственно сумма и произведение k старших собственных значений матрицы A .

Задача 281. Пусть матрица $A \in \mathbb{C}^{m \times n}$ получается из матрицы $B \in \mathbb{C}^{m \times (n-1)}$ добавлением одного столбца. Докажите, что для сингулярных чисел матриц A и B выполняются соотношения разделения $\sigma_k(A) \geq \sigma_k(B) \geq \sigma_{k+1}(A)$, $1 \leq k \leq n-1$.

Задача 282. Пусть $\lambda_1 \geq \dots \geq \lambda_n$ — собственные значения эрмитовой матрицы A и $\mu_1 \geq \dots \geq \mu_n$ — собственные значения матрицы $A + F$, где F — эрмитова неотрицательно определенная матрица ранга 1. Докажите, что $\lambda_1 + \|F\|_2 \geq \mu_1$ и $\mu_{i-1} \geq \lambda_{i-1} \geq \mu_i \geq \lambda_i$ при $2 \leq i \leq n$.

Задача 283. Докажите, что положительная определенность матрицы $A \in \mathbb{C}^{n \times n}$ равносильна существованию разложения $A = C^*C$, где $C \in \mathbb{C}^{n \times n}$ — невырожденная верхняя треугольная матрица.

Задача 284. Докажите, что неотрицательная определенность эрмитовой матрицы равносильна неотрицательности всех ее главных миноров. Приведите пример эрмитовой матрицы, в которой все ведущие миноры неотрицательны, но матрица неотрицательно определенной не является.

Задача 285. Пусть A и B — комплексные неотрицательно определенные матрицы порядка n . Докажите, что матрица $A \circ B$ (поэлементное произведение) будет неотрицательно определенной.

6.14. Конгруэнтность и закон инерции

Пусть V — линейное пространство над полем $\mathbb{P}$ и функция $f(x, y)$ определена при всех $x, y \in V$, принимает значения в $\mathbb{P}$ и линейна по каждому аргументу. Такая функция называется *билинейной формой*. Пусть пространство V конечномерно

и векторы $e_1, \dots, e_n$ образуют его базис. Тогда для векторов $x = \sum_{j=1}^n x_j e_j$ и $y = \sum_{i=1}^n y_i e_i$ находим

$$f(x, y) = \left(\sum_{j=1}^n x_j e_j, \sum_{i=1}^n y_i e_i \right) = \sum_{i=1}^n \sum_{j=1}^n f(e_j, e_i) x_j y_i = [y]_e^\top A [x]_e,$$

где матрица $A \in \mathbb{P}^{n \times n}$ имеет элементы $a_{ij} = f(e_j, e_i)$ и называется *матрицей билинейной формы* $f(x, y)$ в базисе e .

Пусть $g_1, \dots, g_n$ — еще один базис и P_{eg} — матрица перехода от g к e . Тогда

$$\begin{aligned} [x]_e &= P_{eg} [x]_g, \quad [y]_e = P_{eg} [y]_g \Rightarrow \\ &\Rightarrow f(x, y) = [y]_g^\top B [x]_g, \quad B = P_{eg}^\top A P_{eg}. \end{aligned}$$

Матрица A называется *конгруэнтной* матрице B , если $B = P^\top A P$ для некоторой невырожденной матрицы $P \in \mathbb{P}^{n \times n}$. Мы можем утверждать, что *квадратные матрицы конгруэнтны тогда и только тогда, когда они являются матрицами одной и той же билинейной формы в разных базисах*. Бинарное отношение конгруэнтности на множестве $n \times n$ -матриц — это еще один пример отношения эквивалентности.

В случае $\mathbb{P} = \mathbb{C}$ часто рассматриваются *полуторалинейные формы* $f(x, y)$ — они линейны по первому аргументу и *сопряженно линейны* по второму аргументу:

$$f(x, \alpha u + \beta v) = \bar{\alpha} f(x, u) + \bar{\beta} f(x, v) \quad \forall x, u, v \in V, \quad \forall \alpha, \beta \in \mathbb{C}.$$

В базисах e и f получаем $f(x, y) = [y]_e^* A [x]_e = [y]_g^* B [x]_g$, где $B = P_{eg}^* A P_{eg}$. Матрица $A \in \mathbb{C}^{n \times n}$ называется *эрмитово конгруэнтной* матрице $B \in \mathbb{C}^{n \times n}$, если $B = P^* A P$ для некоторой невырожденной матрицы $P \in \mathbb{C}^{n \times n}$.

Если билинейная форма обладает свойством *симметрии* $f(x, y) = f(y, x)$, то ее матрица будет симметричной. В случае комплексного поля обычно рассматривается свойство *сопряженной симметрии* $f(x, y) = \overline{f(y, x)}$, а матрица такой полуторалинейной формы оказывается эрмитовой. С симметричными билинейными и сопряженно симметричными полуторалинейными формами ассоциируются функции $F(x) := f(x, x)$. В первом

случае $F(x)$ называется *квадратичной формой*, а во втором — *эрмитовой квадратичной формой*. При их изучении в вещественном случае естественно интересоваться конгруэнтностью вещественных симметричных матриц, а в комплексном случае — эрмитовой конгруэнтностью эрмитовых матриц.

Теорема 6.14.1 (ЗАКОН ИНЕРЦИИ). *Эрмитовы матрицы эрмитово конгруэнтны в том и только том случае, когда они имеют одно и то же число положительных собственных значений, одно и то же число отрицательных собственных значений и одно и то же число нулевых собственных значений, подсчитываемых с учетом кратностей.*

Доказательство. Любая эрмитова матрица унитарно подобна и поэтому эрмитово конгруэнтна диагональной матрице из ее собственных значений. Если эрмитовы матрицы эрмитово конгруэнтны, то соответствующие диагональные матрицы A и B также эрмитово конгруэнтны, т.е. $B = Q^* A Q$ для невырожденной матрицы $Q \in \mathbb{C}^{n \times n} \Rightarrow r := \text{rank } A = \text{rank } B$. Пусть $A = \text{diag}(\alpha_1, \dots, \alpha_n)$ и $B = \text{diag}(\beta_1, \dots, \beta_n)$, т.е. диагональные элементы матриц A и B равны $\alpha_1, \dots, \alpha_n$ и $\beta_1, \dots, \beta_n$. Не ограничивая общности, будем считать, что $\alpha_i = \beta_i = 0$ при $r + 1 \leq i \leq n$, $\alpha_1, \dots, \alpha_k > 0$, $\alpha_{k+1}, \dots, \alpha_r < 0$, $\beta_1, \dots, \beta_l > 0$, $\beta_{l+1}, \dots, \beta_r < 0$. Докажем, что $k = l$. Для любых векторов $x, y \in \mathbb{C}^n$, связанных условием $x = Qy$, получаем $x^* A x = y^* B y \Rightarrow$

$$\sum_{i=1}^k \alpha_i |x_i|^2 - \sum_{i=k+1}^r |\alpha_i| |x_i|^2 = \sum_{i=1}^l \beta_i |y_i|^2 - \sum_{i=l+1}^r |\beta_i| |y_i|^2.$$

Рассмотрим подпространства

$$L = \{x \in \mathbb{C}^n : x_{k+1} = \dots = x_n = 0\},$$

$$M = \{x \in \mathbb{C}^n : (Q^{-1}x)_1 = \dots = (Q^{-1}x)_l = 0\}.$$

Легко проверяется, что $\dim L = k$ и $\dim M = n - l$. Согласно теореме Грассмана, $\dim L \cap M \geq k + (n - l) - n = k - l$. Если $k > l$, то L и M содержат общий ненулевой вектор x , для которого $x^* A x > 0$, но для $y = Q^{-1}x$ имеет место неравенство $y^* B y \leq 0$. Полученное противоречие означает, что $k \leq l$. Аналогичное рассуждение должно привести к неравенству $k \geq l$. Следовательно, $k = l$.

Остается доказать, что если $k = l$, то матрицы A и B эрмитово конгруэнтны. Пусть $\Omega := \text{diag}(\omega_1, \dots, \omega_n)$, где $\omega_i = \sqrt{|\alpha_i|}$, если $\alpha_i \neq 0$, и $\omega_i = 1$, если $\alpha_i = 0$. Ясно, что $D_A := (\Omega^{-1})^* A \Omega^{-1}$ — это диагональная матрица, в которой k элементов равны 1, $r - k$ элементов равны -1 , а остальные элементы равны нулю. Матрица B эрмитово конгруэнтна какой-то диагональной матрице D_B с тем же свойством. Читателю остается проверить эрмитову конгруэнтность матриц D_A и D_B . Можно доказать даже более общее утверждение о том, что любая вещественная диагональная матрица эрмитово конгруэнтна диагональной матрице с произвольно переставленными диагональными элементами. $\square$

Задача 286. Пусть A — эрмитова матрица порядка n и γ_k — ее ведущий минор порядка n . Предположим, что $\gamma_k \neq 0$ для всех $1 \leq k \leq n$, и положим $\gamma_0 := 1$. Докажите, что число отрицательных собственных значений матрицы A равно числу перемен знака в последовательности $\gamma_0, \gamma_1, \dots, \gamma_n$, т.е. числу значений индекса $1 \leq k \leq n$, таких что γ_{k-1} и γ_k имеют разные знаки.

6.15. Мажоризация и двоякостochasticеские матрицы

При изучении матричных норм очень полезным оказывается бинарное отношение *мажоризации* на множестве векторов. Пусть $x_1 \geq \dots \geq x_n$ и $y_1 \geq \dots \geq y_n$. Будем говорить, что вектор $x = [x_1, \dots, x_n]^T$ *мажорируется* вектором $y = [y_1, \dots, y_n]^T$, если выполнены соотношения

$$\sum_{i=1}^k x_i \leq \sum_{i=1}^k y_i, \quad 1 \leq k \leq n, \quad \sum_{i=1}^n x_i = \sum_{i=1}^n y_i.$$

Обозначения: $x \prec y$ или $y \succ x$. При изучении мажоризации ключевую роль играют *двоякостochasticеские матрицы* — это квадратные вещественные матрицы, в которых все элементы неотрицательны и сумма элементов в каждом столбце совпадает с суммой элементов в каждой строке и равна 1.

Теорема 6.15.1. Пусть элементы векторов $x, y \in \mathbb{R}^n$ удовлетворяют неравенствам $x_1 \geq \dots \geq x_n$ и $y_1 \geq \dots \geq y_n$. Тогда $x \prec y$ в том и только том случае, когда $x = Sy$ для некоторой двоякостochasticеской матрицы $S \in \mathbb{R}^{n \times n}$.

Доказательство. Предположим, что $x = Sy$, где S — двоякостochasticкая матрица с элементами s_{ij} , и докажем, что $x \prec y$:

$$\begin{aligned} \sum_{i=1}^k x_i &\leq \sum_{j=1}^k \underbrace{\left(\sum_{i=1}^k s_{ij} \right)}_{=\gamma_j} y_j + \underbrace{\sum_{j=k+1}^n \sum_{i=1}^k s_{ij} y_{k+1}}_{=k - \sum_{j=1}^k \gamma_j} = \\ &= \sum_{j=1}^k y_j - \sum_{j=1}^k (1 - \gamma_j)(y_j - y_{k+1}) \leq \sum_{j=1}^k y_j. \end{aligned}$$

Теперь предположим, что $x \prec y$. Существование двоякостochasticкой матрицы S , такой что $x = Sy$, будем доказывать индукцией по n . Случай $n = 1$ тривиален. Пусть $n \geq 2$. Из условия $x \prec y$ легко вывести, что $y_n \leq x_1 \leq y_1$, и заведомо имеется номер $2 \leq t \leq n$, для которого $y_t \leq x_1 \leq y_{t-1}$. Точка x_1 отрезка $[y_t, y_{t-1}]$ является выпуклой комбинацией граничных точек:

$$x_1 = \alpha y_{t-1} + \beta y_t,$$

$$\alpha, \beta \geq 0, \quad \alpha + \beta = 1.$$

Введем вектор $z \in \mathbb{R}^n$ с элементами

$$z_1 := \alpha y_{t-1} + \beta y_t, \quad z_t := \beta y_{t-1} + \alpha y_t,$$

$$z_i := y_{i-1}, \quad 2 \leq i \leq t-1, \quad z_i = y_i, \quad t+1 \leq i \leq n.$$

Легко видеть, что $z = Py$, где $P = [p_{ij}]$ отличается от единичной матрицы только 2×2 -блоком

$$\begin{bmatrix} p_{1,t-1} & p_{1t} \\ p_{t,t-1} & p_{tt} \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix}.$$

Ясно, что матрица P двоякостochasticкая.

По построению $x_1 = z_1$. Положим $u := [x_2, \dots, x_n]^\top$ и $v := [z_2, \dots, z_n]^\top$. Чтобы провести индукцию, докажем, что $u \prec v$. В силу неравенств

$$x_t \leq \dots \leq x_1 \leq y_{t-1} \leq \dots \leq y_1$$

находим: $\sum_{i=2}^k x_i \leq \sum_{i=1}^{k-1} y_i = \sum_{i=2}^k z_i$ при $2 \leq k \leq t-1$. Далее, опираясь на неравенство $x \prec y$, при $t \leq k \leq n$ получаем

$$\begin{aligned} \sum_{i=2}^k x_i &\leq \sum_{i=1}^k y_i - x_1 = \sum_{i=1}^t y_i - (\alpha y_{t-1} + \beta y_t) + \sum_{i=t+1}^k y_i = \\ &= \sum_{i=1}^{t-2} y_i + (\beta y_{t-1} + \alpha y_t) + \sum_{i=t+1}^k y_i = \sum_{i=2}^k z_i. \end{aligned}$$

Равенство $\sum_{i=2}^n x_i = \sum_{i=2}^n z_i$ проверяется очевидным образом. Согласно индуктивному предположению $u = Q_1 v$ для некоторой двоякостochasticической матрицы Q_1 порядка $n-1 \Rightarrow x = Qz$ для двоякостochasticической матрицы $Q = \begin{bmatrix} 1 & 0 \\ 0 & Q_1 \end{bmatrix}$. В итоге $x = Qz = (QP)y$. Легко проверяется, что произведение двоякостochasticических матриц остается двоякостochasticической матрицей. $\square$

Напомним, что неравенство $[x_1, \dots, x_n]^\top \leq [y_1, \dots, y_n]^\top$ означает, что $x_i \leq y_i$ при всех $1 \leq i \leq n$.

Утверждение 6.15.1. Пусть $x_1 \geq \dots \geq x_n \geq 0$, $y_1 \geq \dots \geq y_n \geq 0$ и выполняются неравенства

$$\sum_{i=1}^k x_i \leq \sum_{i=1}^k y_i, \quad 1 \leq k \leq n.$$

Тогда существуют вещественные числа $z_1 \geq \dots \geq z_n \geq 0$ такие, что три вектора $x = [x_1, \dots, x_n]^\top$, $y = [y_1, \dots, y_n]^\top$, $z = [z_1, \dots, z_n]^\top$ связаны неравенствами $x \prec z \leq y$.

Доказательство. Если неравенство при $k = n$ обращается в равенство, то можно взять $z = y$. Искомый вектор z реализует минимум линейного функционала $f(z) = z_1 + \dots + z_n$ на некотором полиэдре (минимум достигается, так как функционал ограничен снизу). Если в точке минимума при всех

$1 \leq k \leq n$ имеют место строгие неравенства $\sum_{i=1}^k x_i < \sum_{i=1}^k z_i$, то, очевидно, значение функционала на данном полиэдре можно уменьшить, т. е. это не точка минимума. Если равенство есть при каком-то $1 \leq k \leq n-1$, то задача сводится к аналогичной задаче

для чисел $x_{k+1} \geq \dots \geq x_n \geq 0$ и $z_{k+1} \geq \dots \geq z_n \geq 0$ и можно применить индукцию $\Rightarrow$ в точке минимума достигается равенство $f(z) = x_1 + \dots + x_n$. $\square$

Следующий раздел будет посвящен матричным нормам, инвариантным относительно умножений на унитарные матрицы. Введенное нами понятие мажоризации и теорема 6.15.1 будут ключевыми. Однако прежде чем перейти к матричным нормам, мы обсудим пользу мажоризации как инструмента для изучения связи между собственными значениями и сингулярными числами. Здесь используются два ключевых наблюдения.

Утверждение 6.15.2. Пусть $[x_1, \dots, x_n]^\top \prec [y_1, \dots, y_n]^\top$. Тогда для произвольной выпуклой монотонно возрастающей функции $\phi(t)$ вещественного аргумента t выполняются неравенства $\sum_{i=1}^k \phi(x_i) \leq \sum_{i=1}^k \phi(y_i)$, $1 \leq k \leq n$.

Доказательство оставляем читателю, так как оно по сути повторяет первую часть доказательства теоремы 6.15.1.

Утверждение 6.15.3 (Неравенства Вейля). Для произвольной комплексной матрицы порядка n ее сингулярные числа σ_i и собственные значения λ_i , занумерованные по невозрастанию модуля, связаны неравенствами $\prod_{i=1}^k |\lambda_i| \leq \prod_{i=1}^k \sigma_i$, $1 \leq k \leq n$.

Доказательство. Согласно теореме Шура, для заданной матрицы A и некоторой унитарной матрицы Q матрица $R = Q^* A Q$ оказывается верхней треугольной, причем выбор Q может обеспечить любой предписанный порядок собственных значений на главной диагонали матрицы R , в том числе и интересующий нас — по невозрастанию модуля. Рассмотрим в R ведущую подматрицу R_k порядка k и используем соотношения разделения для собственных значений эрмитовой матрицы $R^* R$ и ее ведущей подматрицы $R_k^* R_k$:

$$\prod_{i=1}^k |\lambda_i|^2 = \det R_k^* R_k = \prod_{i=1}^k (\sigma_i(R_k))^2 \leq \prod_{i=1}^k (\sigma_i(R))^2 = \prod_{i=1}^k \sigma_i^2. \quad \square$$

Следствие 6.15.1. $[\ln |\lambda_1|, \dots, \ln |\lambda_n|]^\top \prec [\ln \sigma_1, \dots, \ln \sigma_n]^\top$.

В качестве выпуклой монотонно возрастающей функции можно взять, например, $\phi(t) = e^{pt}$ при $p > 0$. Тогда, согласно утверждению 6.15.2, получаем неравенства

$$\sum_{i=1}^k |\lambda_i|^p \leq \sum_{i=1}^k \sigma_i^p, \quad 1 \leq k \leq n.$$

Приведем еще один весьма нетривиальный результат, который коротко и элегантно доказывается с использованием двоякостochasticеских матриц.

Теорема 6.15.2 (ТЕОРЕМА ВИЛАНДТА–ХОФФМАНА). Пусть A и B — нормальные матрицы порядка n , $\lambda_1(A), \dots, \lambda_n(A)$ и $\lambda_1(B), \dots, \lambda_n(B)$ — их собственные значения (в общем случае комплексные). Тогда для некоторой подстановки $\tau \in \bar{S}_n$ имеет место неравенство

$$\sum_{i=1}^n |\lambda_i(A) - \lambda_{\tau(i)}(B)|^2 \leq \|A - B\|_F^2.$$

Доказательство. Пусть где P и Q — унитарные матрицы, столбцы которых образуют ортонормированные базисы из собственных векторов матриц A и $B \Rightarrow \Lambda = \text{diag}(\lambda_1(A), \dots, \lambda_n(A)) = P^*AP$, $M = \text{diag}(\lambda_1(B), \dots, \lambda_n(B)) = Q^*AQ$. Используем то, что фробениусова норма не меняется при умножении на унитарные матрицы:

$$\|A - B\|_F = \|P\Lambda P^* - QMQ^*\|_F = \|\Lambda - ZMZ^*\|_F, \quad Z = P^*Q.$$

Дальше учитываем то, что фробениусова норма — это длина на пространстве $n \times n$ -матриц, порожденная скалярным произведением $(A, B) := \text{tr}(B^*A)$:

$$\begin{aligned} \|\Lambda - ZMZ^*\|_F^2 &= (\Lambda, \Lambda) - 2 \text{Re}(\Lambda, ZMZ^*) + (ZMZ^*, ZMZ^*) = \\ &= \|\Lambda\|_F^2 + \|M\|_F^2 - \Phi, \end{aligned}$$

где $\Phi := 2 \text{Re}(\text{tr}(ZM^*Z^*\Lambda))$ можно записать в виде

$$\Phi = \sum_{i=1}^n \sum_{j=1}^n c_{ij} s_{ij}, \quad c_{ij} = 2 \text{Re}(\lambda_i(A) \overline{\lambda_j(B)}), \quad s_{ij} = |z_{ij}|^2.$$

Легко видеть, что $n \times n$ -матрица с элементами $|z_{ij}|^2$ будет двоякостochasticеской. Считая c_{ij} заданными константами, не будем фиксировать значения s_{ij} и рассмотрим Φ как линейный функционал на множестве двоякостochasticеских матриц $S = [s_{ij}]$

порядка n . Ясно, что его максимальное значение достигается в вершине полиэдра двоякостochasticеских матриц, т. е. на некоторой матрице перестановки, обозначим ее через $\Pi \Rightarrow$

$$\begin{aligned} \|A - B\|_F^2 &\geq \|A\|_F^2 + \underbrace{\|M\|_F^2}_{= \|\Pi M \Pi^\top\|_F^2} - 2 \operatorname{Re}(\Lambda, \Pi M \Pi^\top) = \\ &= \|A - \Pi M \Pi^\top\|_F^2. \quad \square \end{aligned}$$

Задача 287. Пусть A — эрмитова матрица порядка n , $\lambda_1 \geq \dots \geq \lambda_n$ — ее собственные значения, $\alpha_1 \geq \dots \geq \alpha_n$ — упорядоченные по невозрастанию элементы главной диагонали. Докажите, что $[\alpha_1, \dots, \alpha_n]^\top \prec [\lambda_1, \dots, \lambda_n]^\top$.

Задача 288. Докажите, что для собственных значений эрмитовых $n \times n$ -матриц A и B , занумерованных в порядке невозрастания, справедливо неравенство

$$\sum_{i=1}^n (\lambda_i(A) - \lambda_i(B))^2 \leq \|A - B\|_F^2.$$

6.16. Унитарно инвариантные нормы

Матричная норма называется *унитарно инвариантной*, если она не меняется при умножении матрицы справа или слева на произвольную унитарную матрицу. Известные примеры — это спектральная норма и фробениусова норма матрицы. Здесь мы дадим полное описание унитарно инвариантных норм и получим общий результат для матричных задач приближения, когда погрешность измеряется в произвольной унитарно инвариантной норме.

Пусть норма на пространстве матриц размера $n \times n$ является унитарно инвариантной. Тогда для матрицы $A \in \mathbb{C}^{n \times n}$ она, очевидно, является функцией от сингулярных чисел $\sigma_1(A) \geq \dots \geq \sigma_n(A) \geq 0$ матрицы A . Пусть в случае произвольной вещественной диагональной матрицы $A = \operatorname{diag}(x_1, \dots, x_n)$ норма имеет вид $\|A\| = f(x_1, \dots, x_n)$. Тогда функция f обязана обладать такими свойствами:

- функция f является *симметрической*: $f(x_{\tau(1)}, \dots, x_{\tau(n)}) = f(x_1, \dots, x_n)$ для любой подстановки $\tau \in S_n$.
- функция $F(x) := f(x_1, \dots, x_n)$ задает векторную норму на пространстве вещественных векторов $x = [x_1, \dots, x_n]^\top$.

- для любых $x_1, \dots, x_n \in \mathbb{R}$ выполняется равенство $f(x_1, \dots, x_n) = f(|x_1|, \dots, |x_n|)$. В таких случаях векторная норма $F(x)$ называется *абсолютной нормой*.

Функцию f с перечисленными свойствами называют *симметрической калибровочной функцией*.

Теорема 6.16.1 (Джон фон Нейман). Для произвольной симметрической калибровочной функции $f(x_1, \dots, x_n)$ формула $\|A\| = f(\sigma_1(A), \dots, \sigma_n(A))$ задает унитарно инвариантную норму на пространстве комплексных $n \times n$ -матриц A и любая унитарно инвариантная норма имеет такой вид для некоторой симметрической калибровочной функции $f(x_1, \dots, x_n)$.

Для доказательства нам понадобятся некоторые обозначения и утверждения, имеющие также самостоятельную ценность.

Пусть $x = [x_1, \dots, x_n]^T$ — вещественный вектор и $\tau \in S_n$ — подстановка, упорядочивающая его элементы по невозрастанию: $x_{\tau(1)} \geq \dots \geq x_{\tau(n)}$. Для вектора с переставленными элементами будем использовать обозначение $x' := [x_{\tau(1)}, \dots, x_{\tau(n)}]^T$. Положим $|x| := [|x_1|, \dots, |x_n|]^T$ и, если $x = |x|$, будем писать $x \geq 0$. Введем также следующие функции Фань Цзы:

$$F_k(x) := \sum_{i=1}^k |x|'_i = \max_{1 \leq i_1 < \dots < i_k \leq n} (|x_{i_1}| + \dots + |x_{i_k}|), \quad 1 \leq k \leq n.$$

Легко видеть, что каждая из них является симметрической калибровочной функцией.

Лемма 6.16.1. Для любой абсолютной нормы $F(x)$ на пространстве $\mathbb{R}^n$ имеет место свойство монотонности: если $|x| \leq |y|$, то $F(x) \leq F(y)$.

Доказательство. Достаточно установить монотонность при увеличении модуля одного произвольного элемента вектора. Пусть

$$0 \leq a < b, \quad x = \begin{bmatrix} a \\ c \end{bmatrix}, \quad y = \begin{bmatrix} b \\ c \end{bmatrix}, \quad z = \begin{bmatrix} -b \\ c \end{bmatrix} \Rightarrow$$

$$\Rightarrow x = \alpha z + \beta y \quad \text{при} \quad \alpha = \frac{1}{2} \left(1 - \frac{a}{b}\right), \quad \beta = \frac{1}{2} \left(1 + \frac{a}{b}\right).$$

Из абсолютности нормы вытекает, что $F(z) = F(y) \Rightarrow F(x) \leq \alpha F(z) + \beta F(y) = (\alpha + \beta)F(y) = F(y)$. $\square$

Лемма 6.16.2 (Фань Цзы). Пусть $x, y \in \mathbb{R}^n$ — произвольные фиксированные векторы и $F_1(x), \dots, F_n(x)$ — функции Фань Цзы. Тогда, если $F_k(x) \leq F_k(y)$ для всех $1 \leq k \leq n$, то $F(x) \leq F(y)$ для произвольной симметрической калибровочной функции $F(x)$.

Доказательство. Условия $F_k(x) \leq F_k(y)$, $1 \leq k \leq n$, — это в точности условия утверждения 6.15.1 $\Rightarrow \exists z: |x|' \prec |z|' \leq |y|'$. По теореме 6.15.1, $|x|' = S|z|'$ для двоякостochasticеской матрицы S . В силу теоремы Биркгоффа (следствие 6.8.1) матрица S является выпуклой комбинацией матриц перестановки: $S = \sum_{i=1}^N \alpha_i P_i$. Кроме того, $F(|z|') = F(P_i|z|')$, так как функция F симметрическая $\Rightarrow$

$$F(x) = F(|x|') = F\left(\sum_{i=1}^N \alpha_i P_i |z|'\right) \leq \sum_{i=1}^N \alpha_i F(P_i |z|') = F(|z|').$$

В силу свойства монотонности (лемма 6.16.1), получаем $F(|z|') \leq F(|y|') = F(y)$. $\square$

Лемма 6.16.3. Пусть сингулярные числа комплексных $n \times n$ -матриц упорядочиваются по невозрастанию. Тогда для каждого $1 \leq k \leq n$ функция $\|A\|_{(k)} := \sum_{i=1}^k \sigma_i(A)$ является унитарно инвариантной нормой на пространстве $\mathbb{C}^{n \times n}$.

Доказательство. Каждой матрице A порядка n поставим в соответствие матрицу $\tilde{A} := \begin{bmatrix} 0 & A \\ A^* & 0 \end{bmatrix}$ порядка $2n$. Несложно проверяется, что матрица $\tilde{A}$ эрмитова, а ее собственные значения в порядке невозрастания имеют вид

$$\sigma_1(A) \geq \dots \geq \sigma_n(A) \geq -\sigma_n(A) \geq \dots \geq -\sigma_1(A).$$

Для эрмитовых матриц $\tilde{A}$ и $\tilde{B}$ применим теорему Лидского в случае $I = \{1, \dots, k\} \Rightarrow \|A + B\|_{(k)} \leq \|A\|_{(k)} + \|B\|_{(k)}$. Таким образом, неравенство треугольника установлено. Остальные свойства нормы практически очевидны. $\square$

Норма $\|A\|_{(n)}$ (сумма всех сингулярных чисел) называется также *ядерной нормой* матрицы A .

Доказательство теоремы 6.16.1. Пусть $F(x)$ — произвольная симметрическая калибровочная функция и $\|A\| := F(\sigma(A))$,

где $\sigma(A) = [\sigma_1(A), \dots, \sigma_n(A)]^\top$. Неочевидно лишь неравенство треугольника. По лемме 6.16.3, функции Фань Цзы $\|A\|_{(k)}$ являются нормами на пространстве $\mathbb{C}^{n \times n} \Rightarrow$

$$F_k(\sigma(A+B)) \leq F_k(\sigma(A)) + F_k(\sigma(B)) = F_k(\sigma(A) + \sigma(B)),$$

$$1 \leq k \leq n.$$

Согласно лемме 6.16.3 $F(\sigma(A+B)) \leq F(\sigma(A) + \sigma(B))$. Поскольку $F(x)$ является векторной нормой на $\mathbb{R}^n$, получаем

$$\|A+B\| \leq F(\sigma(A) + \sigma(B)) \leq F(\sigma(A)) + F(\sigma(B)) = \|A\| + \|B\|. \quad \square$$

Теорема 6.16.2 (ТЕОРЕМА МИРСКОГО). Пусть A и B — произвольные комплексные матрицы порядка n , $\sigma_1(A) \geq \dots \geq \sigma_n(A)$ и $\sigma_1(B) \geq \dots \geq \sigma_n(B)$ — их сингулярные числа, $\Sigma(A) = \text{diag}(\sigma_1(A), \dots, \sigma_n(A))$, $\Sigma(B) = \text{diag}(\sigma_1(B), \dots, \sigma_n(B))$. Тогда для любой унитарно инвариантной нормы справедливо неравенство

$$\|\Sigma(A) - \Sigma(B)\| \leq \|A - B\|.$$

Доказательство. Рассмотрим эрмитовы матрицы $\tilde{A} = \begin{bmatrix} 0 & A \\ A^* & 0 \end{bmatrix}$ и $\tilde{B} = \begin{bmatrix} 0 & B \\ B^* & 0 \end{bmatrix}$ и применим теорему Лидского к матрицам $\hat{B}$ и $\hat{A} - \hat{B}$ при специальном выборе множества индексов I . Собственные значения матриц $\hat{A}$, $\hat{B}$ и $\hat{A} - \hat{B}$ — это плюс-минус сингулярные числа матриц A , B и $A - B$, их списки в порядке невозрастания имеют вид

$$\begin{aligned} \sigma_1(A) \geq \dots \geq \sigma_n(A) &\geq -\sigma_n(A) \geq \dots \geq -\sigma_1(A), \\ \sigma_1(B) \geq \dots \geq \sigma_n(B) &\geq -\sigma_n(B) \geq \dots \geq -\sigma_1(B), \\ \sigma_1(A-B) \geq \dots \geq \sigma_n(A-B) &\geq -\sigma_n(A-B) \geq \dots \geq -\sigma_1(A-B). \end{aligned}$$

Рассмотрим величины $|\sigma_i(A) - \sigma_i(B)|$, $1 \leq i \leq n$, и упорядочим их по невозрастанию:

$$|\sigma_{i_1}(A) - \sigma_{i_1}(B)| \geq \dots \geq |\sigma_{i_n}(A) - \sigma_{i_n}(B)|.$$

Теперь возьмем произвольное $1 \leq k \leq n$ и составим множество $I \subset \{1, \dots, 2n\}$ мощности k из двух подмножеств, $I_1 \subseteq \{1, \dots, n\}$ и $I_2 \subseteq \{n+1, \dots, 2n\}$, которые определим следующим образом:

$$\begin{aligned} i \in I_1 &\Leftrightarrow i = i_l, \quad 1 \leq l \leq k \text{ и } \sigma_{i_l}(A) \geq \sigma_{i_l}(B), \\ i \in I_2 &\Leftrightarrow i = 2n+1-i_l, \quad 1 \leq l \leq k \text{ и } \sigma_{i_l}(A) < \sigma_{i_l}(B). \end{aligned}$$

По теореме Лидского получаем неравенства

$$\begin{aligned} \sum_{i \in I_1} \sigma_i(A) + \sum_{i \in I_2} (-\sigma_i(A)) &\leq \sum_{i \in I_1} \sigma_i(B) + \sum_{i \in I_2} (-\sigma_i(B)) + \\ &+ \sum_{i=1}^k |\sigma_i(A - B)| \Rightarrow \sum_{l=1}^k |\sigma_{i_l}(A) - \sigma_{i_l}(B)| \leq \sum_{i=1}^k |\sigma_i(A - B)|. \end{aligned}$$

Таким образом, условия леммы 6.16.2 выполнены для векторов

$$\begin{aligned} x &= [|\sigma_{i_1}(A) - \sigma_{i_1}(B)|, \dots, |\sigma_{i_n}(A) - \sigma_{i_n}(B)|]^T, \\ y &= [\sigma_1(A - B), \dots, \sigma_n(A - B)]^T. \end{aligned}$$

Поэтому $F(x) \leq F(y)$ для произвольной симметрической калибровочной функции $F(x)$, в том числе и для той, которая в соответствии с теоремой 6.16.1 порождает заданную унитарно инвариантную норму. $\square$

Следствие 6.16.1. Пусть $\sigma_1 \geq \dots \geq \sigma_n$ — сингулярные числа и $A = \sum_{i=1}^n \sigma_i v_i u_i^*$ — сингулярное разложение матрицы A . Тогда для произвольной унитарно инвариантной нормы

$$\min_{\text{rank } B \leq k} \|A - B\| = \|A - A_k\|, \quad A_k = \sum_{i=1}^k \sigma_i v_i u_i^*, \quad 1 \leq k \leq n.$$

Задача 289. Докажите, что ядерная и спектральная норма являются взаимно дуальными.

Задача 290. Пусть $\sigma_1 \geq \dots \geq \sigma_n$ — сингулярные числа и $A = \sum_{i=1}^n \sigma_i v_i u_i^*$ — сингулярное разложение матрицы A . Докажите, что для фробениусовой нормы

$$\min_{\text{rank } B \leq k} \|A - B\|_F = \sqrt{\sum_{i=k+1}^n \sigma_i^2}.$$

Задача 291. Даны комплексные матрицы A и B порядка n , и известно, что матрица AB нормальна. Докажите, что $\|AB\| \leq \|BA\|$ для любой унитарно инвариантной нормы.

ГРУППЫ, ПОЛЯ, УРАВНЕНИЯ

7.1. Линейная независимость автоморфизмов поля

Аutomорфизмом поля M называется изоморфизм поля M на себя. Тожественное отображение является автоморфизмом и называется *тривиальным автоморфизмом*.

Если поле M является расширением поля K , то любой автоморфизм поля M , при котором каждый элемент поля K остается на месте, называется *автоморфизмом поля M над полем K* . Обозначения:

- $\mathcal{A}(M)$ — множество всех автоморфизмов поля M ;
- $\mathcal{A}(M : K)$ — множество всех автоморфизмов M над K .

Пример 1. Отображение $z \rightarrow \bar{z}$ (комплексное число z переводится в комплексно-сопряженное число $\bar{z}$) является автоморфизмом поля комплексных чисел $\mathbb{C}$ над полем вещественных чисел $\mathbb{R}$.

Пример 2. Отображение $a + b\sqrt{2} \rightarrow a - b\sqrt{2}$ при условии $a, b \in \mathbb{Q}$ является автоморфизмом поля $\mathbb{Q}(\sqrt{2})$ над полем $\mathbb{Q}$.

Пример 3. Пусть M — конечное поле с числом элементов p^2 и p — простое число. Отображение $a \rightarrow a^p$ является нетривиальным автоморфизмом поля M над $\mathbb{Z}_p$.

Утверждение 7.1.1. Множества $\mathcal{A}(M)$ и $\mathcal{A}(M : K)$ являются группами относительно композиции автоморфизмов. При этом $\mathcal{A}(M : K) \leq \mathcal{A}(M)$.

Автоморфизмы поля M можно рассматривать как элементы линейного пространства над полем M , составленного из всех функций (отображений) с областью определения M и областью значений M таким образом, что сумма векторов определяется как сумма функций, а умножение вектора на число из M — как поточечное умножение значений функции на это число. Нулевым вектором, очевидно, является функция, которая принимает

значение 0 во всех точках. Очень полезно то, что появляется возможность говорить о линейной независимости автоморфизмов как функций.

Теорема 7.1.1. *Любая конечная система разных автоморфизмов поля M является линейно независимой над M .*

Доказательство. Проведем индукцию по числу автоморфизмов m . Случай $m = 1$ очевиден, так как ненулевой вектор всегда образует линейно независимую систему. Пусть $m \geq 2$. Рассмотрим такую линейную комбинацию разных автоморфизмов $g_1, \dots, g_m \in \mathcal{A}(M)$ с коэффициентами из поля M , которая оказывается тождественно равной нулю:

$$\alpha_1 g_1(a) + \dots + \alpha_m g_m(a) = 0 \quad \forall a \in M. \quad (1)$$

Заменим a на ab и примем во внимание то, что любой автоморфизм сохраняет операции. Тогда из (1) получаем тождество

$$\alpha_1 g_1(a)g_1(b) + \dots + \alpha_{m-1} g_{m-1}(a)g_{m-1}(b) + \alpha_m g_m(a)g_m(b) = 0 \\ \forall a, b \in M. \quad (2)$$

Умножив (1) на $g_m(b)$, приходим к тождеству

$$\alpha_1 g_1(a)g_m(b) + \dots + \alpha_{m-1} g_{m-1}(a)g_m(b) + \alpha_m g_m(a)g_m(b) = 0, \\ \forall a, b \in M. \quad (3)$$

После вычитания тождества (3) из (2) находим

$$\alpha_1 (g_1(b) - g_m(b))g_1(a) + \dots + \alpha_{m-1} (g_{m-1}(b) - g_m(b))g_{m-1}(a) = 0 \\ \forall a, b \in M.$$

По индуктивному предположению,

$$\alpha_i (g_i(b) - g_m(b)) = 0, \quad 1 \leq i \leq m-1, \quad \forall b \in M.$$

Для каждого i можно выбрать b таким образом, что $g_i(b) \neq g_m(b)$, иначе $g_i = g_m$. Следовательно,

$$\alpha_i = 0 \text{ при } 1 \leq i \leq m-1 \Rightarrow \alpha_m g_m = 0 \Rightarrow \alpha_m = 0. \quad \square$$

Теорема остается в силе и в случае отображений поля M в себя, обладающих свойством сохранения операций, но без взаимной однозначности. Такие отображения называются *гомоморфизмами*. Единственным дополнительным требованием будет, конечно, отсутствие в этой системе отображения, тождественно равного нулю. Более того, аналогичный результат получается для

любой конечной системы гомоморфизмов произвольной группы в мультипликативную группу какого-то поля. В последнем случае рассматривается линейное пространство функций, определенных на элементах заданной группы и принимающих значения в заданном поле.

Задача 292. Найдите все автоморфизмы поля вычетов по простому модулю p .

Задача 293. Пусть $M \leq \mathbb{C}$ — поле разложения многочлена $f(x) \in \mathbb{Q}[x]$. Найдите все автоморфизмы поля M в следующих случаях: (1) $f(x) = x^4 - 1$, (2) $f(x) = x^6 - 1$, (3) $f(x) = x^{2011} - 1$.

Задача 294. Докажите, что любая конечная система разных гомоморфизмов группы G в мультипликативную группу K^* поля K является линейно независимой в линейном пространстве функций, определенных на множестве G и принимающих значения из K .

7.2. Неподвижные поля и группы автоморфизмов

Пусть $G = \{g_1, \dots, g_m\}$ — конечное подмножество автоморфизмов поля M , необязательно образующих группу. Рассмотрим множество M^G чисел из M , остающихся на месте при действии каждого автоморфизма из G :

$$M^G := \{a \in M : g(a) = a \ \forall g \in G\}.$$

Утверждение 7.2.1. Множество M^G является подполем поля M . При этом

$$a \in M \setminus M^G \Leftrightarrow \exists g \in G : g(a) \neq a.$$

Множество M^G называется **максимальным неподвижным полем** относительно множества отображений G .

Теорема 7.2.1. Пусть множество G содержит t разных автоморфизмов $g_1, \dots, g_m$ поля M и при этом расширение $M^G \leq M$ является конечным и его размерность равна n . Тогда $t \leq n$.

Доказательство. Пусть числа $\theta_1, \dots, \theta_n$ образуют базис линейного пространства M над полем M^G . Рассмотрим матрицу

$$A = \begin{bmatrix} g_1(\theta_1) & \dots & g_1(\theta_n) \\ \dots & \dots & \dots \\ g_m(\theta_1) & \dots & g_m(\theta_n) \end{bmatrix} \quad (*)$$

и заметим, что ее строки линейно независимы как элементы линейного пространства $M^{1 \times n}$. В самом деле, пусть какая-то их линейная комбинация с коэффициентами $\alpha_1, \dots, \alpha_m \in M$ дает нулевую строку. Тогда функция

$$f := \alpha_1 g_1 + \dots + \alpha_m g_m$$

принимает нулевые значения в точках $\theta_1, \dots, \theta_n$. Произвольное число из M имеет вид

$$\theta = a_1 \theta_1 + \dots + a_n \theta_n, \quad a_1, \dots, a_n \in M^G.$$

Поэтому

$$\begin{aligned} f(\theta) &= \sum_{i=1}^m \alpha_i \sum_{j=1}^n g_i(a_j) g_i(\theta_j) = \sum_{i=1}^m \alpha_i \sum_{j=1}^n a_j g_i(\theta_j) = \\ &= \sum_{j=1}^n \sum_{i=1}^m a_j \alpha_i g_i(\theta_j) = \sum_{j=1}^n a_j f(\theta_j) = 0. \end{aligned}$$

Таким образом, $f(\theta) = 0 \quad \forall \theta \in M \Rightarrow f = 0$. В силу линейной независимости автоморфизмов $\alpha_1 = \dots = \alpha_m = 0$. Из линейной независимости строк матрицы вытекает, что число столбцов в ней не меньше числа строк. $\square$

Теорема 7.2.2. Пусть множество G состоит из автоморфизмов $g_1, \dots, g_m$ поля M и образует группу относительно композиции автоморфизмов. Если числа $\theta_1, \dots, \theta_n \in M$ линейно независимы как элементы линейного пространства M над полем M^G , то $n \leq m$.

Доказательство. От противного, если $m < n$, то имеются нетривиальные линейные комбинации столбцов матрицы A вида (*), дающие нулевой столбец. Среди них рассмотрим линейную комбинацию с наименьшим числом k ненулевых коэффициентов¹⁾. Не ограничивая общности, будем считать, что ненулевыми являются первые k коэффициентов и при этом k -й коэффициент равен 1:

$$\alpha_1 g_i(\theta_1) + \dots + \alpha_{k-1} g_i(\theta_{k-1}) + g_i(\theta_k) = 0, \quad 1 \leq i \leq m. \quad (1)$$

¹⁾ Здесь мы приводим изящное рассуждение Эмиля Артина.

Среди автоморфизмов группы G должно быть тождественное отображение, пусть это g_1 . Тогда равенство, соответствующее $i = 1$, имеет вид

$$\alpha_1\theta_1 + \dots + \alpha_{k-1}\theta_{k-1} + \theta_k = 0.$$

Хотя бы один из коэффициентов не принадлежит полю M^G , в противном случае числа $\theta_1, \dots, \theta_k$ будут линейно зависимыми над полем M^G . Пусть $\alpha_1 \notin M^G$. Поскольку M^G — максимальное неподвижное поле для группы G , существует какой-то автоморфизм из G , пусть это g_k , для которого

$$g_k(\alpha_1) \neq \alpha_1.$$

Применим g_k к обеим частям равенств (1). Вследствие того что G — группа, содержащая ровно m элементов, ее элементы $g_k g_1, \dots, g_k g_m$ являются перестановкой элементов $g_1, \dots, g_m$. Поэтому мы получаем равенства

$$g_k(\alpha_1)g_i(\theta_1) + \dots + g_k(\alpha_{k-1})g_i(\theta_{k-1}) + g_i(\theta_k) = 0, \quad 1 \leq i \leq m. \quad (2)$$

После вычитания равенств (2) из равенств (1) находим

$$(\alpha_1 - g_k(\alpha_1))g_i(\theta_1) + \dots + (\alpha_{k-1} - g_k(\alpha_{k-1}))g_i(\theta_{k-1}) = 0, \\ 1 \leq i \leq m.$$

Это нетривиальная линейная комбинация столбцов матрицы A вида (*), в которой число ненулевых коэффициентов меньше k . Полученное противоречие с выбором k означает, что $n \leq m$. $\square$

Следствие 7.2.1. Если G — конечная группа автоморфизмов поля M , то расширение $M^G \leq M$ конечно и имеет место равенство

$$\dim(M : M^G) = |G|.$$

Доказательство. Согласно доказанной теореме, число линейно независимых элементов пространства M над M^G не превышает $|G|$. Значит, это пространство конечномерно. В то же время, по первой теореме, число разных автоморфизмов не может быть больше его размерности. $\square$

Следствие 7.2.2. Пусть G_1 и G_2 — две конечные группы автоморфизмов поля M . Если $M^{G_1} = M^{G_2}$, то $G_1 = G_2$.

Доказательство. Пусть $G_1 = \{g_1, \dots, g_m\}$. Если $g \in G_2 \setminus G_1$, то получаем разные автоморфизмы $g, g_1, \dots, g_m \Rightarrow m + 1 \leq \dim(M : M^{G_1}) = m$, что невозможно. $\square$

Следствие 7.2.3. Пусть M — расширение поля K и $G = \mathcal{A}(M : K)$ — группа всех автоморфизмов M над K . Тогда

$$K = M^G \Leftrightarrow \dim(M : K) = |G|.$$

Доказательство. Если $K = M^G$, то равенство $\dim(M : K) = |G|$ уже установлено. Обратно, пусть $\dim(M : K) = |G|$. Тогда $K \leq M^G \leq M$ и выполняется равенство $\dim(M : M^G) = |G|$. Следовательно, $\dim(M^G : K) = 1 \Rightarrow K = M^G$. $\square$

Задача 295. Группа G состоит из автоморфизмов $g_1, \dots, g_n$ поля M , а числа $\theta_1, \dots, \theta_n$ образуют базис поля M как линейного пространства над своим подполем K . Верно ли, что $M^G = K$?

7.3. Группы Галуа и поля разложения

Конечное расширение $K \leq M$ называется *конечным расширением Галуа*, если K является максимальным неподвижным полем для группы всех автоморфизмов M над K . Мы уже знаем, что в этом и только этом случае число автоморфизмов M над K является максимально возможным, т. е. равным размерности M над K . В таких случаях группа $\mathcal{A}(M : K)$ называется *группой Галуа*.

Конечное расширение не будет расширением Галуа, если число автоморфизмов меньше размерности расширения. Например, в группе автоморфизмов поля $\mathbb{Q}(\sqrt[3]{2})$ над $\mathbb{Q}$ нет ни одного автоморфизма, кроме тривиального. Число $\theta := \sqrt[3]{2}$ является корнем неприводимого над $\mathbb{Q}$ многочлена $x^3 - 2$. Поэтому автоморфизм $g: \mathbb{Q}(\theta) \rightarrow \mathbb{Q}(\theta)$ полностью определяется образом числа θ :

$$g(a + b\theta + c\theta^2) = a + bg(\theta) + c(g(\theta))^2, \quad a, b, c \in \mathbb{Q}.$$

В силу неприводимости многочлена $x^3 - 2$ над $\mathbb{Q}$ любой его корень при автоморфизме должен переходить в какой-то корень того же многочлена. Но в поле $\mathbb{Q}(\sqrt[3]{2})$ нет невещественных чисел, а многочлен $x^3 - 2$ имеет только один вещественный корень! Значит, $g(\theta) = \theta$, а такой автоморфизм является тривиальным.

Теорема 7.3.1. Пусть поле K вложено в поле M . Расширение $K \leq M$ является конечным расширением Галуа тогда

и только тогда, когда M есть поле разложения некоторого сепарабельного¹⁾ многочлена с коэффициентами из поля K .

Доказательство. Пусть $K \leq M$ является конечным расширением Галуа. Тогда, по определению, $K = M^G$, где $G = \mathcal{A}(M : K)$ — конечная группа всех автоморфизмов поля M над K . Возьмем произвольное число $a \in M$ и рассмотрим числа $g(a)$ при всевозможных автоморфизмах $g \in G$. Оставим среди них только разные числа, пусть это будут числа $g_1(a), \dots, g_k(a)$, и рассмотрим многочлен

$$f(x) := \prod_{i=1}^k (x - g_i(a)).$$

Коэффициенты $f(x)$ остаются на месте при действии любого автоморфизма $g \in G$, поэтому

$$f(x) \in M^G[x] = K[x].$$

Допустим, что $f(x)$ имеет нетривиальное разложение на неприводимые множители $f(x) = f_1(x) \dots f_s(x)$. Тогда какое-то число $g_i(a)$ является корнем неприводимого многочлена $f_1(x)$, а какое-то число $g_j(a)$ будет корнем неприводимого многочлена $f_2(x)$. Автоморфизм $g := g_j g_i^{-1}$ переводит $g_i(a)$ в $g_j(a)$. Но это невозможно, так как корень неприводимого многочлена может переходить только в корень того же неприводимого многочлена. Следовательно, многочлен $f(x)$ неприводим над K . Итак, a есть корень неприводимого многочлена $f(x) \in K[x]$ с простыми корнями, принадлежащими полю M . Теперь возьмем базис $a_1, \dots, a_n$ поля M как линейного пространства над полем K . Пусть число a_i является корнем неприводимого над K многочлена $F_i(x)$, все корни которого являются простыми и принадлежат полю K . Тогда многочлен $F(x) := F_1(x) \dots F_k(x)$ является сепарабельным, а M — его поле разложения.

Пусть теперь известно, что M — поле разложения сепарабельного многочлена $f(x) \in K[x]$. Нам нужно доказать, что K — максимальное неподвижное поле для группы всех автоморфизмов M над K . Обозначим через t число корней многочлена $f(x)$, не принадлежащих полю K , и проведем индукцию по t . Если

¹⁾ Напомним, что многочлен называется сепарабельным, если в его разложении на неприводимые множители каждый множитель имеет только простые корни.

$m = 0$, то $M = K$ и в группе $G := \mathcal{A}(M : K)$ имеется только тривиальный автоморфизм. Таким образом, $K = M^G$.

Теперь предположим, что $m \geq 1$. Тогда $f(x)$ имеет нетривиальное разложение на неприводимые множители

$$f(x) = f_1(x)f_2(x) \dots f_s(x),$$

в котором степень хотя бы одного многочлена не меньше 2. Пусть

$$l := \deg f_1(x) \geq 2.$$

Тогда корни $f_1(x)$ не могут принадлежать K , пусть θ — один из них. Поскольку многочлен $f(x)$ сепарабельный, все корни $f_1(x)$ простые. Пусть $f_1(x)$ имеет разложение

$$f_1(x) = (x - \theta_1) \dots (x - \theta_l), \quad \theta_1, \dots, \theta_l \in M.$$

Будем считать, что $\theta_1 = \theta$, и рассмотрим поле $K(\theta)$. Оно состоит из чисел вида

$$a_0 + a_1\theta + \dots + a_{l-1}\theta^{l-1}, \quad a_0, \dots, a_{l-1} \in K.$$

Существует ровно l изоморфизмов поля $K(\theta)$ над K . Каждый из них определяется образом корня θ , а это может быть только один и притом любой из корней многочлена $f_1(x)$. Обозначим эти изоморфизмы через $g_1, \dots, g_l$ и будем считать, что

$$g_i(\theta) = \theta_i, \quad 1 \leq i \leq l.$$

Ясно, что g_i отображает поле $K(\theta)$ на поле $K(\theta_i)$. Каждый такой изоморфизм может быть продолжен до изоморфизма заданных полей разложения соответствующих многочленов, а в нашем случае — до какого-то автоморфизма поля M .

Пусть a остается на месте при всех автоморфизмах группы $\mathcal{A}(M : K)$. Ясно, что M является полем разложения над $K(\theta)$ для того же многочлена $f(x)$, причем число корней $f(x)$ вне поля $K(\theta)$ строго меньше m . По индуктивному предположению, $K(\theta)$ является максимальным неподвижным полем для группы $\mathcal{A}(M : K(\theta_1))$, поэтому $a \in K(\theta)$ и, следовательно,

$$a = a_0 + a_1\theta + \dots + a_{l-1}\theta^{l-1}, \quad a_0, \dots, a_{l-1} \in K.$$

Отсюда

$$g_i(a) = a = a_0 + a_1\theta_i + \dots + a_{l-1}\theta_i^{l-1}, \quad 1 \leq i \leq l,$$

а это означает, что многочлен

$$\Phi(x) := (a_0 - a) + a_1x + \dots + a_{l-1}x^{l-1}$$

имеет l разных корней. Таким свойством обладает только нулевой многочлен. Поэтому, в частности,

$$a_0 - a = 0 \Rightarrow a = a_0 \in K.$$

Таким образом, если элемент a остается на месте при всех автоморфизмах группы $\mathcal{A}(M : K)$, то он принадлежит K . $\square$

Полученная теорема показывает, что группа Галуа всегда является группой автоморфизмов поля разложения некоторого сепарабельного многочлена над заданным полем. Эту группу часто называют *группой Галуа данного многочлена*.

Если M — поле разложения сепарабельного многочлена над полем K , то из приведенного выше доказательства видно, что любое число из M является корнем неприводимого над K многочлена, все корни которого простые и принадлежат M . Отсюда тривиальным образом вытекает несколько ослабленное утверждение: если число из M является корнем неприводимого над K многочлена, то все корни данного многочлена также принадлежат M .

Для описания таких случаев есть специальный термин. Пусть M — расширение поля K , обладающее тем свойством, что для каждого числа из M , которое является корнем неприводимого над K многочлена, все корни данного многочлена также принадлежат M . Расширение $K \leq M$ с таким свойством называется *нормальным*, а поле M называется *нормальным над K* . Конечное расширение Галуа всегда является нормальным расширением.

Теорема 7.3.2. *Поле M является полем разложения какого-то многочлена над полем K тогда и только тогда, когда расширение $K \leq M$ является конечным нормальным расширением.*

Доказательство. Пусть $f(x) = (x - \theta_1) \dots (x - \theta_n) \in K[x]$ и поле M получено из K присоединением корней $\theta_1, \dots, \theta_n$. Тогда любое число из M представляет собой значение некоторого многочлена

$$\Phi(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$$

в точке

$$x_1 = \theta_1, \dots, x_n = \theta_n.$$

Заметим, что $f(x)$ может иметь кратные корни. Пусть $a = \Phi(\theta_1, \dots, \theta_n)$. Рассмотрим многочлен

$$\phi(x) := \prod_{\sigma \in S_n} (x - \Phi(\theta_{\sigma(1)}, \dots, \theta_{\sigma(n)})).$$

Каждый коэффициент многочлена $\phi(x)$ является симметрическим многочленом от $\theta_1, \dots, \theta_n$. По основной теореме о симметрических многочленах, каждый коэффициент получается с помощью операций умножения и сложения из элементарных симметрических многочленов от $\theta_1, \dots, \theta_n$, а значит и из коэффициентов исходного многочлена $f(x)$, для которого числа $\theta_1, \dots, \theta_n$ суть все его корни с учетом кратностей. Поэтому $\phi(x) \in K[x]$. При этом a является корнем $\phi(x)$ и все корни $\phi(x)$ принадлежат M . Пусть $\psi(x)$ — неприводимый многочлен, для которого элемент a является корнем. Тогда $\phi(x) : \psi(x)$, а это значит, что все корни $\psi(x)$ принадлежат M .

Второе утверждение теоремы почти очевидно. В силу конечности расширения можно выбрать базис $a_1, \dots, a_n$ поля M над K . Затем для каждого числа a_i можно выбрать его минимальный многочлен с коэффициентами из поля K . Все корни минимальных многочленов принадлежат полю M в силу нормальности расширения. В итоге M является полем разложения произведения выбранных минимальных многочленов. $\square$

Полезное общее свойство групп Галуа связано с особенностью их действия на корнях неприводимых многочленов. Говорят, что группа G действует на множестве A транзитивно, если для любых элементов $a, b \in A$ существует элемент $g \in G$ такой, что $g(a) = b$.

Теорема 7.3.3. Пусть G — группа Галуа для расширения $K \leq M$ и $g(x)$ — произвольный неприводимый многочлен над полем K , все корни которого принадлежат M . Группа G действует на множестве корней $g(x)$ транзитивно.

Доказательство. Пусть $n = \deg g(x)$ и $\alpha_1, \dots, \alpha_n \in M$ — все корни $g(x)$. Мы знаем, что любое число из M является корнем неприводимого многочлена с простыми корнями. Ясно, что это многочлен может быть получен из $g(x)$ умножением на ненулевую константу. Таким образом, все корни $g(x)$ простые. Рассмотрим поле $K(\alpha_i)$. Любой его элемент имеет вид

$$a_0 + a_1\alpha_i + \dots + a_{n-1}\alpha_i^{n-1}, \quad a_0, \dots, a_{n-1} \in K,$$

а отображение

$$g: a_0 + a_1\alpha_i + \dots + a_{n-1}\alpha_i^{n-1} \rightarrow a_0 + a_1\alpha_j + \dots + a_{n-1}\alpha_j^{n-1}$$

является изоморфизмом поля $K(\alpha_i)$ на поле $K(\alpha_j)$, переводящим α_i в α_j . Построенный изоморфизм может быть продолжен до автоморфизма поля M . $\square$

Любой автоморфизм группы Галуа G для многочлена степени n над полем K с простыми корнями $\xi_1, \dots, \xi_n$ реализует перестановку этих корней и полностью ею определяется. Группа G оказывается изоморфной какой-то подгруппе в S_n . В духе естественного отождествления изоморфных групп часто полагают, что $G \leq S_n$.

Поле разложения данного многочлена состоит из чисел вида $A(\xi_1, \dots, \xi_n)$, где $A(x_1, \dots, x_n)$ — многочлен от переменных $x_1, \dots, x_n$ с коэффициентами из K . Рассмотрим множество всех алгебраических соотношений между корнями

$$\Phi := \{\phi(x_1, \dots, x_n) \in K[x_1, \dots, x_n] : \phi(\xi_1, \dots, \xi_n) = 0\}$$

и будем говорить, что A равно B по модулю Φ , если $A - B \in \Phi$. Мы получаем отношение эквивалентности, а числа $A(\xi_1, \dots, \xi_n)$ находятся во взаимно-однозначном соответствии с его классами эквивалентности. В группу G входят те и только те подстановки $g \in S_n$, которые сохраняют любое алгебраическое соотношение между корнями. Последнее означает, что если $\phi(x_1, \dots, x_n) \in \Phi$, то $\phi(x_{g(1)}, \dots, x_{g(n)}) \in \Phi$.

Задача 296. Приведите пример расширения полей $K \leq L \leq M$ и автоморфизма поля L , который не продолжается до автоморфизма поля M .

Задача 297. Приведите пример конечного нормального расширения, которое не является расширением Галуа.

7.4. Вычисление группы Галуа

Рассмотрим многочлен $f(x) = (x - \xi_1) \dots (x - \xi_n)$ и предположим, что его коэффициенты принадлежат полю K , а корни являются простыми. Будем считать, что $\xi_1, \dots, \xi_n \in M$, где M — поле разложения для $f(x)$ над K . Введем независимые переменные (буквы) $u_1, \dots, u_n$ и положим

$$\theta = \theta(\xi_1, \dots, \xi_n, u_1, \dots, u_n) := \xi_1 u_1 + \dots + \xi_n u_n \in M[u_1, \dots, u_n].$$

Пусть σ — произвольная подстановка степени n . Ее действие на θ определяется следующим образом:

$$\sigma\theta := \theta(\xi_{\sigma(1)}, \dots, \xi_{\sigma(n)}, u_1, \dots, u_n) = \xi_{\sigma(1)}u_1 + \dots + \xi_{\sigma(n)}u_n.$$

Рассмотрим многочлен

$$\Phi(x, u_1, \dots, u_n) := \prod_{\sigma \in S_n} (x - \sigma\theta)$$

и заметим, что его коэффициенты остаются на месте при любых перестановках корней $\xi_1, \dots, \xi_n$. Отсюда вытекает, что они получаются с помощью умножений и сложений из коэффициентов $f(x)$ и поэтому принадлежат полю K . Таким образом,

$$\Phi(x, u_1, \dots, u_n) \in K[x, u_1, \dots, u_n].$$

Пусть разложение многочлена $\Phi(x, u_1, \dots, u_n)$ на неприводимые множители над полем K имеет вид

$$\Phi(x, u_1, \dots, u_n) = \Phi_1(x, u_1, \dots, u_n) \dots \Phi_m(x, u_1, \dots, u_n).$$

Очевидно, что многочлены вида $x - \sigma\theta$ каким-то образом распределяются по множителям $\Phi_1, \dots, \Phi_m$. Будем считать, что $x - \theta$ входит в состав Φ_1 , т.е. многочлен Φ_1 делится на $x - \theta$. Тогда соответствующее ему подмножество подстановок, обозначим его через F , содержит единичную подстановку $e \in S_n$. Таким образом,

$$\Phi_1(x, u_1, \dots, u_n) = \prod_{\sigma \in F} (x - \sigma\theta), \quad e \in F.$$

Мы уже отмечали, что любой автоморфизм поля M над K однозначно определяется перестановкой корней $\xi_1, \dots, \xi_n$: если $g \in \mathcal{A}(M : K)$, то соответствующая подстановка σ задается правилом $g(\xi_i) = \xi_{\sigma(i)}$. Поэтому группу $\mathcal{A}(M : K)$ можно рассматривать как подгруппу симметрической группы S_n . Мы примем именно такую точку зрения и будем считать, что $\sigma \in \mathcal{A}(M : K)$. Любой автоморфизм $g \in \mathcal{A}(M : K)$ естественным образом порождает взаимно-однозначное и сохраняющее операции отображение на кольце многочленов над M : если $\Psi \in M[x, u_1, \dots, u_n]$, то $g\Psi$ определяется как многочлен от тех же переменных, в котором для каждого одночлена его коэффициент $a \in M$ переводится в $g(a)$.

Утверждение 7.4.1. Множество F является подгруппой в S_n и существуют подстановки $\sigma_1 = e, \sigma_2, \dots, \sigma_m$ такие, что

$$\Phi_i(x, u_1, \dots, u_n) = \prod_{\sigma \in \sigma_i F} (x - \sigma\theta) = \sigma_i \Phi_1(x, u_1, \dots, u_n),$$

$$1 \leq i \leq m.$$

Доказательство. Для любой подстановки τ многочлен $\tau\Phi_1$ получается из Φ_1 некоторой перестановкой переменных $u_1, \dots, u_n$ и поэтому остается неприводимым над K . Пусть $\tau \in F$. Поскольку $e \in F$, многочлен $\tau\Phi_1$ будет иметь множитель $x - \tau\theta$. Но этот же множитель есть в составе Φ_1 . В силу неприводимости получаем $\tau\Phi_1 = \Phi_1$. Ясно также, что если $\tau\Phi_1 = \Phi_1$, то $\tau \in F$. Таким образом,

$$F = \{\tau \in S_n : \tau\Phi_1 = \Phi_1\}.$$

То, что это группа, проверяется уже очевидным образом. Если многочлен Φ_i делится на $x - \sigma_i\theta$, то в силу неприводимости многочленов Φ_1 и Φ_i и условия $e \in F$ получаем $\sigma_i\Phi_1 = \Phi_i$. $\square$

Утверждение 7.4.2. Группа F совпадает с группой Галуа для многочлена $f(x)$ над полем K .

Доказательство. Пусть G — группа Галуа для расширения $K \leq M$. Если $g \in G$, то $g\Phi_1 = \Phi_1 \Rightarrow g \in F \Rightarrow G \leq F$. С другой стороны, многочлен Φ_1 можно рассматривать как неприводимый многочлен над полем $K' := K(u_1, \dots, u_n)$ рациональных функций от переменных $u_1, \dots, u_n$. Рациональная функция $\theta = \xi_1 u_1 + \dots + \xi_n u_n$ принадлежит полю $M' := K'(\xi_1, \dots, \xi_n)$, которое является полем разложения того же многочлена $f(x)$ над полем K' . Поэтому

$$|F| = \dim(K'(\theta) : K') \leq \dim(M' : K') = |\mathcal{A}(M' : K')|.$$

Заметим также, что $M' = K(\xi_1, \dots, \xi_n, u_1, \dots, u_n) = M(u_1, \dots, u_n)$. Значит, любой автоморфизм $g \in \mathcal{A}(M' : K')$ отображает элементы из M в элементы из M и потому может рассматриваться как отображение поля M в себя. Данное отображение является автоморфизмом поля M над полем K . Таким образом, $\mathcal{A}(M' : K') \leq \mathcal{A}(M : K) = G$. Отсюда $|F| \leq |G|$ и, поскольку $G \leq F$, получаем $G = F$. $\square$

Подгруппа подстановок, оставляющих на месте множитель $\Phi_i = \sigma_i\Phi_1$, имеет вид $\sigma_i F \sigma_i^{-1} \cong F$. Ее также можно рассматривать как группу Галуа многочлена $f(x)$, отвечающую другой

нумерации корней. Множители Φ_i иногда называют *резольвентами Галуа* многочлена $f(x)$.

Теорема 7.4.1 (ТЕОРЕМА ДЕДЕКИНДА). Пусть $f(x)$ — многочлен степени n с целыми коэффициентами, имеющий только простые корни, G — его группа Галуа над полем рациональных чисел. Пусть p — простое число и G_p — группа Галуа того же многочлена по модулю p над полем вычетов по модулю p . Тогда группа G_p изоморфна некоторой подгруппе группы G .

Доказательство. По заданному многочлену $f(x) \in \mathbb{Z}[x]$ построим многочлен Φ и его разложение на неприводимые над $\mathbb{Z}$ множители $\Phi_1, \dots, \Phi_m$. После этого рассмотрим $f(x)$ по модулю p как многочлен над $\mathbb{Z}_p$. Полагая, что элементы $\xi_1, \dots, \xi_n$ суть его корни в соответствующем поле разложения, построим по аналогии многочлен от $x, u_1, \dots, u_n$ с коэффициентами из $\mathbb{Z}_p$ и заметим, что этот многочлен есть прежний многочлен Φ по модулю p , а каждый из его неприводимых множителей над $\mathbb{Z}_p$ будет делителем какого-то из многочленов $\Phi_1, \dots, \Phi_m$ по модулю p . $\square$

Задача 298. Многочлен $f(x)$ над полем вычетов по простому модулю p разлагается на s неприводимых множителей степени $n_1, \dots, n_s$. Пусть группа Галуа G для $f(x)$ рассматривается как подгруппа симметрической группы степени $n = n_1 + \dots + n_s$. Докажите, что $G = \langle \sigma \rangle$, где подстановка σ есть произведение s независимых циклов, длины которых равны $n_1, \dots, n_s$.

Задача 299. Найдите группы Галуа для следующих многочленов над полем рациональных чисел: $f_1(x) = x^3 - 3x + 1$, $f_2(x) = x^3 + x + 1$, $f_3(x) = x^4 + x^2 + 1$.

Задача 300. Пусть K — бесконечное поле, G — произвольная подгруппа симметрической группы S_n . Докажите существование многочлена

$$f(x_1, \dots, x_n) \in K[x_1, \dots, x_n],$$

такого что равенство $f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = f(x_1, \dots, x_n)$ выполняется в том и только том случае, когда $\sigma \in G$.

Задача 301. Пусть K — поле нулевой характеристики, $f(x)$ — многочлен степени n над K , имеющий только простые корни, и $\Phi_i(x, u_1, \dots, u_n)$ — его резольвента Галуа. Докажите, что переменным $u_1, \dots, u_n$ можно придать такие целые значения, при которых Φ_i будет неприводимым многочленом кольца $K[x]$.

7.5. Теория Галуа

В теории Галуа устанавливается и изучается взаимно-однозначное соответствие между промежуточными полями расширения Галуа и подгруппами группы Галуа. Ее главные положения содержатся в следующих двух теоремах.

Теорема 7.5.1. Пусть M — конечное расширение поля K , $G = \mathcal{A}(M : K)$, $K = M^G$, $K \leq L \leq M$ и $H \leq G$. Тогда

$$L = M^H \Leftrightarrow H = \mathcal{A}(M : L).$$

Доказательство. Условие $K = M^G$ означает, что M — поле разложения некоторого сепарабельного многочлена $f(x) \in K[x]$. Тогда M является полем разложения того же $f(x)$ как многочлена над полем L . Поэтому расширение $L \leq M$ также является конечным расширением Галуа. Следовательно, если $H = \mathcal{A}(M : L)$, то $L = M^H$.

Если известно, что $L = M^H$, то L не может быть максимальным неподвижным полем ни для какой другой группы автоморфизмов поля M , кроме группы H . Поэтому $H = \mathcal{A}(M : L)$. $\square$

Следствие 7.5.1. Если $K \leq M$ — конечное расширение Галуа, то число промежуточных полей между K и M конечно.

Теорема 7.5.2. Пусть M — конечное расширение поля K , $G = \mathcal{A}(M : K)$, $K = M^G$, $K \leq L \leq M$, $H = \mathcal{A}(M : L)$, $F = \mathcal{A}(L : K)$. Тогда

$$H \trianglelefteq G \Leftrightarrow K = L^F \Rightarrow F \cong G/H.$$

Доказательство. Докажем, что нормальность подгруппы $H \leq G$ равносильна инвариантности поля L относительно автоморфизмов группы G . Последнее означает, что каждый автоморфизм из G переводит числа из L в какие-то числа из того же поля L . Для доказательства примем во внимание следующие соотношения:

$$H \trianglelefteq G \Leftrightarrow g^{-1}hg \in H \quad \forall g \in G, \forall h \in H;$$

$$a \in L \Leftrightarrow h(a) = a \quad \forall h \in H; \quad h \in H \Leftrightarrow h(a) = a \quad \forall a \in L.$$

Отсюда

$$H \trianglelefteq G \Leftrightarrow (g^{-1}hg)(a) = a \quad \forall a \in L, \forall g \in G, \forall h \in H \Leftrightarrow$$

$$\Leftrightarrow h(g(a)) = g(a) \quad \forall a \in L, \forall g \in G, \forall h \in H \Leftrightarrow$$

$$\Leftrightarrow g(a) \in L \quad \forall a \in L, \forall g \in G.$$

Теперь предположим, что $H \leq G$. Вследствие инвариантности L относительно группы G , автоморфизмы $g \in G$ можно рассматривать также как отображения из L в L . А именно, g индуцирует отображение $g_L: L \rightarrow L$, определенное правилом $g_L(a) := g(a)$ при $a \in L$. Легко проверяется, что g_L будет автоморфизмом поля L и отображение $\tau: g \rightarrow g_L$ будет гомоморфизмом группы G в группу F .

Найдем ядро гомоморфизма τ . При всех $a \in L$ имеем

$$(\tau(g))(a) = g_L(a) = g(a).$$

Равенство $g(a) = a$ выполняется для всех $a \in L$ в том и только том случае, когда $g \in H$. Поэтому ядром гомоморфизма τ является группа H . По теореме о гомоморфизмах

$$\tau(G) \cong G/H.$$

Таким образом, $\dim(L : K) \geq |F| \geq |G/H| = \dim(L : K)$. Группа $\tau(G)$ является подгруппой группы F , и при этом $|\tau(G)| = |G/H| = |F|$. Поэтому $F = \tau(G) \cong G/H$.

Далее, пусть $K = L^F$. Тогда любое число $a \in L$ является корнем неприводимого многочлена над K , все корни которого принадлежат L . Для любого автоморфизма $g \in G$ число $g(a)$ будет корнем того же многочлена и, следовательно, $g(a) \in L$. Тем самым мы доказали, что поле L инвариантно относительно группы G , что равносильно нормальности подгруппы H в группе G . $\square$

Задача 302. Докажите, что расширение $\mathbb{Q} \leq \mathbb{Q}(\sqrt{3} + \sqrt{5})$ является конечным расширением Галуа. Найдите все промежуточные поля между $\mathbb{Q}$ и $\mathbb{Q}(\sqrt{3} + \sqrt{5})$.

Задача 303. Найдите все промежуточные поля между $\mathbb{Q}$ и полем разложения многочлена $x^4 + 1 \in \mathbb{Q}[x]$.

Задача 304. Найдите число промежуточных полей между $\mathbb{Z}_3$ и полем разложения многочлена $x^8 - 1 \in \mathbb{Z}_3[x]$. Сколько из них будут нормальными над $\mathbb{Z}_3$?

Задача 305. Пусть $p_1 < \dots < p_n$ — последовательность простых чисел. Найдите порядок группы Галуа для многочлена $f(x) = (x^2 - p_1) \dots (x^2 - p_n) \in \mathbb{Q}[x]$.

7.6. Примитивные расширения

Алгебраическое расширение $K \leq M$ называется *примитивным*, если $M = K(\theta)$ для какого-то числа $\theta \in M$. Соответствующее число θ называется *примитивным элементом*.

Теорема 7.6.1. Пусть M — алгебраическое расширение поля K и число промежуточных полей между K и M конечно. Тогда расширение $M \geq K$ является примитивным.

Доказательство. Легко проверяется, что алгебраическое расширение с конечным числом промежуточных полей должно быть конечномерным. В случае конечного поля K поле M также конечно, при этом очевидно, что поля K и M имеют одну и ту же характеристику p . Как мы знаем, M получается из $\mathbb{Z}_p$ присоединением какого-то одного элемента ζ . Отсюда, конечно, следует, что $M = K(\zeta)$. Таким образом, теорема доказана для конечных полей.

Пусть поле K бесконечно, а M получается из K присоединением алгебраических чисел $\theta_1, \dots, \theta_s$. Рассмотрим поля $K(\theta_1 + a\theta_2)$ при $a \in K$. Согласно условию теоремы, число различных полей такого вида конечно. Поэтому

$$K(\theta_1 + a_1\theta_2) = K(\theta_1 + a_2\theta_2) \text{ для каких-то } a_1 \neq a_2.$$

Положим $\zeta := \theta_1 + a_1\theta_2$. Тогда $(a_1 - a_2)\theta_2 = (\theta_1 + a_1\theta_2) - (\theta_1 + a_2\theta_2) \in K(\zeta)$. Отсюда $\theta_2 \in K(\zeta) \Rightarrow \theta_1 \in K(\zeta) \Rightarrow K(\theta_1, \theta_2) \leq K(\zeta)$. Следовательно,

$$M = K(\zeta_2, \theta_3, \dots, \theta_s), \quad \text{где } \zeta_2 := \zeta.$$

Это первый шаг нашего построения. На втором шаге мы получим $K(\zeta_2, \theta_3) \leq K(\zeta_3)$ и $M = K(\zeta_3, \theta_4, \dots, \theta_s)$. На $(s-1)$ -м шаге мы найдем число ζ_s , для которого

$$M = K(\zeta_{s-1}, \theta_s) = K(\zeta_s). \quad \square$$

Следствие 7.6.1. Пусть поле M является примитивным расширением бесконечного поля K и получается из него присоединением алгебраических элементов $\theta_1, \dots, \theta_s$. Тогда существуют числа $a_2, \dots, a_s \in K$ такие, что

$$M = K(\zeta), \quad \zeta = \theta_1 + a_2\theta_2 + \dots + a_s\theta_s.$$

Следствие 7.6.2. Любое конечное расширение Галуа является примитивным.

Примитивность чрезвычайно упрощает изучение автоморфизмов поля над заданным полем. В самом деле, если $M = K(\zeta)$, то

$$\dim(M : K) = \deg f(x),$$

где $f(x) \in K[x]$ — минимальный многочлен для числа $\zeta \in M$. Ясно также, что число разных автоморфизмов поля M над K равно числу различных корней многочлена $f(x)$, которые принадлежат полю M . Таким образом, $|\mathcal{A}(M : K)| = \dim(M : K)$ тогда и только тогда, когда все корни неприводимого многочлена $f(x)$ являются простыми и принадлежат M .

Если все рассматриваемые расширения являются примитивными, то для теорем 7.2.1, 7.2.2 и 7.3.1 можно предложить другие, более простые доказательства. Как мы видим, теория Галуа имеет дело именно с такими ситуациями. Можно ли установить примитивность расширений, не опираясь на результаты этой теории? В случае конечных полей ответ очевиден: можно, так как вообще все конечные расширения конечного поля примитивны. Покажем, как это делается в случае полей нулевой характеристики.

Теорема 7.6.2. Пусть M — поле разложения многочлена над полем K нулевой характеристики. Тогда расширение $M \geq K$ является примитивным.

Доказательство. Пусть $\theta_1, \dots, \theta_s$ — корни заданного многочлена над K . Каждый из них является корнем некоторого неприводимого над K многочлена, все корни которого простые и принадлежат M . Пусть $\alpha := \theta_1$ и $\beta := \theta_2$ — корни многочленов $f(x)$ и $g(x)$ степеней m и n соответственно. Мы полагаем, что $f(x)$ и $g(x)$ имеют только простые корни, неприводимы над K , но над M справедливы разложения

$$f(x) = (x - \alpha_1) \dots (x - \alpha_m) \in K[x], \quad \alpha_1 = \alpha,$$

$$g(x) = (x - \beta_1) \dots (x - \beta_n) \in K[x], \quad \beta_1 = \beta.$$

Выберем число $0 \neq a \in K$ таким образом, что

$$\zeta := \alpha + a\beta \neq \alpha_i + a\beta_j \quad \text{при} \quad 2 \leq i \leq m, \quad 1 \leq j \leq n.$$

Это можно сделать, так как поле K бесконечно. Рассмотрим многочлен

$$h(x) := g\left(\frac{\zeta - x}{a}\right) \in K[\zeta].$$

Ясно, что $h(\alpha) = 0$ и $h(\alpha_i) \neq 0$ при $2 \leq i \leq m$. Таким образом, для многочленов $f(x)$ и $h(x)$ число α является единственным общим корнем. Следовательно, их наибольший общий делитель имеет вид $c(x - \alpha) \in K(\zeta)[x]$. Отсюда $\alpha \in K(\zeta)$, $\beta \in K(\zeta)$, и поэтому

$$K(\alpha, \beta) \leq K(\zeta).$$

Далее, по теореме 7.3.2, любое число из поля разложения M многочлена над K является корнем некоторого неприводимого многочлена, все корни которого принадлежат M . Над полем нулевой характеристики неприводимый многочлен имеет лишь простые корни. Теперь мы можем повторить рассуждение для пары $\zeta_2 := \zeta$ и θ_3 и найти число $\zeta_3 \in M$ такое, что $K(\zeta_2, \theta_3) \leq K(\zeta_3)$. Продолжая в том же духе, мы получим числа ζ_i такие, что

$$M = K(\zeta_{i-1}, \theta_i, \dots, \theta_s) = K(\zeta_i, \theta_{i+1}, \dots, \theta_s), \quad 2 \leq i \leq s-1.$$

На последнем шаге находим $M = K(\zeta_s)$. $\square$

Задача 306. Приведите пример конечного алгебраического расширения, которое не является примитивным.

Задача 307. Пусть $\mathbb{Q}(x)$ — поле рациональных функций от переменной x над полем рациональных чисел $\mathbb{Q}$. Покажите, что имеется бесконечно много промежуточных полей между $\mathbb{Q}$ и $\mathbb{Q}(x)$.

Задача 308. Пусть G — конечная группа автоморфизмов поля M . Докажите, что существует число $a \in M$, такое что числа $g(a)$ будут разными для разных автоморфизмов $g \in G$.

7.7. Циклические и радикальные расширения

Конечное расширение Галуа с циклической группой Галуа называется *циклическим*. Расширение $K \leq L$ называется *простым радикальным расширением*, если L является полем разложения многочлена $f(x) = x^p - a$, где $a \in K$ и p — простое число.

Если $a = 1$, то простое радикальное расширение будем называть *простым корневым расширением*. Число p будем называть *степенью* соответствующего расширения (при этом размерность расширения необязательно равна p).

Лемма 7.7.1. Пусть $\mathbb{Q} \leq K \leq \mathbb{C}$. Тогда простое корневое расширение степени p для поля K является циклическим.

Доказательство. Пусть ε — первообразный корень степени p из единицы. По условию число p простое, поэтому минимальный

многочлен для ε над $\mathbb{Q}$ имеет вид $1 + x + \dots + x^{p-1}$. Группа G всех автоморфизмов поля $\mathbb{Q}(\varepsilon)$ над $\mathbb{Q}$ состоит из отображений $g_1, \dots, g_{p-1}$, полностью определенных равенствами

$$g_i(\varepsilon) = \varepsilon^i, \quad 1 \leq i \leq p-1.$$

Отсюда $(g_i g_j)(\varepsilon) = \varepsilon^{ij}$, и поэтому $g_i g_j = g_k$, где k — остаток при делении числа ij на p . В силу цикличности мультипликативной группы поля вычетов по модулю p , существует натуральное число k такое, что числа

$$k, k^2, \dots, k^{p-1}$$

имеют разные ненулевые остатки при делении на p . Пусть $g := g_k$. Тогда

$$g(\varepsilon) = \varepsilon^k, \quad g^2(\varepsilon) = \varepsilon^{k^2}, \quad \dots, \quad g^{p-1}(\varepsilon) = \varepsilon^{k^{p-1}}.$$

Значит, порядок элемента g группы G равен $|G| = p-1$, поэтому G является циклической группой.

Теперь рассмотрим расширение $K \leq K(\varepsilon)$ и минимальный многочлен $\phi(x)$, получаемый для ε над полем K . Пусть

$$\phi(x) = (x - \varepsilon^{i_1}) \dots (x - \varepsilon^{i_s}) \in K[x], \quad \varepsilon = \varepsilon^{i_1}.$$

Аutomорфизмы группы $\mathcal{A}(K(\varepsilon) : K)$ определяются соответствиями

$$\varepsilon \rightarrow \varepsilon^{i_l}, \quad 1 \leq l \leq s.$$

Каждый из них ассоциируется с одним и только одним автоморфизмом группы $G = \mathcal{A}(\mathbb{Q}(\varepsilon) : \mathbb{Q})$, определяемым тем же соответствием. Построенное отображение группы $\mathcal{A}(K(\varepsilon) : K)$ в группу G сохраняет операции в рассматриваемых группах. Поэтому группа $\mathcal{A}(K(\varepsilon) : K)$ изоморфна некоторой подгруппе циклической группы G и потому является циклической. $\square$

Лемма 7.7.2. Пусть $\mathbb{Q} \leq K \leq L \leq \mathbb{C}$, p — простое число и поле K содержит все корни p -й степени из единицы. Тогда расширение $K \leq L$ является циклическим размерности p в том и только том случае, когда оно является простым радикальным расширением степени p .

Доказательство. Рассмотрим простое радикальное расширение $K \leq K(\theta)$, где $\theta^p = a \in K$. Если $a = b^p$ для какого-то числа $b \in K$, то θ получается из b умножением на некоторый корень степени p из единицы, т.е. на число из K , и поэтому $\theta \in K$. Это означает, что $K(\theta) = K$. Теперь предположим, что

$a \neq b^p$ при всех $b \in K$. Тогда многочлен $x^p - a$ неприводим над K . От противного, пусть

$$x^p - a = \phi(x)\psi(x), \quad 1 \leq \deg \phi(x) = k \leq p-1.$$

Свободный член $c_k \in K$ многочлена $\phi(x)$ имеет вид

$$c_k = (-1)^k \varepsilon^m \theta^k \in K, \quad m - \text{целое число} \Rightarrow c := \varepsilon^m \theta^k \in K.$$

Отсюда $c^p = a^k$. В силу взаимной простоты чисел k и p найдутся целые числа s и t такие, что $ks + pt = 1$. Находим

$$a = a^{ks} a^{pt} = c^{ps} a^{pt} = (c^s a^t)^p \Rightarrow b^p = a \text{ для } b := c^s a^t \in K.$$

Итак, нетривиальное расширение получается только в случае неприводимого над K многочлена $x^p - a$. Следовательно, группа $G = \mathcal{A}(K(\varepsilon) : K)$ содержит ровно p автоморфизмов и, в силу простоты p , является циклической. Заметим, что ее автоморфизмы $g_1, \dots, g_p$ однозначно определяются равенствами

$$g_i(\theta) = \varepsilon^i \theta, \quad 1 \leq i \leq p \Rightarrow (g_i g_j)(\theta) = \varepsilon^{i+j} \theta.$$

Теперь предположим, что группа Галуа расширения $K \leq L$ является циклической группой порядка p и порождается элементом g порядка p . Положим ¹⁾

$$\theta := 1 + \varepsilon g(a) + \varepsilon^2 g^2(a) + \dots + \varepsilon^{p-1} g^{p-1}(a).$$

Аutomорфизмы $g^0, g^1, \dots, g^{p-1}$ являются попарно различными и поэтому линейно независимы над L . Значит, $\theta \neq 0$ для какого-то числа $a \in L$. Зафиксируем именно такое число a . Далее,

$$g^k(\theta) = \varepsilon^{-k} \theta \Rightarrow g^k(\theta^p) = (g^k(\theta))^p = \theta^p \text{ для всех } 1 \leq k \leq p.$$

Мы видим, что число θ^p остается на месте при всех автоморфизмах группы Галуа для L над K . Следовательно, $\theta^p \in K$. $\square$

Задача 309. Докажите, что любое конечное расширение конечного поля является циклическим.

7.8. Полициклические расширения

Конечное расширение Галуа $K \leq M$ называется *полициклическим*, если M получается из K с помощью цепочки расширений

$$K = K_0 \leq K_1 \leq \dots \leq K_s = M,$$

¹⁾ Функция $\theta = \theta(g, a)$ называется *резольвентой Лагранжа*.

в которой каждое звено

$$K_{i-1} \leq K_i, \quad 1 \leq i \leq s,$$

является циклическим расширением. Подчеркнем, что полициклическое расширение является конечным расширением Галуа по определению.

Согласно теории Галуа, для группы $G = \mathcal{A}(M : K)$ существует цепочка подгрупп

$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_s = \{e\}, \quad (1)$$

в которой каждая фактор-группа G_i/G_{i-1} является циклической. Такая цепочка называется *полициклическим рядом* группы G , а сама группа G в этом случае называется *полициклической*.

Лемма 7.8.1. Пусть H — произвольная нормальная подгруппа полициклической группы G . Тогда фактор-группа G/H является полициклической.

Доказательство. Пусть группа G обладает полициклическим рядом (1) и H — нормальная подгруппа группы G . Рассмотрим гомоморфизм $\phi: G \rightarrow \hat{G} := G/H$, определенный правилом $\phi(g) := gH$, и порождаемую им цепочку

$$\hat{G} = \phi(G) = \phi(G_0) \supseteq \phi(G_1) \supseteq \dots \supseteq \phi(G_s) = \{e\}. \quad (2)$$

То, что группа $\phi(G_i)$ будет нормальной подгруппой в группе $\phi(G_{i-1})$, проверяется непосредственным образом: для любых элементов $g_i \in G_i$ и $g_{i-1} \in G_{i-1}$

$$\phi(g_i) \phi(g_{i-1}) \phi(g_i^{-1}) = \phi(g_i g_{i-1} g_i^{-1}) \in \phi(G_{i-1}).$$

Пусть $P := G_{i-1}$ и $Q := G_i$. Тогда ϕ можно рассматривать как гомоморфизм группы P на группу $\phi(P)$. На фактор-группе P/Q он индуцирует корректно определенное отображение

$$\bar{\phi}: gQ \rightarrow \phi(g)\phi(Q), \quad g \in P.$$

Проверка корректности:

$$\begin{aligned} g_1 Q = g_2 Q &\Rightarrow g_1^{-1} g_2 \in Q \Rightarrow \phi(g_1^{-1} g_2) \in \phi(Q) \Rightarrow \\ &\Rightarrow \phi(g_1) \phi(Q) = \phi(g_2) \phi(Q). \end{aligned}$$

Легко видеть, что

$$\begin{aligned}\bar{\phi}(g_1 Q \cdot g_2 Q) &= \phi(g_1 g_2) \phi(Q) = \phi(g_1) \phi(Q) \cdot \phi(g_2) \phi(Q) = \\ &= \bar{\phi}(g_1 Q) \cdot \bar{\phi}(g_2 Q).\end{aligned}$$

Таким образом, $\bar{\phi}$ сохраняет операцию и поэтому является гомоморфизмом группы P/Q на группу $\phi(P)/\phi(Q)$. Образ циклической группы при гомоморфизме будет также циклической группой. Поэтому каждая фактор-группа ряда (2) является циклической. Следовательно, группа $\phi(G) = G/H$ является полициклической. $\square$

Для дальнейшего нам понадобится понятие *полного прообраза* множества $B' \subseteq B$ при отображении $\phi: A \rightarrow B$. Так называется множество A' всех элементов из A , которые переходят в какой-либо элемент из B' . Обозначение: $\phi^{-1}(B) := A'$.

Лемма 7.8.2. *Если нормальная подгруппа H группы G и фактор-группа G/H представляют собой полициклические группы, то группа G является полициклической.*

Доказательство. Пусть $\hat{G} := G/H$ и даны два полициклических ряда:

$$\hat{G} = \hat{G}_0 \supseteq \hat{G}_1 \supseteq \dots \supseteq \hat{G}_s = \{e\},$$

$$H = H_0 \supseteq H_1 \supseteq \dots \supseteq H_t = \{e\},$$

и пусть $\phi: G \rightarrow \hat{G}$ — гомоморфизм, определенный правилом $\phi(g) = gH$. Тогда искомым полициклический ряд группы G имеет вид

$$\begin{aligned}G = \phi^{-1}(\hat{G}_0) \supseteq \phi^{-1}(\hat{G}_1) \supseteq \dots \supseteq \phi^{-1}(\hat{G}_s) = \\ = H = H_0 \supseteq H_1 \supseteq \dots \supseteq H_t = \{e\}.\end{aligned}$$

Нам нужно доказать цикличность фактор-группы вида P/Q , где

$$P := \phi^{-1}(\hat{G}_{i-1}), \quad Q := \phi^{-1}(\hat{G}_i).$$

Для этого будем рассматривать ϕ как гомоморфизм группы P на группу $\phi(P)$. Точно так же, как в доказательстве предыдущей леммы, введем индуцированный гомоморфизм

$$\bar{\phi}: P/Q \rightarrow \phi(P)/\phi(Q), \quad \bar{\phi}(gQ) := \phi(g)\phi(Q), \quad g \in P.$$

В данном случае подгруппа Q является полным прообразом подгруппы $\phi(Q)$ — как следствие, $\bar{\phi}$ оказывается *изоморфизмом*. Для доказательства вспомним, что элементы фактор-группы $\phi(P)/\phi(Q)$ — это смежные классы вида $\phi(g)\phi(Q)$, единицей является сама подгруппа $\phi(Q)$. Найдем прообразы единицы:

$$\begin{aligned}\bar{\phi}(gQ) = \phi(Q) &\Rightarrow \phi(g)\phi(Q) = \phi(Q) \\ \Rightarrow \phi(g) \in \phi(Q) &\Rightarrow g \in \phi^{-1}(\phi(Q)) = Q \Rightarrow gQ = Q.\end{aligned}$$

Следовательно, единственным прообразом единицы группы $\phi(P)/\phi(Q)$ является единица группы P/Q — среди смежных классов группы P по подгруппе Q это сама подгруппа Q . Непосредственно по определению $\phi(gQ) = \phi(g)\phi(Q)$, т. е. для каждого элемента из $\phi(P)/\phi(Q)$ имеется переходящий в него элемент из P/Q . Таким образом,

$$\phi^{-1}(\hat{G}_{i-1})/\phi^{-1}(\hat{G}_i) \cong \hat{G}_{i-1}/\hat{G}_i. \quad \square$$

Задача 310. Покажите, что при последовательном построении циклических расширений может возникнуть расширение, которое не является полициклическим.

Задача 311. Пусть $\varepsilon \in \mathbb{C}$ — первообразный корень степени p из единицы, p — простое число, L — поле разложения многочлена $f(x)$, неприводимого над полем $K \geq \mathbb{Q}$. Докажите, что если $\varepsilon \notin L$, то многочлен $f(x)$ неприводим над $K(\varepsilon)$.

7.9. Теорема Абеля–Галуа

Рассмотрим уравнение $f(x) = 0$, где $f(x) \in K[x]$ — многочлен степени $n \geq 1$. Такое уравнение называется *алгебраическим* или *полиномиальным* уравнением степени n над полем K . В данном разделе мы будем считать, что $K = \mathbb{Q}$.

Вопрос о разрешимости алгебраического уравнения в радикалах можно сформулировать таким образом. Поле разложения для $f(x)$ будем называть также полем разложения уравнения $f(x) = 0$ и будем говорить, что уравнение $f(x) = 0$ *разрешимо в радикалах*, если его поле разложения содержится в поле K_s , которое получается из K с помощью цепочки расширений

$$K = K_0 \leq K_1 \leq \dots \leq K_s,$$

в которой каждое звено $K_{i-1} \leq K_i$ является простым радикальным расширением.

В такой постановке применять теорию Галуа напрямую нельзя. Чтобы увидеть причину, рассмотрим цепочку $K_0 < K_1 < K_2$, в которой:

- K_0 — поле рациональных чисел,
- K_1 — поле разложения многочлена $x^2 - 2 \in K_0[x]$,
- K_2 — поле разложения многочлена $x^2 - \sqrt{2} \in K_1[x]$.

Каждое из расширений $K_0 < K_1$ и $K_1 < K_2$ является конечным расширением Галуа. Однако расширение $K_0 < K_2$ таковым не является! Число $\sqrt[4]{2}$ принадлежит K_2 и является корнем неприводимого над $\mathbb{Q}$ многочлена $x^4 - 2$. Если бы поле K_2 было конечным расширением Галуа над K_0 , то оно включало бы все корни данного многочлена. Вопреки этому, многочлен $x^4 - 2$ имеет также пару невещественных корней, которые не принадлежат K_2 .

Расширение $K_0 \leq K_s$ в общем случае не является расширением Галуа. Но это препятствие для применения теории Галуа легко устраняется.

Лемма 7.9.1. *Если поле L получается из K с помощью какой-то цепочки простых радикальных расширений, то существует конечное расширение Галуа $M \geq K$, которое содержит L и получается из K с помощью цепочки простых радикальных расширений.*

Доказательство. Будем вести индукцию по числу звеньев в исходной цепочке

$$K = K_0 \leq \dots \leq K_s = L.$$

Пусть уже построено конечное расширение Галуа $M' \geq K$, которое содержит поле K_{s-1} и получается из K с помощью цепочки простых радикальных расширений. Пусть K_s получается из K_{s-1} как поле разложения многочлена

$$x^p - a, \quad a \in K_{s-1} \leq M', \quad p - \text{простое число.}$$

Пусть $\phi(x)$ — минимальный многочлен, получаемый для a над полем K . Поле M' является нормальным над K , поэтому не только a , но и все остальные корни $\phi(x)$ принадлежат M' . Таким образом,

$$\phi(x) = (x - a_1) \dots (x - a_l) \in K[x], \quad a_1, \dots, a_l \in M', \quad a_1 = a.$$

Рассмотрим расширение $M' \leq M_1 \leq \dots \leq M_l$, где M_i — поле разложения многочлена $x^p - a_i$ над M_{i-1} , $1 \leq i \leq l$. Поле $M := M_l$

получается из M' с помощью цепочки простых радикальных расширений, и в то же время над полем M' оно является полем разложения многочлена

$$\phi(x^p) = (x^p - a_1) \dots (x^p - a_l) \in K[x] \subseteq M'[x].$$

Пусть M' является полем разложения многочлена $\psi(x) \in K[x]$. Тогда поле M будет полем разложения многочлена $\psi(x)\phi(x^p)$ над полем K . Очевидно также, что $L \leq M$. Поэтому расширение $M \geq K$ является искомым. $\square$

Лемма 7.9.2. *Если поле L получается из K с помощью какой-то цепочки простых радикальных расширений, то оно содержится в некотором полициклическом расширении M поля K .*

Доказательство. Достаточно заметить, что любое простое радикальное расширение $K' \leq K'''$, в котором K''' есть поле разложения многочлена $x^p - a$, можно получить в два приема: сначала строится расширение $K' \leq K''$, присоединяющее к K' все корни степени p из единицы, затем к полю K'' присоединяется корень многочлена $x^p - a$. Тогда каждое из расширений $K' \leq K''$ и $K'' \leq K'''$ будет циклическим. $\square$

Теорема 7.9.1. *Пусть задано алгебраическое уравнение над $\mathbb{Q}$. Для разрешимости в радикалах необходимо и достаточно, чтобы его поле разложения было полициклическим расширением поля $\mathbb{Q}$.*

Доказательство. Поле разложения данного уравнения обозначим через L . В случае разрешимости в радикалах поле L вложено в поле M , которое является полициклическим расширением поля $\mathbb{Q}$. Имеем $\mathbb{Q} \leq L \leq M$. Группа Галуа $G = \mathcal{A}(M : \mathbb{Q})$ является полициклической. Промежуточное поле L является конечным расширением поля $\mathbb{Q}$ (как поле разложения) и поэтому соответствующая ему подгруппа $H \leq G$ является нормальной. При этом $\mathcal{A}(L : \mathbb{Q}) \cong G/H$ и мы уже знаем, что фактор-группа G/H должна быть полициклической. Необходимость доказана.

Пусть G является группой Галуа для расширения $\mathbb{Q} = K \leq M$, где M — поле разложения заданного многочлена, и обладает полициклическим рядом

$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_s = \{e\}$$

с фактор-группами порядков $p_i := |G_i/G_{i-1}|$, где p_i равно 1 либо является простым числом. Пусть M' получается из M с помощью

цепочки простых корневых расширений, степени которых равны $p_1, \dots, p_s$. Согласно лемме 7.8.2, расширение $K \leq M'$ является полициклическим. Пусть K' — промежуточное поле между K и M' , полученное из K с помощью цепочки простых корневых расширений, имеющих степени $p_1, \dots, p_s$, и пусть $H \trianglelefteq G$ — подгруппа, соответствующая полю K' . Докажем, что расширение $K' \leq M'$ является полициклическим. Множества $H_i := G_i \cap H$ будут подгруппами, причем $H_{i-1} \supseteq H_i$ и довольно просто проверяется, что цепочка

$$H = H_0 \supseteq H_1 \supseteq \dots \supseteq H_s = \{e\}$$

будет полициклическим рядом для H .

Согласно лемме 7.7.2, циклическое расширение размерности p_i над любым полем, содержащим корни p_i -й степени из единицы, является простым радикальным расширением. Достаточность доказана. $\square$

Теорема 7.9.2 (ТЕОРЕМА АБЕЛЯ–ГАЛУА). *Среди алгебраических уравнений степени $n \geq 5$ над полем рациональных чисел существуют уравнения, которые нельзя разрешить в радикалах.*

Доказательство. Достаточно доказать неразрешимость в радикалах для какого-то одного алгебраического уравнения степени $n = 5$. Рассмотрим, например, уравнение

$$f(x) = x^5 - 4x + 2 = 0.$$

Многочлен $f(x)$ неприводим над $\mathbb{Q}$ по признаку Эйзенштейна. Перемены знака в последовательности значений

$$f(-2) = -20, \quad f(0) = 3, \quad f(1) = -1, \quad f(2) = 30$$

показывают, что $f(x)$ имеет три вещественных корня. Производная $f'(x) = 5x^4 - 4$ обнуляется только в двух вещественных точках: $\pm \sqrt[4]{4/5}$. Поэтому $f(x)$ не может иметь более трех вещественных корней. Таким образом, $f(x)$ имеет пару комплексно-сопряженных корней, обозначим их через x_1, x_2 ($x_1 \neq \bar{x}_2$), и три вещественных корня, обозначим их через x_3, x_4, x_5 .

Любой автоморфизм группы Галуа для многочлена $f(x)$ осуществляет перестановку корней x_1, x_2, x_3, x_4, x_5 и может рассматриваться как подстановка из симметрической группы степени 5. При этом автоморфизм $z \rightarrow \bar{z}$ (комплексное число переводится в комплексно-сопряженное число) переставляет корни x_1 и x_2

и оставляет корни x_3, x_4, x_5 на месте. Пусть G — группа Галуа данного многочлена. Мы полагаем, что $G \leq S_5$, и знаем, что G содержит транспозицию (12) . Отсюда можно вывести, что $G = S_5$.

Будем использовать то, что группа G действует транзитивно на корнях многочлена $f(x)$ (теорема 7.3.3). Корни помечены номерами 1, 2, 3, 4, 5, и каждый элемент $g \in G$ рассматривается как подстановка на множестве номеров $A := \{1, 2, 3, 4, 5\}$. Таким образом, для любых $i, j \in A$ существует подстановка g такая, что $g(i) = j$. Будем говорить, что номер i связан с номером j , если $i = j$ либо в G существует транспозиция (ij) . Легко проверяется, что это отношение связности номеров является отношением эквивалентности на A . Поэтому множество A разбивается на непересекающиеся классы связных между собой номеров. Рассмотрим класс связности $A(1)$ для номера 1. В нем заведомо есть номер 2. Предположим, что

$$A(1) = \{1, 2, \dots, k\} \quad \text{и} \quad l = k + 1 \neq A(1).$$

Пусть $m \in A(l)$, $i \in A(1)$. Тогда

$$\begin{pmatrix} 1 & i & i_3 & i_4 & i_5 \\ l & j & j_3 & j_4 & j_5 \end{pmatrix} (1i) \begin{pmatrix} l & j & j_3 & j_4 & j_5 \\ 1 & i & i_3 & i_4 & i_5 \end{pmatrix} = (lj).$$

Если $j \in A(1)$, то и $l \in A(1)$. Это противоречит нашему выбору l . Значит, для каждого номера $i \in A(1)$ должен найтись номер $j \in A(l)$, причем соответствие является взаимно однозначным. Следовательно, $|A(1)| = |A(l)|$, т.е. все классы связности имеют одно и то же число номеров. Это число обязано быть делителем общего числа номеров. Но у нас всего 5 номеров. Поэтому первоначальный выбор номера l невозможен. А это означает, что $k = 5$ и $A(1) = A$. Таким образом, группа G содержит все транспозиции и поэтому совпадает с S_5 .

Остается доказать, что группа S_5 не является полициклической. Пусть $H \triangleleft S_5$ и фактор-группа S_5/H является циклической. Тогда она заведомо является абелевой:

$$aH \cdot bH = bH \cdot aH \Rightarrow a^{-1}b^{-1}ab \in H \quad \forall a, b \in S_5.$$

Возьмем $a = (ij)$ и $b = (jk)$. Тогда

$$(ij)(jk)(ij)(jk) = (jik).$$

Таким образом, H содержит все тройные циклы. Отсюда легко вывести, что H содержит и все двучленные произведения незави-

симых транспозиций. В итоге оказывается, что $H = A_5$ (напомним, что A_5 — это стандартное обозначение для знакопеременной группы степени 5, т.е. для группы всех четных подстановок степени 5).

Далее, предположим, что $H \trianglelefteq A_5$ и фактор-группа A_5/H является циклической и, следовательно, абелевой. Очевидно, что $(ijk), (klm) \in A_5$. Поэтому

$$(kji)(mlk)(ijk)(klm) = (kjm).$$

Значит, H содержит все тройные циклы и по этой причине $H = A_5$. Следовательно, группа S_5 не обладает полициклическим рядом. $\square$

Задача 312. Пусть M — поле разложения многочлена $x^5 - 25x + 5$ над полем рациональных чисел $\mathbb{Q}$. Докажите, что $\dim(M : \mathbb{Q}) = 120$.

Задача 313. Пусть известно, что подгруппа $G \leq S_n$ действует на множестве номеров $A = \{1, 2, \dots, n\}$ транзитивно, содержит хотя бы одну транспозицию и хотя бы один цикл длины $n - 1$. Докажите, что $G = S_n$.

Задача 314. Пусть p — простое число. Докажите, что любая подгруппа группы S_p , действующая транзитивно на множестве номеров $A = \{1, 2, \dots, p\}$, содержит хотя бы один цикл длины p .

Задача 315. Найдите многочлен с целыми коэффициентами, степень которого равна 6, а группа Галуа над $\mathbb{Q}$ изоморфна S_6 .

Задача 316. Докажите, что уравнение $x^5 - x - 1 = 0$ неразрешимо в радикалах.

7.10. Казус Руффини

Теорема Абеля–Галуа исторически связана также с именем итальянского математика Руффини. Он первым объявил, что обладает ее доказательством. В действительности же он получил утверждение, которое опирается на неочевидное предположение и может рассматриваться только как некоторый шаг в доказательстве теоремы. Впрочем, судите сами — вот в точности то, что удалось доказать Руффини.

Пусть нас интересуют корни многочлена

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 = (x - x_1) \dots (x - x_n).$$

Пусть K — некоторое расширение поля $\mathbb{Q}$, которое мы скоро определим удобным для нас образом. В качестве основного поля, которому принадлежат коэффициенты $f(x)$, рассмотрим поле рациональных функций от элементарных симметрических многочленов от независимых переменных (букв) $x_1, \dots, x_n$ над полем K . Обозначим это поле через L . В силу формул Виета,

$$L = K(a_0, \dots, a_{n-1}) \subset K(x_1, \dots, x_n).$$

Поле $M = K(x_1, \dots, x_n)$ является, очевидно, полем разложения многочлена $f(x)$.

Разрешимость в радикалах предполагает, что корни многочлена $f(x)$, и в частности x_1 , могут быть выражены через его коэффициенты с помощью *радикалов* $\theta_1, \dots, \theta_s$, т.е. величин, удовлетворяющих следующим уравнениям:

$$\theta_1^{p_1} = \phi_1(a_0, \dots, a_{n-1}),$$

$$\theta_2^{p_2} = \phi_2(a_0, \dots, a_{n-1}, \theta_1), \dots, \theta_s^{p_s} = \phi_s(a_0, \dots, a_{n-1}, \theta_1, \dots, \theta_{s-1}),$$

$$x_1 = \phi_{s+1}(a_0, \dots, a_{n-1}, \theta_1, \dots, \theta_s).$$

Предполагается, что $\phi_1, \dots, \phi_{s+1}$ — рациональные функции от своих аргументов. Не ограничивая общности, будем считать, что $p_1, \dots, p_s$ — простые числа, а в качестве K выберем поле, полученное из $\mathbb{Q}$ присоединением всех комплексных корней из единицы степеней $p_1, \dots, p_s$.

Теорема 7.10.1 (Руффини). *Если $\theta_1, \dots, \theta_s \in M$, то $n \leq 4$.*

Доказательство. От противного, пусть $n \geq 5$. Каждая подстановка $\sigma \in S_n$ определяет отображение

$$h(x_1, \dots, x_n) \rightarrow \sigma h(x_1, \dots, x_n) := h(x_{\sigma(1)}, \dots, x_{\sigma(n)}), \quad h, \sigma h \in M.$$

Очевидно, ϕ_1 является симметрической функцией от $x_1, \dots, x_n$ и поэтому $\sigma \phi_1 = \phi_1$ для любой подстановки $\sigma \in S_n$. Введем в рассмотрение два тройных цикла:

$$\sigma_1 = (1, 2, 3), \quad \sigma_2 = (3, 4, 5),$$

и для каждого $1 \leq i \leq s$ докажем следующее:

$$\sigma_1 \phi_i = \phi_i, \quad \sigma_2 \phi_i = \phi_i \Rightarrow \sigma_1 \phi_{i+1} = \phi_{i+1}, \quad \sigma_2 \phi_{i+1} = \phi_{i+1}.$$

В самом деле,

$$\sigma_1 \theta_i^{p_i} = (\sigma_1 \theta_i)^{p_i} = \sigma_1 \phi_i = \phi_i \Rightarrow \sigma_1 \theta_i = \varepsilon_1 \theta_i, \quad \varepsilon_1 \in \mathbb{C}, \quad \varepsilon_1^{p_i} = 1,$$

$$\sigma_2 \theta_i^{p_i} = (\sigma_2 \theta_i)^{p_i} = \sigma_2 \phi_i = \phi_i \Rightarrow \sigma_2 \theta_i = \varepsilon_2 \theta_i, \quad \varepsilon_2 \in \mathbb{C}, \quad \varepsilon_2^{p_i} = 1.$$

Далее, $\theta_i = \sigma_1^3 \theta_i = \varepsilon_1^3 \theta_i \Rightarrow \varepsilon_1^3 = 1$. Аналогично, $\varepsilon_2^3 = 1$. Произведение $\sigma_1 \sigma_2$ представляет собой цикл длины 5. Поэтому $(\varepsilon_1 \varepsilon_2)^5 = 1 \Rightarrow \varepsilon_1 \varepsilon_2 = 1$. Кроме того, произведение $\sigma_1 \sigma_2 \sigma_1$ — это также цикл длины 5 $\Rightarrow 1 = \varepsilon_1^{10} \varepsilon_2^5 = \varepsilon_1 \varepsilon_2^5 \Rightarrow \varepsilon_1 = \varepsilon_2 = 1$. В итоге равенство $\sigma_1 f_{s+1} = f_{s+1}$ приводит к очевидному противоречию $x_1 = \sigma_1 x_1 = x_2$. $\square$

Заметим, что простота чисел $p_1, \dots, p_s$ пока не использовалась.

Чтобы превратить результат Руффини в полноценное доказательство неразрешимости в радикалах в случае $n \geq 5$, нужно обосновать предположение о том, что $\theta_1, \dots, \theta_s \in M$. Впервые это смог сделать Абель. Мы можем здесь опереться на уже изученные нами свойства нормальных расширений.

Теорема 7.10.2. Пусть M — поле разложения некоторого многочлена над полем L , которое содержит все рациональные числа и все корни из единицы простых степеней $p_1, \dots, p_s$. Предположим, что $\xi_1^{p_1} \in L$, $\xi_i^{p_i} \in L(\xi_1, \dots, \xi_{i-1})$, $2 \leq i \leq s$, и пусть $\alpha \in L(\xi_1, \dots, \xi_s) \cap M$. Тогда существуют величины $\theta_1, \dots, \theta_s \in M$ такие, что $\alpha \in L(\theta_1, \dots, \theta_s)$ и $\theta_1^{p_1} \in L$, $\theta_i^{p_i} \in L(\theta_1, \dots, \theta_{i-1})$, $2 \leq i \leq s$.

Доказательство. Пусть p — простое число, L содержит все корни из единицы степени p и $\xi^p = a \in M'$, где M' — некоторое конечное расширение поля L . Пусть $\alpha \in M'(\xi) \cap M$. Тогда

$$\alpha = a_0 + a_1 \xi + \dots + a_{p-1} \xi^{p-1}, \quad a_0, \dots, a_{p-1} \in M'.$$

Если $\alpha \notin M'$, то хотя бы один из коэффициентов $a_1, \dots, a_{p-1}$ отличен от нуля, пусть это будет a_l . Положим $\theta := a_l \xi^l$. Числа l и p взаимно просты $\Rightarrow lu + pv = 1$ для некоторых целых чисел u и $v \Rightarrow \xi = a_l^{-u} \theta^u$. Заметим также, что множество величин $\theta^u, (\theta^u)^2, \dots, (\theta^u)^{p-1}$ совпадает с множеством величин $\theta, \theta^2, \dots, \theta^{p-1}$. Поэтому α можно записать в виде

$$\alpha = b_0 + \theta + b_2 \theta^2 + \dots + b_{p-1} \theta^{p-1}, \quad b_0, b_2, \dots, b_{p-1} \in M'.$$

Теперь докажем, что $\theta \in M$.

Пусть $g(x)$ — минимальный многочлен для α над полем L . Поскольку поле M нормально над L , не только α , но и каждый из остальных корней многочлена $g(x)$ принадлежит M . Обозначим через ε первообразный корень p -й степени из единицы и докажем, что $\alpha_i := b_0 + \theta\varepsilon^i + b_2(\theta\varepsilon^i)^2 + \dots + b_{p-1}(\theta\varepsilon^i)^{p-1}$ также является корнем $g(x)$. Легко видеть, что $g(\alpha_i)$ можно записать в виде

$$g(\alpha_i) = c_0 + c_1(\theta\varepsilon^i) + \dots + c_{p-1}(\theta\varepsilon^i)^{p-1}, \quad c_0, \dots, c_{p-1} \in M'.$$

Многочлены $G(x) := c_0 + c_1x + \dots + c_{p-1}x^{p-1} \in M'[x]$ и $x^p - a \in M'[x]$ имеют общий корень α , но второй из них неприводим над $M' \Rightarrow G(x) = 0$. Далее,

$$\begin{aligned} \alpha_i\varepsilon^{-i} &= b_0\varepsilon^{-i} + \theta + b_1\theta^2\varepsilon^i + \dots + b_{p-1}\theta^{p-1}\varepsilon^{i(p-2)} \in M \Rightarrow \\ &\Rightarrow \theta = \frac{1}{p} \sum_{i=0}^{p-1} \alpha_i\varepsilon^{-i} \in M. \end{aligned}$$

Взяв $M' = L(\xi_1, \dots, \xi_{s-1})$ и $\xi = \xi_s$, находим $\alpha \in L(\xi_1, \dots, \xi_{s-1}, \theta_s)$, $\theta_s = \theta \in M$. Теперь положим $M' := L(\xi_1, \dots, \xi_{s-2})$, $\xi := \xi_{s-1}$, $\alpha := \theta_s^{p_s} \in M \cap L(\xi_1, \dots, \xi_{s-1})$. Получаем $\theta_s^{p_s} \in L(\xi_1, \dots, \xi_{s-2}, \theta_{s-1})$, $\theta_{s-1} \in M$, $\theta_s^{p_{s-1}} \in M \cap L(\xi_1, \dots, \xi_{s-2})$. И так далее. $\square$

Задача 317. Докажите, что если группа Галуа неприводимого над $\mathbb{Q}$ многочлена $f(x)$ простой степени p состоит из подстановок вида $\sigma(i) = a_\sigma i + b_\sigma \pmod{p}$, где a_σ не делится на p , то уравнение $f(x) = 0$ разрешимо в радикалах¹⁾.

7.11. Концептуальный вывод основной теоремы алгебры

Концептуальное, «наиболее алгебраическое» доказательство основной теоремы алгебры опирается на теорию Галуа и следующую теорему Силова: в любой группе порядка $n = p^s t$, где $p \nmid t$ — простое число, существует подгруппа порядка p^s .

¹⁾ Обратное тоже верно, но доказывается труднее. Несложно заметить, что никакая подстановка такого вида, отличная от единичной, не может иметь более одной неподвижной точки. В итоге отсюда получается обнаруженное Абелем и Галуа нетривиальное утверждение: неприводимое над $\mathbb{Q}$ уравнение простой степени разрешимо в радикалах в том и только том случае, когда в каждой тройке корней любой корень рационально выражается через два остальных.

Случай комплексного многочлена $f(x) = a_0 + a_1x + \dots + a_nx^n$ элементарным образом сводится к проблеме существования комплексного корня для вещественного многочлена

$$f(x)\bar{f}(x) := (a_0 + a_1x + \dots + a_nx^n)(\bar{a}_0 + \bar{a}_1x + \dots + \bar{a}_nx^n) \in \mathbb{R}[x],$$

$$f(\zeta)\bar{f}(\zeta) = 0 \Rightarrow f(\zeta) = 0 \quad \text{или} \quad \bar{f}(\zeta) = 0 \quad (\Rightarrow f(\bar{\zeta}) = 0).$$

Чтобы доказать, что вещественный многочлен степени $n \geq 1$ имеет комплексный корень, рассмотрим его поле разложения M над $\mathbb{R}$ и группу Галуа $G = \mathcal{A}(M : \mathbb{R})$. Предположим, что $\dim(M : \mathbb{R}) = 2^s m$, где m — нечетное число. По теореме Силова, существует подгруппа $H \leq G$ порядка 2^s . Согласно теории Галуа, подгруппе H соответствует промежуточное поле $L = M^H$ размерности $\dim(L : \mathbb{R}) = m$. Поле L является расширением поля $\mathbb{R}$ нечетной размерности. Если $m > 1$, то должен найтись неприводимый вещественный многочлен нечетной степени, что невозможно. Поэтому $m = 1$ и $L = \mathbb{R}$. Вот главный вывод из нашего рассуждения: $\dim(M : \mathbb{R}) = 2^s$. Чтобы продолжить, нам нужно следующее утверждение, которое мы применим в частном случае, когда $p = 2$.

Лемма 7.11.1. *Для любого простого числа p любая группа порядка p^s обладает полициклическим рядом, в котором каждая фактор-группа имеет порядок p .*

Доказательство. Проведем индукцию по s . При $s = 1$ группа является циклической, а значит и полициклической. Пусть $s \geq 2$. Согласно теореме 2.9.1, в данной группе, обозначим ее G , имеется элемент a , коммутирующий со всеми элементами этой группы. Пусть H — подгруппа порядка p в циклической группе $\langle a \rangle$, порожденной элементом a . Очевидно, что H является нормальной подгруппой в G . Порядок фактор-группы $F := G/H$ равен $p^{s-1} < p^s$, по индуктивному предположению она является полициклической: $F = F_0 \triangleright F_1 \triangleright \dots \triangleright F_{s-1} = \{e\}$, $|F_i/F_{i-1}| = p$, $1 \leq i \leq s-1$. Рассмотрим гомоморфизм $\phi: G \rightarrow F$, определенный правилом $\phi(g) := gH$. Легко проверяется, что для любой подгруппы $T \leq F$ ее полный прообраз $\phi^{-1}(T)$ будет подгруппой в G . Полный прообраз нормальной подгруппы будет также нормальной подгруппой. В цепочке подгрупп $G = \phi^{-1}(F_0) \triangleright \phi^{-1}(F_1) \triangleright \dots \triangleright \phi^{-1}(F_{s-1}) \triangleright \{e\}$ каждая фактор-группа имеет порядок p . $\square$

Из данной леммы следует, что поле M может быть получено из $\mathbb{R}$ с помощью присоединения корней квадратных уравнений.

Все эти корни принадлежат $\mathbb{C}$, поэтому $M \leq \mathbb{C}$. Еще одно следствие доказанной выше леммы связано с построением правильных p -угольников.

Утверждение 7.11.1. Пусть p — простое число. Тогда условие $p = 2^s + 1$ для натурального числа s является достаточным для возможности построения правильного p -угольника с помощью циркуля и линейки.

Доказательство. В рассматриваемом случае число $\cos(2\pi/p)$ принадлежит некоторому полициклическому расширению поля $\mathbb{Q}$, в котором каждое звено есть расширение размерности 2. Значит, очередное поле получается из предыдущего с помощью присоединения корня квадратного уравнения. Именно такие построения выполняются с помощью циркуля и линейки. $\square$

Задача 318. Пусть $K = \mathbb{Q}$, расширения $K \leq L$ и $L \leq M$ являются полициклическими и известно, что расширение $K \leq M$ является конечным расширением Галуа. Докажите, что оно будет полициклическим.

7.12. Теорема Силова

Для полноты картины докажем теорему Силова, которая включает утверждение из предыдущего раздела, а также и другие наблюдения о группах с числом элементов, равным простому числу p в некоторой степени. Такие группы называются *примарными* или *p -группами*.

Начнем с частного случая. Рассмотрим группу $M_n(p)$ обратимых матриц порядка n над полем вычетов по модулю p и ее подгруппу $T_n(p)$, состоящую из верхних треугольных матриц с единичной главной диагональю. Нетрудно подсчитать, что

$$|M_n(p)| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1}) = p^d q,$$

$$|T_n(p)| = p^d, \quad d = (n-1)n/2, \quad p \nmid q.$$

Таким образом, в группе $M_n(p)$ порядка $p^d q$ имеется подгруппа $T_n(p)$ порядка p^d . Заметим, что $T_n(p)$ является p -подгруппой максимально возможного порядка среди всех p -подгрупп группы $M_n(p)$. Существование таких подгрупп в общем случае — это первое из утверждений теоремы Силова.

Нам понадобится следующая лемма о разбиении группы на непересекающиеся подмножества — некоторый аналог разбиения на смежные классы по подгруппе.

Лемма 7.12.1. Для любых подгрупп B и C конечной группы A существуют элементы $a_1, \dots, a_l \in A$, такие что имеет место равенство

$$\sum_{i=1}^l \frac{|C|}{|C \cap a_i B a_i^{-1}|} = \frac{|A|}{|B|}. \quad (*)$$

Доказательство. Прежде всего заметим, что множества $Ca_i B$ для различных элементов $a \in A$ либо совпадают, либо не пересекаются. Пусть различных множеств такого вида всего l и они определяются элементами $a_1, \dots, a_l \in A$. Тогда

$$\sum_{i=1}^l |Ca_i B| = |A|.$$

При каждом i множество $Ca_i B$ представляет собой объединение каких-то непересекающихся левых смежных классов по подгруппе B . Равенство $c_1 a_i B = c_2 a_i B$ равносильно равенству $c_1 (a_i B a_i^{-1}) = c_2 (a_i B a_i^{-1})$ и выполняется в том и только том случае, когда

$$c_1^{-1} c_2 \in C \cap a_i B a_i^{-1}.$$

Следовательно,

$$|Ca_i B| = \frac{|C|}{|C \cap a_i B a_i^{-1}|} |B|. \quad \square$$

Теорема 7.12.1 (ТЕОРЕМА СИЛОВА). Пусть p — простое число и t взаимно просто с p . Тогда для любой группы порядка $n = p^s t$ справедливы следующие утверждения:

- 1) Существует подгруппа порядка p^s .
- 2) Все подгруппы порядка p^s являются сопряженными.
- 3) Каждая p -подгруппа содержится в какой-то подгруппе порядка p^s .
- 4) Число разных подгрупп порядка p^s является делителем числа t и имеет остаток 1 при делении на p .

Доказательство. Пусть G — произвольная группа порядка $p^s t$, $p \nmid t$ — простое число. Заметим, что произвольную группу порядка n , в том числе G , можно рассматривать как подгруппу группы $M_n(p)$, составленную из каких-то матриц перестановок.

1. Пусть $A := M_n(p)$, $B := T_n(p)$ и $C := G$. Правая часть формулы (*) на p не делится, поэтому хотя бы одно из слагаемых

левой части на p не делится. Пусть это i -е слагаемое. Тогда искомая подгруппа есть $C \cap a_i B a_i^{-1}$.

2. Применим ту же формулу (*) в другой ситуации. Пусть $A := G$ — данная группа, а C и B — ее подгруппы порядка p^s . Правая часть формулы (*) на p не делится, поэтому хотя бы одно слагаемое левой части на p не делится. Если это i -е слагаемое, то

$$C = a_i B a_i^{-1}.$$

3. Пусть $A := G$ — данная группа, B — ее подгруппа порядка p^s и C — какая-то p -подгруппа. Тогда в левой части формулы (*) должно быть слагаемое, которое на p не делится. Если это i -е слагаемое, то

$$C \cap a_i B a_i^{-1} = C \Rightarrow C \subseteq a_i B a_i^{-1}.$$

4. Пусть $A := G$ — данная группа и B — ее подгруппа порядка p^s . Исследуем условие совпадения двух сопряженных подгрупп:

$$a_1 B a_1^{-1} = a_2 B a_2^{-1} \Leftrightarrow a_1^{-1} a_2 B (a_1^{-1} a_2)^{-1} = B \Leftrightarrow a_1^{-1} a_2 \in N(B),$$

где $N(B) = \{a \in A: a B a^{-1} \subseteq B\}$ — нормализатор подгруппы B . Легко проверяется, что нормализатор подгруппы $B \leq A$ является подгруппой в A . Пусть число смежных классов группы A по подгруппе $N(B)$ равно t . Ровно столько имеется разных подгрупп, сопряженных с подгруппой B . Поскольку $|N(B)| \geq |B|$, число t должно быть делителем числа m .

Теперь рассмотрим множество сопряженных подгрупп

$$X := \{x_1, \dots, x_t\}, \quad x_i := a_i B a_i^{-1}, \quad 1 \leq i \leq t,$$

и действие группы B на X сопряжением:

$$b: x_i \rightarrow b x_i b^{-1} = b (a_i B a_i^{-1}) b^{-1}, \quad b \in B.$$

Каждый элемент $x_i \in X$ порождает свою орбиту $B(x_i) := \{b(x_i): b \in B\}$, при этом орбиты разных элементов либо совпадают, либо не пересекаются. Таким образом, все множество X представляет собой объединение непересекающихся орбит. Длина каждой орбиты должна быть делителем порядка группы B , поэтому каждая длина либо делится на простое число p , либо равна 1.

Докажем, что на множестве X имеется ровно одна орбита длины 1 — это и будет означать, что остаток числа t при делении на p равен 1. Допустим, что имеются две подгруппы,

каждая из которых сопряжена только с собой. Пусть это подгруппы B и aBa^{-1} . В этом случае множество $BaBa^{-1}$ оказывается подгруппой. Для проверки запишем произвольные элементы $u, v \in BaBa^{-1}$ в виде

$$u = b_1ab_2a^{-1}, \quad v = b_3ab_4a^{-1}, \quad b_1, b_2, b_3, b_4 \in B.$$

Тогда для некоторых элементов $b_5, b_6, b_7, b_8 \in B$ получаем

$$\begin{aligned} uv &= (b_1b_3)(b_3^{-1}ab_2a^{-1}b_3)(ab_4a^{-1}) = (b_1b_3)(b_5ab_6a^{-1})(ab_4a^{-1}) = \\ &= (b_1b_3b_5)a(b_6b_4)a^{-1} \in BaBa^{-1}, \\ u^{-1} &= ab_2^{-1}a^{-1}b_1^{-1} = b_1^{-1}(b_1ab_2a^{-1}b_1^{-1}) = b_1(b_7ab_8a^{-1}) = \\ &= (b_1b_7)ab_8a^{-1} \in BaBa^{-1}. \end{aligned}$$

Далее, $|BaBa^{-1}| = |B||aBa^{-1}|/|B \cap aBa^{-1}|$. Если $B \neq aBa^{-1}$, то мы получаем подгруппу, порядок которой делится на p^{s+1} , что невозможно. $\square$

Задача 319. Докажите, что любая группа порядка pq , где p и q — разные простые числа, является полициклической.

Задача 320. В конечной группе имеется элемент, коммутирующий только сам с собой и с единицей. Докажите, что порядок группы не делится на 4.

Глава 8

КОЛЬЦА И ИДЕАЛЫ

8.1. Идеалы и вычеты

Множество $R \subseteq K$ называется (двусторонним) *идеалом* кольца K , если вместе с любыми двумя элементами оно содержит их противоположные элементы и сумму, а также обладает *свойством поглощения*:

$$a \in K, b \in R \Rightarrow ab, ba \in R.$$

Само кольцо K и множество $\{0\}$ очевидно являются идеалами. Они называются *тривиальными идеалами*. Идеал $\{0\}$ называется *нулевым идеалом*. Идеал, отличный от K , называется *собственным*. Запись $R \leq K$ означает, что R является идеалом кольца K .

Подобно пересечению и сумме подпространств, из уже имеющих идеалов A_i можно получать их теоретико-множественное *пересечение* и *сумму*

$$A_1 + \dots + A_s := \{a_1 + \dots + a_s : a_1 \in A_1, \dots, a_s \in A_s\}.$$

Утверждение 8.1.1. *Пересечение любого семейства идеалов и сумма любого конечного числа идеалов также являются идеалами.*

Пересечение всех идеалов, содержащих непустое подмножество $G \subseteq K$, обозначается через $\langle G \rangle$ и называется идеалом, *порожденным* элементами множества G . Среди всех идеалов, содержащих G , этот идеал *минимален* в том смысле, что любой строго меньший идеал не содержит хотя бы один элемент из G .

Утверждение 8.1.2. *Если K — коммутативное ассоциативное кольцо с единицей, то идеал $\langle G \rangle$ состоит из элементов вида $f_1 g_1 + \dots + f_s g_s$, где $g_1, \dots, g_s$ — произвольные*

элементы из G , $f_1, \dots, f_s$ — произвольные элементы из K , s — произвольное натуральное число.

Произведением идеалов A и B называется идеал C , порожденный всеми элементами вида ab , где $a \in A$ и $b \in B$. Обозначение: $C = AB$. Легко видеть, что $AB \subseteq A \cap B$. Частным идеалов A и B называется множество $A : B := \{x \in K : \langle x \rangle B \subseteq A\}$. Тривиально проверяется, что частное является идеалом. Если идеал B порождается одним элементом $b \in B$, то вместо $A : \langle b \rangle$ принято писать $A : b$.

В определенном смысле роль идеалов в теории колец родственна роли нормальных подгрупп в теории групп. Пусть a — произвольный элемент из K . Множество вида

$$a + R = \{a + r : r \in R\}$$

называется *вычетом* кольца K по идеалу R . Обозначение: $a + R = [a] = [a]_R$. Ясно, что

$$[a] = [b] \Leftrightarrow a - b \in R.$$

Операции сложения и умножения вводятся в полной аналогии с такими операциями для уже знакомых нам вычетов в кольце целых чисел или в кольце многочленов:

$$[a] + [b] := [a + b], \quad [a][b] := [ab].$$

Корректность сложения проверяется очевидным образом:

$$[a] = [f], [b] = [g] \Rightarrow a - f, b - g \in R \Rightarrow$$

$$(a + b) - (f + g) = (a - f) + (b - g) \in R \Rightarrow [a + b] = [f + g].$$

Для операции умножения доказательство корректности существенно опирается на свойство поглощения идеала R :

$$a - f, b - g \in R \Rightarrow a(b - g), (a - f)g \in R \Rightarrow$$

$$ab - fg = a(b - g) + (a - f)g \in R \Rightarrow [ab] = [fg].$$

Дистрибутивность умножения вычетов относительно сложения вытекает сразу же из дистрибутивности в кольце K . Таким образом, множество вычетов является кольцом относительно сложения и умножения вычетов. Это кольцо называется *кольцом вычетов* или *фактор-кольцом* кольца K по идеалу R . Обозначение: K/R .

В полной аналогии с группами и полями, чтобы отождествлять формально разные кольца K и $\hat{K}$, вводится понятие изоморфизма. Взаимно однозначное отображение $h: K \rightarrow \hat{K}$ называется *изоморфизмом*, если оно сохраняет операции: $h(a + b) = h(a) + h(b)$ и $h(ab) = h(a)h(b)$ для любых элементов $a, b \in K$. Если операции сохраняются без условия взаимной однозначности, то отображение называется *гомоморфизмом*.

Теорема 8.1.1. Для любого гомоморфизма h кольца K в кольцо $\hat{K}$ его ядро $\ker h$ (все элементы из K , отображаемые в нуль кольца $\hat{K}$) является идеалом в K , а образ $h(K) = \operatorname{im} h$ (все элементы из $\hat{K}$ вида $h(a)$, $a \in K$) — это кольцо относительно операций в кольце $\hat{K}$, изоморфное кольцу вычетов $K/\ker h$.

Доказательство проводится по аналогии с теоремой о гомоморфизме групп.

Пример 1. Четные числа образуют идеал $R = 2\mathbb{Z}$ в кольце целых чисел $K = \mathbb{Z}$. Фактор-кольцо K/R изоморфно кольцу $\mathbb{Z}_2$.

Пример 2. Пусть K — кольцо вещественных функций на отрезке $[0, 1]$ относительно операций сложения и умножения функций, R — подмножество функций, равных нулю на отрезке $[1/3, 2/3]$. Фактор-кольцо K/R изоморфно кольцу вещественных функций с областью определения, равной отрезку $[1/3, 2/3]$.

Подобно расширениям полей, нас будут интересовать также и расширения колец. Кольцо K называется *подкольцом* кольца L , если его аддитивная группа является подгруппой аддитивной группы кольца L , а операция умножения является замкнутой на K , т. е. произведения любых элементов из K принадлежат K . Если K содержит единицу, то обычно рассматривают подкольца, которые также содержат единицу.

Задача 321. Пусть K — множество вещественных верхних треугольных матриц порядка $n \geq 2$ с операциями сложения и умножения матриц, R — подмножество верхних треугольных матриц с нулевой главной диагональю. Докажите, что K — некоммутативное ассоциативное кольцо с единицей, R — его идеал, а фактор-кольцо K/R изоморфно кольцу диагональных матриц порядка n .

Задача 322. Кольцо K образовано какими-то $n \times n$ -матрицами над полем P , его операции — сложение и умножение

матриц. Докажите, что для любого идеала J кольца K множество $J^\perp := \{B \in K : \text{tr}(AB) = 0 \ \forall A \in J\}$ также является идеалом кольца K .

Задача 323. Найдите все нетривиальные идеалы в кольце вещественных матриц порядка n .

8.2. Идеалы и модули

Будем считать, что K — коммутативное ассоциативное кольцо с единицей. Если $G = \{g_1, \dots, g_s\}$ — конечное множество, то идеал $R = \langle G \rangle$ называется *конечно порожденным* и для него употребляется запись $\langle G \rangle = \langle g_1, \dots, g_s \rangle$. Идеал, порожденный каким-то одним элементом, называется *главным идеалом*.

Пусть K — коммутативное ассоциативное кольцо с единицей. Тогда $\langle g_1, \dots, g_s \rangle = \{f_1 g_1 + \dots + f_s g_s : f_1, \dots, f_s \in K\}$ и очевидно, что $K = \langle 1 \rangle$, т.е. тривиальный идеал $R = K$ является главным.

Пример 1. В кольце целых чисел $\mathbb{Z}$ любой идеал является главным: пусть n — минимальное натуральное число в ненулевом идеале $R \leq \mathbb{Z}$; тогда если $m \in R$, то остаток при делении m на n должен быть нулевым, а это значит, что R состоит из всех чисел, кратных n .

Пример 2. В кольце многочленов $K = \mathbb{C}[x, y]$ идеал $R = \langle x, y \rangle$ не является главным: иначе многочлены x и y имели бы нетривиальный общий делитель.

Пример 3. Рассмотрим бесконечное множество переменных (букв)

$$G = \{x_1, x_2, \dots\},$$

и пусть K — кольцо всех многочленов от любого конечного набора этих переменных. Нетрудно проверить, что идеал $R := \langle G \rangle < K$ не является конечно порожденным, в отличие от $K = \langle 1 \rangle$.

Коммутативное ассоциативное кольцо с единицей, в котором каждый идеал является конечно порожденным, называется *нётеровым* — в честь Эмми Нётер.

Обратим внимание на то, что конечно порожденный идеал R кольца K напоминает конечномерное векторное пространство в том смысле, что любой элемент $f \in R$ является линейной комбинацией одной и той же системы элементов $g_1, \dots, g_s \in R$ с коэффициентами из кольца K .

Данная аналогия приводит к общему понятию *модуля над кольцом* K , или K -модуля. Так называется непустое множество V с операцией сложения, превращающей его в аддитивную абелеву группу, и операцией умножения элементов модуля V на элементы кольца K . Подобно умножению векторов на числа, если $\alpha \in K$ и $v \in V$, то результат умножения v на α обозначается αv и является элементом модуля V . Более того, должны выполняться аксиомы, буквально копирующие определение векторного пространства над полем:

- 1) $\alpha(\beta v) = (\alpha\beta)v$,
- 2) $(\alpha + \beta)v = \alpha v + \beta v$,
- 3) $\alpha(v + w) = \alpha v + \alpha w$,
- 4) $1 \cdot v = v$.

В этих аксиомах α и β — произвольные элементы кольца K , а v и w — произвольные элементы модуля V .

Непустое подмножество $V_1 \subseteq V$ называется *подмодулем* модуля V , если V_1 есть подгруппа аддитивной группы модуля V , замкнутая относительно умножений на элементы кольца K .

Если можно найти конечную систему элементов $v_1, \dots, v_n \in M$, такую что M состоит из всех линейных комбинаций $\alpha_1 v_1 + \dots + \alpha_n v_n$ с произвольными коэффициентами из K , то модуль M называется *конечно порожденным* или *модулем конечно-го типа*. Как видим, если K — нётерово кольцо, то любой его идеал можно рассматривать как конечно порожденный модуль над кольцом K .

В общем определении модуля от кольца требуется только ассоциативность и наличие единицы, в таких случаях следует иметь в виду, что $\alpha\beta$ и $\beta\alpha$ могут быть разными элементами кольца. Однако здесь и ниже в этой главе мы рассматриваем только коммутативные кольца.

Задача 324. Докажите, что нётеровость кольца равносильна отсутствию бесконечно растущих последовательностей идеалов $R_1 \subsetneq R_2 \subsetneq \dots$.

Задача 325. Докажите, что кольцо многочленов $K[x]$ над полем K является нётеровым.

Задача 326. Покажите, что в конечно порожденном модуле могут быть подмодули, не являющиеся конечно порожденными.

8.3. Радикалы и нильпотенты

В дальнейшем, если явно не сказано, мы рассматриваем только коммутативные ассоциативные кольца с единицей.

Радикалом идеала R в кольце K называется множество всех элементов из K , которые при возведении в некоторую степень дают элемент из R . Обозначение: $\text{rad}(R)$.

Если $R = \text{rad}(R)$, то идеал R называется *радикальным*.

Утверждение 8.3.1. *Радикал идеала также является идеалом.*

Доказательство. Рассмотрим произвольный идеал R , и пусть $a^k \in R$ и $b^l \in R$. Тогда каждый член бинома Ньютона

$$(a + b)^{k+l} = \sum_{i=0}^{k+l} \binom{k+l}{i} a^i b^{k+l-i}$$

принадлежит R , так как либо $i \geq k$, либо $k + l - i \geq l$. Значит, если $a, b \in \text{rad}(R)$, то и $a + b \in \text{rad}(R)$. Пусть теперь $a \in \text{rad}(R)$ и b — произвольный элемент кольца. Тогда если $a^k \in R$, то $(ab)^k = a^k b^k \in R \Rightarrow ab \in \text{rad}(R)$. $\square$

Утверждение 8.3.2. *Радикал пересечения идеалов равен пересечению их радикалов.*

Доказательство. Пусть даны идеалы A и B . Если $c \in \text{rad}(A \cap B)$, то найдется $n \in \mathbb{N}$ такое, что $c^n \in A \cap B \Rightarrow c^n \in A \Rightarrow c \in \text{rad}(A)$. По той же причине $c \in \text{rad}(B)$ и, следовательно, $c \in \text{rad}(A) \cap \text{rad}(B)$. Теперь предположим, что $c \in \text{rad}(A) \cap \text{rad}(B) \Rightarrow \exists k, l \in \mathbb{N}$ такие, что $c^k \in A$ и $c^l \in B$. Отсюда $c^{kl} \in A \cap B \Rightarrow c \in \text{rad}(A \cap B)$. $\square$

Следствие 8.3.1. *Пересечение радикальных идеалов является радикальным идеалом.*

Радикал нулевого идеала называется *нильпотентным* или *нильрадикалом*, а каждый его элемент называется *нильпотентным элементом* или *нильпотентом*.

Задача 327. Докажите, что единственным нильпотентным элементом кольца вычетов по нильпотентному радикалу является нуль.

Задача 328. Пусть K — коммутативное ассоциативное кольцо с единицей. Докажите, что многочлен $f(x) \in K[x]$ является нильпотентным элементом в кольце $K[x]$ тогда

и только тогда, когда каждый из его коэффициентов является нильпотентным элементом в кольце K .

Задача 329. Пусть K — коммутативное ассоциативное кольцо с единицей и ненулевой многочлен $f(x) \in K[x]$ является делителем нуля в кольце $K[x]$. Докажите, что $af(x) = 0$ для некоторого ненулевого элемента $a \in K$.

Задача 330. Пусть R — нильпотентный радикал в нётеровом кольце. Докажите, что можно найти натуральное число n такое, что произведение произвольных n элементов из R будет равно нулю.

Задача 331. Пусть K — подкольцо в (некоммутативном) кольце $\mathbb{Q}^{n \times n}$ и

$$R := \{A \in K : \operatorname{tr} AB = 0 \ \forall B \in K\}.$$

Докажите, что R — самый большой идеал в K , состоящий из нильпотентных матриц.

8.4. Простые и примарные идеалы

Идеал $R < K$ называется *простым*, если произведение двух элементов из K принадлежит R в том и только случае, когда хотя бы один из них входит в R . Тривиально проверяется, что любой простой идеал является радикальным.

По аналогии с разложением целых чисел на множители запись

$$R = \bigcap_{1 \leq i \leq m} R_i$$

будем также называть *разложением с идеалами* R_i и *нетривиальным разложением*, если $R < R_i$ для всех i . Если нетривиального разложения нет, то идеал называется *неприводимым*. По аналогии с целыми числами, в теории идеалов об R говорят как о наименьшем общем кратном идеалов $R_1, \dots, R_m$, а каждый из идеалов, содержащих R , называется его делителем.

Лемма 8.4.1. *Радикальный идеал является непростым в том и только том случае, когда он допускает нетривиальное разложение с радикальными идеалами.*

Доказательство. Пусть K — коммутативное ассоциативное кольцо с единицей, в котором идеал R имеет вид $R = A \cap B$. Предположим, что каждый из идеалов A и B строго больше R .

Тогда для любых элементов $a \in A \setminus B$ и $b \in B \setminus A$ находим $ab \in R$. В то же время $a \notin R$ и $b \notin R$. Поэтому идеал R не является простым. В этом рассуждении радикальность идеалов не использовалась.

Пусть известно, что идеал R непростой. Тогда можно найти элементы $a, b \in K$ со следующими свойствами:

$$ab \in R, \quad a, b \notin R.$$

Рассмотрим идеалы $A := R + \langle a \rangle$ и $B := R + \langle b \rangle$ и заметим, что каждый из них строго больше R . Пусть $c \in A \cap B$. Тогда

$$c = r_1 + h_1 a = r_2 + h_2 b, \quad r_1, r_2 \in R, \quad h_1, h_2 \in K.$$

Поскольку $ab \in R$, отсюда выводим

$$c^2 = (r_1 + h_1 a)(r_2 + h_2 b) \in R.$$

В случае радикального идеала R получаем $c \in R$. Значит, $A \cap B = R$ и, согласно утверждению 8.3.2, $R = \text{rad}(R) = \text{rad}(A) \cap \text{rad}(B)$. $\square$

Теорема 8.4.1. *В нётеровом кольце любой собственный радикальный идеал R допускает разложение*

$$R = \bigcap_{1 \leq i \leq m} R_i$$

с конечным числом простых идеалов R_i . Более того, существует разложение, в котором ни один из идеалов R_i не является частью идеала R_j при $i \neq j$, и в любом таком разложении набор простых идеалов R_i один и тот же.

Доказательство. Если идеал R простой, то все доказано, так как в силу леммы 8.4.1 он не может иметь нетривиального разложения. Если радикальный идеал R не является простым, то по той же лемме он допускает нетривиальное разложение с радикальными идеалами $R = R_{11} \cap R_{21}$. Если каждый из них простой, то существование разложения доказано. Если нет, то хотя бы один из радикальных идеалов R_{11} и R_{21} непростой и поэтому допускает нетривиальное разложение. В итоге $R = R_{12} \cap R_{22} \cap R_{32}$. Мы можем продолжать в том же духе до тех пор, пока не возникнет разложение, в котором все идеалы будут простыми. Если этого не случилось, то должна получиться строго растущая последовательность идеалов. Последнее в нётеровом кольце невозможно. Поэтому разложение с конечным

числом простых идеалов обязательно существует. Если в этом разложении $R_i \subseteq R_j$ при $i \neq j$, то идеал R_j можно из разложения изъять. В итоге получается разложение с условием $R_i \subsetneq R_j$ при $i \neq j$.

Чтобы доказать единственность, рассмотрим равенство $\bigcap_{i=1}^m A_i = \bigcap_{j=1}^n B_j$, в котором все идеалы простые и слева и справа ни один из идеалов не является частью другого. Для произвольного идеала A_i имеет место разложение

$$A_i = B := \bigcap_{j=1}^n (A_i + B_j).$$

В самом деле, включение $A_i \subseteq B$ очевидно. Обратное включение: любой элемент идеала B допускает представления

$$B \ni b = a_1 + b_1 = \dots = a_n + b_n, \\ a_1, \dots, a_n \in A_i, \quad b_j \in B_j, \quad 1 \leq j \leq n;$$

далее, $b_1 \dots b_n \in A_i \Rightarrow b^n = (a_1 + b_1) \dots (a_n + b_n) \in A_i \Rightarrow b \in A_i$ (любой простой идеал радикален). В силу леммы 8.4.1, простота идеала A_i означает, что $A_i = A_i + B_k$ для некоторого $k \Rightarrow B_k \subseteq A_i$. Аналогично, $A_l \subseteq B_k$ для некоторого $l \Rightarrow A_l \subseteq B_k \subseteq A_i \Rightarrow l = i \Rightarrow A_i = B_k$. Следовательно, каждый из идеалов A_i совпадает с одним из идеалов B_j . $\square$

Смысл доказанной теоремы имеет родство с основной теоремой арифметики. Обратим внимание на то, что разложения с простыми идеалами строятся не для произвольных, а только для радикальных идеалов. В случае произвольных идеалов при получении разложений используются *примарные* идеалы.

Идеал $R < K$ называется *примарным*, если из условия $ab \in R$ следует, что если $a \notin R$, то $b \in \text{rad}(R)$. Это равносильно утверждению о том, что в кольце вычетов K/R любой делитель нуля нильпотентен. Заметим, что если идеал R прост, то кольцо вычетов K/R делителей нуля не имеет. Любой простой идеал очевидно примарен.

Пример 1. Идеал $R = \langle (x^2 + 1)(x - 1)(x + 1) \rangle < \mathbb{R}[x]$ является радикальным и обладает следующим разложением с простыми идеалами: $R = \langle x^2 + 1 \rangle \cap \langle x - 1 \rangle \cap \langle x + 1 \rangle$.

Пример 2. Идеал $R = \langle x^2 \rangle < \mathbb{R}[x]$ примарен, но не является радикальным и не имеет разложения с конечным числом простых

идеалов, так как R не является простым, а идеалы его разложения должны порождаться делителями многочлена x^2 и их пересечение непременно оказалось бы шире, чем R .

Теорема 8.4.2 (ЛАСКЕР–НЁТЕР). *В нётеровом кольце любой собственный идеал допускает разложение с конечным числом примарных идеалов.*

Доказательство. В нётеровом кольце K любой идеал имеет разложение с неприводимыми идеалами. Если это не так, то в кольце найдется максимальный собственный идеал R , не имеющий такого разложения, — максимальность означает, что для любого строго большего собственного идеала такое разложение существует. Конечно же, идеал R приводим, и возникает противоречие: он допускает нетривиальное разложение, в котором каждый идеал строго больше и поэтому имеет разложение с неприводимыми идеалами.

Остается доказать, что любой неприводимый собственный идеал примарен. Пусть R — такой идеал, $ab \in R$ и $a \notin R$. Множество $R_n := \{x \in K : xb^n \in R\}$ является идеалом кольца K , при этом $R_1 \subseteq R_2 \subseteq \dots$ и, в силу нётеровости, $R_n = R_{n+1}$ для какого-то n . Пусть $c \in (R + \langle a \rangle) \cap (R + \langle b^n \rangle)$. Тогда $c = r_1 + au = r_2 + b^n v$, где $r_1, r_2 \in R$ и $u, v \in K$. Отсюда $cb = r_1 b + abu \in R \Rightarrow r_2 b + b^{n+1} v \in R \Rightarrow b^{n+1} v \in R \Rightarrow v \in R_{n+1} = R_n \Rightarrow b^n v \in R \Rightarrow c \in R \Rightarrow R = (R + \langle a \rangle) \cap (R + \langle b^n \rangle)$. Поскольку идеал $R + \langle a \rangle$ строго больше R , из неприводимости R получаем: $R + \langle b^n \rangle = R \Rightarrow b^n \in R \Rightarrow b \in \text{rad}(R)$. $\square$

Утверждение 8.4.1. *Радикал примарного идеала q является простым и никакой строго меньший простой идеал не содержит q .*

Доказательство. Пусть $p = \text{rad}(q)$, $ab \in p$ и $b \notin p$. Тогда $(ab)^n \in q$ для какого-то $n \in \mathbb{N} \Rightarrow b^n \notin q$, иначе $b \in p$. В силу примарности q , находим: $a^n \in \text{rad}(q) = p \Rightarrow a \in p$. Для промежуточного простого идеала R получаем: $q \subseteq R \subseteq p \Rightarrow p = \text{rad}(q) \subseteq \subseteq \text{rad}(R) \subseteq \text{rad}(p) = p \Rightarrow R = \text{rad}(R) = p$. $\square$

Если $p = \text{rad}(q)$, то примарный идеал q называется *p -примарным* или *ассоциированным с простым идеалом p* . В этом случае говорят также, что простой идеал p ассоциирован с примарным идеалом q . Для идеала A разложение

$$A = \bigcap_{1 \leq i \leq m} q_i \quad (*)$$

называется *минимальным примарным разложением*, если радикалы примарных идеалов $q_1, \dots, q_m$ попарно различны и ни один из примарных идеалов $q_1, \dots, q_m$ не содержит пересечение остальных примарных идеалов из данного разложения.

Теорема 8.4.3. Пусть K — коммутативное ассоциативное кольцо с единицей и его идеал A есть пересечение конечного числа примарных идеалов. Тогда он имеет также минимальное примарное разложение вида (*) и в любом минимальном разложении множество идеалов $p_i = \text{rad}(q_i)$ совпадает с подмножеством простых идеалов среди всего множества идеалов вида $\text{rad}(A : b)$, где $b \in K$.

Доказательство. Прежде всего заметим, что пересечение p -примарных идеалов является p -примарным. Поэтому из любого примарного разложения можно получить такое примарное разложение, в котором радикалы примарных компонент попарно различны. Пересечение не изменится, если мы выбросим любую компоненту, содержащую пересечение остальных компонент. После конечного числа изъятий таких компонент не останется и в итоге будет получено какое-то минимальное разложение вида (*) с примарными компонентами q_i , ассоциированными с попарно различными простыми идеалами $p_i = \text{rad}(q_i)$. Далее, если $b \in q_i$, то $1 \in q_i : b$, и поэтому $q_i : b = K$. Теперь предположим, что $b \notin q_i$, и пусть $a^n \in q_i : b \Rightarrow a^n b \in q_i \Rightarrow a \in \text{rad}(q_i) = p_i$. Следовательно, $q_i \subseteq q_i : b \subseteq \text{rad}(q_i : b) \subseteq p_i$ и, после взятия радикалов, $\text{rad}(q_i : b) = p_i$. Используя эти наблюдения, находим

$$\text{rad}(A : b) = \text{rad}\left(\bigcap_i q_i : b\right) = \bigcap_i \text{rad}(q_i : b) = \bigcap_{b \notin q_i} \text{rad}(q_i : b) = \bigcap_{b \notin q_i} p_i.$$

Если идеал $\text{rad}(A : b)$ прост, то он совпадает с каким-то из простых идеалов p_i . Кроме того, если $b \in \bigcap_{j \neq i} q_j \setminus q_i$, то $\text{rad}(A : b) = p_i$. $\square$

Теперь мы понимаем, что простые идеалы $p_i = \text{rad}(q_i)$, определенные минимальным примарным разложением идеала A , не зависят от того, как строится это разложение. Они называются *ассоциированными* с идеалом A . Минимальные из них, т.е. не содержащие других ассоциированных с A простых идеалов, называются *минимальными* или *изолированными* простыми компонентами идеала A .

Задача 332. Докажите, что идеал, порожденный многочленами x, y, z в кольце $\mathbb{C}[x, y, z]$, является простым.

Задача 333. Докажите, что если идеал принадлежит объединению конечного числа простых идеалов, то он принадлежит по крайней мере одному из них.

Задача 334. Докажите, что все нильпотентные элементы принадлежат пересечению всех простых идеалов.

Задача 335. Докажите, что идеал в коммутативном ассоциативном кольце с единицей является простым тогда и только тогда, когда его фактор-кольцо является целостным.

Задача 336. Что можно сказать о простоте суммы простых идеалов?

Задача 337. Докажите, что радикал идеала R в нётеровом кольце равен пересечению всех содержащих R простых идеалов.

8.5. Кольца частных, расширения и сужения идеалов

Для заданного кольца K , в том числе и с делителями нуля, можно строить различные кольца частных. Для этого можно использовать любое мультипликативно замкнутое множество $S \subset K$. Так называется подмножество ненулевых элементов кольца K , содержащее единицу и замкнутое относительно умножения: если $a, b \in S$, то $ab \in S$. Подобно построению поля частных, мы вводим *формальные дроби* a/b , где $a, b \in K$ и $b \in S$.

Дроби a/b и c/d объявляются равными, если элемент $ad - bc$ можно сделать нулем с помощью умножения на некоторый элемент $h \in S$:

$$a/b = c/d \Leftrightarrow \exists h \in S : h(ad - bc) = 0.$$

Ясно, что данное правило отождествления рефлексивно и симметрично. Проверим транзитивность:

$$\begin{aligned} a/b = c/d, c/d = f/g &\Rightarrow h_1 ad = h_1 bc, h_2 cg = h_2 df, h_1, h_2 \in S \Rightarrow \\ &\Rightarrow h_1 h_2 adg = h_1 h_2 bcf = h_1 h_2 bdf \Rightarrow \\ &\Rightarrow h(ag - bf) = 0, \quad h := h_1 h_2 d \in S. \end{aligned}$$

Операции сложения и умножения определяются естественными правилами для дробей (корректность проверяется без труда):

$$a/b + c/d := (ad + bc)/(bd), \quad (a/b)(c/d) := (ac)/(bd).$$

Полученное кольцо формальных дробей называется *кольцом частных кольца K относительно мультипликативно замкнутого множества S* . Обозначение: $S^{-1}K$.

Пример. Пусть $a \in K$ не является нильпотентом и $S = \{a^l : l = 0, 1, \dots\}$. В данном случае $S^{-1}K = \{b/a^n : b \in K, 0 \leq n \in \mathbb{Z}\}$. Кольцо $S^{-1}K$ — коммутативное ассоциативное кольцо с единицей, в котором элемент a обратим.

Элементарно проверяется, что для любого простого идеала $p < K$ множество $S = K \setminus p$ мультипликативно замкнуто. В этом случае описанный нами метод построения кольца частных называется *локализацией кольца K по простому идеалу p* и вместо $S^{-1}K$ применяется обозначение K_p .

Отображение $\phi: K \rightarrow S^{-1}K$, определенное правилом $\phi(a) = a/1$, называется *естественным гомоморфизмом*. Если A — идеал в K , то его образ $\phi(A)$ обычно не является идеалом в $K' := S^{-1}K$. Однако, как и любое подмножество, в кольце K' оно порождает идеал $\langle \phi(A) \rangle_{K'} = \phi(A)K'$, который называется *расширением идеала $A \leq K$ в кольце K'* . Для любого идеала $A' \leq K'$ его полный прообраз $\phi^{-1}(A')$ всегда является идеалом в K и называется *сужением идеала $A' \leq K'$ в кольце K* .

Утверждение 8.5.1. Если A — идеал кольца K , то $\phi^{-1}(\phi(A)) = A_S$, где

$$A_S = \{x \in K : xs \in A \text{ для некоторого } s \in S\}.$$

Ядром естественного гомоморфизма $\phi: K \rightarrow S^{-1}K$ является идеал

$$0_S := \{x \in K : xs = 0 \text{ для некоторого } s \in S\}.$$

Доказательство элементарно и предоставляется читателю. Обратим внимание на то, что если $0_S \supsetneq 0$, то естественный гомоморфизм не является вложением (нет инъективности).

Утверждение 8.5.2. Пусть K — коммутативное ассоциативное кольцо с единицей, $q_1, \dots, q_n$ — его примарные идеалы, A — их пересечение, S — произвольное мультипликативно

замкнутое множество. Тогда если $S \cap q_i = \emptyset$ при $1 \leq i \leq m$ и $S \cap q_i \neq \emptyset$ при $m+1 \leq i \leq n$, то

$$A_S = \bigcap_{1 \leq i \leq m} q_i.$$

Если S пересекается с каждым из идеалов $q_1, \dots, q_n$, то $A_S = K$.

Доказательство. Пусть $x \in A_S \Leftrightarrow \exists s \in S : xs \in A$. Если $S \cap q_i = \emptyset$, то $s \notin \text{rad}(q_i)$.

Идеал q_i является примарным: $xs \in q_i \Rightarrow x \in q_i \Rightarrow A_S \subseteq B := \bigcap_{1 \leq i \leq m} q_i$. Теперь предположим, что $x \in B$ и $s_i \in S \cap q_i$ при $m+1 \leq i \leq n$. Тогда, в силу мультипликативной замкнутости множества S , элемент $s := s_{m+1} \dots s_n$ принадлежит S и, в силу свойства поглощения, $s \in C := \bigcap_{m+1 \leq i \leq n} q_i \Rightarrow xs \in B \cap C = A \Rightarrow B \subseteq A_S$. Если S пересекается с каждым идеалом q_i , то $1 \times s = s \in A = C \Rightarrow 1 \in A_S \Rightarrow A_S = K$. $\square$

Утверждение 8.5.3. Если p — простой идеал в нётеровом кольце K , то для любого натурального числа n в минимальном примарном разложении идеала

$$p^n = \bigcap_{1 \leq i \leq m} q_i$$

имеется примарная компонента q_j , радикал которой равен p . При этом $q_j = (p^n)_S$, где $S = K \setminus p$, и $p \subsetneq \text{rad}(q_i)$ для любого $i \neq j$.

Доказательство. Положим $p_i = \text{rad}(q_i)$. Если $x \in p$, то, очевидно,

$$\begin{aligned} x^n \in p^n = \bigcap_{1 \leq i \leq m} q_i &\Rightarrow x \in \text{rad}\left(\bigcap_{1 \leq i \leq m} q_i\right) = \bigcap_{1 \leq i \leq m} \text{rad}(q_i) = \\ &= \bigcap_{1 \leq i \leq m} p_i \Rightarrow p \subseteq p_i \quad \forall i. \end{aligned}$$

Далее, $\bigcap_{1 \leq i \leq m} p_i \subseteq \text{rad}(p^n) \subseteq \text{rad}(p) = p$, а это возможно только если $p_j \subseteq p$ для какого-то j . С учетом полученного выше включения, для этого номера j получаем: $p_j = p$. Множество S не пересекает $p = p_j$, а значит, оно не пересекает и q_j . В то же время оно имеет общий элемент с каждым из простых идеалов p_i при $i \neq j$. Если $s \in p_i \cap S$, то для какого-то натурального N имеем

$s^N \in q_i$ и, в силу мультипликативной замкнутости множества S , находим: $s^N \in S$. Значит, S пересекается с каждым из примарных идеалов q_i при $i \neq j$. Согласно утверждению 8.5.2, $(p^n)_S = q_j$. $\square$

Примарный идеал $q_j = (p^n)_{K \setminus p}$ из только что доказанного утверждения называется *n -й символической степенью простого идеала p* и обозначается через $p^{(n)}$. Заметим, что его расширение в кольце частных K_p совпадает с обычной n -й степенью идеала p' , который в этом кольце является расширением простого идеала $p < K$. Надо иметь в виду, что термин *расширение* в данной ситуации не означает, что $p^{(n)}$ может быть вложено в $(p')^n$. Так бывает лишь в тех случаях, когда естественный гомоморфизм оказывается инъективным.

Задача 338. Приведите примеры инъективных и неинъективных естественных гомоморфизмов кольца K в кольцо частных K_p , полученное локализацией K по простому идеалу p .

Задача 339. Докажите, что кольцо частных нётерова кольца по любой мультипликативно замкнутой системе также нётерово.

8.6. Максимальные идеалы и локальные кольца

Собственный идеал называется *максимальным*, если он не является строгим подмножеством другого собственного идеала. Кольцо называется *локальным*, если оно имеет лишь один максимальный идеал.

Утверждение 8.6.1. Если p — простой идеал кольца K , то кольцо частных K_p является локальным. Его единственный максимальный идеал состоит из всех дробей a/b при $a \in p$, $b \notin p$.

Пример. Рассмотрим непрерывные функции от x в окрестности точки x_0 и назовем две функции эквивалентными, если они совпадают в некоторой окрестности этой точки. Классы эквивалентных функций называются *ростками* в точке x_0 . Для них естественным образом можно ввести операции сложения и умножения, в результате получается *кольцо ростков*. Пусть J — нетривиальный идеал этого кольца и $f(x) \in J$. Тогда $f(x_0) = 0$, иначе идеал совпадает со всем кольцом. Множество функций $\{f: f(x_0) = 0\}$ образует единственный нетривиальный идеал,

который, конечно же, оказывается единственным максимальным идеалом кольца ростков.

Теорема 8.6.1. *Любой максимальный идеал в коммутативном ассоциативном кольце с единицей является простым.*

Доказательство. Пусть R — максимальный идеал кольца K , $a, b \in K \not\geq R$ и $ab \in R$. Допустим, что $a \notin R$. Тогда множество

$$aK + R = \{aq + r : q \in K, r \in R\}$$

является идеалом, строго большим, чем R . Значит, $aK + R = K \Rightarrow aq + r = 1$ для каких-то элементов $q \in K$ и $r \in R \Rightarrow abq + br = b \in R$. $\square$

Теорема 8.6.2. *Кольцо вычетов по некоторому идеалу в коммутативном ассоциативном кольце с единицей является полем тогда и только тогда, когда этот идеал максимален.*

Доказательство. Пусть R — максимальный идеал в коммутативном ассоциативном кольце K с единичным элементом 1. Ясно, что вычет $[1]$ — это единица фактор-кольца K/R . Докажем, что произвольный ненулевой вычет $[a] \in K/R$ является обратимым. Для этого заметим, что множество $aK + R$ является идеалом, строго большим, чем R . Поэтому $aK + R = K \Rightarrow 1 \in aK + R \Rightarrow 1 = aq + r$ для каких-то элементов $q \in K$ и $r \in R \Rightarrow [a][q] = [1]$. Обратно, пусть K/R — поле, а идеал L строго больше R . Для любого элемента $a \in L \setminus R$ вычет $[a]$ обратим $\Rightarrow 1 - ab \in R$ для некоторого $b \in K \Rightarrow 1 \in L \Rightarrow L = K$. $\square$

Теорема 8.6.3. *Пусть K — произвольное коммутативное ассоциативное кольцо с единицей. Тогда любой нетривиальный идеал в K содержится в некотором максимальном идеале.*

Эта теорема довольно просто доказывается, если кольцо K является нётеровым. Если ни один идеал, содержащий нетривиальный идеал R_1 , не является максимальным, то имеется строго растущая последовательность идеалов $R_1 \subset R_2 \subset \dots$. Их объединение также является идеалом, который порождается какими-то элементами $f_1, \dots, f_s$. Очевидно, что все эти элементы принадлежат какому-то одному идеалу $R_k \Rightarrow R_k = R_{k+1}$. Поэтому бесконечно растущей последовательности идеалов не существует, а идеал R_k и будет искомым максимальным идеалом.

Однако в общем случае доказательство опирается на так называемую *аксиому выбора* и *метод трансфинитной индукции* — мощный инструмент для того, чтобы доказывать существование каких-то объектов или свойств без какого-либо намека на то, как можно практически выполнить построение или проверить установленные свойства. Как это делается, мы скоро увидим.

Задача 340. Докажите, что коммутативное ассоциативное кольцо с единицей, имеющее ровно два разных идеала, является полем.

Задача 341. Докажите, что если радикал идеала R является максимальным идеалом, то R — примарный идеал.

Задача 342. Пусть коммутативное ассоциативное кольцо с единицей имеет ровно один простой идеал. Докажите, что каждый необратимый элемент такого кольца является нильпотентом. Верно ли обратное?

Задача 343. Пусть K — коммутативное ассоциативное кольцо с единицей, а идеал R — пересечение всех его максимальных идеалов. Докажите, что a принадлежит R в том и только том случае, когда элемент $1 - ab$ является обратимым для любого $b \in K$.

Задача 344. Докажите, что в нётеровом кольце каждый делитель нуля принадлежит простому идеалу, в котором все ненулевые элементы являются делителями нуля.

Задача 345. Пусть кольцо K нётерово и $a \in K$ не является нильпотентным элементом. Докажите, что существует идеал $J < K$, не содержащий ни одного из элементов вида a^n при $n \in \mathbb{N}$ и такой, что любой строго больший идеал этим свойством уже не обладает. Докажите также, что любой идеал J такого типа является простым.

Задача 346. Пусть K — коммутативное ассоциативное кольцо с единицей. Докажите, что нильпотентный радикал кольца многочленов $K[x]$ совпадает с пересечением всех максимальных идеалов кольца $K[x]$.

Задача 347. Докажите, что если коммутативное ассоциативное кольцо с единицей обладает единственным максимальным идеалом, то он совпадает с множеством всех необратимых элементов.

Задача 348. В коммутативном ассоциативном кольце с единицей имеется ненулевой элемент, а множество всех необратимых элементов замкнуто относительно сложения. Докажите, что такое кольцо является локальным.

Задача 349. Докажите, что в локальном кольце уравнение $x^2 = x$ имеет ровно два решения: 0 и 1.

8.7. Упорядоченные множества

Аксиома выбора. Для любого непустого множества M существует функция, которая определена на всех его непустых подмножествах, а ее значение на каждом таком подмножестве есть какой-то элемент данного подмножества.

Данное утверждение, как и положено аксиоме, кажется очень естественным и легко принимается как нечто очевидное. Однако, удивительные следствия этой аксиомы, которые мы обсудим ниже, совсем не кажутся очевидными. Напротив, они являются в высшей степени нетривиальными утверждениями.

Многие множества рассматриваются как *частично упорядоченные*. Таковым называется множество M с бинарным отношением «меньше или равно», которое определяется непустым множеством $N \subset M \times M$, $(a, b) \in N \Leftrightarrow a \leq b$, и обладает следующими свойствами:

- $a \leq a \quad \forall a \in M$ (рефлексивность);
- $a \leq b, b \leq a \Rightarrow a = b$ (антисимметричность);
- $a \leq b, b \leq c \Rightarrow a \leq c$ (транзитивность).

Если $a \leq b$ и $a \neq b$, то пишем $a < b$. Важным примером частично упорядоченного множества является отношение включения между подмножествами какого-либо множества.

Элемент $b \in M$ частично упорядоченного множества M называется *нижней границей* (*верхней границей*) или *нижней гранью* (*верхней гранью*) непустого подмножества $X \subseteq M$, если $x \geq b$ ($x \leq b$) для каждого $x \in X$. Элемент $a \in X$ называется *минимальным* (*максимальным*) элементом подмножества X , если ни для какого $x \in X$ не выполняется неравенство $x < a$ ($x > a$). Другими словами, минимальный (максимальный) элемент меньше (больше) любого отличного от него элемента, с которым он сравним.

Если любые два элемента множества сравнимы, то оно называется *линейно упорядоченным* или *цепью*. Цепь называется

максимальной, если она не содержится в какой-либо строго большей цепи. Линейно упорядоченное множество называется *вполне упорядоченным* или имеющим *полный порядок*, если в нем любое непустое подмножество обладает минимальным элементом. Если a — минимальный элемент подмножества X , то будем писать $a = \min(X)$. Сразу же заметим, что для любого немаксимального элемента a во вполне упорядоченном множестве M имеется *строго следующий за ним* элемент $a' \in M$. При этом ближайшего предшествующего элемента может не быть.

Простейшим примером вполне упорядоченного множества служит множество натуральных чисел с привычным отношением порядка. Множество целых чисел с естественным порядком уже не является вполне упорядоченным, хотя, проявив смекалку, можно построить новое отношение порядка, которое обеспечит полную упорядоченность. Для других множеств вопрос о том, *каким образом* их можно сделать вполне упорядоченными, остается, как правило, без ответа. Да и *можно ли вообще* это сделать? Оказывается, что положительный ответ на последний вопрос может не дать никакого ключа для ответа на первый вопрос!

Теорема 8.7.1 (ТЕОРЕМА ЦЕРМЕЛО). *Любое непустое множество можно сделать вполне упорядоченным.*

Сначала докажем одно замечательное свойство вполне упорядоченных множеств, установленное Г. Кантором. Пусть P и Q — вполне упорядоченные множества с отношениями порядка $\leq_P$ и $\leq_Q$. отображение $\phi: P \rightarrow Q$ называется *монотонным*, если $a <_P b \Rightarrow \phi(a) <_Q \phi(b)$. Монотонное взаимно-однозначное отображение называется *изоморфизмом*. Соответствующие вполне упорядоченные множества P и Q называются *изоморфными*. Обозначение: $P \cong Q$.

Если $a \in P$, то множество вида $P_a := \{x \in P: x <_P a\}$ будем называть *начальным фрагментом* множества P .

Теорема 8.7.2 (ТЕОРЕМА КАНТОРА). *Пусть P и Q — произвольные вполне упорядоченные множества. Тогда имеет место один из трех случаев:*

- 1) $P \cong Q$, либо
- 2) $P \cong Q_b$ для некоторого элемента $b \in Q$, либо
- 3) $Q \cong P_a$ для некоторого элемента $a \in P$.

Доказательство. Пусть $a_0 := \min(P)$ и $b_0 := \min(Q)$. Рассмотрим всевозможные монотонные функции ϕ , определенные на каких-то начальных фрагментах P_a или на всем множестве P и такие, что $\phi(a_0) = b_0$ и $\phi(c) = \min(Q \setminus \phi(P_c))$ для любого $c \neq a_0$ из области определения функции ϕ . Во-первых, множество Φ всех таких функций непусто: ему принадлежит, например, функция ϕ с областью определения $\{a_0\}$ (если P содержит не менее двух элементов, то $\{a_0\} = P_{a'_0}$, где a'_0 строго следует за элементом a). Во-вторых, функции $\phi_1, \phi_2 \in \Phi$ принимают одно и то же значение там, где определены обе: пусть a — минимальный элемент среди всех $x \in P$, для которых $\phi_1(x) \neq \phi_2(x) \Rightarrow \phi_1(x) = \phi_2(x)$ для всех $x < a \Rightarrow \phi_1(a) = \min(Q \setminus \phi_1(P_a)) = \min(Q \setminus \phi_2(P_a)) = \phi_2(a)$. Возникло противоречие с выбором точки a .

Предположим, что в множестве P имеются точки, в которых не определена ни одна из функций множества Φ . В силу полной упорядоченности существует минимальная точка $a \in P$ с таким свойством. Тогда имеется функция ϕ , определенная при всех $x \in P_a$. Если $\phi(P_a) = Q$, то имеет место случай (3). Если $\phi(P_a) \neq Q$, то функция ϕ однозначно доопределяется и в точке a , что противоречит выбору этой точки. Теперь предположим, что для каждой точки $x \in P$ можно найти определенную в ней функцию ϕ_x . Тогда функция $\phi(x) := \phi_x(x)$ определена при всех $x \in P$. Если $\phi(P) = Q$, то имеет место случай (1). Если $\phi(P) \neq Q$, то обозначим через b минимальный элемент множества $Q \setminus \phi(P)$. Тогда в каждую точку $y \in Q_b$ отображается какой-то и притом единственный элемент из P . Кроме того, $Q \setminus \phi(P_x) \supseteq Q \setminus \phi(P) \Rightarrow \phi(x) = \min(Q \setminus \phi(P_x)) \leq \min(Q \setminus \phi(P)) = b$. Значит, реализуется случай (2).

Никакие два случая не могут иметь место одновременно. Если, скажем, $P \cong Q_b$ и $Q \cong P_a$, то множество P изоморфно какому-то начальному фрагменту P_c . Пусть $h: P \rightarrow P_c$ — соответствующий изоморфизм. Тогда $h(a) \geq a \forall a \in P$. В противном случае для какого-то $a \in P$ имеем: $a > h(a) \Rightarrow a > h(a) > h(h(a)) > \dots$ и возникает бесконечно убывающая последовательность, что невозможно во вполне упорядоченном множестве. Следовательно, $h(c) \geq c \Rightarrow h(c) \notin P_c$. $\square$

Следствие 8.7.1. Из двух произвольных непустых множеств хотя бы одно из них взаимно-однозначно отображается на подмножество другого.

Доказательство. По теореме Цермело, эти множества можно сделать вполне упорядоченными. После этого нужно применить теорему 8.7.2. $\square$

Множества называются *равномощными*, если их элементы находятся во взаимно-однозначном соответствии.

Теорема 8.7.3 (ТЕОРЕМА КАНТОРА–БЕРНШТЕЙНА–ШРЕДЕРА). *Если каждое из двух множеств равномощно подмножеству другого, то множества равномощны.*

Доказательство. Пусть A_0 — первое множество и $A_1 \subseteq A_0$ — подмножество, равномощное второму множеству. Используя композицию отображений, получаем взаимно-однозначное отображение $f: A_0 \rightarrow A_2 \subseteq A_1 \subseteq A_0$. Докажем, что A_0 равномощно A_1 . Для этого рассмотрим цепочку подмножеств

$$A_0 \supseteq A_1 \supseteq A_2 \supseteq A_3 \supseteq \dots,$$

$$A_{2k} := f(A_{2k-2}), \quad A_{2k+1} := f(A_{2k-1}), \quad k = 1, 2, \dots$$

Положим $C_i := A_i \setminus A_{i-1}$ и $C := \bigcap_{i \geq 0} A_i$. Тогда $A_0 = \left(\bigcup_{i \geq 0} C_i \right) \cup C$,

$A_1 = \left(\bigcup_{i \geq 1} C_i \right) \cup C$. Множества $C, C_0, C_1, \dots$ попарно не пересекаются, а взаимно-однозначное отображение $A_0 \rightarrow A_1$ составляется из взаимно-однозначных отображений $C_{2k} \rightarrow C_{2k+2}$ и тождественных отображений $C \rightarrow C$ и $C_{2k+1} \rightarrow C_{2k+1}$ при $k = 0, 1, \dots$ $\square$

Задача 350. Пусть Q — множество всех подмножеств непустого множества P . Докажите, что любое отображение множества Q на часть множества P не является взаимно-однозначным.

Задача 351. Приведите пример счетных вполне упорядоченных множеств, которые не являются изоморфными.

Задача 352. Будем писать $x \prec y$, если $x, y \in \mathbb{R}^n$ — столбцы с неубывающими элементами и $x = Sy$ для некоторой (зависящей от x и y) $n \times n$ -матрицы S , все элементы которой неотрицательны и сумма элементов в каждом столбце и в каждой строке одна и та же и равна 1 (матрица S с такими свойствами называется двоякостохастической). Докажите, что отношение $x \prec y$ задает частичный порядок на $\mathbb{R}^n$.

8.8. Неконструктивные построения

Доказательство теоремы Цермело. Пусть дано непустое множество M . Согласно аксиоме выбора на его подмножествах $N \subsetneq M$, включающих также и пустое подмножество, существует функция f , такая что $f(N)$ представляет собой какой-то элемент множества $M \setminus N$. Положим $a_0 := f(\emptyset)$. Далее, назовем $P \subseteq M$ правильным фрагментом, если P можно вполне упорядочить таким образом, что $a = f(P_a) \quad \forall a \in P$. Заметим, что минимальный элемент любого правильного фрагмента один и тот же и равен a_0 . Кроме того, пусть $a_1 := f(\{a_0\})$, $a_2 := f(\{a_0, a_1\})$ и так далее, $a_k := f(\{a_0, \dots, a_{k-1}\})$. Тогда любое множество $\{a_0, \dots, a_k\}$ является правильным фрагментом.

Пусть P и Q — два правильных фрагмента. Согласно теореме 8.7.2 либо множества P и Q изоморфны, либо одно из них изоморфно начальному фрагменту другого множества. Допустим, что h осуществляет изоморфизм между P и Q или между P и начальным фрагментом Q_b . Тогда $h(x) = x$ для всех $x \in P$. Если это не так, то имеется P -минимальный элемент a , такой что $h(a) \neq a$. Значит, $h(x) = x$ при всех $x <_P a$. Но тогда $P_a = \{x \in P: x <_P a\} = \{y \in Q: y <_Q h(a)\} = Q_{h(a)}$. Следовательно, $a = f(P_a) = f(Q_{h(a)}) = h(a)$, что противоречит выбору a . Таким образом, из двух правильных фрагментов P и Q один является частью другого и при этом $a \leq_P b \Leftrightarrow a \leq_Q b \quad \forall a, b \in P \cap Q$.

Теперь рассмотрим объединение R всех правильных фрагментов. Нетрудно показать, что R является правильным фрагментом. Докажем, что $R = M$. Если $R \subsetneq M$, то $c := f(R) \in M \setminus R$ и на множестве $Q := R \cup \{c\}$ можно ввести полный порядок, объявив, что $a < c$ для любого $a \in R$. Получается, что множество Q также является правильным фрагментом, т. е. множество R не является объединением всех правильных фрагментов, что противоречит его определению. $\square$

Теорема 8.8.1 (ТЕОРЕМА ХАУСДОРФА). Пусть M — частично упорядоченное множество и A — произвольная цепь, составленная из его элементов. Тогда A содержится в некоторой максимальной цепи.

Доказательство. Если $A = M$, то все доказано. Если нет, то положим $B := M \setminus A$. По теореме Цермело, множество B можно сделать вполне упорядоченным, соответствующий полный

порядок обозначим символом $\leq_B$ и заметим, что он никак не связан с заданным частичным порядком на множестве M . Пусть $b_0 = \min_B(B)$. Рассмотрим множество H всевозможных функций h , определенных на B или на его начальном фрагменте, принимающих значения 0 или 1 и обладающих следующими свойствами: $h(x) = 1$, если x сравним с каждым элементом $a \in A$ и в случае $x \neq b_0$ также с каждым элементом $y <_B x$, для которого $h(y) = 1$, иначе $h(x) = 0$. Легко видеть, что множество H непусто и если функции $h_1, h_2 \in H$ определены обе в точке x , то $h_1(x) = h_2(x)$. Более того, существует функция $h \in H$, определенная в каждой точке множества B . От противного, в силу полной упорядоченности имеется B -минимальный элемент $x \in B$, на котором не определена ни одна из функций. Но тогда в каждой точке $y <_B x$ определена какая-то функция $h_y \in H$ и функция $h(y) := h_y(y)$ принадлежит H . Выяснив, сравним ли элемент x в смысле заданного частичного порядка с элементами $a \in A$ и элементами $x <_B b$, для которых $h(x) = 1$, мы можем доопределить h в точке x , а это противоречит выбору элемента $x \in B$. Множество $R := A \cup \{x \in B : f(x) = 1\}$ является искомой максимальной цепью, содержащей цепь A . В самом деле, если $x \notin R$, то $x \in B$ и $h(x) = 0$. Такой элемент x не сравним ни с одним элементом из R . $\square$

Теперь сформулируем прямое следствие доказанной теоремы, которое оказывается наиболее удобным на практике.

Теорема 8.8.2 (лемма Цорна). *Предположим, что в частично упорядоченном множестве M любая цепь имеет верхнюю границу. Тогда для любого элемента $a \in M$ существует сравнимый с ним максимальный элемент $b \in M$, т.е. $a \leq b$ и неравенство $b < c$ невозможно ни для одного элемента $c \in M$.*

Доказательство. Рассмотрим цепь, состоящую из одного элемента $a \in M$. Тогда a содержится в некоторой максимальной цепи R . Пусть b — любая верхняя граница для цепи R . В силу максимальной цепи непременно $b \in R$. Очевидно, что $a \leq b$. При этом b является максимальным элементом в M , так как нет ни одного строго большего элемента. Если допустить противное, то найдется $c \in M$, для которого $b < c$. Но тогда множество $R \cup \{c\}$ является цепью, строго большей, чем цепь R . Это означает, что R не является максимальной цепью. $\square$

Доказательство теоремы 8.6.3. Пусть K — коммутативное ассоциативное кольцо с единицей 1. Множество M всех идеалов кольца K , не совпадающих с K , частично упорядочено по включению множеств. Рассмотрим произвольную цепь A идеалов $R_\alpha < K$ и обозначим через $R = \bigcup R_\alpha$ объединение всех идеалов данной цепи. Тогда R является идеалом и при этом $R < K$. В противном случае $1 \in R \Rightarrow 1 \in R_\alpha$ для какого-то идеала $R_\alpha \Rightarrow R_\alpha = K \Rightarrow R_\alpha$ не является нетривиальным идеалом. Полученное противоречие означает, что $R < K$. Таким образом, цепь A имеет верхнюю границу R и мы имеем право применить лемму Цорна. Следовательно, для любого идеала $P < K$ найдется идеал Q такой, что $P \leq Q < K$ и нет ни одного нетривиального идеала, строго большего Q . Таким образом, Q является искомым максимальным идеалом. $\square$

Отметим здесь еще одно интересное применение леммы Цорна — для доказательства существования *базиса Гамеля*. В линейном пространстве V так называется линейно независимое множество G векторов таких, что любой вектор из V является линейной комбинацией конечного числа векторов из G . Под *линейно независимым множеством* понимается множество, в котором любая конечная система векторов линейно независима.

Теорема 8.8.3. Пусть V — произвольное линейное пространство над произвольным полем. Тогда любое линейно независимое множество $H \subseteq V$ можно вложить в множество G , которое является базисом Гамеля для пространства V .

Доказательство. Рассмотрим множество M всех линейно независимых множеств Q , содержащих заданное множество H . Частичный порядок на M задается включением множеств. Легко видеть, что для любой цепи линейно независимых множеств объединение всех множеств цепи будет также линейно независимым множеством. Оно же будет верхней границей данной цепи. По лемме Цорна, любое линейно независимое множество H входит в некоторое линейно независимое множество G , для которого большего линейно независимого множества уже нет. Покажем, что любой вектор $v \in V$ является линейной комбинацией какой-то конечной системы векторов из G . Если допустить противное, то найдется вектор v , который линейно независим с любой конечной системой векторов из G . Поэтому множество

$G \cup \{v\}$ является линейно независимым, что противоречит максимальнойности множества G . $\square$

Задача 353. A — бесконечное множество. Докажите, что множества A и $A \times \mathbb{N}$ равноможны.

Задача 354. Докажите, что объединение равноможных бесконечных множеств равноможно каждому из них.

Задача 355. Докажите, что аддитивная группа поля $\mathbb{R}$ изоморфна аддитивной группе поля $\mathbb{C}$.

Задача 356. Докажите, что между любыми базисами Гамеля одного и того же линейного пространства можно установить взаимно-однозначное соответствие.

Задача 357. Пусть K — произвольное коммутативное ассоциативное кольцо с единицей и $a \in K$ — элемент, не являющийся нильпотентным. Докажите, что среди идеалов, не содержащих ни одну натуральную степень элемента a , имеется простой идеал.

8.9. Алгебраическое замыкание поля

Рассмотрим результат, очень важный для алгебры и одновременно показывающий силу леммы Цорна и теоремы о максимальном идеале.

Алгебраически замкнутое расширение L поля K называется *алгебраическим замыканием* поля K , если никакое строго меньшее расширение не является алгебраически замкнутым. Обозначение: $L = K^{\text{alg}}$.

Теорема 8.9.1. Для произвольного поля K алгебраическое замыкание K^{alg} существует и определено однозначно с точностью до изоморфизма.

Доказательство. Сначала установим существование какого-нибудь алгебраически замкнутого поля M , содержащего K . Следуя Артину, каждому многочлену f над K , отличному от константы, поставим в соответствие букву x_f и рассмотрим кольцо R всех многочленов от конечных наборов букв x_f с коэффициентами из поля K . Пусть J — идеал, порожденный всеми многочленами вида $f(x_f)$, отличными от констант. Если $J = R$, то $1 \in J$ и для каких-то многочленов $f_1(x_{f_1}), \dots, f_s(x_{f_s})$ и каких-то многочленов $g_1, \dots, g_s$ от конечных наборов букв x_f выполняется равенство

$$f_1(x_{f_1})g_1 + \dots + f_s(x_{f_s})g_s = 1.$$

Это равенство сохранится, если данные многочлены рассматривать над любым расширением поля K . Заведомо есть такое расширение, в котором каждый многочлен f_i имеет корень α_i . При подстановке α_i вместо x_{f_i} получаем $f_i(\alpha_i) = 0$. Поэтому указанное равенство невозможно, а идеал $J \neq R$ содержится в некотором максимальном идеале F .

Поле $M_1 := R/F$ можно рассматривать как расширение поля K , в котором каждый из неконстантных многочленов с коэффициентами из K получает хотя бы один корень: для многочлена $f(x_f)$ корнем является вычет $[x_f]$.

Точно так же можно построить поле $M_2 \geq M_1$ с аналогичным свойством для многочленов с коэффициентами из M_1 и цепочку расширений $K \leq M_1 \leq M_2 \leq M_3 \leq \dots$, в которой каждый неконстантный многочлен над M_i имеет хотя бы один корень в поле M_{i+1} . Нетрудно проверить, что объединение $M := \bigcup M_i$ является полем. При этом M есть алгебраически замкнутое расширение поля K . Теперь рассмотрим пересечение всех подполей поля M , которые являются алгебраически замкнутыми расширениями поля K . Это и будет минимальное алгебраически замкнутое поле, содержащее исходное поле K . Таким образом, существование алгебраического замыкания доказано.

Пусть K^{alg} — любое алгебраическое замыкание поля K . Покажем, что любое другое алгебраическое замыкание поля K ему изоморфно. Для этого рассмотрим произвольное алгебраическое расширение L поля K и докажем, что L изоморфно какому-то подполю в K^{alg} . Рассмотрим множество пар (P, h) , где $K \leq P \leq L$ и h — изоморфизм поля P на какое-то подполе поля K^{alg} . В этом множестве заведомо есть пара (K, id) , где id — тождественное отображение K на K . Введем частичный порядок:

$$(P, h) \leq (P', h') \Leftrightarrow P \leq P' \text{ и } h(a) = h'(a) \quad \forall a \in P.$$

Далее, каждая цепь на рассмотренном множестве пар (P, h) имеет верхнюю границу. По лемме Цорна существует максимальная пара $(P, h) \geq (K, \text{id})$. Если $P < L$, то поле P можно расширить путем присоединения корня $\theta \in L$ какого-либо неприводимого многочлена, а изоморфизм h можно продолжить до изоморфизма поля $P(\theta)$ на более широкое подполе того же поля K^{alg} . Значит, $P = L$.

Таким образом, если L — алгебраическое замыкание поля K , то оно изоморфно подполю поля K^{alg} , которое, конечно же, также

будет алгебраическим замыканием поля K и поэтому должно совпадать с K^{alg} . $\square$

Задача 358. Докажите, что любой элемент алгебраического замыкания поля K является корнем некоторого многочлена с коэффициентами из K .

Задача 359. Докажите, что алгебраически замкнутое поле обязано иметь бесконечно много элементов.

8.10. Алгебраическая зависимость и независимость

Пусть поле K расширено до поля L . Система элементов $a_1, \dots, a_d \in L$ называется *алгебраически зависимой* над полем K , если $f(a_1, \dots, a_d) = 0$ для некоторого ненулевого многочлена $f(x_1, \dots, x_d) \in K[x_1, \dots, x_d]$. В противном случае система называется *алгебраически независимой* над полем K .

Элемент a_{d+1} называется *алгебраически зависимым от* элементов $a_1, \dots, a_d \in L$, если a_{d+1} является алгебраическим над полем $K(a_1, \dots, a_d)$. В противном случае a_{d+1} называется *алгебраически независимым от* $a_1, \dots, a_d$.

Лемма 8.10.1. Если элемент a_{d+1} алгебраически зависит от элементов $a_1, \dots, a_d$, то система $a_1, \dots, a_{d+1}$ является алгебраически зависимой.

Доказательство. Согласно условию, элемент a_{d+1} является корнем ненулевого многочлена $f(x) = b_0 + b_1x + \dots + b_nx^n$ с коэффициентами из поля $K(a_1, \dots, a_d)$. Заметим, что

$$b_i = \frac{u_i(a_1, \dots, a_d)}{v_i(a_1, \dots, a_d)},$$

где

$$u_i(x_1, \dots, x_d), v_i(x_1, \dots, x_d) \in K[x_1, \dots, x_d].$$

Многочлены v_i в знаменателях, конечно же, ненулевые. Можно также считать, что $b_n \neq 0$. Тогда $u_n(x_1, \dots, x_d) \neq 0$ и многочлен

$$F(x_1, \dots, x_{d+1}) := v_0 \dots v_n f = v_1 \dots v_n u_0 + \dots + v_0 \dots v_{n-1} u_n x_{d+1}^n$$

заведомо является ненулевым: достаточно заметить, что ненулевые одночлены, входящие в состав многочлена $v_0 \dots v_{n-1} u_n x_{d+1}^n$, не могут сократиться, так как только в них присутствует x_{d+1}^n . Легко видеть, что $F(a_1, \dots, a_{d+1}) = 0$. $\square$

Лемма 8.10.2. Пусть система $a_1, \dots, a_d$ является алгебраически зависимой над полем K и при этом первый элемент a_1

не является алгебраическим над полем K . Тогда для некоторого $i \geq 2$ элемент a_i алгебраически зависит от предыдущих элементов $a_1, \dots, a_{i-1}$.

Доказательство. Рассмотрим ненулевой многочлен F над K , обращающийся в нуль в точке $(a_1, \dots, a_d)$. Пусть в состав F входят буквы $x_1, \dots, x_t$ и не входят буквы $x_{t+1}, \dots, x_d$. Случай $t = 1$ невозможен, иначе элемент a_1 был бы алгебраическим над полем K . Таким образом, $2 \leq t \leq d$ и F можно рассматривать как многочлен от x_t с коэффициентами из кольца $K[x_1, \dots, x_{t-1}]$:

$$F = g_0(x_1, \dots, x_{t-1}) + g_1(x_1, \dots, x_{t-1})x_t + \dots + g_n(x_1, \dots, x_{t-1})x_t^n, \\ g_n \neq 0.$$

Если $g_n(a_1, \dots, a_{t-1}) = 0$, то элементы $a_1, \dots, a_{t-1}$ алгебраически зависимы. Если $t = 2$, то это невозможно, так как означало бы алгебраичность элемента a_1 . Поэтому $t \geq 3$. Ясно также, что можно вести индукцию по t . Если $g_n(a_1, \dots, a_{t-1}) \neq 0$, то a_t является корнем ненулевого многочлена

$$f(x_t) = g_0(a_1, \dots, a_{t-1}) + g_1(a_1, \dots, a_{t-1})x_t + \dots \\ \dots + g_n(a_1, \dots, a_{t-1})x_t^n,$$

а значит, алгебраически зависит от $a_1, \dots, a_{t-1}$. $\square$

Лемма 8.10.3. Если элемент ζ алгебраически зависит от элементов $b_1, \dots, b_t$, а каждый из этих элементов алгебраически зависит от элементов $a_1, \dots, a_s$, то ζ алгебраически зависит от $a_1, \dots, a_s$.

Доказательство. Рассмотрим поля $K_1 := K(a_1, \dots, a_s)$, $K_2 := K_1(b_1, \dots, b_t)$ и цепочку расширений $K_1 \leq K_2 \leq K_2(\zeta)$. Каждое из расширений $K_1 \leq K_2$ и $K_2 \leq K_2(\zeta)$ конечно $\Rightarrow$ расширение $K_1 \leq K_2(\zeta)$ также конечно $\Rightarrow \zeta$ является алгебраическим элементом над K_1 . $\square$

Лемма 8.10.4. Предположим, что элементы $a_1, \dots, a_m$ алгебраически независимы над полем K и каждый из них алгебраически зависит от элементов $b_1, \dots, b_n$. Тогда $m \leq n$.

Доказательство. Согласно лемме 8.10.1 система $a_1, b_1, \dots, b_n$ алгебраически зависима, а согласно лемме 8.10.2 какой-то элемент этой системы алгебраически зависит от предыдущих элементов. Не ограничивая общности, будем считать, что это элемент b_n . Тогда система $a_2, \dots, a_m$ алгебраически независима и согласно лемме 8.10.3 каждый из ее элементов алгебраически

зависит от элементов $a_1, b_1, \dots, b_{n-1}$. Если допустить, что $m > n$, то при повторении подобной процедуры на n -м шаге мы получим факт алгебраической зависимости элемента a_{n+1} от элементов $a_1, \dots, a_n$. $\square$

Для нас особенно интересны случаи, когда число алгебраически независимых элементов расширения ограничено какой-то константой. Максимальное число d элементов поля L , алгебраически независимых над K , называется *степенью трансцендентности* расширения $K \leq L$. Обозначение: $d = \text{trdeg}(L) = \text{trdeg}_K(L) = \text{trdeg}(L : K)$.

Алгебраически независимая система $a_1, \dots, a_d \in L \geq K$ называется *базисом трансцендентности* расширения $K \leq L$, если любой элемент $a \in L$ алгебраически зависит от $a_1, \dots, a_d$.

Если поле L является полем частных кольца $L_0 \supseteq K$, то под *степенью трансцендентности* кольца L_0 над полем K понимается степень трансцендентности поля L над K .

Теорема 8.10.1. *Число элементов в любом базисе трансцендентности расширения $K \leq L$ одно и то же и равно степени трансцендентности данного расширения.*

Доказательство. Для двух базисов трансцендентности достаточно два раза применить лемму 8.10.4. $\square$

Теорема 8.10.2. *Пусть имеется цепочка расширений полей $K \leq L \leq M$. Тогда*

$$\text{trdeg}(M : K) = \text{trdeg}(M : L) + \text{trdeg}(L : K).$$

Доказательство. Пусть $\alpha_1, \dots, \alpha_k$ — базис трансцендентности поля L над полем K и $\beta_1, \dots, \beta_l$ — базис трансцендентности M над L .

Тогда, во-первых, система $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l$ будет алгебраически независимой над K . Предположим, что

$$f(\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l) = 0$$

для некоторого многочлена $f(x_1, \dots, x_k, y_1, \dots, y_l)$ с коэффициентами из K . В силу алгебраической независимости системы $\beta_1, \dots, \beta_l$ над $K(\alpha_1, \dots, \alpha_k) \leq L$ находим

$$f(\alpha_1, \dots, \alpha_k, y_1, \dots, y_l) = 0.$$

Каждый коэффициент последнего многочлена представляет собой равное нулю значение некоторого многочлена над K от $x_1, \dots, x_k$ в точке $(\alpha_1, \dots, \alpha_k)$ и, вследствие алгебраической неза-

висимости системы $\alpha_1, \dots, \alpha_k$ над K , этот многочлен обязан быть нулевым. Значит, f является нулевым многочленом.

Во-вторых, любой элемент $\zeta \in M$ алгебраически зависит от $\beta_1, \dots, \beta_l$ над полем L , т.е. ζ есть корень ненулевого многочлена, коэффициенты которого являются рациональными функциями от $\beta_1, \dots, \beta_l$ над полем L . Отсюда легко вывести, что ζ будет также корнем ненулевого многочлена, коэффициенты которого суть многочлены от $\beta_1, \dots, \beta_l$ над L . Значит, ζ алгебраически зависит над K от $\beta_1, \dots, \beta_l$ и от принадлежащих L коэффициентов этих многочленов. Каждый из перечисленных элементов алгебраически зависит от $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l$ над полем K . Остается применить лемму 8.10.3. $\square$

В тех случаях, когда имеются сколь угодно большие алгебраически независимые системы, удобно ввести понятие *алгебраически независимого множества* — это множество, в котором любая конечная система элементов является алгебраически независимой. Элемент a называется *алгебраически зависимым от множества G* , если он алгебраически зависит от какой-то конечной системы элементов из G . В противном случае он называется алгебраически независимым от множества G . В общем случае базис трансцендентности расширения $K \leq L$ может определяться как алгебраически независимое множество G , такое что любой элемент из L алгебраически зависит от множества G .

Понятия алгебраической зависимости и независимости полезны также и при расширении колец. В таких случаях мы будем предполагать, что кольцо K и его расширение L являются целостными кольцами. Тогда алгебраическая зависимость системы элементов из L над кольцом K эквивалентна их алгебраической зависимости как элементов поля частных для L над полем частных для K . Степень трансцендентности расширения колец определяется как степень трансцендентности соответствующего расширения полей частных.

Предположим, что поле K расширено до поля L , и пусть G — некоторое подмножество элементов из L . Через $K(G)$ обозначается минимальное подполе поля L , а через $K[G]$ — минимальное подкольцо, которое содержит K и G .

С каждым элементом $g \in G$ свяжем переменную (букву) x_g , рассмотрим множество $X := \{x_g : g \in G\}$ и обозначим через $K[X]$ кольцо всех многочленов от любого конечного набора букв из X и через R — его подмножество, состоящее из многочленов,

обращающихся в нуль при замене входящих в него букв x_g на g . По сути R — это множество алгебраических соотношений между элементами множества G . Элементарно проверяется, что R является простым идеалом в $K[X]$, фактор-кольцо $K[X]/R$ не имеет делителей нуля и изоморфно кольцу $K[G]$, а его поле частных изоморфно полю $K(G)$.

Задача 360. Докажите, что если элементы $\alpha_1, \dots, \alpha_d$ алгебраически независимы над полем K , то кольцо $K[\alpha_1, \dots, \alpha_d]$ изоморфно кольцу многочленов $K[x_1, \dots, x_d]$ от букв $x_1, \dots, x_d$.

Задача 361. Докажите, что базис трансцендентности расширения полей $K \leq K(\theta_1, \dots, \theta_n)$ можно составить из части элементов $\theta_1, \dots, \theta_n$.

Задача 362. Докажите, что произвольное алгебраически независимое множество можно достроить до базиса трансцендентности.

8.11. Целая алгебраическая зависимость

Пусть K и L — коммутативные ассоциативные кольца с единицей, и пусть L является расширением кольца K . Элемент $\lambda \in L$ называется *целым алгебраическим* или просто *целым* над кольцом K , если λ удовлетворяет уравнению

$$\lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_1\lambda + a_0 = 0, \quad a_0, \dots, a_{n-1} \in K,$$

т.е. является корнем многочлена степени n над K со старшим коэффициентом 1. Данное уравнение называется *уравнением целой зависимости* элемента λ от элементов $a_0, \dots, a_{n-1}$. Если λ не является корнем многочлена такого же вида, но меньшей степени, то λ называется *целым алгебраическим элементом степени n* .

Доказательство следующей леммы открывает нам новую роль характеристического многочлена матрицы.

Лемма 8.11.1. Пусть K и L — коммутативные ассоциативные кольца с единицей и кольцо L является K -модулем, порожденным элементами $x_1, \dots, x_n \in L$, т.е.

$$L = \{a_1x_1 + \dots + a_nx_n : a_1, \dots, a_n \in K\}.$$

Тогда каждый элемент кольца L является целым алгебраическим степени не выше n над кольцом K .

$$\lambda x_n = a_{n1}x_1 + \dots + a_{nn}x_n.$$
$$\begin{bmatrix} a_{11} - \lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - \lambda & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} - \lambda \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \dots \\ 0 \end{bmatrix}. \quad (*)$$
$$\widehat{A(\lambda)}A(\lambda) = \det A(\lambda) \cdot I, \quad (**)$$
$$f(\lambda) x_i = 0, \quad 1 \leq i \leq n. \quad (***)$$
$$1 = \alpha_1 x_1 + \dots + \alpha_n x_n, \quad \alpha_1, \dots, \alpha_n \in K.$$

Найдем сумму равенств (***), умножив i -е из них на α_i . В результате

$$f(\lambda) = f(\lambda) \cdot 1 = f(\lambda) \cdot \left(\sum_{i=1}^n \alpha_i x_i \right) = \sum_{i=1}^n \alpha_i f(\lambda) x_i = 0,$$

что и требовалось доказать. $\square$

Лемма 8.11.2. Пусть K — коммутативное ассоциативное кольцо с единицей и кольцо $L = K[x_1, \dots, x_n]$ получено из K кольцевым присоединением целых над K элементов $x_1, \dots, x_n$. Тогда L является конечно порожденным K -модулем.

Доказательство. Пусть $L_0 = K$ и $L_i := K[x_1, \dots, x_i]$. Любой элемент $\theta \in L_i$ имеет вид $\theta = \phi(x)$, где $\phi(X)$ — многочлен от буквы X с коэффициентами из L_{i-1} . В то же время x_i удовлетворяет уравнению целой зависимости $h(x) = 0$, в котором старший коэффициент многочлена $h(X) \in L_{i-1}[X]$ равен 1. Пусть $N = \deg h(X)$. Применив алгоритм деления столбиком, найдем неполное частное $q(X) \in L_{i-1}[X]$ и остаток $r(X) \in L_{i-1}[X]$, дающие разложение

$$\phi(X) = h(X)q(X) + r(X), \quad \text{где } r(X) = 0 \text{ либо } \deg r(X) < N.$$

Поскольку $h(x_i) = 0$, отсюда сразу же вытекает равенство

$$\theta = \phi(x_i) = r(x_i) = a_0 + a_1 x_i + \dots + a_{N-1} x_i^{N-1},$$

$$a_0, \dots, a_{N-1} \in L_{i-1}.$$

Значит, в качестве системы, порождающей модуль L_i над кольцом L_{i-1} , можно взять элементы $1, x_i, \dots, x_i^{N-1}$. Чтобы завершить доказательство, примем во внимание следующее очевидное утверждение относительно трех колец $A \subseteq B \subseteq C$: если C — конечно порожденный B -модуль и B — конечно порожденный A -модуль, то C является конечно порожденным A -модулем. $\square$

Следствие 8.11.1. Пусть K — коммутативное ассоциативное кольцо с единицей и кольцо $L = K[x_1, \dots, x_n]$ получено из K кольцевым присоединением целых над K элементов $x_1, \dots, x_n$. Тогда каждый элемент кольца L является целым над K .

Пусть кольцо K вложено в кольцо L . Множество L_K всех элементов из L , целых над K , называется *целым замыканием* кольца K в кольце L . Если $L_K = L$, то кольцо L называется *целым* над K . Целостное кольцо называется *целозамкнутым*,

если оно совпадает со своим целым замыканием в своем поле частных. Простейший пример — кольцо целых чисел $\mathbb{Z}$.

Лемма 8.11.3. Пусть K и L — коммутативные ассоциативные кольца с единицей. Тогда целое замыкание кольца K в L совпадает с радикалом идеала $\langle K \rangle = KL$ кольца L .

Доказательство. Пусть $\theta \in L$ — целый элемент над K с уравнением целой зависимости $\theta^N + \sum_{i=0}^{N-1} a_i \theta^i = 0$. Тогда $\theta^N \in KL \Rightarrow \theta \in \text{rad}(KL)$. Теперь пусть $\theta \in \text{rad}(KL) \Rightarrow \theta^N \in KL$ для натурального $N \Rightarrow \theta^N = \sum_{i=1}^s a_i b_i$, где $a_i \in K$, $b_i \in L$. Значит, θ^N принадлежит K -модулю с конечной системой порождающих его элементов $b_1, \dots, b_s$. Согласно лемме 8.11.2 каждый элемент конечно порожденного K -модуля цел над $K \Rightarrow \theta^N$ — целый элемент над K . Следовательно, элемент θ цел над K . $\square$

Следствие 8.11.2. Пусть $K \subseteq L$ — коммутативные ассоциативные кольца с единицей. Тогда множество всех элементов из L , целых над K , является подкольцом кольца L .

Лемма 8.11.4. Пусть $K \subseteq L$ — целостные кольца и L цело над K . Тогда для того чтобы K было полем, необходимо и достаточно, чтобы L было полем.

Доказательство. Если K — поле, то нам нужно доказать обратимость произвольного ненулевого элемента $x \in L$. По условию теоремы, x цел над K . Рассмотрим его уравнение целой зависимости:

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0, \quad a_0, \dots, a_{n-1} \in K.$$

Если степень n минимально возможная, то $a_0 \neq 0$ — иначе x был бы делителем нуля в поле K . Любой ненулевой элемент поля K , в том числе a_0 , обратим. Используя обратный к нему элемент, находим

$$xu = 1, \quad u := -a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1).$$

Теперь предположим, что L — поле и $0 \neq x \in K$. Согласно условию, элемент x^{-1} цел над K , т.е. удовлетворяет уравнению целой зависимости

$$(x^{-1})^n + \sum_{i=1}^{n-1} a_i (x^{-1})^i = 0, \quad a_0, \dots, a_{n-1} \in K.$$

Умножив обе части на x^{n-1} , получаем

$$x^{-1} = - \sum_{i=1}^{n-1} a_i x^{n-1-i} \in K. \quad \square$$

Лемма 8.11.5. Пусть $K \subseteq L$ — ассоциативные коммутативные кольца с единицей, L цело над K и p' — простой идеал кольца L . Тогда $p = p' \cap K$ является простым идеалом кольца K и, кроме того, для того чтобы идеал p' был максимальным, необходима и достаточна максимальность идеала p .

Доказательство. Проверка простоты идеала p — это легкое упражнение. Остальное следует из леммы 8.11.4. Чтобы ее применить, заметим, что правило $a + p \rightarrow a + p'$ задает вложение кольца K/p в кольцо L/p' , поэтому в случае $a \in K$ мы имеем право отождествлять вычеты $a + p = [a]_p$ и $a + p' = [a]_{p'}$. В силу простоты p и p' кольца K/p и L/p' целостны. Далее, пусть $x \in L$ и

$$\begin{aligned} x^n + \sum_{i=0}^{n-1} a_i x^i &= 0, \quad a_i \in K \Rightarrow \\ &\Rightarrow [x]_{p'}^n + \sum_{i=0}^{n-1} [a_i]_{p'} [x]_{p'}^i = 0, \quad [a_i]_{p'} = [a_i]_p \in K/p. \end{aligned}$$

Максимальность идеалов p и p' равносильна тому, что соответствующее кольцо вычетов является полем. $\square$

Теорема 8.11.1. Пусть $K \subseteq L$ — ассоциативные коммутативные кольца с единицей и L цело над K . Тогда для любого простого идеала p в K существует простой идеал p' в L такой, что $p = p' \cap K$.

Доказательство. Множество $S = K \setminus p$ мультипликативно замкнуто, и кольцо $S^{-1}K$ вложено в $S^{-1}L$. Возьмем произвольный элемент $s \in S$, и пусть $x \in L$ удовлетворяет уравнению целой зависимости

$$\begin{aligned} x^n + \sum_{i=0}^{n-1} a_i x^i &= 0, \quad a_i \in K \Rightarrow \\ &\Rightarrow (x/s)^n + \sum_{i=0}^{n-1} (a_i/s^{n-i})(x/s)^i = 0, \quad a_i/s^{n-i} \in S^{-1}K. \end{aligned}$$

Мы видим, что кольцо $S^{-1}L$ цело над $S^{-1}K$. Обозначим через m' максимальный идеал кольца $S^{-1}L$. Согласно теореме 8.6.1 идеал m' прост $\Rightarrow$ идеал $m = m' \cap S^{-1}K$ также прост и согласно лемме 8.11.5 является максимальным идеалом в кольце $S^{-1}K = K_p$. Мы знаем, что это кольцо локально, и поэтому m — это его единственный максимальный идеал, имеющий вид $m = \{b/s : b \in p, s \in S\}$.

Пусть $\phi: a \rightarrow a/1$ — естественный гомоморфизм кольца L в кольцо частных $S^{-1}L$ относительно мультипликативно замкнутого множества S . Его сужение на K будет, очевидно, естественным гомоморфизмом кольца K в кольцо частных $S^{-1}K$. Пусть $\phi(a) \in m \Rightarrow a/1 = b/s, b \in p, s \in S \Rightarrow (as - b)s_1 = 0, s_1 \notin p \Rightarrow as - b \in p \Rightarrow as \in p \Rightarrow a \in p$. Значит, $\phi^{-1}(m) = p$. Далее,

$$a \in \phi^{-1}(m) \Leftrightarrow a/1 \in m = m' \cap K_p \Leftrightarrow a \in \phi^{-1}(m') \cap K.$$

Таким образом, $p = \phi^{-1}(m) = \phi^{-1}(m') \cap K$. Нетрудно понять, что полный прообраз простого идеала всегда прост. Поэтому искомым простой идеал p' кольца L имеет вид $\phi^{-1}(m')$. $\square$

Теорема 8.11.2. Пусть $K \subseteq L$ — целостные кольца, кольцо K целостно замкнуто и элемент $\theta \in L$ цел над K . Тогда θ есть алгебраический элемент над полем частных кольца K и его приведенный минимальный многочлен имеет все коэффициенты, принадлежащие кольцу K .

Доказательство. Напомним, что приведенным называется многочлен со старшим коэффициентом 1. Пусть степень приведенного минимального многочлена для θ над полем частных кольца K равна n , и пусть $x_1, \dots, x_n$ — его корни с учетом кратностей и среди них $x_1 = \theta$ (для поля нулевой характеристики все корни, конечно, простые). Корни принадлежат полю разложения этого многочлена, и существует изоморфизм этого поля, при котором $\theta = x_1$ переходит в x_i . Поэтому каждый из корней удовлетворяет уравнению целой зависимости для θ и, следовательно, является целым над K . В силу формул Виета каждый коэффициент минимального многочлена принадлежит кольцу $K[x_1, \dots, x_n]$. Согласно лемме 8.11.2 это кольцо есть конечно порожденный K -модуль, и по лемме 8.11.1 каждый его элемент, в том числе и каждый коэффициент интересующего нас минимального многочлена, цел над K . $\square$

Задача 363. Докажите, что любое факториальное кольцо целостно замкнуто.

Задача 364. Известно, что целостное кольцо L цело над целостным кольцом K и отображение $f: K \rightarrow \mathbb{C}$ является гомоморфизмом. Докажите, что f можно продолжить до гомоморфизма кольца L в $\mathbb{C}$.

8.12. Дифференцирования в кольцах и полях

Наша ближайшая цель — показать, что вычисление степени трансцендентности расширения $K \leq L$ сводится к вычислению размерности некоторого линейного пространства над полем L . Это будет пространство дифференцирований поля L .

Отображение $D: L \rightarrow L$ называется *дифференцированием поля L , аннулирующим поле K* , если оно обладает следующими свойствами:

- $D(a + b) = D(a) + D(b) \quad \forall a, b \in L$;
- $D(ab) = D(a)b + aD(b) \quad \forall a, b \in L$;
- $D(a) = 0 \quad \forall a \in K$.

Множество всех таких отображений обозначим через $\mathcal{D}(L, K)$.

Множество дифференцирований непусто, так как в него заведомо входит *нулевое* отображение, обнуляющее все элементы. Мы скоро увидим, что наличие ненулевых дифференцирований связано с неалгебраичностью расширения $K \leq L$.

Пусть $f(x_1, \dots, x_n)$ — многочлен над L . Его частные производные $\partial f / \partial x_i$ определяются как производные этого же многочлена как многочлена от x_i с коэффициентами из поля рациональных функций от тех же переменных, но без x_i . Через f_D обозначим многочлен, полученный заменой коэффициентов на их образы при дифференцировании D .

Лемма 8.12.1. Пусть $f(a_1, \dots, a_n)$ — значение многочлена f над полем L в точке $(a_1, \dots, a_n) \in L^n$ и D — произвольное дифференцирование поля L . Тогда

$$D(f(a_1, \dots, a_n)) = f_D(a_1, \dots, a_n) + \sum_{i=1}^n \frac{\partial f}{\partial x_i}(a_1, \dots, a_n) D(a_i).$$

Следствие 8.12.1. Пусть расширение $K \leq L$ таково, что любой элемент поля L является корнем многочлена, имеющего коэффициенты из K и только простые корни в своем поле разложения¹⁾. Тогда нулевое дифференцирование

¹⁾ Такое расширение называется сепарабельным алгебраическим расширением.

является единственным дифференцированием, аннулирующим поле K .

Доказательство. Пусть $f(x) \in K[x]$ — минимальный многочлен для алгебраического элемента $\alpha \in L$. Минимальный многочлен неприводим и по условию теоремы имеет только простые корни. Значит, $f'(\alpha) \neq 0$. Поскольку $f(\alpha) = 0$, при дифференцировании находим: $f'(\alpha)D(\alpha) = D(f(\alpha)) = D(0) = 0 \Rightarrow D(\alpha) = 0$. $\square$

Следствие 8.12.2. Если $L = K(\alpha_1, \dots, \alpha_n)$, то дифференцирование $D: L \rightarrow L$, аннулирующее поле K , однозначно определяется значениями $D(\alpha_1), \dots, D(\alpha_n)$.

Доказательство. Поле L состоит из элементов вида

$$\frac{u(\alpha_1, \dots, \alpha_n)}{v(\alpha_1, \dots, \alpha_n)}, \quad u, v \in K[x_1, \dots, x_n], \quad v \neq 0.$$

Из предыдущих утверждений ясно, что значения $D(u(\alpha_1, \dots, \alpha_n))$ и $D(v(\alpha_1, \dots, \alpha_n))$ определены однозначно, если известны значения $D(\alpha_1), \dots, D(\alpha_n)$. Остается принять во внимание формулу

$$D(a/b) = (D(a)b - aD(b))/b^2, \quad b \neq 0, \quad (*)$$

которая выводится непосредственно из второй аксиомы дифференцирования, примененной к произведению $(a/b)b = a$. $\square$

Лемма 8.12.2. Пусть $K \subseteq L$ — ненулевые целостные кольца и D — отображение из L в L такое, что $D(a+b) = D(a) + D(b)$, $D(ab) = D(a)b + aD(b)$ для всех $a, b \in L$ и $D(a) = 0$ для всех $a \in K$. Тогда D может быть продолжено до дифференцирования на поле частных для L с аннулированием поля частных для K .

Доказательство. Искомое отображение определяется формулой (*). Аксиомы дифференцирования проверяются вполне рутинным образом. Для удобства примем обозначение $a' = D(a)$. Тогда

$$\begin{aligned} \left(\frac{a}{b} + \frac{c}{d}\right)' &= \left(\frac{ad+bc}{bd}\right)' = \frac{(ad+bc)'(bd) - (ad+bc)(bd)'}{(bd)^2} = \\ &= \frac{(a'd + ad' + b'c + bc')(bd) - (b'd + bd')(ad+bc)}{(bd)^2} = \\ &= \frac{a'b - ab'}{b^2} + \frac{c'd - cd'}{d^2} = \left(\frac{a}{b}\right)' + \left(\frac{c}{d}\right)'. \end{aligned}$$

Вторая и третья аксиомы проверяются аналогично. $\square$

Теорема 8.12.1. Пусть $L = K(\alpha_1, \dots, \alpha_n)$ и $R < K[x_1, \dots, x_n]$ — идеал алгебраических соотношений между элементами $\alpha_1, \dots, \alpha_n$, включающий все многочлены, обнуляющиеся в точке $(\alpha_1, \dots, \alpha_n)$. Тогда для существования аннулирующего K дифференцирования $D: L \rightarrow L$ с заданными значениями $D(\alpha_1) = c_1, \dots, D(\alpha_n) = c_n$ необходимо и достаточно, чтобы эти значения удовлетворяли системе уравнений

$$\sum_{i=1}^n \frac{\partial f}{\partial x_i} (\alpha_1, \dots, \alpha_n) c_i = 0 \quad \forall f \in R. \quad (**)$$

Доказательство. Необходимость вытекает из леммы 8.12.1. Докажем достаточность. Пусть $c_1, \dots, c_n$ удовлетворяют системе уравнений (**). Сначала определим дифференцирование на элементах вида $u(\alpha_1, \dots, \alpha_n)$, где u — многочлен с коэффициентами из поля K :

$$D(u(\alpha_1, \dots, \alpha_n)) := \sum_{i=1}^n \frac{\partial u}{\partial x_i} (\alpha_1, \dots, \alpha_n) c_i.$$

При наличии алгебраических соотношений между элементами может случиться так, что $u(\alpha_1, \dots, \alpha_n) = v(\alpha_1, \dots, \alpha_n)$ для разных многочленов u и v . Однако, это равносильно условию $u - v \in R$. В этом случае

$$\begin{aligned} D(u(\alpha_1, \dots, \alpha_n)) - D(v(\alpha_1, \dots, \alpha_n)) &= \\ &= \sum_{i=1}^n \frac{\partial (u - v)}{\partial x_i} (\alpha_1, \dots, \alpha_n) c_i = 0. \end{aligned}$$

Таким образом, отображение D определено корректно на кольце элементов вида $u(\alpha_1, \dots, \alpha_n)$. Нетрудно проверить, что при этом выполнены все аксиомы дифференцирования. В силу леммы 8.12.2, с сохранением тех же аксиом отображение D можно доопределить на поле частных для этого кольца. Остается заметить, что это поле частных совпадает с L . $\square$

На множестве дифференцирований $\mathcal{D}(L, K)$ можно естественным образом ввести операцию сложения и операцию умножения дифференцирования на число из поля L . Пусть $D, D_1, D_2 \in \mathcal{D}(L, K)$ и $\alpha \in L$. Тогда по определению

$$(D_1 + D_2)(a) := D_1(a) + D_2(a), \quad (\alpha D)(a) := \alpha D(a) \quad \forall a \in L.$$

Легко проверить, что $D_1 + D_2$ и αD также являются дифференцированиями поля L с аннулированием поля K . Более того, эти операции превращают $\mathcal{D}(L, K)$ в линейное пространство над полем L .

Лемма 8.12.3. *Линейное пространство $\mathcal{D}(L, K)$ над полем L изоморфно линейному пространству решений однородной системы линейных алгебраических уравнений $(**)$ относительно элементов $c_1, \dots, c_n \in L$.*

Лемма является непосредственным следствием теоремы 8.12.1.

Теорема 8.12.2. *Пусть любой неприводимый многочлен с коэффициентами из поля L имеет только простые корни в своем поле разложения, и предположим, что L имеет конечную степень трансцендентности над полем K . Тогда*

$$\dim \mathcal{D}(L, K) = \text{trdeg}(L : K).$$

Доказательство. Пусть элементы $\zeta_1, \dots, \zeta_d \in L$ образуют базис трансцендентности расширения $K \leq L$. В силу леммы 8.12.3, $\dim \mathcal{D}(L_1, K) = d$, где $L_1 := K(\zeta_1, \dots, \zeta_d)$ и расширение $L_1 \leq L$ удовлетворяет предположениям следствия 8.12.1. Отсюда вытекает, что любое дифференцирование $D \in \mathcal{D}(L_1, K)$ однозначно продолжается до дифференцирования из $\mathcal{D}(L, K)$, поэтому $\mathcal{D}(L, K) \cong \mathcal{D}(L_1, K)$. $\square$

Задача 365. *Докажите, что множество всех элементов из поля L , которые при фиксированном дифференцировании переходят в нуль, является подполем поля L .*

Задача 366. *Докажите, что существует бесконечно много разных дифференцирований поля $\mathbb{R}$, аннулирующих поле $\mathbb{Q}$.*

8.13. Теорема Гильберта о базисе

Теорема Гильберта о базисе утверждает, что в кольце многочленов от конечного числа переменных над произвольным полем любой идеал является конечно порожденным¹⁾. В современной,

¹⁾ Реакция некоторых современников Гильберта в связи с опубликованным им доказательством была, по-видимому, чрезмерно бурной: «это не математика, а теология» (Гордан), использованные методы «неудобны, чудовищны, сверхъестественны» (Линдемман).

несколько более общей формулировке этот результат выглядит следующим образом.

Теорема 8.13.1. *Кольцо многочленов $K[x]$ над любым нётеровым кольцом K является нётеровым.*

Доказательство. Рассмотрим произвольный идеал R в кольце $K[x]$. Обозначим через $a_i(f)$ коэффициент многочлена $f(x)$ при x^i и введем множества

$$J_i := \{a_i(f) \in K : f(x) \in R, \deg f = i\} \cup \{0\}, \quad i = 0, 1, \dots$$

Легко видеть, что J_i является идеалом в K и, кроме того, $J_0 \subseteq J_1 \subseteq \dots$. Тогда объединение $J = \bigcup J_i$ является конечно порожденным идеалом и, следовательно, совпадает с J_n для какого-то n . Значит, $J_i = J_n = J$ при $i \geq n$. В идеале J_i выберем систему порождающих его элементов $a_j^{(i)}$, $1 \leq j \leq s_i$, и зафиксируем соответствующие им многочлены $a_j^{(i)} = a_i(f_j^{(i)})$, $\deg f_j^{(i)} = i$, $1 \leq j \leq s_i$. Положим

$$G := \{f_j^{(i)} \in R : 1 \leq j \leq s_i, 0 \leq i \leq n\}$$

и докажем, что если $f(x) \in R$, то непременно $f(x) \in \langle G \rangle$. Проведем индукцию по степени многочлена $f(x)$. Пусть утверждение уже доказано для всех многочленов степени m и ниже, и пусть $f(x)$ — произвольный многочлен степени $m+1$. Тогда старший коэффициент многочлена $f(x)$ принадлежит J_l , где $l = \min(m+1, n)$. В силу нётеровости кольца K

$$a_{m+1}(f) = \sum_{j=1}^{s_l} c_j a_l(f_j^{(l)}), \quad c_j \in K, \quad \deg f_j^{(l)} = l, \quad 1 \leq j \leq s_l.$$

Положим

$$g(x) := \sum_{j=1}^{s_l} c_j f_j^{(l)}(x) \in \langle G \rangle.$$

Старшие коэффициенты $f(x)$ и $g(x)$ равны. Поэтому многочлен $f(x) - x^{m+1-l}g(x) \in R$ имеет степень m или ниже. По индуктивному предположению $f(x) - x^{m+1-l}g(x) \in \langle G \rangle$ и, следовательно, $f(x) \in \langle G \rangle$. $\square$

Следствие 8.13.1. *Для произвольного поля K кольцо $K[x_1, \dots, x_n]$ нётерово.*

Полезное применение теоремы связано с системой уравнений (***) из предыдущего раздела. В общем случае в этой си-

стеме бесконечное число уравнений, однако каждое уравнение определяется многочленом из идеала в нётеровом кольце, и поэтому система равносильна некоторой подсистеме, состоящей из конечного числа уравнений.

Задача 367. Известно, что кольцо $K[x]$ нётерово. Следует ли отсюда нётеровость кольца K ?

Задача 368. Пусть L — множество формальных степенных рядов вида $f(x) = \sum_{i=0}^{\infty} a_i x^i$ с коэффициентами из поля K .

Если $g(x) = \sum_{i=0}^{\infty} b_i x^i$, то сложение рядов и их умножение определяется правилами

$$f(x) + g(x) := \sum_{i=0}^{\infty} (a_i + b_i) x^i, \quad f(x)g(x) := \sum_{i=0}^{\infty} \left(\sum_{j=0}^i a_j b_{i-j} \right) x^i.$$

Докажите, что множество L с операциями сложения и умножения рядов является коммутативным ассоциативным кольцом с единицей¹⁾. Будет ли оно нётеровым?

Задача 369. Докажите, что множество минимальных простых идеалов (минимальность означает, что никакой строго меньший идеал не является простым) нётерова кольца конечно.

Задача 370. Пусть K — произвольное поле и L — его расширение, R — идеал кольца $K[x_1, \dots, x_n]$ и $\langle R \rangle_L$ — идеал кольца $L[x_1, \dots, x_n]$, порожденный множеством R . Докажите, что $\langle R \rangle_L \cap K[x_1, \dots, x_n] = R$.

8.14. Деление с остатком и базисы Грёбнера

Пусть K — произвольное поле и нас интересуют идеалы в кольце $K[x_1, \dots, x_n]$. Мы теперь знаем, что каждый из них является конечно порожденным, т.е. имеет вид $J = \langle f_1, \dots, f_s \rangle$. Система $f_1, \dots, f_s$ называется *базисом* идеала J . Конечно, базисов может быть много и, более того, в них может быть разное число многочленов.

Рассмотрим совершенно законный вопрос: если задан произвольный многочлен $f(x_1, \dots, x_n)$, то как узнать, принадлежит ли

¹⁾ Стандартное обозначение для кольца рядов: $K[[x]]$.

он идеалу J ? Можно ли вообще это сделать за конечное число арифметических операций с коэффициентами многочленов? Положительный ответ получен Бухбергером, и он существенно опирается на использование специальных базисов, которые он назвал *базисами Грёбнера* (в честь своего учителя).

Для дальнейших построений выберем некоторый порядок на множестве ненулевых одночленов (мономов), входящих в состав многочленов. Нам важно, чтобы множество мономов оказалось вполне упорядоченным множеством и чтобы порядок сохранялся при умножении мономов на один и тот же моном. Порядок с означенными свойствами называется *мономиальным*. Уже известный нам словарный (лексикографический) порядок этими свойствами обладает. Обычно считается, что $x_1 > x_2 > \dots > x_n$. Однако мы можем выбрать подстановку σ и потребовать, чтобы $x_{\sigma(1)} > x_{\sigma(2)} > \dots > x_{\sigma(n)}$, — в результате получится новая версия словарного порядка. Еще один популярный пример мономиального порядка: считается, что моном больше любого монома меньшей степени, а на каждом подмножестве мономов одной и той же степени вводится словарный порядок. Ниже будем полагать, что используется стандартный словарный порядок.

Для старшего члена многочлена $\phi \in K[x_1, \dots, x_n]$ примем обозначение

$$\text{LT}(\phi) = a x_1^{\alpha_1} \dots x_n^{\alpha_n}, \quad 0 \neq a \in K,$$

и введем понятие (старшей) *мультистепени* многочлена:

$$\text{multideg}(\phi) := (\alpha_1, \dots, \alpha_n).$$

Мы полагаем, что неравенство $(\alpha_1, \dots, \alpha_n) \geq (\beta_1, \dots, \beta_n)$ понимается в смысле словарного порядка (в общем случае можно выбрать и зафиксировать произвольный мономиальный порядок).

Пусть $f \in K[x_1, \dots, x_n]$ и задана произвольная система ненулевых многочленов $f_1, \dots, f_s \in K[x_1, \dots, x_n]$. Система многочленов $Q = (q_1, \dots, q_s)$ и многочлен r называются *неполным частным и остатком при делении f на систему $F = (f_1, \dots, f_s)$* , если:

- $f = f_1 q_1 + \dots + f_s q_s + r$,
- $\text{multideg}(f_i q_i) \leq \text{multideg}(f)$, $1 \leq i \leq s$,
- ни один одночлен в составе многочлена r не делится ни на один старший член многочленов $f_1, \dots, f_s$.

Обозначение: $r = \text{REM}(f : F) = \text{REM}(f : f_1, \dots, f_s)$. Заметим, что определение остатка существенно опирается на то, как упорядочены одночлены, и в общем случае неполное частное и остаток не определяются однозначно.

Прежде всего нам нужно доказать, что хотя бы одно представление указанного выше вида существует. Для этого сформулируем *алгоритм деления с остатком*, обобщающий деление столбиком:

1) Полагаем

$$k := 0, \quad h^0 := f, \quad Q^0 = (q_1^0, \dots, q_s^0) := (0, \dots, 0), \quad r^0 := 0.$$

2) Если $h^k = 0$, то работа алгоритма завершается, при этом $Q := Q^k$ и $r := r^k$.

3) Пусть $h^k \neq 0$ и уже определены h^k , $Q^k = (q_1^k, \dots, q_s^k)$, r^k . Находим множество N_k номеров $i \in \{1, \dots, s\}$ таких, что $\text{LT}(h^k) : \text{LT}(f_i)$.

4) Если $N_k = \emptyset$, то полагаем

$$Q^{k+1} := Q^k, \quad r^{k+1} := r^k + \text{LT}(h^k), \quad h^{k+1} := h^k - \text{LT}(h^k).$$

Если $N_k \neq \emptyset$, то находим минимальный номер i в множестве N_k и полагаем

$$q_i^{k+1} := q_i^k + \frac{\text{LT}(h^k)}{\text{LT}(f_i)}, \quad h^{k+1} := h^k - \frac{\text{LT}(h^k)}{\text{LT}(f_i)} f_i, \\ q_j^{k+1} := q_j^k \text{ при } j \neq i, \quad r^{k+1} := r^k.$$

5) Полагаем $k := k + 1$ и переходим к пункту 2.

Смысл алгоритма такой: если старший член f делится на старший член какого-то f_i , то выполняем деление так же, как при делении столбиком, в противном случае рассмотренный старший член f отправляем в остаток. На каждом шаге f меняется и теряет очередной старший член.

Утверждение 8.14.1. *Алгоритм деления с остатком находит неполное частное и остаток за конечное число шагов.*

Система многочленов $f_1, \dots, f_s$ называется *базисом Грёбнера* идеала J , если старший член любого многочлена из J делится на старший член хотя бы одного из многочленов этой системы.

Лемма 8.14.1. *Пусть система многочленов $f_1, \dots, f_s$ образует базис Грёбнера идеала J и f — произвольный многочлен. Тогда остаток от деления f на $(f_1, \dots, f_s)$ определяется*

однозначно и не зависит от порядка многочленов $f_1, \dots, f_s$. Более того,

$$f \in J \Leftrightarrow \text{REM}(f : f_1, \dots, f_s) = 0.$$

Доказательство. Допустим, что имеются два разных остатка, r_1 и r_2 , для одного и того же многочлена f . Тогда $r_1 - r_2 \in J$. Поэтому старший член многочлена $r_1 - r_2$ делится на старший член хотя бы одного из многочленов $f_1, \dots, f_s$, что невозможно, так как этим свойством не обладает ни один из одночленов в составе r_1 или r_2 . Следовательно, $r_1 - r_2 = 0$.

Далее, пусть $f \in J$ и $r = \text{REM}(f : f_1, \dots, f_s)$. Ясно, что $r \in J \Rightarrow$ старший одночлен в составе r делится на старший член хотя бы одного из многочленов $f_1, \dots, f_s$, что противоречит определению остатка, если $r \neq 0$. Значит, $r = 0$. Обратное очевидно: если $r = 0$, то $f \in J$. $\square$

Чтобы доказать существование базиса Грёбнера, нам нужно понятие *мономиального идеала*. Так называется идеал, порожденный конечной или бесконечной системой мономов (ненулевых одночленов).

Утверждение 8.14.2. Для того чтобы многочлен f принадлежал мономиальному идеалу, необходимо и достаточно, чтобы каждый моном в составе f делился хотя бы на один из мономов системы, порождающей данный идеал.

Доказательство. Пусть $cx_1^{\gamma_1} \dots x_n^{\gamma_n}$ — произвольный член в составе f . Тогда

$cx_1^{\gamma_1} \dots x_n^{\gamma_n} = ax_1^{\alpha'_1} \dots x_n^{\alpha'_n} x_1^{\alpha_1} \dots x_n^{\alpha_n} + \dots + bx_1^{\beta'_1} \dots x_n^{\beta'_n} x_1^{\beta_1} \dots x_n^{\beta_n}$, где все числовые коэффициенты ненулевые, а $x_1^{\alpha_1} \dots x_n^{\alpha_n}, \dots, x_1^{\beta_1} \dots x_n^{\beta_n}$ — какая-то конечная подсистема мономов из тех, которые порождают заданный идеал. При этом, конечно же,

$x_1^{\gamma_1} \dots x_n^{\gamma_n} = x_1^{\alpha'_1} \dots x_n^{\alpha'_n} x_1^{\alpha_1} \dots x_n^{\alpha_n} = \dots = x_1^{\beta'_1} \dots x_n^{\beta'_n} x_1^{\beta_1} \dots x_n^{\beta_n}$, т.е. одночлен $cx_1^{\gamma_1} \dots x_n^{\gamma_n}$ делится на каждый из мономов $x_1^{\alpha_1} \dots x_n^{\alpha_n}, \dots, x_1^{\beta_1} \dots x_n^{\beta_n}$. $\square$

Лемма 8.14.2 (лемма Диксона). Любой мономиальный идеал порождается конечной подсистемой из порождающих его мономов.

Доказательство можно провести по индукции по аналогии с теоремой Гильберта о базисе. Кроме того, отметим наглядный характер леммы Диксона в случае $n = 2$. Моном $x_1^i x_2^j$ соот-

ветствует точке (i, j) неотрицательного квадранта на плоскости, а множество порождаемых им мономов — целым точкам с первой координатой не меньше i и второй координатой не меньше j . Все множество мономов мономиального идеала есть объединение всех таких областей, и геометрически очевидно, что даже при бесконечном числе областей оно всегда может быть получено объединением лишь *конечного числа* из них.

Теорема 8.14.1. *Любой идеал в кольце многочленов $K[x_1, \dots, x_n]$ над полем K обладает базисом Грёбнера.*

Доказательство. Обозначим через $\text{LT}(J)$ множество старших членов всех многочленов, входящих в идеал J . По лемме Диксона, идеал $\hat{J} := \langle \text{LT}(J) \rangle$ имеет базис, составленный из конечного числа порождающих его мономов. Обозначим через $f_1, \dots, f_s$ многочлены, для которых эти мономы являются старшими членами. Система $f_1, \dots, f_s$ и будет искомым базисом Грёбнера. В самом деле, старший член многочлена $f \in J$ делится на старший член хотя бы одного из многочленов $f_1, \dots, f_s$ и в то же время система $f_1, \dots, f_s$ порождает J . $\square$

В следующем разделе мы дадим другое, конструктивное доказательство существования базиса Грёбнера.

Задача 371. Пусть $f \notin \langle x_1, \dots, x_n \rangle \subset K[x_1, \dots, x_n]$, где K — произвольное поле. Докажите, что $\langle x_1, \dots, x_n, f \rangle = K[x_1, \dots, x_n]$.

Задача 372. Базис Грёбнера называется *редуцированным*, если каждый из старших коэффициентов входящих в него многочленов равен 1 и для каждого многочлена базиса ни один из одночленов в его составе не делится на старший коэффициент какого-либо другого многочлена этого базиса. Докажите, что редуцированный базис Грёбнера определяется однозначно с точностью до порядка многочленов в базисе.

8.15. Критерий Бухбергера

Рассмотрим ненулевые многочлены f и g и назовем *многочленом сизигии* или *S -многочленом* для них многочлен вида

$$S(f, g) := \frac{h}{\text{LT}(f)} f - \frac{h}{\text{LT}(g)} g,$$

где $h := x_1^{\gamma_1} \dots x_n^{\gamma_n}$ есть моном наименьшей мультистепени, который делится на каждый из одночленов $\text{LT}(f)$ и $\text{LT}(g)$.

Пример. $S(2x_1x_2 + x_2^3, x_1^2 + x_1x_2) =$

$$\frac{x_1^2x_2}{2x_1x_2}(2x_1x_2 + x_2^3) - \frac{x_1^2x_2}{x_1^2}(x_1^2 + x_1x_2) = \frac{1}{2}x_1x_2^3 - x_1x_2^2.$$

Смысл сизигий хорошо объясняется следующей леммой.

Лемма 8.15.1. Пусть многочлены $f_1, \dots, f_s$ над полем K имеют одну и ту же мультистепень β , а их линейная комбинация $f = c_1f_1 + \dots + c_sf_s$ с коэффициентами $c_1, \dots, c_s \in K$ имеет строго меньшую мультистепень. Тогда

$$f = \sum_{i \neq j} c_{ij}S(f_i, f_j), \quad c_{ij} \in K, \quad \text{multideg}(S(f_i, f_j)) < \beta.$$

Доказательство. Пусть $d_i \in K$ — старший коэффициент многочлена f_i и $h_i := f_i/d_i$. Тогда $h_i - h_j = S(f_i, f_j)$ и $c_1d_1 + \dots + c_sd_s = 0$. Следовательно,

$$\begin{aligned} f = \sum_{i=1}^s c_id_ih_i &= \sum_{i=1}^{s-1} \left(\sum_{j=1}^i c_jd_j \right) (h_i - h_{i+1}) = \\ &= \sum_{i=1}^{s-1} \left(\sum_{j=1}^i c_jd_j \right) S(f_i, f_{i+1}). \quad \square \end{aligned}$$

Теорема 8.15.1 (КРИТЕРИЙ БУХБЕРГЕРА). Система $f_1, \dots, f_s$ является базисом Грёбнера идеала, который порождается этой системой, в том и только том случае, когда остаток при делении любого многочлена сизигии для f_i и f_j при $i \neq j$ на систему $(f_1, \dots, f_s)$ равен нулю.

Доказательство. Необходимость следует из леммы 8.14.1. Для доказательства достаточности рассмотрим произвольный многочлен $f \in J := \langle f_1, \dots, f_s \rangle$ мультистепени $\alpha = \text{multideg}(f)$ и его запись в виде

$$f = \sum_{i=1}^s f_i g_i \quad (\Delta)$$

с минимально возможным значением величины

$$\beta := \max_{1 \leq i \leq s} \text{multideg}(f_i g_i).$$

Ясно, что $\alpha \leq \beta$. Если $\alpha = \beta$, то старший член f делится на старший член какого-то из многочленов f_i . Если это верно для

любого многочлена $f \in J$, то система $f_1, \dots, f_s$ является базисом Грёбнера для J , что и требуется доказать.

Допустим, что $\alpha < \beta$, и покажем, что в этом случае найдется разложение вида (Δ) , для которого максимальная мультистепень слагаемых строго меньше β . Это будет противоречить определению величины β . Таким образом, равенство $\alpha = \beta$ будет установлено и, следовательно, теорема будет доказана.

Положим $\beta_i := \text{multideg}(f_i g_i)$ и запишем f в виде

$$f = \sum_{\beta_i = \beta} f_i \text{LT}(g_i) + \sum_{\beta_i = \beta} f_i (g_i - \text{LT}(g_i)) + \sum_{\beta_i < \beta} f_i g_i.$$

Максимальная мультистепень слагаемых второй и третьей сумм строго меньше β . Обозначим первую сумму через A . Согласно лемме 8.15.1,

$$A = \sum_{i \neq j} c_{ij} S(f_i \text{LT}(g_i), f_j \text{LT}(g_j)), \quad c_{ij} \in K.$$

Пусть $\text{LT}(f_i) = c_i \widehat{f}_i$, $\text{LT}(g_i) = d_i \widehat{g}_i$, $c_i, d_i \in K$. Тогда $\widehat{g}_i \widehat{f}_i = \widehat{g}_j \widehat{f}_j$, и мы получаем

$$\begin{aligned} S(f_i \text{LT}(g_i), f_j \text{LT}(g_j)) &= \frac{\widehat{g}_i \widehat{f}_i}{d_i \widehat{g}_i \text{LT}(f_i)} d_i \widehat{g}_i f_i - \frac{\widehat{g}_j \widehat{f}_j}{d_j \widehat{g}_j \text{LT}(f_j)} d_j \widehat{g}_j f_j = \\ &= h_{ij} S(f_i, f_j), \end{aligned}$$

причем

$$\text{multideg}(h_{ij}) < \beta - \gamma_{ij}, \quad \gamma_{ij} := \text{multideg}(S(f_i, f_j)).$$

Наступает момент, когда мы готовы использовать предположение о том, что многочлен $S(f_i, f_j)$ при делении на систему $(f_1, \dots, f_s)$ дает нулевой остаток. Это означает, что

$$S(f_i, f_j) = \sum_{k=1}^s f_k q_{ijk}, \quad \text{multideg}(f_k q_{ijk}) \leq \gamma_{ij},$$

где неравенство для мультистепеней есть следствие утверждения 8.14.1 об алгоритме деления с остатком. Итак,

$$A = \sum_{i \neq j} \sum_{k=1}^s c_{ij} h_{ij} q_{ijk} f_k, \quad c_{ij} \in K.$$

При этом

$$\text{multideg}(h_{ij}(q_{ijk}f_k)) < (\beta - \gamma_{ij}) + \gamma_{ij} = \beta.$$

Мы получаем противоречие с минимальностью β . $\square$

Доказанный критерий подсказывает, как можно построить алгоритм вычисления базиса Грёбнера. В его формулировке ниже мы используем один и тот же символ для обозначения системы многочленов и множества многочленов данной системы, при этом порядок многочленов в системе при выполнении деления с остатком может быть каждый раз произвольным.

Алгоритм 8.15.1 (АЛГОРИТМ БУХБЕРГЕРА). *По заданной системе многочленов $F = \{f_1, \dots, f_s\}$ вычисляется базис Грёбнера $G = \{g_1, \dots, g_t\}$ идеала $J = \langle f_1, \dots, f_s \rangle$.*

1) $H := F$.

2) $G := H$.

3) Для каждой пары многочленов $p, q \in H$, $p \neq q$, нужно вычислить остаток r при делении многочлена сизигии $S(p, q)$ на систему G и, если $r \neq 0$, то $H := H \cup \{r\}$.

4) Если $H = G$, то алгоритм завершает работу, иначе все повторяется начиная с пункта 2.

Утверждение 8.15.1. *Алгоритм Бухбергера завершает работу за конечное число шагов, при этом система многочленов из последнего построенного множества G является искомым базисом Грёбнера.*

Доказательство. Предположим, что множество G строго расширяется после каждого цикла вычислений. Тогда идеал, порожденный его старшими членами, также каждый раз расширяется. В самом деле, если $r \neq 0$, то r не делится на старший член ни одного из многочленов множества G . В то же время, в силу теоремы Гильберта о базисе, бесконечной строго расширяющейся последовательности идеалов быть не может. Значит, рано или поздно выполнится равенство $H = G$ и в этом случае алгоритм завершит работу. Согласно критерию Бухбергера, полученная система G будет базисом Грёбнера идеала $\langle G \rangle$. $\square$

Заметим, что есть много возможностей, чтобы сделать приведенный выше алгоритм более эффективным на практике. Для этого, в частности, используется общее понятие сизигии старших членов системы многочленов $f_1, \dots, f_s$. Сизигией для дан-

ной системы называют систему многочленов $g_1, \dots, g_s$, для которых имеет место равенство

$$\sum_{i=1}^s \text{LT}(f_i)g_i = 0.$$

Для практических вычислений обычно применяются алгоритмы Фожера. Тем не менее рост числа многочленов при построении базиса Грёбнера путем расширения какого-то заданного базиса идеала является серьезной и, по-видимому, непреодолимой проблемой.

Задача 373. Докажите, что остаток при делении на базис Грёбнера не зависит от порядка многочленов в базисе.

Задача 374. Пусть принят словарный (лексикографический) порядок мономов, при котором $x > y > z$. Найдите базис Грёбнера идеалов $I = \langle x - y, y - z \rangle$ и $J = \langle x + y, x - z \rangle$.

АЛГЕБРАИЧЕСКИЕ МНОГООБРАЗИЯ

9.1. Множества нулей и аннуляторы

Множество $V \subseteq K^n$ называется *алгебраическим многообразием*, если оно является множеством *всех общих нулей* конечной системы полиномиальных уравнений

$$f_1(X_1, \dots, X_n) = 0,$$

$$\dots\dots\dots$$

$$f_m(X_1, \dots, X_n) = 0,$$

где $f_1, \dots, f_m$ — многочлены от n переменных с коэффициентами из поля K . Обозначение: $V = \mathcal{V}(f_1, \dots, f_m)$.

В книгах по алгебраической геометрии переменные многочлена f часто обозначаются большими буквами $X_1, \dots, X_n$. Переменная X_i связывается с i -й координатой в пространстве K^n , поэтому само пространство точек нередко обозначается через $K_{X_1, \dots, X_n}$. Иногда вводится мультибуква $X = (X_1, \dots, X_n)$ и возникают обозначения $f(X) := f(X_1, \dots, X_n)$, $K[X] := K[X_1, \dots, X_n]$, $K_X := K_{X_1, \dots, X_n}$.

Очевидно, самое большое алгебраическое многообразие порождается нулевым многочленом $f = 0$ и совпадает с $K^n = \mathcal{V}(0)$. По определению, пустое множество также считается алгебраическим многообразием. Оно порождается любой системой многочленов, которые не имеют общих нулей, например $\emptyset = \mathcal{V}(1)$. Алгебраическое многообразие $\mathcal{V}(f)$, порождаемое одним ненулевым многочленом f , называется *гиперповерхностью*.

Теперь возьмем произвольное множество $S \subseteq K^n$. Множество всех обнуляющих его многочленов

$$\mathcal{I}(S) := \{f(X) \in K[X] : f(\xi) = 0 \ \forall \xi \in S\}$$

называется *аннулятором* данного множества. Для произвольного множества многочленов $P \subseteq K[X]$ множество всех общих для них нулей

$$\mathcal{V}(P) := \{\xi \in K^n : f(\xi) = 0 \ \forall f(X) \in P\}$$

называется *множеством нулей* для P .

Утверждение 9.1.1. Для произвольного множества точек $S \subseteq K^n$ его аннулятор $\mathcal{I}(S) \subseteq K[X]$ является идеалом кольца $K[X]$. Для произвольного множества многочленов $P \subseteq K[X]$ его множество нулей $\mathcal{V}(P)$ является алгебраическим многообразием в пространстве K^n . Всегда справедливы включения

$$S \subseteq \mathcal{V}(\mathcal{I}(S)), \quad P \subseteq \mathcal{I}(\mathcal{V}(P)).$$

Доказательство. Отметим только нетривиальную часть: в силу теоремы Гильберта о базисе любой идеал в $K[X]$ порождается конечной системой многочленов и для идеала $J := \langle P \rangle$ эти многочлены можно выбрать из множества P . Пусть $J = \langle f_1, \dots, f_s \rangle$, где $f_1, \dots, f_s \in P$. Произвольный многочлен $f \in P \subseteq J$ записывается в виде $f = f_1 g_1 + \dots + f_s g_s$ для каких-то многочленов $g_1, \dots, g_s \in K[X]$. Отсюда ясно, что если $f_1(\xi) = \dots = f_s(\xi) = 0$, то $f(\xi) = 0$ для любого многочлена $f \in P$. $\square$

Утверждение 9.1.2. Алгебраическое многообразие V совпадает с множеством нулей его аннулятора: $\mathcal{V}(\mathcal{I}(V)) = V$.

Доказательство. Пусть V — множество нулей идеала I и пусть $\xi \in \mathcal{V}(\mathcal{I}(V))$, т.е. точка ξ обнуляется каждым многочленом из $\mathcal{I}(V)$, а поэтому и каждым многочленом из $I \subseteq \mathcal{I}(V)$. Следовательно, $\xi \in V$. Таким образом, $\mathcal{V}(\mathcal{I}(V)) \subseteq V \subseteq \mathcal{V}(\mathcal{I}(V))$. Второе включение содержится в утверждении 9.1.1. $\square$

Утверждение 9.1.3. Аннулятор $I = \mathcal{I}(S)$ произвольного множества точек S является радикальным идеалом.

Доказательство. Если $f^N(\xi) = 0$, то, очевидно, $f(\xi) = 0$. $\square$

Следствие 9.1.1. Если I — нерадикальный идеал, то $I \neq \mathcal{I}(\mathcal{V}(I))$.

Если идеал $I \subseteq K[X]$ радикальный и поле K алгебраически замкнуто, то всегда имеет место равенство $I = \mathcal{I}(\mathcal{V}(I))$. Это уже весьма нетривиальное утверждение, эквивалентное знаменитой теореме Гильберта о нулях. Оно будет доказано в последующих разделах, а пока мы займемся более простыми наблюдениями.

Утверждение 9.1.4. *Пересечение любого числа и объединение конечного числа алгебраических многообразий также являются алгебраическими многообразиями.*

Доказательство. Пусть $V = \bigcap_{\alpha} V_{\alpha}$ и $V_{\alpha} = \mathcal{V}(P_{\alpha})$, где $P_{\alpha} = \{f_{1,\alpha}, \dots, f_{n_{\alpha},\alpha}\}$. Тогда очевидно, что $V = \mathcal{V}(\bigcup_{\alpha} P_{\alpha})$ и, согласно утверждению 9.1.1, множество V является алгебраическим многообразием. В случае объединения достаточно рассмотреть случай двух многообразий: если $V_1 = \mathcal{V}(f_1, \dots, f_s)$, $V_2 = \mathcal{V}(g_1, \dots, g_t)$, то

$$V_1 \cup V_2 = \mathcal{V}(P), \quad P = \{f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t\}.$$

Ясно, что $V_1 \cup V_2 \subseteq \mathcal{V}(P)$. Теперь предположим, что $\xi \in \mathcal{V}(P)$. Если $g_j(\xi) = 0$ для всех j , то $\xi \in V_2$. Если $g_j(\xi) \neq 0$ для какого-то j , то из равенств $f_i(\xi)g_j(\xi) = 0$ находим $f_i(\xi) = 0$ для всех $i \Rightarrow \xi \in V_1 \cup V_2$. $\square$

Полученное утверждение показывает, что система алгебраических многообразий обладает всеми свойствами абстрактных замкнутых множеств в топологии. Система $\mathcal{T}$ подмножеств в K^n называется *топологией замкнутых множеств*, если: (а) пустое множество и все пространство K^n входят в $\mathcal{T}$; (б) пересечение произвольного числа множеств из $\mathcal{T}$ принадлежит $\mathcal{T}$; (с) объединение любого конечного числа множеств из $\mathcal{T}$ принадлежит $\mathcal{T}$. Таким образом, алгебраические многообразия задают некоторую топологию, в которой они и только они объявляются замкнутыми (*алгебраически замкнутыми*) множествами, а их дополнения в K^n — открытыми (*алгебраически открытыми*) множествами. Эта топология называется *топологией Зарисского*.

Пересечение всех алгебраических многообразий, содержащих заданное множество $S \subseteq K^n$, называется *алгебраическим замыканием* множества S . Ясно, что оно является минимальным алгебраическим многообразием, в которое входят все точки из множества S . Для алгебраического замыкания множества S мы будем использовать обозначение $\bar{S}$.

Утверждение 9.1.5. *Алгебраическое замыкание множества $S \subseteq K^n$ совпадает с множеством нулей его аннулятора:*

$$\bar{S} = \mathcal{V}(\mathcal{I}(S)).$$

Доказательство. Пусть $S \subseteq W \subseteq V := \mathcal{V}(\mathcal{I}(S))$, где W — алгебраическое многообразие. Тогда

$$\mathcal{I}(S) \supseteq \mathcal{I}(W) \supseteq \mathcal{I}(V) \Rightarrow V = \mathcal{V}(\mathcal{I}(S)) \subseteq \mathcal{V}(\mathcal{I}(W)) \subseteq \mathcal{V}(\mathcal{I}(V)).$$

В силу утверждения 9.1.4 находим: $V = \mathcal{V}(\mathcal{I}(V))$ и $W = \mathcal{V}(\mathcal{I}(W))$. Таким образом,

$$V \subseteq W \subseteq V \Rightarrow W = V. \quad \square$$

Задача 375. Является ли идеал $\langle xy \rangle$ аннулятором своего множества нулей?

Задача 376. Идеалы I и J порождают алгебраические многообразия $V = \mathcal{V}(I)$ и $W = \mathcal{V}(J)$. Докажите, что $V \cup W = \mathcal{V}(I \cap J)$ и $V \cap W = \mathcal{V}(I + J)$.

Задача 377. Даны алгебраические многообразия V и W . Верно ли, что $\mathcal{I}(V \cup W) = \mathcal{I}(V) \cap \mathcal{I}(W)$ и $\mathcal{I}(V \cap W) = \mathcal{I}(V) + \mathcal{I}(W)$?

Задача 378. Докажите, что алгебраическое замыкание объединения конечного числа множеств равно объединению их алгебраических замыканий.

Задача 379. В пространстве $\mathbb{R}^2$ найдите алгебраическое замыкание круга

$$S = \{(x_1, x_2) \in \mathbb{R}^2: x_1^2 + x_2^2 < 1\}.$$

9.2. Условие совместности

Непустота алгебраического многообразия $V = \mathcal{V}(f_1, \dots, f_s)$ — это вопрос о совместности системы полиномиальных уравнений. Если K — поле коэффициентов заданных многочленов, то общих нулей в пространстве K^n может и не быть. Но они могут появиться в пространстве L^n над полем L , которое является расширением поля K .

Если $\langle f_1, \dots, f_s \rangle = K[X] \equiv K[X_1, \dots, X_n]$, то общего нуля в K^n заведомо нет: многочлен-константа $1 \in K[X]$ не обращается в нуль ни в одной точке. По той же причине общий нуль не может появиться ни при каком расширении поля K .

Идеал $I \leq K[X]$ в общем случае не будет идеалом кольца $L[X]$, но, безусловно, $I \subseteq L[X]$. Ясно, что множество точек

$$\mathcal{V}_L(I) := \{\xi \in L^n: f(\xi) = 0 \forall f \in I\}$$

является алгебраическим многообразием пространства L^n , а для произвольного множества точек $S \subseteq L^n$ множество многочленов

$$\mathcal{I}_K(S) := \{f \in K[X] : f(\xi) = 0 \ \forall \xi \in S\}$$

является идеалом в $K[X]$.

Теорема 9.2.1. Пусть K — произвольное поле. Для идеала I в кольце $K[X]$ алгебраическое многообразие $\mathcal{V}_L(I)$ является непустым хотя бы для одного расширения L поля K в том и только том случае, когда $I \neq K[X]$.

Доказательство. Мы уже знаем, что если $I = K[X]$, то общего нуля нет ни при каком расширении поля K . Пусть $I \neq K[X] \equiv K[X_1, \dots, X_n]$. По теореме 8.6.3, в этом случае I принадлежит какому-то максимальному идеалу R , а согласно теореме 8.6.2, кольцо вычетов $K[X]/R$ является полем. Это и будет искомое поле L . Оно содержит вычеты, порожденные многочленами-константами, т. е. элементами поля K , — поэтому можно считать, что K вложено в L . Искомый нуль определяется вычетами

$$x_1 = [X_1], \quad \dots, \quad x_n = [X_n].$$

В самом деле, для произвольного многочлена

$$f(X_1, \dots, X_n) = \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n} \in R$$

получаем

$$\begin{aligned} f(x_1, \dots, x_n) &= \sum [a_{i_1, \dots, i_n}] [X_1]^{i_1} \dots [X_n]^{i_n} = \\ &= \left[\sum a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n} \right] = [f(X_1, \dots, X_n)] = 0. \end{aligned}$$

Остается принять во внимание, что любой многочлен из идеала I принадлежит также идеалу R . Поэтому общий нуль для R будет общим и для I . $\square$

Мы скоро докажем, что если поле K алгебраически замкнуто, то при том же условии общий нуль всегда найдется в том же пространстве K^n . По сути это обобщение основной теоремы алгебры на случай системы полиномиальных уравнений.

Задача 380. Пусть K — произвольное поле, I — произвольный максимальный идеал в $K[X_1, \dots, X_n]$. Докажите, что алгебраическое многообразие $\mathcal{V}_K(I)$ не может содержать

более одной точки. Могут ли новые точки появиться при расширении поля K ?

Задача 381. Даны многочлены $f(X, Y)$, $g(X, Y)$ над произвольным полем K . Докажите, что если многочлен $g(X, Y)$ неприводим над K и не является делителем многочлена $f(X, Y)$, то система уравнений $f(X, Y) = g(X, Y) = 0$ может иметь лишь конечное число решений.

9.3. Теорема Нётер о нормализации

Чтобы получить упомянутое выше обобщение основной теоремы алгебры, нам нужно достаточно простое, но фундаментальное утверждение, известное как теорема Нётер о нормализации. Оно же позволит прояснить общее строение алгебраических многообразий.

Теорема 9.3.1 (ТЕОРЕМА НЁТЕР О НОРМАЛИЗАЦИИ). Пусть K — бесконечное поле и степень трансцендентности расширения $K \leq K(x_1, \dots, x_n)$ равна d . Тогда в кольце $K[x_1, \dots, x_n]$ можно найти элементы $y_1, \dots, y_n$, обладающие такими свойствами:

- $K[x_1, \dots, x_n] = K[y_1, \dots, y_n]$;
- $y_1, \dots, y_d$ образуют базис трансцендентности расширения $K \leq K(x_1, \dots, x_n)$;
- y_i является целым алгебраическим над кольцом $K[y_1, \dots, y_{i-1}]$ при $d < i \leq n$;
- $x_1, \dots, x_n$ и $y_1, \dots, y_n$ связаны линейными соотношениями

$$y_i = x_i - \sum_{j=i+1}^n a_{ij}x_j, \quad a_{ij} \in K, \quad i+1 \leq j \leq n, \quad 1 \leq i \leq n.$$

Доказательство. Если элементы $x_1, \dots, x_n$ алгебраически независимы над полем K , то доказывать нечего. Пусть они алгебраически зависимы над полем K , т.е. имеется ненулевой многочлен $f(X_1, \dots, X_n)$ с коэффициентами из поля K , для которого $f(x_1, \dots, x_n) = 0$.¹⁾

¹⁾ Обратим внимание на то, что $X_1, \dots, X_n$ — это переменные и равенство $f(X_1, \dots, X_n) = 0$ понимается в том смысле, что каждый из коэффициентов данного многочлена равен нулю. В то же время равенство $f(x_1, \dots, x_n) = 0$ означает, что точка $(x_1, \dots, x_n)$ является нулем многочлена f .

Пусть степень многочлена f равна N и многочлен f_N определяется как сумма одночленов степени N из состава f .

Пусть $Y_1, \dots, Y_n$ — новые переменные и $c_1, \dots, c_{n-1}$ — какие-то элементы поля K . При любом выборе этих элементов получаем

$$g(Y_1, \dots, Y_n) := f(Y_1 + c_1 Y_n, \dots, Y_{n-1} + c_{n-1} Y_n, Y_n) = \\ = f_N(c_1, \dots, c_{n-1}, 1) Y_n^N + \Phi,$$

где Φ можно рассматривать как многочлен от Y_n над кольцом $K[Y_1, \dots, Y_{n-1}]$, и в этом качестве его степень строго меньше N . Предположение о бесконечности поля K дает возможность выбрать $c_1, \dots, c_{n-1}$ таким образом, что

$$c := f_N(c_1, \dots, c_{n-1}, 1) \neq 0.$$

При таком выборе рассмотрим многочлен

$$F(Y_1, \dots, Y_n) := c^{-1} g(Y_1, \dots, Y_n) = \\ = Y_n^N + \alpha_{N-1} Y_n^{N-1} + \dots + \alpha_1 Y_n + \alpha_0, \\ \alpha_0, \dots, \alpha_{N-1} \in K[Y_1, \dots, Y_{n-1}].$$

Возьмем $z_i := x_i - c_i x_n$ при $1 \leq i < n$ и $z_n := x_n$. Тогда $K[z_1, \dots, z_n] = K[x_1, \dots, x_n]$, $F(z_1, \dots, z_n) = 0$ и z_n — целый алгебраический элемент над кольцом $K[z_1, \dots, z_{n-1}]$.

Чтобы завершить доказательство, используем индукцию. Пусть уже доказано, что

$$K[z_1, \dots, z_{n-1}] = K[y_1, \dots, y_{n-1}],$$

где $y_1, \dots, y_d$ образуют базис трансцендентности поля $K(z_1, \dots, z_{n-1})$, а при $d < i \leq n$ элемент y_i является целым алгебраическим над кольцом $K[y_1, \dots, y_{n-1}]$. Линейные соотношения между элементами $z_1, \dots, z_{n-1}$ и $y_1, \dots, y_{n-1}$ запишем в виде матричного равенства:

$$\begin{bmatrix} y_1 \\ \dots \\ y_{n-1} \end{bmatrix} = B \begin{bmatrix} z_1 \\ \dots \\ z_{n-1} \end{bmatrix}, \\ B = \begin{bmatrix} 1 & -b_{12} & -b_{13} & \dots & -b_{1,n-1} \\ & 1 & -b_{23} & \dots & -b_{2,n-1} \\ & & \dots & \dots & \dots \\ & & & 1 & -b_{n-2,n-1} \\ & & & & 1 \end{bmatrix} \in K^{(n-1) \times (n-1)}.$$

Мы уже установили, что

$$\begin{bmatrix} z_1 \\ \dots \\ z_n \end{bmatrix} = C \begin{bmatrix} x_1 \\ \dots \\ x_n \end{bmatrix}, \quad C = \begin{bmatrix} 1 & & & -c_1 \\ & \ddots & & \\ & & 1 & -c_{n-1} \\ & & & 1 \end{bmatrix} \in K^{n \times n}.$$

Положим $y_n := x_n$. Тогда

$$\begin{bmatrix} y_1 \\ \dots \\ y_n \end{bmatrix} = A \begin{bmatrix} x_1 \\ \dots \\ x_n \end{bmatrix}, \quad A = \begin{bmatrix} B & \\ & 1 \end{bmatrix} C \in K^{n \times n}.$$

Понятно, что A — верхняя треугольная матрица с единичной главной диагональю и нужные нам линейные соотношения между $y_1, \dots, y_n$ и $x_1, \dots, x_n$ установлены. $\square$

Основные утверждения теоремы справедливы и в случае конечного поля: кольцо $K[x_1, \dots, x_n]$ можно получить из K кольцевым присоединением новых элементов $y_1, \dots, y_n$ таким образом, что каждый элемент y_i этого кольца при $d < i \leq n$ будет цел над $K[y_1, \dots, y_{i-1}]$. Снимается лишь утверждение о линейной связи между $x_1, \dots, x_n$ и $y_1, \dots, y_n$.

Как и раньше, основная идея доказательства заключается в получении таких элементов $y_1, \dots, y_n$, что $K[x_1, \dots, x_n] = K[y_1, \dots, y_n]$ и y_n цел над $K[y_1, \dots, y_{n-1}]$. Но реализуется она иначе. Теперь замена переменных ищется в виде

$$X_1 = Y_1 + Y_n^{\beta_1}, \dots, X_{n-1} = Y_{n-1} + Y_n^{\beta_{n-1}}, X_n = Y_n.$$

Числа $\beta_1, \dots, \beta_{n-1}$ подбираются, конечно же, на основе уравнения алгебраической зависимости $f(x_1, \dots, x_n) = 0$. Главное при их выборе — сделать так, чтобы старший член многочлена

$$F(Y_n) := f(Y_1 + Y_n^{\beta_1}, \dots, Y_{n-1} + Y_n^{\beta_{n-1}}, Y_n)$$

от буквы Y_n был элементом поля K .

Задача 382. Пусть $f(X_1, \dots, X_n)$ — ненулевой многочлен над конечным полем K . Докажите существование натуральных чисел $\beta_1, \dots, \beta_{n-1}$ таких, что старший член многочлена

$$F(Y_n) := f(Y_1 + Y_n^{\beta_1}, \dots, Y_{n-1} + Y_n^{\beta_{n-1}}, Y_n) \in (K[Y_1, \dots, Y_{n-1}])[Y_n]$$

принадлежит полю K .

9.4. Теорема Гильберта о нулях

Наша основная цель в этом разделе — доказать две очень важные теоремы.

Теорема 9.4.1 (ОБОБЩЕНИЕ ОСНОВНОЙ ТЕОРЕМЫ АЛГЕБРЫ). *Если поле K алгебраически замкнуто, то любой собственный идеал I кольца $K[X_1, \dots, X_n]$ имеет непустое множество нулей в пространстве K^n .*

Теорема 9.4.2 (ТЕОРЕМА ГИЛЬБЕРТА О НУЛЯХ). *Пусть поле K алгебраически замкнуто, I — идеал кольца $K[X_1, \dots, X_n]$ и многочлен $f \in K[X_1, \dots, X_n]$ обращается в нуль на множестве нулей идеала I . Тогда существует натуральное число N , такое что $f^N \in I$.*

Следствие 9.4.1. *Если поле K алгебраически замкнуто, то аннулятор множества нулей произвольного идеала I кольца $K[X_1, \dots, X_n]$ совпадает с его радикалом:*

$$I(\mathcal{V}(I)) = \text{rad}(I).$$

Заметим, что при ссылках на теорему о нулях распространилась мода использовать ее немецкое имя: Nullstellensatz.

Поле L , возникшее при изучении условия совместности полиномиальных уравнений, получается из поля K *кольцевым присоединением* элементов $x_1, \dots, x_n$:

$$L = K(x_1, \dots, x_n) = K[x_1, \dots, x_n].$$

Заметим, что так же устроено расширение поля K путем присоединения конечного числа алгебраических над K элементов.

Лемма 9.4.1. *Если поле L получается из бесконечного поля K кольцевым присоединением конечного числа элементов, то каждый элемент из L является целым алгебраическим над полем K .*

Доказательство. Пусть степень трансцендентности расширения $K \leq L$ равна d . По теореме Нётер о нормализации $L = K[x_1, \dots, x_n]$, где $x_1, \dots, x_d$ — базис трансцендентности, а если $d < i \leq n$, то x_i — целый алгебраический элемент над кольцом $K[x_1, \dots, x_{i-1}]$. Рассмотрим кольца $L_i := K[x_1, \dots, x_i]$ и заметим, что, согласно лемме 8.11.2, при $d < i \leq n$ кольцо L_i является конечно порожденным модулем над кольцом L_{i-1} . Теперь можно применить лемму 8.11.1 и вывести из нее, что *каждый* элемент

кольца L_i , а не только x_i , является целым алгебраическим над кольцом L_{i-1} .

Кольца L_i целостные, так как вложены в поле $L_n = L$, и мы только что выяснили, что L_i цело над L_{i-1} при $d < i \leq n$. По условию теоремы, L_n — это поле. Значит, по лемме 8.11.4 кольцо L_{n-1} должно быть полем. По той же причине каждое кольцо L_i при $d \leq i \leq n$ будет полем. Если $d > 0$, то L_d не может быть полем в силу алгебраической независимости элементов $x_1, \dots, x_d$ над K . Таким образом, $d = 0$, а это значит, что каждый элемент поля L является целым алгебраическим над полем K . $\square$

Доказательство теоремы 9.4.1 (ОБОБЩЕНИЕ ОСНОВНОЙ ТЕОРЕМЫ АЛГЕБРЫ). Согласно теореме 9.2.1 существует поле $L = K[x_1, \dots, x_n]$, в котором

$$h(x_1, \dots, x_n) = 0 \quad \forall h(X_1, \dots, X_n) \in I.$$

Из алгебраической замкнутости поля K следует его бесконечность. Поэтому выполнены все условия леммы 9.4.1 и из нее вытекает, что каждый элемент x_i является алгебраическим над полем K . Любой многочлен положительной степени над алгебраически замкнутым полем распадается на линейные множители $\Rightarrow x_i \in K$. $\square$

Доказательство теоремы 9.4.2 (ТЕОРЕМА ГИЛЬБЕРТА О НУЛЯХ). Согласно теореме Гильберта о базисе (теорема 8.13.1 и следствие 8.13.1) идеал I является конечно порожденным. Пусть $I = \langle f_1, \dots, f_s \rangle$ и f — произвольный ненулевой многочлен, обращающийся в нуль на всех общих нулях многочленов $f_1, \dots, f_s$.

Все многочлены принадлежат кольцу $K[X_1, \dots, X_n]$. Воспользуемся идеей Рабиновича: введем еще одну букву Z и будем считать, что все многочлены принадлежат кольцу $K[X_1, \dots, X_n, Z]$. Очевидно, что система многочленов

$$f_1(X_1, \dots, X_n), \dots, f_s(X_1, \dots, X_n), 1 - Zf(X_1, \dots, X_n)$$

общих нулей иметь не может $\Rightarrow \langle f_1, \dots, f_s, 1 - Zf \rangle = K[X_1, \dots, X_n, Z]$. Значит, для каких-то многочленов $g_1, \dots, g_s, g \in K[X_1, \dots, X_n, Z]$ имеем

$$f_1 g_1 + \dots + f_s g_s + (1 - Zf)g = 1.$$

Это равенство можно рассматривать, как равенство многочленов с коэффициентами из поля $K(X_1, \dots, X_n, Z)$. Поэтому

при замене переменных на любые рациональные функции от $X_1, \dots, X_n$, Z равенство сохраняется. Положим $Z := 1/f$. Тогда

$$\sum_{i=1}^s f_i(X_1, \dots, X_n) g_i(X_1, \dots, X_n, 1/f) = 1.$$

Пусть N — наивысшая степень буквы Z в одночленах, составляющих $g_1, \dots, g_s$. После умножения обеих частей последнего равенства на f^N находим

$$f^N = \sum_{i=1}^s f_i h_i \in I,$$

$$h_i := g_i(X_1, \dots, X_n, 1/f) f^N \in K[X_1, \dots, X_n]. \quad \square$$

Доказательство следствия 9.4.1. В силу теоремы о нулях, если многочлен зануляется на множестве нулей идеала I , то какая-то его степень принадлежит этому идеалу, а значит, сам многочлен принадлежит его радикалу: $\mathcal{I}(\mathcal{V}(I)) \subseteq \text{rad}(I)$. Обратное включение очевидно: $f \in \text{rad}(I) \Rightarrow \exists N \in \mathbb{N} : f^N \in I \Rightarrow f^N \in \mathcal{I}(\mathcal{V}(I)) \Rightarrow f \in \mathcal{I}(\mathcal{V}(I))$. $\square$

В качестве теоремы Гильберта о нулях довольно часто приводится именно следствие 9.4.1. Оно содержит в себе также обобщенную основную теорему алгебры: аннулятор пустого многообразия совпадает с кольцом $K[X]$ (радикал собственного идеала также является собственным идеалом, для которого множество нулей непусто).

Следствие 9.4.1 приводит также к важному результату, который мы сформулируем в виде отдельной теоремы.

Теорема 9.4.3. *В случае алгебраически замкнутого поля K правило $V \rightarrow \mathcal{I}(V)$ устанавливает взаимно однозначное соответствие между алгебраическими многообразиями пространства K^n и радикальными идеалами кольца $K[X]$.*

Доказательство. Разные идеалы могут иметь одно и то же множество нулей. Однако разные радикальные идеалы не могут породить одно и то же многообразие: в силу теоремы Гильберта о нулях аннулятор данного многообразия равен радикалу каждого из идеалов, а равенство радикалов для радикальных идеалов равносильно равенству идеалов. Поэтому отображение $V \rightarrow \mathcal{I}(V)$ инъективно. Вот доказательство сюръективности: если $I = \text{rad}(I)$ — произвольный радикальный идеал, то, по той же теореме Гильберта о нулях, $\mathcal{V}(I) \rightarrow \mathcal{I}(\mathcal{V}(I)) = \text{rad}(I) = I$. $\square$

Задача 383. Обязан ли аннулятор множества нулей идеала кольца многочленов с вещественными коэффициентами совпадать с радикалом этого идеала?

Задача 384. Верно ли, что $I = \mathcal{I}(\mathcal{V}(I))$ для произвольного радикального идеала I ?

Задача 385. Даны комплексные однородные многочлены $f_1, \dots, f_s \in \mathbb{C}$ от переменных $X_1, \dots, X_n$, степень многочлена f_i равна p_i . Пусть

$$A_p := \{X_1^{\alpha_1} \dots X_n^{\alpha_n} : \sum_{i=1}^n \alpha_i = p\},$$

$$\mathcal{R}_{ip} := \{f_i g : g \in A_{p-p_i}\}, \quad p \geq \max_i p_i.$$

Предположим, что существует число p такое, что каждый одночлен из A_p является линейной комбинацией многочленов из $\bigcup_i \mathcal{R}_{ip}$ с комплексными коэффициентами. Докажите, что в этом и только этом случае многообразие $\mathcal{V}(f_1, \dots, f_s)$ состоит из единственной точки $(0, \dots, 0)$.

9.5. Неприводимые многообразия

Алгебраическое многообразие называется *неприводимым*, если его нельзя представить в виде объединения двух строго меньших алгебраических многообразий.

Утверждение 9.5.1. *Неприводимость алгебраического многообразия V равносильна простоте идеала $\mathcal{I}(V)$.*

Доказательство. Пусть V — алгебраическое многообразие в пространстве K^n над полем K . Предположим, что идеал $I := \mathcal{I}(V)$ непростой. Тогда, согласно определению простого идеала, над K существуют многочлены $f_1, f_2 \notin I$ такие, что $f_1 f_2 \in I$. Отсюда очевидным образом следует приводимость многообразия V :

$$V_1 := \mathcal{V}(f_1) \cap V \neq V, \quad V_2 := \mathcal{V}(f_2) \cap V \neq V, \quad V = V_1 \cup V_2.$$

Далее, если $V = V_1 \cup V_2$ для каких-то многообразий $V_1, V_2 \subsetneq V$, то для любых многочленов $f_i \in \mathcal{I}(V_i)$ имеем: $f_1 f_2 \in I$. Поскольку $V_i \subsetneq V$, можно выбрать $f_i \notin I$. Значит, идеал I непростой. $\square$

Ниже и далее мы постоянно будем использовать следующее утверждение.

Утверждение 9.5.2. Объединение и пересечение алгебраических многообразий V и W — это множества нулей пересечения и суммы их аннуляторов I и J :

$$V \cup W = \mathcal{V}(I \cap J), \quad V \cap W = \mathcal{V}(I + J).$$

Доказательство. Включение $V \cup W \subseteq \mathcal{V}(I \cap J)$ очевидно. Ранее мы установили, что $V \cup W = \mathcal{V}(IJ)$ (см. доказательство утверждения 9.1.4). Далее, $IJ \subseteq I \cap J \Rightarrow \mathcal{V}(I \cap J) \subseteq \mathcal{V}(IJ) = V \cup W$. Теперь рассмотрим пересечение многообразий: любая его точка — это общий нуль как для I , так и для J , а значит и для суммы $I + J$; любой общий нуль идеала $I + J$ — это общий нуль каждого из идеалов I и J , а значит и точка пересечения порожденных ими многообразий. $\square$

Теорема 9.5.1. Любое алгебраическое многообразие представимо в виде объединения конечного числа неприводимых многообразий, которые определены однозначно при условии, что ни одно из них не является частью другого.

Доказательство. Легко видеть, что для любого алгебраического многообразия V идеал $R = \mathcal{I}(V)$ является радикальным. Согласно теореме 8.4.1, любой радикальный идеал, в том числе R , есть пересечение конечного числа однозначно определенных простых идеалов, из которых ни один не является частью другого:

$$R = \bigcap_{1 \leq i \leq s} R_i \quad \Leftrightarrow \quad V = \mathcal{V}(\mathcal{I}(V)) = \bigcup_{1 \leq i \leq s} \mathcal{V}(R_i).$$

Мы уже знаем, что простота идеалов R_i равносильна неприводимости алгебраических многообразий $\mathcal{V}(R_i)$. $\square$

Задача 386. Пусть $V = \bigcup_{1 \leq i \leq s} V_i$ — объединение неприводимых алгебраических многообразий V_i и W — объединение их собственных подмногообразий $W_i \subsetneq V_i$. Докажите, что $W \neq V$.

Задача 387. Докажите, что любое линейное подпространство в n -мерном пространстве над произвольным полем является неприводимым алгебраическим многообразием.

Задача 388. Пусть $f(X_1, \dots, X_n)$ — произвольный неприводимый многочлен с комплексными коэффициентами. Докажите, что комплексное алгебраическое многообразие $\mathcal{V}(f)$ неприводимо.

Задача 389. Докажите, что множество всех комплексных $t \times n$ -матриц ранга не выше r есть неприводимое алгебраическое многообразие в пространстве $\mathbb{C}^{m \times n}$.

Задача 390. Докажите неприводимость алгебраического многообразия

$$V = \mathcal{V}(X_1X_3 - X_2^2, X_2X_3 - X_1^5, X_1X_2 - X_3) \subset \mathbb{C}^3.$$

9.6. Координатные кольца и полиномиальные отображения

Пусть V — неприводимое алгебраическое многообразие в n -мерном пространстве над полем K . Кольцо вычетов $K[X]/I$ по идеалу $I = \mathcal{I}(V) \subseteq K[X] \cong K[X_1, \dots, X_n]$ называется *координатным кольцом многообразия V* . Если $f(X_1, \dots, X_n)$ — произвольный многочлен над K , то, согласно определению операций в кольце вычетов, $f([X_1], \dots, [X_n]) = [f(X_1, \dots, X_n)]$. Следовательно,

$$K[X]/I = K[x_1, \dots, x_n], \quad \text{где } x_1 = [X_1], \dots, x_n = [X_n].$$

Обозначение: $K[V] := K[X]/I$.

Полезно иметь в виду, что вычеты $x_1, \dots, x_n$ можно рассматривать как *координатные функции, определенные на многообразии V* . В самом деле, два многочлена принимают одинаковые значения в точках многообразия V тогда и только тогда, когда их разность принадлежит идеалу I . Поэтому каждому вычету $[f]$ однозначно соответствует функция, которая задается правилом $\xi \rightarrow f(\xi)$ и рассматривается только на многообразии V . Таким образом, область определения многочлена сужается до точек многообразия V . Указанное соответствие является изоморфизмом кольца вычетов и кольца таких функций относительно операций поточечного сложения и умножения функций. При этом вычету $x_i = [X_i]$ соответствует функция, определенная правилом $\xi = (\xi_1, \dots, \xi_n) \rightarrow \xi_i$. Мы будем использовать одну и ту же букву для обозначения вычета и соответствующей ему функции.

Утверждение 9.6.1. Координатное кольцо является целостным кольцом с единицей.

Доказательство. Рассмотрим равное нулю произведение вычетов и используем простоту идеала $I = \mathcal{I}(V)$ в случае неприводимого многообразия V :

$$[f][g] = 0, f, g \in K[X] \Rightarrow fg \in I \Rightarrow f \in I \text{ или } g \in I \Rightarrow \\ \Rightarrow [f] = 0 \text{ или } [g] = 0. \quad \square$$

Рассмотрим произвольное расширение $K(x_1, \dots, x_n)$ поля K путем присоединения абстрактных элементов $x_1, \dots, x_n$. В любом таком случае кольцо $K[x_1, \dots, x_n]$ будет координатным кольцом неприводимого многообразия $\mathcal{V}_K(I) \subseteq K^n$, обнуляемого идеалом

$$I := \{f \in K[X]: f(x_1, \dots, x_n) = 0\}. \quad (*)$$

Если поле K алгебраически замкнуто, то между простыми идеалами в $K[X]$ и неприводимыми многообразиями имеется взаимно однозначное соответствие. В этом случае $\mathcal{V}(I) \neq \emptyset$ при $I \neq K[X]$.

Точка $x = (x_1, \dots, x_n)$, принадлежащая пространству L^n над некоторым расширением L поля K и обладающая свойством (*), называется *главной точкой* многообразия V . Обратим внимание на то, что главная точка многообразия в общем случае ему не принадлежит.

Утверждение 9.6.2. *Алгебраическое многообразие имеет главную точку в том и только том случае, когда оно неприводимо.*

Доказательство. Если главная точка x существует, то идеал I обязательно будет простым: если $f(x)g(x) = 0$, то непременно $f(x) = 0$ или $g(x) = 0$. Поэтому, согласно определению главной точки, $f \in I$ или $g \in I$. Из простоты идеала I вытекает неприводимость многообразия $\mathcal{V}(I)$. Если дано неприводимое многообразие V , то главной является точка $x = (x_1, \dots, x_n) \in (K(V))^n$ с координатами $x_i = [X_i]$. $\square$

При рассмотрении изоморфизмов координатных колец всегда предполагается, что исходное поле остается неподвижным. В алгебраической геометрии обычно интересуются такими свойствами неприводимых многообразий, которые сохраняются при переходе к любому многообразию с изоморфным координатным кольцом. Пусть $V \subseteq K^n$ и $W \subseteq K^m$ — неприводимые многообразия с изоморфными координатными кольцами $K[x_1, \dots, x_n]$ и $K[y_1, \dots, y_m]$. В этом случае V и W называются *изоморфными*.

Отображение $p: K^n \rightarrow K^m$ называется *полиномиальным*, если значение каждой координаты образа точки является значением некоторого многочлена от координат ее прообраза. Для разных координат многочлены в общем случае различны, но каждый из них не зависит от выбора точки. Пусть

$$\xi = (\xi_1, \dots, \xi_n) \in K^n, \quad \theta = (\theta_1, \dots, \theta_m) \in K^m.$$

Тогда

[illegible]

Множества $V \subseteq K^n$ и $W \subseteq K^m$ называются *полиномиально эквивалентными*, если существуют полиномиальные отображения

$$p: K^n \rightarrow K^m, \quad q: K^m \rightarrow K^n$$

такие, что

$$q(p(\xi)) = \xi \quad \forall \xi \in V, \quad p(q(\theta)) = \theta \quad \forall \theta \in W.$$

Теорема 9.6.1. *Неприводимые многообразия изоморфны в том и только том случае, когда они полиномиально эквивалентны.*

Доказательство. Пусть $V \subseteq K^n$ и $W \subseteq K^m$ — неприводимые многообразия и их координатные кольца изоморфны над полем K :

$$K[x_1, \dots, x_n] \cong K[y_1, \dots, y_m].$$

Обозначим через $p_j(X_1, \dots, X_n)$ и $q_i(Y_1, \dots, Y_m)$ многочлены, которые при данном изоморфизме реализуют соответствия

$$p_i(x_1, \dots, x_n) \leftrightarrow y_i, \quad q_i(y_1, \dots, y_m) \leftrightarrow x_i.$$

Эти многочлены задают полиномальные отображения

$$p: K[X] \rightarrow K[Y], \quad q: K[Y] \rightarrow K[X],$$

для которых

$$\begin{aligned} q(p(x)) &= x \quad \forall x \in K[x_1, \dots, x_n], \\ p(q(y)) &= y \quad \forall y \in K[y_1, \dots, y_m], \end{aligned} \tag{I}$$

откуда сразу же вытекают равенства

$$q(p(\xi)) = \xi \quad \forall \xi \in V, \quad p(q(\theta)) = \theta \quad \forall \theta \in W. \quad (\text{II})$$

Теперь предположим, что полиномиальная эквивалентность задается отображениями p и q , для которых выполнены равенства (II). Как уже отмечалось, x_i — это полиномиальная функция на V , определенная правилом $x_i(\xi) = \xi_i$. Таким образом, $x = (x_1, \dots, x_n)$ — это тождественное отображение, при котором $x(\xi) = \xi$. Аналогично, $y_j(\theta) = \theta_j$ и $y(\theta) = \theta$. Из соотношений (II) следует, что

$$q_j(p(x(\xi))) = x_j(\xi) \quad \forall \xi \in V,$$

а это и есть первое из соотношений (I). Второе выводится аналогично. Произвольный элемент кольца $K[x_1, \dots, x_n]$ имеет вид $f(x_1, \dots, x_n)$, где $f \in K[X_1, \dots, X_n]$. Отображение $\phi: K[x_1, \dots, x_n] \rightarrow K[y_1, \dots, y_m]$ определим правилом

$$\begin{aligned} f(x) &= f(x_1, \dots, x_n) \rightarrow \\ &\rightarrow f(q_1(y_1, \dots, y_m), \dots, q_n(y_1, \dots, y_m)) = (f \circ q)(y). \end{aligned}$$

Несложно проверяется, что оно определено корректно, сохраняет операции и является взаимно однозначным отображением кольца $K[x_1, \dots, x_n]$ на $K[y_1, \dots, y_m]$. $\square$

Задача 391. Найдите все неприводимые многообразия, которые содержат свою главную точку.

Задача 392. Приведите пример координатного кольца, которое не является факториальным.

Задача 393. Неприводимое многообразие W является подмногообразием неприводимого многообразия V . Докажите что координатное кольцо многообразия W есть гомоморфный образ координатного кольца многообразия V .

Задача 394. Пусть дано неприводимое многообразие в пространстве K^n над полем K и известно, что $(x_1, \dots, x_n)$ и $(y_1, \dots, y_n)$ — его главные точки. Докажите, что поля $K(x_1, \dots, x_n)$ и $K(y_1, \dots, y_n)$ изоморфны.

Задача 395. Пусть K — произвольное поле и $p: K^n \rightarrow K^m$ — полиномиальное отображение. Докажите, что для любого множества точек $S \subseteq K^m$ его полный прообраз $p^{-1}(S)$ является алгебраическим многообразием в K^n .

Задача 396. Алгебраическое многообразие в пространстве $\mathbb{C}_{XYZ}$ задано уравнениями $Y - X^2 = 0$, $X + Z = 0$. Докажите, что оно изоморфно $\mathbb{C}_X$.

Задача 397. Докажите, что алгебраическое многообразие $\mathcal{V}(Y^5 - X^2) \subset \mathbb{R}_{XY}$ не изоморфно $\mathbb{R}_X$.

9.7. Рациональные отображения

Поле частных кольца $K[V]$ называется *координатным полем* многообразия V или *полем рациональных функций* на V . Обозначение: $K(V)$.

Каждый элемент $\Phi \in K(V) = K(x_1, \dots, x_n)$ имеет вид

$$f(x_1, \dots, x_n)/g(x_1, \dots, x_n),$$

где $f, g \in K[X_1, \dots, X_n]$ и $g(x_1, \dots, x_n) \neq 0$. Последнее означает, что g не обращается в нуль хотя бы в одной точке из V . Элемент Φ можно рассматривать как рациональную функцию

$$\Phi(X_1, \dots, X_n) = f(X_1, \dots, X_n)/g(X_1, \dots, X_n),$$

определенную на множестве

$$\text{dom}_V \Phi := V \setminus \mathcal{V}(g) \subseteq V.$$

Любая функция, заданная как отношение многочленов и определенная хотя бы в одной точке многообразия V , называется *рациональной функцией* на V .

Рациональные функции на V считаются равными, если их значения совпадают на V во всех точках, где определены обе функции. Пересечение областей определения непусто в силу неприводимости многообразия V . Нетрудно проверить, что рациональные функции на V образуют поле относительно операций сложения и умножения функций и это поле изоморфно полю $K(V)$.

Пусть $X = (X_1, \dots, X_n)$ и $x = (x_1, \dots, x_n)$. Для каждой точки $\xi \in V$ рассмотрим идеал

$$m_\xi := \{f(x) \in K[V] : f \in K[X], f(\xi) = 0\}.$$

Это максимальный идеал в кольце $K[V]$. При локализации кольца $K[V]$ по m_ξ получается локальное кольцо $\mathcal{O}_\xi$ ¹⁾. Его элементы можно рассматривать как рациональные функции на множестве V , определенные в точке ξ и отождествляемые, если на V их значения совпадают во всех общих точках их областей

¹⁾ Общая конструкция локализации по простому идеалу обсуждалась в разделе 8.5.

определения. Если Φ — рациональная функция, определенная во всех точках из V , то, очевидно,

$$\Phi \in \bigcap_{\xi \in V} \mathcal{O}_\xi.$$

Теорема 9.7.1. *Если рациональная функция Φ определена в каждой точке неприводимого многообразия V в пространстве над алгебраически замкнутым полем, то она является многочленом на V .*

Доказательство. Пусть I — аннулятор многообразия V и J — множество всех многочленов, которые при умножении на Φ дают функцию, совпадающую на V с некоторым многочленом. Ясно, что J — это идеал кольца $K[X]$. Кроме того, $I \subseteq J$. Поэтому нули идеала J принадлежат V . Но очевидно, что для каждой точки многообразия V в J имеется многочлен, отличный от нуля в этой точке. Значит, множество нулей идеала J пусто. Из обобщения основной теоремы алгебры следует, что $1 \in J \Rightarrow \Phi \in K[V]$. $\square$

Следствие 9.7.1. *Координатное кольцо $K[V]$ совпадает с пересечением локальных колец $\mathcal{O}_\xi$ для всех точек $\xi \in V$.*

По аналогии с полиномиальными отображениями можно рассматривать *рациональные отображения* $\Phi: K^n \rightarrow K^m$ и $\Psi: K^m \rightarrow K^n$. Неприводимые многообразия $V \subseteq K^n$ и $W \subseteq K^m$ называются *рационально эквивалентными*, если

$$\Psi(\Phi(\xi)) = \xi \quad \forall \xi \in A, \quad \Phi(\Psi(\theta)) = \theta \quad \forall \theta \in B,$$

$$A := \{\xi: \Phi(\xi) \in \text{dom}_W \Psi\} \cap \text{dom}_V \Phi \neq \emptyset,$$

$$B := \{\theta: \Psi(\theta) \in \text{dom}_V \Phi\} \cap \text{dom}_W \Psi \neq \emptyset.$$

Теорема 9.7.2. *Для рациональной эквивалентности неприводимых многообразий необходимо и достаточно, чтобы их координатные поля были изоморфны.*

Доказательство проводится по аналогии с доказательством теоремы о полиномиальной эквивалентности многообразий.

Пусть V и W — алгебраические многообразия, $V_1 \subsetneq V$ и $W_1 \subsetneq W$ — собственные подмногообразия. Тогда множества $A = V \setminus V_1$ и $B = W \setminus W_1$ называются *алгебраически открытыми* в V и W соответственно. Рациональное отображение из A в B называется *морфизмом*, если оно определено в каждой точке множества A . Если обратное отображение существует и

является морфизмом из B в A , то множества A и B называются *рационально изоморфными*¹⁾.

Рациональные отображения имеют непосредственное отношение к вопросу о *рациональной параметризации* многообразий, т.е. о поиске ненулевых рациональных функций $\phi_i(t_1, \dots, t_d)$, которые при подстановке $X_1 = \phi_1, \dots, X_n = \phi_n$ в каждое из уравнений многообразия дают равенства, верные во всех точках $(t_1, \dots, t_d) \in K^d$, в которых их знаменатели не обращаются в нуль.

Задача 398. Пусть $V \subseteq K^n$ — непустое неприводимое многообразие и многочлен f не обращается в нуль хотя бы в одной точке из V . Докажите, что множество $V \setminus V(f)$ рационально изоморфно некоторому алгебраическому многообразию с координатным кольцом, изоморфным $K[V][f^{-1}]$.

Задача 399. Докажите, что алгебраически открытое множество $\mathbb{C}^2 \setminus \{(0,0)\}$ не является рационально изоморфным какому-либо алгебраическому многообразию.

Задача 400. Приведите пример неизоморфных многообразий, которые являются рационально эквивалентными.

Задача 401. Найдите рациональную параметризацию кривой в пространстве $\mathbb{C}^2$, заданной уравнением $Y^2 = X^2 + X^3$.

9.8. Проекция многообразия

Что происходит с алгебраическими многообразиями при полиномиальных отображениях, как устроены их образы?

Они могут и не быть многообразиями. Например, пусть

$$V = \{(\xi_1, \xi_2) \in \mathbb{C}^2 : \xi_1 \xi_2 - 1 = 0\}.$$

Тогда при отображении $p: (\xi_1, \xi_2) \rightarrow \xi_1$ множество $p(V) = \mathbb{C}^1 \setminus \{0\}$ не является алгебраическим многообразием в $\mathbb{C}^1$. В то же время оно не так сильно отличается от многообразия: его алгебраическое замыкание получается добавлением всего одной точки. В целом схожая картина наблюдается и в общем случае, хотя число добавляемых точек не обязательно конечно.

¹⁾ Довольно часто (хотя и не всегда) алгебраически открытое множество оказывается рационально изоморфным какому-то алгебраическому многообразию — в ряде книг такие множества тоже называют многообразиями.

Близость множества $S \subseteq V$ к неприводимому многообразию V понимается в том смысле, что S содержит любую точку из V вне некоторого собственного подмногообразия $W \subsetneq V$. Сказанное означает, что $V \setminus W \subseteq S \subseteq V$.

Начнем с изучения простейших полиномиальных отображений — проекций на координатные подпространства. Пусть $l \leq m$ и рассматриваются проекции

$$p_{lm}: (\xi_1, \dots, \xi_m) \rightarrow (\xi_1, \dots, \xi_l), \quad p_l := p_{l, n}.$$

Считаем заданным алгебраическое многообразие V в пространстве K^n над алгебраически замкнутым полем K . Введем следующие обозначения:

$$I := \mathcal{I}(V), \quad I_l := I \cap K[X_1, \dots, X_l], \quad V_l := \mathcal{V}(I_l) \subseteq K^l.$$

Очевидно, I_l — это идеал кольца $K[X_1, \dots, X_l]$, а V_l — его множество нулей в пространстве K^l .

Утверждение 9.8.1. *Если идеал $I \subseteq K[X_1, \dots, X_n]$ радикальный, то каждый из идеалов $I_l \subseteq K[X_1, \dots, X_l]$ будет радикальным. Если идеал I простой, то идеал I_l также будет простым.*

Доказательство. Предположим, что идеал I радикальный. Если $f^N \in I_l$, то, конечно же, $f^N \in I \Rightarrow f \in I \cap K[X_1, \dots, X_l] = I_l$. Радикальность идеала I_l доказана. Теперь предположим, что идеал I простой, $f, g \in K[X_1, \dots, X_l]$ и $fg \in I_l$. Поскольку $fg \in I$, получаем $f \in I$ или $g \in I \Rightarrow f \in I_l$ или $g \in I_l$. $\square$

Утверждение 9.8.2. *Многообразие V_l является алгебраическим замыканием множества $p_l(V)$ в пространстве K^l .*

Доказательство. Точка $(\xi_1, \dots, \xi_l) \in K^l$ принадлежит $p_l(V)$ в том и только том случае, когда существуют величины $\xi_{l+1}, \dots, \xi_n \in K$ такие, что точка $(\xi_1, \dots, \xi_n)$ принадлежит V . Отсюда ясно, что любой многочлен из I_l обращается в нуль в каждой точке множества $p_l(V)$. Обратно, пусть $f \in K[X_1, \dots, X_l]$ обнуляет каждую точку из $p_l(V)$. Тогда $f \in I \cap K[X_1, \dots, X_l]$. Значит, $\mathcal{I}(p_l(V)) = I_l$ и $V_l = \mathcal{V}(I_l) = \mathcal{V}(\mathcal{I}(p_l(V)))$ есть алгебраическое замыкание множества $p_l(V)$. $\square$

Теорема 9.8.1. *Пусть V — непустое неприводимое многообразие в пространстве K^n над алгебраически замкнутым полем K . Тогда для любого собственного подмногооб-*

разия $W \subsetneq V \subseteq K^n$ найдется собственное подмногообразие $W_l \subsetneq V_l \subseteq K^l$, такое что

$$V_l \setminus W_l \subseteq p_l(V \setminus W) \subseteq V_l.$$

Доказательство. Неприводимость многообразия V позволяет ввести координатное кольцо $K[V] = K[x_1, \dots, x_n]$ и его поле частных $K(V) = K(x_1, \dots, x_n)$. Сначала докажем теорему для $l = n - 1$. Ключевую роль будут играть три многочлена, которые ниже получают обозначения f , g и h .

Прежде всего выберем многочлен $f \in \mathcal{I}(W) \setminus \mathcal{I}(V) \neq \emptyset$ и запишем его в виде

$$f(X_1, \dots, X_n) = \sum_{i=0}^r f_i(X_1, \dots, X_{n-1}) X_n^i,$$

$$f_r(X_1, \dots, X_{n-1}) \neq 0.$$

Случай I.. Предположим, что элемент x_n не является алгебраическим над полем $K(x_1, \dots, x_{n-1})$. По определению проекции, если $(\xi_1, \dots, \xi_{n-1}) \in p_{n-1}(V)$, то существует элемент $\xi_n \in K$, для которого $(\xi_1, \dots, \xi_{n-1}, \xi_n) \in V$. В данном случае мы докажем, что $p_{n-1}(V) = V_{n-1}$ и, более того, если $(\xi_1, \dots, \xi_{n-1}) \in V_{n-1}$, то

$$(\xi_1, \dots, \xi_{n-1}, \xi_n) \in V \quad \text{для любого} \quad \xi_n \in K.$$

В самом деле, рассмотрим произвольный многочлен $\phi(X_1, \dots, X_n)$. Мы знаем, что

$$\phi \in I \quad \Leftrightarrow \quad \phi(x_1, \dots, x_n) = 0.$$

Таким образом, если $\phi \in I$, то x_n — корень многочлена

$$\phi(x_1, \dots, x_{n-1}, X_n) = \sum_i [\phi_i(X_1, \dots, X_{n-1})] X_n^i.$$

В силу неалгебраичности x_n все коэффициенты этого многочлена должны быть нулевыми $\Rightarrow$ если $(\xi_1, \dots, \xi_{n-1}) \in V_{n-1}$, то $\phi_i(\xi_1, \dots, \xi_{n-1}) = 0$ для всех i . Поэтому $\phi(\xi_1, \dots, \xi_{n-1}, \xi_n) = 0$ при любом выборе числа $\xi_n \in K$.

В качестве искомого многообразия W_{n-1} в данном случае можно взять

$$W_{n-1} := \mathcal{V}(f_0, \dots, f_r) \cap V_{n-1}.$$

Во-первых, $W_{n-1} \neq V_{n-1}$, иначе $f \in I$. Во-вторых, в точке $(\xi_1, \dots, \xi_{n-1}) \in V_{n-1} \setminus W_{n-1}$ хотя бы один из многочленов $f_0, \dots, f_r$ отличен от нуля. В итоге

$$\exists \xi_n \in K : f(\xi_1, \dots, \xi_n) \neq 0 \Rightarrow (\xi_1, \dots, \xi_n) \in V \setminus W.$$

СЛУЧАЙ II.. Пусть x_n — алгебраический элемент над полем $K(x_1, \dots, x_{n-1})$, и пусть $G(X_n)$ — его минимальный многочлен над кольцом $K[x_1, \dots, x_{n-1}]$ (ненулевой многочлен минимальной степени, обнуляющий x_n). Ясно, что он получается из минимального многочлена над полем $K(x_1, \dots, x_{n-1})$ умножением на ненулевой элемент кольца $K[x_1, \dots, x_{n-1}]$ и может быть записан в виде $G(X_n) = g(x_1, \dots, x_{n-1}, X_n)$, где

$$g(X_1, \dots, X_n) = \sum_{i=0}^s g_i(X_1, \dots, X_{n-1}) X_n^i,$$

$$[g_s] = g_s(x_1, \dots, x_{n-1}) \neq 0.$$

Далее, $[f] \neq 0$ — алгебраический элемент над полем $K(x_1, \dots, x_{n-1})$. Рассмотрим его минимальный многочлен $H(X_n)$ над кольцом $K[x_1, \dots, x_{n-1}]$ и запишем его в виде $H(X_n) = h(x_1, \dots, x_{n-1}, X_n)$, где

$$h(X_1, \dots, X_n) = \sum_{i=0}^t h_i(X_1, \dots, X_{n-1}) X_n^i,$$

$$[h_t] = h_t(x_1, \dots, x_{n-1}) \neq 0.$$

Имеет место равенство $h(x_1, \dots, x_{n-1}, [f]) = \sum_{i=0}^t [h_i] [f]^i = 0$, и заметим, что

$$[h_0] = h_0(x_1, \dots, x_{n-1}) \neq 0.$$

От противного, пусть это не так. Если $t \geq 2$, то это противоречит минимальности многочлена g . Если $t = 1$, то получаем: $h_1(x_1, \dots, x_{n-1})f(x_1, \dots, x_n) = 0 \Rightarrow f(x_1, \dots, x_n) = 0$ — используем то, что координатное кольцо является целостным. Равенство $f(x_1, \dots, x_n) = 0$ означает, что f зануляется во всех точках V , а это противоречит выбору многочлена $f(X_1, \dots, X_n)$.

В качестве W_{n-1} теперь выберем

$$W_{n-1} := \mathcal{V}(h_0 g_s) \cap V_{n-1}.$$

Поскольку каждый из многочленов h_0 и g_s отличен от нуля хотя бы в одной точке из V_{n-1} , находим

$$\mathcal{V}(h_0) \cap V_{n-1} \neq V_{n-1}, \quad \mathcal{V}(g_s) \cap V_{n-1} \neq V_{n-1} \Rightarrow W_{n-1} \neq V_{n-1},$$

иначе многообразие V_{n-1} было бы приводимым.

Пусть $(\xi_1, \dots, \xi_{n-1}) \in V_{n-1} \setminus W_{n-1} \Rightarrow g_s(\xi_1, \dots, \xi_{n-1}) \neq 0$. Отсюда следует, что $g(\xi_1, \dots, \xi_{n-1}, X_n)$ — ненулевой многочлен степени $s \geq 1$. Пусть $\xi_n \in K$ — любой из его корней. Тогда $g(\xi_1, \dots, \xi_n) = 0$. Покажем, что

$$\phi(\xi_1, \dots, \xi_n) = 0 \quad \forall \phi \in I.$$

Условие $\phi \in I$ означает, что $\phi(x_1, \dots, x_n) = 0 \Rightarrow x_n$ является корнем многочлена $\phi(x_1, \dots, x_{n-1}, X_n)$. Поэтому данный многочлен делится на минимальный многочлен $g(x_1, \dots, x_{n-1}, X_n)$ для элемента x_n . Частное, получаемое при делении, будет многочленом с коэффициентами из поля $K(x_1, \dots, x_{n-1})$. Но из метода деления столбиком легко увидеть, что частное будет многочленом с коэффициентами из кольца $K[x_1, \dots, x_{n-1}]$, деленным на некоторую степень, скажем μ , старшего коэффициента делителя:

$$\begin{aligned} (g_s(x_1, \dots, x_{n-1}))^\mu \phi(x_1, \dots, x_{n-1}, X_n) &= \\ &= g(x_1, \dots, x_{n-1}, X_n) q(x_1, \dots, x_{n-1}, X_n). \end{aligned}$$

Отсюда

$$\begin{aligned} (g_s(\xi_1, \dots, \xi_{n-1}))^\mu \phi(\xi_1, \dots, \xi_{n-1}, X_n) &= \\ &= g(\xi_1, \dots, \xi_{n-1}, X_n) q(\xi_1, \dots, \xi_{n-1}, X_n). \end{aligned}$$

В силу нашего выбора $g_s(\xi_1, \dots, \xi_{n-1}) \neq 0$. Поэтому равенство $g(\xi_1, \dots, \xi_{n-1}, \xi_n) = 0$ влечет за собой $\phi(\xi_1, \dots, \xi_{n-1}, \xi_n) = 0$.

Далее, по построению, $h_0(\xi_1, \dots, \xi_{n-1}) \neq 0 \Rightarrow$ равенство $h(\xi_1, \dots, \xi_n) = 0$ невозможно, если $f(\xi_1, \dots, \xi_n) = 0$. Значит, $f(\xi_1, \dots, \xi_n) \neq 0 \Rightarrow (\xi_1, \dots, \xi_n) \notin W$. Случай II разобран полностью.

Ничто не мешает применить те же рассуждения, считая, что в пространстве K^{n-1} заданы многообразия V_{n-1} и W_{n-1} . Поэтому мы можем утверждать, что существуют многообразия $W_{n-1} \subsetneq V_{n-1}$ и $W_{n-2} \subsetneq V_{n-2}$ такие, что

$$\begin{aligned} V_{n-1} \setminus W_{n-1} &\subseteq p_{n-1,n}(V \setminus W) \subseteq V_{n-1}, \\ V_{n-2} \setminus W_{n-2} &\subseteq p_{n-2,n-1}(V_{n-1} \setminus W_{n-1}) \subseteq V_{n-2}. \end{aligned}$$

Отсюда находим

$$\begin{aligned} V_{n-2} \setminus W_{n-2} &\subseteq p_{n-2,n-1}(V_{n-1} \setminus W_{n-1}) \subseteq \\ &\subseteq p_{n-2,n-1}(p_{n-1,n}(V \setminus W)) = p_{n-2}(V \setminus W). \end{aligned}$$

Таким образом, теорема доказана для $l = n - 2$ и очевидно, что описанный метод позволяет получить ее для произвольного l . $\square$

Обратим внимание на одно очень важное обстоятельство, связанное с различием случаев I и II. В случае I над любой точкой $(\xi_1, \dots, \xi_{n-1})$ из $V_{n-1} \setminus W_{n-1}$ имеется бесконечно много точек вида $(\xi_1, \dots, \xi_{n-1}, \xi_n)$ из V . Более того, эти точки принадлежат V при любом $\xi_n \in K$ и все они, за исключением конечного числа корней многочлена $f(\xi_1, \dots, \xi_{n-1}, X_n)$, не попадают в W . В случае II над каждой точкой $(\xi_1, \dots, \xi_{n-1})$ из $V_{n-1} \setminus W_{n-1}$ имеется конечное число точек вида $(\xi_1, \dots, \xi_{n-1}, \xi_n)$ из V и при этом каждая из них не входит в многообразие W . Эта особенность случая II нам скоро понадобится, поэтому сформулируем ее в виде отдельного утверждения.

Теорема 9.8.2. Пусть K — алгебраически замкнутое поле и $V \subseteq K_{X_1, \dots, X_n}$ — непустое неприводимое многообразие с координатным кольцом $K[x_1, \dots, x_n]$. Тогда если элементы $x_{i+1}, \dots, x_n$ алгебраичны над $K(x_1, \dots, x_i)$, то для любого собственного подмногообразия $W \subsetneq V$ существует собственное подмногообразие $W_l \subsetneq V_l$ такое, что для каждой точки $\zeta = (\xi_1, \dots, \xi_l) \in V_l \setminus W_l$ ее полный прообраз $p_l^{-1}(\zeta)$ состоит из конечного числа точек, каждая из которых принадлежит $V \setminus W$.

Доказательство. Если $l = n - 1$, то рассмотрим те же три многочлена f, g и h , которые возникли в доказательстве теоремы 9.8.1. Пусть $W_{n-1} := \mathcal{V}(h \circ g_s) \cap V_{n-1}$ и $\zeta = (\xi_1, \dots, \xi_{n-1}) \in V_{n-1} \setminus W_{n-1}$. Тогда $(\xi_1, \dots, \xi_n) \in V$ в том и только том случае, когда $g(\xi_1, \dots, \xi_n) = 0$, т.е. ξ_n — корень многочлена $g(\xi_1, \dots, \xi_{n-1}, X_n)$. При этом автоматически $(\xi_1, \dots, \xi_n) \notin W$. Доказательство содержится в разборе случая II из доказательства теоремы 9.8.1. Если $l = n - 2$, то в силу уже доказанного существует собственное подмногообразие $W_{n-2} \subsetneq V_{n-2}$ такое, что над каждой точкой $(\xi_1, \dots, \xi_{n-2}) \in V_{n-2} \setminus W_{n-2}$ имеется конечное число точек $(\xi_1, \dots, \xi_{n-2}, \xi_{n-1}) \in V_{n-1}$, при этом каждая из них принадлежит $V_{n-1} \setminus W_{n-1}$ и, следовательно, над каждой точкой $(\xi_1, \dots, \xi_{n-1})$ расположено конечное число точек $(\xi_1, \dots, \xi_{n-1}, \xi_n) \in V$, каждая из них принадлежит $V \setminus W$. Таким

образом, теорема получена для $l = n - 2$. Для меньших значений l повторяются те же рассуждения. $\square$

Теорема 9.8.3. Пусть K — алгебраически замкнутое поле, $p: K^n \rightarrow K^m$ — произвольное полиномиальное отображение, V — неприводимое многообразие в K^n и U — алгебраическое замыкание его образа $p(V)$. Тогда для любого собственного подмногообразия $W \subsetneq V$ существует собственное подмногообразие $Z \subsetneq U$ такое, что

$$U \setminus Z \subseteq p(V \setminus W) \subseteq U.$$

Доказательство. Пусть $V = \mathcal{V}(f_1, \dots, f_s)$ и отображение p задается многочленами $p_i(X_1, \dots, X_n)$. Тогда уравнения

$$Y_i = p_i(X_1, \dots, X_n), \quad 1 \leq i \leq m,$$

$$f_j(X_1, \dots, X_n) = 0, \quad 1 \leq j \leq s,$$

определяют некоторое алгебраическое многообразие $V' \subseteq K^{m+n}$. Считаем, что переменные упорядочены в такой последовательности: $Y_1, \dots, Y_m, X_1, \dots, X_n$. Тогда интересующее нас множество $p(V) \subseteq K^m$ есть в точности $p_m(V')$. Легко доказывается, что из неприводимости многообразия V вытекает неприводимость многообразия V' . Поэтому выполнены условия теоремы 9.8.1. $\square$

Задача 402. Пусть $p: K^n \rightarrow K^m$ — произвольное полиномиальное отображение. Докажите, что алгебраическое замыкание образа $p(V)$ неприводимого многообразия $V \subseteq K^n$ является неприводимым многообразием в K^m .

Задача 403. В пространстве $\mathbb{C}^{m \times n}$ найдите алгебраическое замыкание множества матриц ранга r .

9.9. Конструктивные множества

Образы многообразий можно описать более детально. Мы это сделаем, опираясь на следующее утверждение, которое является одновременно обобщением (многообразие V может быть приводимым) и ослаблением (многообразие W считается пустым) теоремы 9.8.3.

Утверждение 9.9.1. Пусть K — алгебраически замкнутое поле, $p: K^n \rightarrow K^m$ — произвольное полиномиальное отображение, V — произвольное алгебраическое многообразие в K^n

и U — алгебраическое замыкание его образа $p(V)$. Тогда существует собственное подмногообразие $Z \subsetneq U$ такое, что

$$U \setminus Z \subseteq p(V) \subseteq U.$$

Доказательство. Пусть $V = V_1 \cup \dots \cup V_s$ — однозначно определенное разложение на неприводимые компоненты $V_i \subset V$, и пусть U_i — алгебраическое замыкание множества $p(V_i)$. Нетрудно проверить, что алгебраическое замыкание U множества $p(V)$ имеет вид $U = U_1 \cup \dots \cup U_s$. Согласно теореме 9.8.3 существуют подмногообразия $Z_i \subsetneq U_i$ такие, что $U_i \setminus Z_i \subseteq p(V_i) \subseteq U_i$. Положим $Z := Z_1 \cup \dots \cup Z_s$. Тогда без особых затруднений находим $Z \subsetneq U$, и вполне очевидно, что

$$U \setminus Z \subseteq \bigcup_{1 \leq i \leq s} U_i \setminus Z_i \subseteq \bigcup_{1 \leq i \leq s} p(V_i) = p(V) \subseteq U. \quad \square$$

Объединение конечного числа разностей алгебраических многообразий называется *конструктивным множеством*.

Теорема 9.9.1. Пусть K — алгебраически замкнутое поле и $p: K^n \rightarrow K^m$ — произвольное полиномиальное отображение. Для произвольного алгебраического многообразия $V \subseteq K^n$ его образ $p(V)$ является конструктивным множеством в пространстве K^m .

Доказательство. Обозначим через U_1 алгебраическое замыкание множества $p(V)$. Тогда, согласно утверждению 9.9.1, для какого-то собственного подмногообразия $Z_1 \subsetneq V_1$ имеет место включение $U_1 \setminus Z_1 \subseteq p(V) \subseteq U_1$. Если $U_1 \setminus Z_1 = p(V)$, то все доказано. В противном случае

$$V_1 := V \cap p^{-1}(Z_1) \subsetneq V, \quad (U_1 \setminus Z_1) \cup p(V_1) = p(V).$$

Пусть U_2 — алгебраическое замыкание множества $p(V_1)$. Тогда должно найтись собственное подмногообразие $Z_2 \subsetneq U_2$, для которого $U_2 \setminus Z_2 \subseteq p(V)$. В итоге

$$(U_1 \setminus Z_1) \cup (U_2 \setminus Z_2) \subseteq p(V).$$

Если достигнуто равенство, то все доказано. Если нет, то

$$V_2 := V_1 \cap p^{-1}(Z_1) \subsetneq V_1, \quad (U_1 \setminus Z_1) \cup (U_2 \setminus Z_2) \cup p(V_2) = p(V).$$

Действуя в том же духе, мы получим последовательность многообразий

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq \dots,$$

которая не может быть бесконечной в силу нётеровости кольца многочленов. Значит, через конечное число шагов, скажем s , мы придем к равенству

$$(U_1 \setminus Z_1) \cup \dots \cup (U_s \setminus Z_s) = p(V). \quad \square$$

Задача 404. Докажите, что при полиномиальном отображении любое конструктивное множество переходит в конструктивное множество.

Задача 405. Полиномиальное отображение $p: \mathbb{C}^4 \rightarrow \mathbb{C}^8$ задается как сумма кронекеровых произведений (если $a = [a_1, \dots, a_n]$ и $b = [b_1, \dots, b_m]$, то $a \otimes b := [a_1 b, \dots, a_n b]$):

$$\begin{bmatrix} a \\ b \end{bmatrix} \rightarrow a \otimes b \otimes b + b \otimes a \otimes b + b \otimes b \otimes a \in \mathbb{C}^8, \quad a, b \in \mathbb{C}^2.$$

Докажите, что образ $p(\mathbb{C}^4)$ не является алгебраическим многообразием. Найдите его алгебраическое замыкание. Представьте $p(\mathbb{C}^4)$ как конструктивное множество.

9.10. Размерность и степень

Геометрические свойства многообразий не должны зависеть от выбора системы координат. Тем не менее, выбор системы координат может помочь в прояснении устройства многообразия. Пусть поле K алгебраически замкнуто. В этом случае любое неприводимое алгебраическое многообразие в пространстве K^n очень похоже на график некоторой функции, определенной в каждой точке пространства K^d и принимающей значения в пространстве K^{n-d} . Отличие от классического графика в том, что над каждой точкой из K^d может быть несколько различных точек, притом число этих точек конечно, ограничено общей константой и всюду за вычетом собственного подмногообразия равно этой константе. Число d является важнейшим атрибутом многообразия — его естественно трактовать как *размерность* многообразия.

Упомянутое выше число различных точек — это *степень проекции* $p_d: V \rightarrow K^d$, определяемая как размерность поля $K(x_1, \dots, x_n)$ как линейного пространства над полем $K(x_1, \dots, x_d)$ ¹⁾.

¹⁾ Как и сама проекция, ее степень зависит от системы координат — например, для гиперповерхности $Y - X^2 = 0$ в пространстве $\mathbb{C}_2$ имеем:

Перейдем к строгим формулировкам. Пусть $V \subseteq K^n$ — произвольное неприводимое многообразие. Его *размерностью* называется степень трансцендентности $d = \text{trdeg}(K(V) : K)$. Обозначение: $d = \dim V$.

По определению пустое многообразие имеет размерность $d = -1$. Алгебраическое многообразие размерности 1 называется *алгебраической кривой*. Под *размерностью приводимого многообразия* понимается максимальная из размерностей его неприводимых компонент.

Будем говорить, что точка $\xi = (\xi_1, \dots, \xi_d, \xi_{d+1}, \dots, \xi_n) \in K_{X_1, \dots, X_n}$ расположена *над* точкой $p_d(\xi) := (\xi_1, \dots, \xi_d) \in K_{X_1, \dots, X_d}$, а точка вида $p_d(\xi)$ — *под* точкой ξ .

Теорема 9.10.1. Пусть K — алгебраически замкнутое поле нулевой характеристики, V — неприводимое многообразие в пространстве $K_{X_1, \dots, X_n}$ и $K[x_1, \dots, x_n]$ — его координатное кольцо. Предположим, что степень трансцендентности расширения $K \leq K(x_1, \dots, x_n)$ равна

$$d = \text{trdeg}(K(x_1, \dots, x_n) : K)$$

и элементы $x_1, \dots, x_d$ образуют базис трансцендентности. Тогда в пространстве $K_{X_1, \dots, X_d}$ существует собственное алгебраическое подмногообразие Z такое, что над каждой точкой из $K_{X_1, \dots, X_d} \setminus Z$ расположено в точности

$$\delta = \dim(K(x_1, \dots, x_n) : K(x_1, \dots, x_d))$$

различных точек многообразия V .

Доказательство. Если $f(X_1, \dots, X_n) \in I = \mathcal{I}(V)$, то $f(x_1, \dots, x_n) = 0$. Значит, если $d = n$, то в силу трансцендентности элементов $x_1, \dots, x_n$ над полем K получаем $f(X_1, \dots, X_n) = 0 \Rightarrow \Rightarrow$ идеал I нулевой и $V = \mathcal{V}(I) = K_{X_1, \dots, X_n}$.

Далее полагаем, что $d < n$. Начнем с наблюдения, которое сразу же вытекает из теоремы 9.8.1. В силу трансцендентности элементов $x_1, \dots, x_d$ пересечение $I \cap K_{X_1, \dots, X_d}$ состоит из одного нулевого многочлена, поэтому алгебраическое замыкание проекции $p_d(V)$ совпадает с пространством $K_{X_1, \dots, X_d}$. Согласно теореме 9.8.1, над каждой точкой из $K_{X_1, \dots, X_d}$ вне некоторого

$\dim(\mathbb{C}(x, y) : \mathbb{C}(x)) = 1$, $\dim(\mathbb{C}(x, y) : \mathbb{C}(y)) = 2$. Тем не менее, в определенном смысле почти для всех плоскостей размерности $n - d$ число точек пересечения с многообразием V одно и то же. Его и принято называть *степенью многообразия*.

собственного подмногообразия имеется хотя бы одна точка, принадлежащая многообразию V .

Нам нужно получить более тонкое утверждение — о том, что над любой точкой вне собственного подмногообразия лежат в точности δ различных точек из V . Для этого мы используем понятие дискриминанта, которое уже появлялось в разделе 3.11. Пусть имеется многочлен

$$a(X) = a_0 + a_1X + \dots + a_NX^N = a_N(X - \theta_1) \dots (X - \theta_N)$$

с корнями $\theta_1, \dots, \theta_N$, принадлежащими его полю разложения. Напомним, что *дискриминантом* многочлена $a(X)/a_N$ называется величина

$$D := \prod_{1 \leq i < j \leq N} (\theta_i - \theta_j)^2.$$

Из основной теоремы о симметрических многочленах и из формул Виета вытекает, что D есть многочлен от $a_0/a_N, \dots, a_{N-1}/a_N$ над тем же кольцом, которому принадлежат коэффициенты. Другими словами, дискриминант многочлена $a(X)/a_N$ является многочленом от коэффициентов многочлена $a(X)$, деленным на некоторую степень старшего коэффициента a_N . Очевидно, дискриминант многочлена отличен от нуля в том и только том случае, когда многочлен имеет только простые корни.

Для каждого $d + 1 \leq i \leq n$ элемент x_i алгебраичен над полем $K(x_1, \dots, x_{i-1})$. Соответствующий минимальный многочлен выберем таким образом, чтобы все коэффициенты принадлежали кольцу $K[x_1, \dots, x_{i-1}]$, и запишем его в виде $g_i(x_1, \dots, x_{i-1}, X_i)$, где

$$g_i(X_1, \dots, X_i) = \sum_{j=0}^{\delta_i} g_{ij}(X_1, \dots, X_{i-1}) X_i^j,$$

$$[g_i, \delta_i] = g_{i, \delta_i}(x_1, \dots, x_{i-1}) \neq 0.$$

Частное $g_i(X_1, \dots, X_{i-1}, X_i)/g_{i, \delta_i}(X_1, \dots, X_{i-1})$ — это многочлен от X_i с коэффициентами из поля $K(X_1, \dots, X_{i-1})$. Его дискриминант $D_i(X_1, \dots, X_{i-1})$ имеет вид

$$D_i(X_1, \dots, X_{i-1}) = \frac{h_i(X_1, \dots, X_{i-1})}{(g_{i, \delta_i}(X_1, \dots, X_{i-1}))^{\mu_i}},$$

$$h_i \in K[X_1, \dots, X_{i-1}], \quad \mu_i \in \mathbb{N}.$$

Заметим, что $h_i(x_1, \dots, x_{i-1}) \neq 0$, иначе многочлен $g_i(x_1, \dots, x_{i-1}, X_i)$ имел бы кратные корни, а это невозможно, так как для любого алгебраического элемента над полем нулевой характеристики все корни его минимального многочлена простые.

Пусть $V_i \subseteq K_{X_1, \dots, X_i}$ — алгебраическое замыкание проекции многообразия V на координатное подпространство $K_{X_1, \dots, X_i}$. Как мы уже знаем, каждое многообразие V_i неприводимо. Предположим, что заданы собственные подмногообразия $W_i \subsetneq V_i$, и пусть $Z_n := \emptyset$. Тогда, согласно теореме 9.8.2, существует собственное подмногообразие $Z_{n-1} \subsetneq V_{n-1}$ такое, что для каждой точки из $V_{n-1} \setminus Z_{n-1}$ в $V_n = V$ имеется лишь конечное число лежащих над ней точек и каждая из них принадлежит $V_n \setminus (Z_n \cup W_n)$. Далее, существует собственное подмногообразие $Z_{n-2} \subsetneq V_{n-2}$ такое, что для каждой точки из $V_{n-2} \setminus Z_{n-2}$ в V_{n-1} имеется конечное число лежащих над ней точек и каждая из них принадлежит $V_{n-1} \setminus (Z_{n-1} \cup W_{n-1})$. Продолжая в том же духе, получаем собственные подмногообразия $Z_i \subsetneq V_i$ при всех $d \leq i \leq n$, обладающие следующим свойством: пусть $Z := Z_d \cup W_d$, тогда над любой точкой $(\xi_1, \dots, \xi_d) \in V_d \setminus Z$ лежит конечное число точек вида $(\xi_1, \dots, \xi_n) \in V$ и для каждой из них, т. е. для всех возможных значений $\xi_{d+1}, \dots, \xi_n$, выполняются соотношения

$$(\xi_1, \dots, \xi_i) \in V_i \setminus (Z_i \cup W_i), \quad d+1 \leq i \leq n.$$

Теперь положим $W_{i-1} := \mathcal{V}(g_{i, \delta_i} h_i) \cap V_{i-1}$ при $d+1 \leq i \leq n$ и $W_n := \emptyset$. Как легко видеть, $W_i \neq V_i$. Поэтому существуют рассмотренные выше подмногообразия $Z_i \subsetneq V_i$. Возьмем произвольную точку $(\xi_1, \dots, \xi_d) \in V_d \setminus Z$ и рассмотрим произвольную расположенную над ней точку $(\xi_1, \dots, \xi_n)$ многообразия V . Ясно, что должны выполняться равенства

$$g_i(\xi_1, \dots, \xi_i) = 0, \quad d+1 \leq i \leq n.$$

При этом, согласно определению многообразия Z и отмеченному выше свойству точек $(\xi_1, \dots, \xi_n)$,

$$g_{i, \delta_i}(\xi_1, \dots, \xi_{i-1}) \neq 0, \quad h_i(\xi_1, \dots, \xi_{i-1}) \neq 0.$$

Таким образом, многочлен $g_i(\xi_1, \dots, \xi_{i-1}, X_i)$ имеет в точности δ_i различных корней и каждая точка $(\xi_1, \dots, \xi_i)$, где ξ_i — корень

этого многочлена, принадлежит $V_i \setminus (Z_i \cup W_i)$. Значит, общее число различных точек V над точкой $(\xi_1, \dots, \xi_d) \in V_d \setminus Z$ равно

$$\prod_{d+1 \leq i \leq n} \delta_i = \prod_{d+1 \leq i \leq n} \dim(K(x_1, \dots, x_{i+1}) : K(x_1, \dots, x_i)) = \delta. \quad \square$$

Если система координат $X_1, \dots, X_d$ выбрана в соответствии с теоремой Нётер о нормализации, то над каждой точкой из $K_{X_1, \dots, X_d}$ найдется точка многообразия V . Другими словами, проекция $p_d(V)$ многообразия V на координатное подпространство $K_{X_1, \dots, X_d}$ совпадает с этим подпространством. Чтобы это доказать, нам понадобится следующая красивая лемма.

Лемма 9.10.1 (лемма НАКАЯМЫ). Пусть L — коммутативное ассоциативное кольцо с единицей, J — его идеал, M — модуль над L , порожденный своими элементами $b_1, \dots, b_s$, и предположим, что $JM = M$, где

$$JM := \{a_1 b_1 + \dots + a_s b_s : a_1, \dots, a_s \in J\}.$$

Тогда существует элемент $a \in J$ такой, что $ab = b$ для любого $b \in M$.

Доказательство. Пусть модуль M порождается элементами $b_1, \dots, b_s$. Тогда

$$b_1 = \alpha_{11} b_1 + \dots + \alpha_{1s} b_s,$$

$$\dots \dots \dots$$

$$b_s = \alpha_{s1} b_1 + \dots + \alpha_{ss} b_s,$$

где $\alpha_{ij} \in J$. Очевидно,

$$\det \begin{bmatrix} 1 - \alpha_{11} & -\alpha_{12} & \dots & -\alpha_{1s} \\ -\alpha_{21} & 1 - \alpha_{22} & \dots & -\alpha_{2s} \\ \dots & \dots & \dots & \dots \\ -\alpha_{s1} & -\alpha_{s2} & \dots & 1 - \alpha_{ss} \end{bmatrix} = 1 - a, \quad a \in J.$$

Применение присоединенной матрицы (как мы уже делали раньше, например при доказательстве леммы 8.11.1) дает равенства $(1 - a)b_i = 0$ для $1 \leq i \leq s$, и очевидно, что элемент a является искомым. $\square$

Следствие 9.10.1. Пусть $L \subseteq M$ — коммутативные ассоциативные кольца с единицей и при этом M — модуль конечно типа над L . Тогда $JM \subsetneq M$ для любого собственного идеала J кольца L .

Теорема 9.10.2. *Предположим, что в условиях теоремы 9.10.1 каждый из элементов $x_1, \dots, x_n$ является целым алгебраическим над кольцом $K[x_1, \dots, x_d]$. Тогда над каждой точкой из $K_{X_1, \dots, X_d}$ находится хотя бы одна точка многообразия V , а различных точек не более*

$$\delta = \dim(K(x_1, \dots, x_n) : K(x_1, \dots, x_d)).$$

Доказательство. Полный прообраз $p_d^{-1}(\zeta)$ точки $\zeta = (\xi_1, \dots, \xi_d) \in K_{X_1, \dots, X_d}$ есть алгебраическое многообразие, порожденное идеалом

$$I_\zeta = \langle X_1 - \xi_1, \dots, X_d - \xi_d \rangle + I, \quad I = \mathcal{I}(V).$$

Допустим от противного, что для какой-то точки ζ множество $p_d^{-1}(\zeta)$ пусто. Тогда в силу обобщения основной теоремы алгебры $I_\zeta = K[X_1, \dots, X_n]$. Следовательно,

$$\langle x_1 - \xi_1, \dots, x_d - \xi_d \rangle = K[x_1, \dots, x_n]. \quad (*)$$

Положим $L := K[x_1, \dots, x_d]$ и $M := K[x_1, \dots, x_n]$. Мы уже знаем что из целой алгебраичности элементов $x_{d+1}, \dots, x_n$ над L вытекает конечная порожденность M как модуля над кольцом L . Согласно (*), любой элемент $b \in M$ есть линейная комбинация вида

$$b = (x_1 - \xi_1)b_1 + \dots + (x_d - \xi_d)b_d, \quad \text{где } b_1, \dots, b_d \in M.$$

При этом очевидно, что $x_1 - \xi_1, \dots, x_d - \xi_d \in J$, где J — идеал кольца $L = K[x_1, \dots, x_d]$, порожденный элементами $x_1 - \xi_1, \dots, x_d - \xi_d$. По лемме Накаямы существует элемент $a \in J$ такой, что $ab = b$ для любого $b \in M$. В кольце M есть единица, поэтому можно взять $b = 1$. Значит, J содержит единицу, которую, как легко видеть, он иметь не может. Следовательно, $p_d^{-1}(\zeta) \neq \emptyset$ для любой точки $\zeta \in K_{X_1, \dots, X_d}$.

Пусть множество $p_d^{-1}(\zeta)$ содержит s различных точек многообразия V . Над бесконечным полем всегда можно найти ненулевой многочлен, скажем $f(X_1, \dots, X_n)$, принимающий различные значения в этих точках. Пусть m — степень минимального многочлена для $f(x_1, \dots, x_n)$ как элемента расширения $K(x_1, \dots, x_n) \supseteq K(x_1, \dots, x_d)$. Кольцо $K[x_1, \dots, x_d]$ изоморфно $K[X_1, \dots, X_d]$ и поэтому целозамкнуто. Согласно теореме 8.11.2

все коэффициенты *приведенного* минимального многочлена ¹⁾ принадлежат кольцу $K[x_1, \dots, x_d]$. Итак, мы имеем соотношение

$$\sum_{i=0}^{m-1} a_i(x_1, \dots, x_d)(f(x_1, \dots, x_n))^i + (f(x_1, \dots, x_n))^m = 0,$$

$$a_0, \dots, a_{m-1} \in K[X_1, \dots, X_d],$$

которое тождественно выполняется во всех точках многообразия V . Отсюда ясно, что $s \leq m \leq \delta$. $\square$

Изложение части уже полученных и некоторых новых результатов удобно проводится на языке *конечных отображений*, называемых также *конечными морфизмами*. Пусть $V \subseteq K^n$ и $W \subseteq K^m$ — неприводимые алгебраические многообразия и $f: V \rightarrow W$ — отображение, заданное полиномами, которые переводят точки из V в точки из W . Оно называется *морфизмом* многообразия V в многообразие W и естественным образом порождает отображение f_* координатного кольца $K[W]$ в координатное кольцо $K[V]$:

$$f_*(h(y)) := h(f(x)) \in K[V], \quad h(y) \in K[W].$$

Отображение f_* является гомоморфизмом, и его образ $f_*(K[W])$ — это подкольцо кольца $K[V]$. Отображение f называется *конечным отображением* или *конечным морфизмом*, если кольцо $K[V]$ цело над кольцом $f_*(K[W])$.

Теорема 9.10.3. Пусть $V \subseteq K^n$, $W \subseteq K^m$ — неприводимые многообразия над алгебраически замкнутым полем K и $f: V \rightarrow W$ — конечное отображение. Тогда:

- для любого алгебраического подмногообразия $Z \subseteq V$ его образ $f(Z) \subseteq W$ является алгебраическим подмногообразием в многообразии W ,
- $f(V) = W$ в том и только том случае, когда ядро отображения f_* состоит только из нуля (сюръективность отображения $f: V \rightarrow W$ равносильна инъективности отображения $f_*: K[W] \rightarrow K[V]$),
- для каждой точки $\zeta \in f(V)$ ее полный прообраз $f^{-1}(\zeta)$ содержит конечное число точек.

¹⁾ Приведенность означает, что старший коэффициент равен 1.

Доказательство. Пусть функция $h(x) \in K[V]$ удовлетворяет уравнению целой зависимости вида

$$(h(x))^N + \sum_{i=0}^{N-1} a_i(f(x))(h(x))^i = 0, \quad a_0(y), \dots, a_{N-1}(y) \in K[W].$$

Это означает, что

$$(h(\xi))^N + \sum_{i=0}^{N-1} a_i(f(\xi))(h(\xi))^i = 0 \quad \forall \xi \in V,$$

и очевидно, то же будет верно для всех точек $\xi \in Z \subseteq V$. Поэтому кольцо $K[Z]$ цело над кольцом $f_*(K[Z'])$, где $Z' \subseteq W$ — любое подмногообразие, содержащее образ $f(Z)$. Как следствие, $K(Z)$ является модулем конечного типа над $f_*(K[Z'])$.

Пусть $Z' = \bar{f(Z)}$ — алгебраическое замыкание образа $f(Z)$. Тогда отображение f_* инъективно, если его рассматривать как отображение из $K[Z']$ в $K[Z]$. Пусть $h(y) \in K[Z']$ и $h(f(\xi)) = 0$ для всех $\xi \in Z$. Согласно утверждению 9.1.5, если многочлен обращается в нуль на некотором множестве, то он обращается в нуль и на его алгебраическом замыкании $\Rightarrow h(\zeta) = 0$ для всех $\zeta \in Z' \Rightarrow h(y) = 0$.

Теперь возьмем произвольную точку $\zeta = (\zeta_1, \dots, \zeta_m) \in Z'$ и рассмотрим идеал

$$I = \langle h_1(y) - \zeta_1, \dots, h_m(y) - \zeta_m \rangle \subsetneq K[Z'],$$

где $h_1(y), \dots, h_m(y)$ — координатные функции кольца $K[Z']$. Идеал I , очевидно, собственный, и в силу инъективности отображения $f_*: K[Z'] \rightarrow K[Z]$ его образ

$$f_*(I) = \langle h_1(f(x)) - \zeta_1, \dots, h_m(f(x)) - \zeta_m \rangle \subsetneq f_*(K[Z'])$$

будет собственным идеалом в кольце $f_*(K[Z'])$. Согласно следствию 9.10.1 из леммы Накаямы, $f_*(I)K[Z] \neq K[Z]$. Значит, в силу обобщения основной теоремы алгебры, идеал $f_*(I)K[Z]$ имеет хотя бы один общий нуль $\xi \in Z$. Получаем

$$h_1(f(\xi)) = \zeta_1, \quad \dots, \quad h_m(f(\xi)) = \zeta_m.$$

Таким образом, $Z' = f(Z)$, т. е. первое утверждение теоремы доказано.

Далее, пусть $h(y) \in K[W]$ и $h(f(x)) = 0$. Если $h(y) \neq 0$, то $h(\zeta) \neq 0$ хотя бы в одной точке $\zeta \in W$ и при этом $\zeta \notin f(V)$.

Таким образом, если $\ker f_* \neq 0$, то $f(V) \neq W$. Обратно, если $f(V) = \overline{f(V)} \neq W$, то заведомо есть многочлен, который обращается в нуль на множестве $f(V)$, но отличен от нуля в какой-то точке из W . Значит, имеется ненулевая функция $h(y)$, для которой $h(f(x)) = 0 \Rightarrow \ker f_* \neq 0$.

Третье утверждение теоремы оставляем в качестве упражнения. $\square$

Следствие 9.10.2. В условиях теоремы 9.10.2 множества $p_i(V)$ являются алгебраическими многообразиями.

Задача 406. Докажите, что алгебраическое многообразие имеет размерность нуль в том и только том случае, когда оно состоит из конечного числа точек.

Задача 407. Докажите, что размерность алгебраического замыкания проекции многообразия не может быть выше размерности данного многообразия.

Задача 408. Докажите, что если алгебраическое многообразие в $\mathbb{C}^n$ задано как множество нулей одного неприводимого многочлена степени δ , то его пересечение почти с любой прямой содержит ровно δ различных точек.

9.11. Размерность собственного подмногообразия

Теорема 9.11.1. Размерность собственного подмногообразия неприводимого многообразия V строго меньше размерности V .

Доказательство. Рассмотрим расщепление собственного подмногообразия на неприводимые компоненты, и пусть W — неприводимая компонента максимальной размерности и J — простой идеал, который ее аннулирует. Если неприводимое многообразие V обнуляется простым идеалом I , то согласно условию теоремы $J \supseteq I$.

Пусть K — исходное поле, а $K[V]$ и $K[W]$ — координатные кольца неприводимых многообразий V и W . Отображение $f + I \rightarrow f + J$, $f \in K[X]$, является корректно определенным гомоморфизмом кольца $K[V]$ на $K[W]$. Обозначим его ядро через R . Тогда $K[W] \cong K[V]/R$, т.е. элементы кольца $K[W]$ можно считать вычетами кольца $K[V]$ по идеалу R . Рассмотрим произвольные d элементов

$$u_1 + R, \dots, u_d + R \in K[W], \quad u_1, \dots, u_d \in K[V].$$

Согласно условию, идеал R не является нулевым. Возьмем $0 \neq u \in R$. Пусть

$$d = \text{trdeg}(K(V) : K).$$

Тогда система элементов $u_1, \dots, u_d, u$ алгебраически зависима над полем K , т.е. для некоторого ненулевого многочлена $f \in K[X_1, \dots, X_d, X_{d+1}]$ выполняется равенство $f(u_1, \dots, u_d, u) = 0$. Многочлен f можно считать неприводимым над K . Поскольку $u \neq 0$, он не может иметь вид cu , где $c \in K$ — некоторая константа. Поэтому f не делится на u и, следовательно, $f(X_1, \dots, X_d, 0) \neq 0$. В то же время

$$f(u_1 + R, \dots, u_d + R, 0) = 0.$$

Таким образом, любые d элементов кольца $K[W]$ алгебраически зависимы над K . $\square$

Задача 409. Докажите, что множество всех вырожденных комплексных матриц порядка n является алгебраическим многообразием в $\mathbb{C}^{n^2}$. Найдите его размерность.

9.12. Размерность многообразия и ранг матрицы Якоби

Пусть $V \subseteq K_{X_1, \dots, X_n}$ — неприводимое алгебраическое многообразие с координатным кольцом $K[x_1, \dots, x_n]$. В точке $\xi = (\xi_1, \dots, \xi_n) \in V$ естественным образом вводится понятие касательной плоскости $T_V(\xi)$ как множества точек из K^n , удовлетворяющих системе линейных алгебраических уравнений вида

$$\sum_{i=1}^n \frac{\partial f}{\partial X_i}(\xi) (X_i - \xi_i) = 0 \quad \forall f \in I,$$

где I — идеал, состоящий из всех обнуляющих V многочленов. Матрица коэффициентов этой системы имеет бесконечное число строк, соответствующих различным многочленам $f \in I$ и составленных из значений частных производных многочлена f по переменным $X_1, \dots, X_n$ в точке ξ . Эта матрица называется *матрицей Якоби* идеала I в точке ξ . Обозначение: $J_V(\xi)$. Направляющее пространство касательной плоскости (множество решений соответствующей однородной системы) называется *касательным*

пространством. Очевидно, что размерность касательной плоскости связана с рангом матрицы Якоби соотношением

$$\dim T_V(\xi) = n - \text{rank } J_V(\xi).$$

Под *рангом точки* $\xi \in V$ понимается ранг матрицы Якоби $J_V(\xi)$ в этой точке. Таким образом, размерность касательной плоскости в точке $\xi \in V$ есть размерность пространства, в котором содержится многообразие V , минус ранг данной точки.

При выборе главной точки $x = (x_1, \dots, x_n)$ с координатами $x_i = [X_i]$ матрица $J_V(x)$ имеет элементы, принадлежащие координатному кольцу $K[x_1, \dots, x_n]$, и может также рассматриваться как матрица над полем $K(x_1, \dots, x_n)$.

Лемма 9.12.1. *Ранг матрицы Якоби $J_V(x)$ связан с размерностью неприводимого многообразия V соотношением*

$$\dim V = n - \text{rank } J_V(x).$$

Доказательство. Согласно теореме 8.12.2, степень трансцендентности координатного поля $K(x_1, \dots, x_n)$ над полем K равна размерности линейного пространства обнуляющих K дифференцирований поля $K(x_1, \dots, x_n)$ над тем же самым полем $K(x_1, \dots, x_n)$. В разделе 8.12 отмечалось также, что данное пространство дифференцирований изоморфно линейному подпространству решений

$$(c_1, \dots, c_n) \in (K(x_1, \dots, x_n))^n$$

однородной системы уравнений вида

$$\sum_{i=1}^n \frac{\partial f}{\partial X_i}(x) c_i = 0 \quad \forall f \in I. \quad \square$$

Теорема 9.12.1. *Для неприводимого многообразия V существует собственное подмногообразие $W \subsetneq V$ такое, что для любой точки $\xi \in V \setminus W$ выполняются равенства*

$$\dim T_V(\xi) = \min_{\zeta \in V} \dim T_V(\zeta) = n - \max_{\zeta \in V} \text{rank } J_V(\zeta) = \dim V.$$

Доказательство. Пусть идеал I порождается многочленами $f_1, \dots, f_m$. Матрица $J_V(x)$ рассматривается над полем $K(x_1, \dots, x_n)$, и пусть ее ранг равен рангу $m \times n$ -подматрицы A , расположенной на строках, отвечающих порождающим многочленам.

Для любой матрицы, в том числе и для A , существуют невырожденные матрицы $\hat{P}$ и $\hat{Q}$ над тем же самым полем, для которых

$$\hat{P}A\hat{Q} = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}, \quad I_r \text{ — единичная матрица порядка } r = \text{rank } A.$$

В силу доказанной выше леммы, $r = n - \dim V$. Элементы матрицы A принадлежат на самом деле кольцу $K[x_1, \dots, x_n]$. Очевидно, что каждую из матриц $\hat{P}$ и $\hat{Q}$ можно преобразовать в матрицу с элементами из того же кольца путем умножения на некоторые ненулевые элементы этого кольца:

$$P = \phi(x_1, \dots, x_n)\hat{P}, \quad Q = \psi(x_1, \dots, x_n)\hat{Q}, \quad \phi, \psi \in K[X_1, \dots, X_n].$$

Таким образом, элементы матриц

$$A = A(x), \quad P = P(x), \quad Q = Q(x), \quad x = (x_1, \dots, x_n),$$

принадлежат координатному кольцу $K[x_1, \dots, x_n]$ и выполняется равенство

$$P(x)A(x)Q(x) = \phi(x)\psi(x) \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}.$$

Следовательно, для любой точки $\xi \in V$

$$P(\xi)A(\xi)Q(\xi) = \phi(\xi)\psi(\xi) \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}.$$

Пусть $p = \det P$ и $q = \det Q$. Очевидно, что p, q, ϕ, ψ — это многочлены, не равные нулю тождественно на V . Поэтому множество нулей каждого из них не покрывает множество $V \Rightarrow W_1 := \mathcal{V}(pq\phi\psi) \cap V \neq V \Rightarrow$ в любой точке $\xi \in V \setminus W_1$ имеет место равенство $\text{rank } A(\xi) = r$.

Далее, пусть r' — максимальный ранг точек многообразия V . Обозначим через W_2 множество точек из V , для которых ранг строго меньше. Это множество состоит из тех и только тех точек $\xi \in V$, в которых для матрицы Якоби $J_V(\xi)$ обращаются в нуль все миноры порядка $r' - 1$. Таким образом, W_2 — это алгебраическое многообразие, строго меньшее, чем V . В силу неприводимости V подмногообразие $W := W_1 \cup W_2$ будет для V собственным. Оно же и является искомым подмногообразием. $\square$

Точка ξ неприводимого многообразия V называется *регулярной* (неособой, гладкой, простой), если $\dim T_V(\xi) = \dim V$, и *особой* или *сингулярной* в противном случае. Согласно теореме 9.12.1, регулярные точки неприводимого многообразия —

это точки максимального ранга, а особые точки — точки строго меньшего ранга.

Задача 410. Пусть I — произвольный идеал с множеством нулей V . Верно ли, что ранг матрицы Якоби идеала I в каждой точке ξ многообразия $V(I)$ равен рангу матрицы $J_V(\xi)$?

Задача 411. Докажите, что размерности рационально эквивалентных неприводимых многообразий равны.

Задача 412. Докажите, что любое неприводимое многообразие размерности d рационально эквивалентно неприводимой многообразию в пространстве размерности $d + 1$.

Задача 413. Пусть V — непустое неприводимое многообразие, $K[x_1, \dots, x_n]$ — его координатное кольцо, $m_\xi \subseteq K[V]$ — идеал полиномиальных функций на V , обращающихся в нуль в точке $\xi \in V$. Докажите, что фактор-кольцо m_ξ/m_ξ^2 как линейное пространство над полем K изоморфно касательному пространству к многообразию V в точке ξ . Идеал m_ξ определяется как идеал, порожденный всеми произведениями ab , где $a, b \in m_\xi$.

9.13. Размерность пересечения многообразий

Напомним, что гиперповерхностью называется множество нулей одного многочлена.

Лемма 9.13.1. Пусть V — неприводимое многообразие размерности d в пространстве над алгебраически замкнутым полем и W — произвольная гиперповерхность, имеющая непустое пересечение с многообразием V . Тогда если $V \cap W \neq V$, то размерность любой неприводимой компоненты многообразия $V \cap W$ равна $d - 1$.

Доказательство. Размерность каждой неприводимой компоненты многообразия

$$A := V \cap W \subseteq V$$

не больше чем $d - 1$ (теорема 9.11.1 о размерности собственного подмногообразия). Покажем, что если W — гиперповерхность, то она не может быть меньше.

Пусть W задается уравнением $f(X_1, \dots, X_n) = 0$. Полагаем, что система координат выбрана в соответствии с теоремой Нётер

о нормализации: в координатном кольце $R := K[x_1, \dots, x_n]$ элементы $x_1, \dots, x_d$ алгебраически независимы над полем K , и каждый элемент, в том числе и $f(x_1, \dots, x_n)$ (функция с областью определения V и одновременно вычет, вместо $[f]$ далее пишем просто f), является целым алгебраическим над целозамкнутым кольцом $Q := K[x_1, \dots, x_d]$. Минимальный многочлен для f над полем $K(x_1, \dots, x_d)$ можно выбрать в виде (теорема 8.11.2)

$$h(X) = \sum_{i=0}^{s-1} h_i(x_1, \dots, x_d) X^i + X^s, \quad h_0, \dots, h_{s-1} \in Q.$$

Для произвольной точки $(\xi_1, \dots, \xi_n) \in V$ имеем

$$\begin{aligned} h(f(\xi_1, \dots, \xi_n)) = 0 \Rightarrow \sum_{i=0}^{s-1} h_i(\xi_1, \dots, \xi_d) (f(\xi_1, \dots, \xi_n))^i + \\ + (f(\xi_1, \dots, \xi_n))^s = 0. \end{aligned}$$

Если $f(\xi_1, \dots, \xi_n) = 0$, то $h_0(\xi_1, \dots, \xi_d) = 0 \Rightarrow p_d(A) \subseteq A'$, где $A' \subseteq K_{X_1, \dots, X_d}$ — гиперповерхность, заданная уравнением $h_0(X_1, \dots, X_d) = 0$. Наша цель — доказать, что $p_d(A) = A'$.

Множество fR — это главный идеал кольца R , в котором каждая функция обнуляется на $A \subsetneq V$. Добавив к нему все функции, обнуляющие A , получаем идеал $\text{rad}(fR)$. Теорема 9.10.3 утверждает, что множество $p_d(A)$ алгебраически замкнуто. Все функции кольца $Q \subset R$, которые обращаются в нуль на $p_d(A)$, составляют идеал $\text{rad}(fR) \cap Q$. Мы сейчас докажем, что

$$\text{rad}(fR) \cap Q = \text{rad}(h_0Q). \quad (*)$$

То, что правая часть есть часть левой части, совсем просто. Начнем с того, что из уравнения для f видно, что $h_0 \in fR$. Далее, пусть $g \in \text{rad}(h_0Q)$. Тогда для некоторой функции $q \in Q$ и некоторого $l \in \mathbb{N}$ находим

$$g^l = h_0q \in fR \Rightarrow g \in \text{rad}(fR).$$

Обратное включение получается сложнее. Здесь нам понадобятся определители операторов умножения на различные элементы поля, которое рассматривается как конечномерное линейное пространство над своим подполем. Определитель линейного оператора — это определитель матрицы, которая его представляет в произвольно выбранном базисе (все матрицы одного оператора в разных базисах подобны, поэтому их определители не

зависят от выбора базиса). Пусть поле M получается из поля L присоединением конечного числа алгебраических элементов. Тогда M есть конечномерное линейное пространство над полем L . Для произвольно взятого и зафиксированного элемента $a \in M$ преобразование $b \rightarrow ab$ является, очевидно, линейным оператором на M . Его определитель будем обозначать через $\det(a)$ и называть *определителем элемента* $a \in M$. Очевидно, что $\det(a) \in L$. В теории полей этот определитель называется *нормой* элемента a .

Под *характеристическим многочленом элемента* $a \in M$ понимается характеристический многочлен оператора умножения на элемент a . Это характеристический многочлен матрицы данного оператора в произвольно выбранном базисе (такие матрицы подобны и их характеристические многочлены совпадают). Для матрицы $A \in L^{m \times m}$ это многочлен вида $\phi(\lambda) := \det(A - \lambda I)$, его степень равна m , старший коэффициент и свободный член суть $(-1)^m$ и $\phi(0) = \det A$.

Утверждение 9.13.1. Пусть поле M является линейным пространством размерности ν над своим подполем L и $\phi(\lambda) \in L[\lambda]$ — характеристический многочлен элемента $a \in M$. Пусть $\psi(\lambda) \in L[\lambda]$ — приведенный минимальный многочлен этого же элемента, и пусть его степень равна μ . Тогда ν делится на μ и справедлива формула

$$\det(a) = \phi(0) = (-1)^\nu (\psi(0))^\tau, \quad \nu = \mu\tau.$$

Для доказательства рассмотрим цепочку расширений

$$L \leq L(a) \leq M, \quad \dim(L(a) : L) = \mu, \quad \dim(M : L(a)) = \tau.$$

Базисом пространства $L(a)$ над L является система элементов $1, a, \dots, a^{\mu-1}$. Если $u_1, \dots, u_\tau$ — базис пространства M над $L(a)$, то система элементов

$$u_1, au_1, \dots, a^{\mu-1}u_1, u_2, au_2, \dots, a^{\mu-1}u_2, \dots, u_\tau, au_\tau, \dots, a^{\mu-1}u_\tau$$

является базисом пространства M над полем L . Пусть

$$\psi(\lambda) = \lambda^\mu + \sum_{i=0}^{\mu-1} c_i \lambda^i, \quad c_0, \dots, c_{\mu-1} \in L \Rightarrow a^\mu = - \sum_{i=0}^{\mu-1} c_i a^i.$$

Тогда матрица A оператора умножения на a в рассмотренном выше базисе получает блочно диагональный вид

$$A = \begin{bmatrix} B & & \\ & \ddots & \\ & & B \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & 0 & \dots & 0 & -c_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & -c_{\mu-1} \end{bmatrix} \in L^{\mu \times \mu}.$$

Значит, $\det(a) = \det A = (\det B)^\tau = ((-1)^\mu c_0)^\tau = (-1)^\nu (\psi(0))^\tau$.

Теперь мы готовы закончить обоснование равенства (*). Предположим, что

$$g \in \operatorname{rad}(fR) \cap Q \Rightarrow g^l = fq, \quad q \in R, \quad l \in \mathbb{N}.$$

В линейном пространстве $K(x_1, \dots, x_n)$ над полем $K(x_1, \dots, x_d)$ рассмотрим линейный оператор умножения на g . Поскольку $g \in K(x_1, \dots, x_d)$, его матрица будет скалярной в любом базисе $\Rightarrow \det(g) = g^\nu$, где $\nu := \dim(K(x_1, \dots, x_n) : K(x_1, \dots, x_d))$. Для определителя элемента g^l получается равенство

$$\det(g^l) = (\det(g))^l = g^{\nu l} = \det(f) \det(q), \quad \det(f), \det(q) \in Q.$$

Приведенный минимальный многочлен элемента f над $K(x_1, \dots, x_d)$ ранее получил обозначение $h(X)$ и, в силу целозамкнутости кольца Q , все его коэффициенты принадлежат Q . Согласно утверждению 9.13.1, $\det(f) = (-1)^\nu h_0^\tau$, $\tau = \nu / \deg h$. Таким образом, $g \in \operatorname{rad}(\det(f)Q) = \operatorname{rad}(h_0^\tau Q) = \operatorname{rad}(h_0 Q)$ и тем самым равенство (*) установлено. Его прямым следствием является нужное нам равенство $p_d(A) = A'$.

Итак, алгебраическое многообразие $p_d(A)$ есть гиперповерхность пространства K^d , заданная уравнением $h_0(X_1, \dots, X_d) = 0$. Размерность гиперповерхности в d -мерном пространстве равна $d - 1$, и, следовательно,

$$d - 1 = \dim p_d(A) \leq \dim A \leq d - 1 \Rightarrow \dim A = d - 1.$$

Остается понять, почему *каждая* неприводимая компонента многообразия A имеет размерность $d - 1$. Пусть $A_1, \dots, A_r$ — различные неприводимые компоненты и $p_1, \dots, p_r$ — аннулирующие их простые идеалы. Таким образом, $\operatorname{rad}(fR) = \bigcap_{1 \leq i \leq r} p_i$. Для определенности рассмотрим компоненту A_1 и ее идеал $p := p_1$. Напомним, что если целостное кольцо содержит поле K , то его степень трансцендентности над K определяется как сте-

пень трансцендентности соответствующего поля частных над полем K . Нам нужно получить равенство

$$\text{trdeg}_K(R/p) = \text{trdeg}_K(R) - 1.$$

В теории колец оно известно как утверждение, эквивалентное *теореме Крулля о главном идеале*. Понятно, что мы уже получили его доказательство в случае $r = 1$. Теперь покажем, как оно сводится именно к этому случаю.

Возьмем функцию $g \in \left(\bigcap_{2 \leq i \leq r} p_i \right) \setminus p$ и в пространстве K^{n+1}

рассмотрим график $\bar{V}$ функции $\xi_{n+1} = 1/g(\xi_1, \dots, \xi_n)$, определенной во всех точках $(\xi_1, \dots, \xi_n) \in V \subseteq K^n$, кроме тех из них, для которых $g(\xi_1, \dots, \xi_n) = 0$. Точки $(\xi_1, \dots, \xi_{n+1}) \in \bar{V}$ определяются системой полиномиальных уравнений, в которую входят уравнения аннулятора многообразия V и дополнительное уравнение

$$g(X_1, \dots, X_n)X_{n+1} - 1 = 0.$$

Очевидно, что каждой функции $f(x_1, \dots, x_n)$ координатного кольца $R = K[V]$ соответствует некоторая функция координатного кольца $\bar{R} = K[\bar{V}]$, а именно — функция, которая определяется тем же многочленом $f(X_1, \dots, X_n)$, но рассматривается на многообразии $\bar{V}$. Данное соответствие является гомоморфизмом кольца R в кольцо $\bar{R}$, и, более того, оно инъективно: если многочлен обращается в нуль на V вне точек его собственного подмногообразия, то этот многочлен обращается в нуль и на данном подмногообразии. Таким образом, кольцо R можно считать вложенным в кольцо $\bar{R}$, а элементы $x_1, \dots, x_n$ — принадлежащими одновременно R и $\bar{R}$, и, следовательно ¹⁾,

$$R = K[x_1, \dots, x_n], \quad \bar{R} = K[x_1, \dots, x_n, x_{n+1}] = R[x_{n+1}].$$

Итак, $\bar{R}$ — это целостное кольцо с единицей, которое получается из поля K кольцевым присоединением элементов $x_1, \dots, x_n$ и $x_{n+1} := 1/g \in K(x_1, \dots, x_n)$. Элемент x_{n+1} удовлетворяет уравнению $gX_{n+1} - 1 = 0$ и поэтому алгебраичен над K . Следовательно,

$$\text{trdeg}_K(\bar{R}) = \text{trdeg}_K(R) = d.$$

¹⁾ Можно заметить, что кольцо $\bar{R}$ изоморфно кольцу частных $\bar{R} := S^{-1}R$ по мультипликативно замкнутой системе $S = \{g^i : i = 0, 1, \dots\}$ (см. раздел 8.5), а рассмотренное нами вложение представляет собой естественный гомоморфизм $R \rightarrow \bar{R}$, определенный правилом $a \rightarrow a/1$.

Пространство $K^n = K_{X_1, \dots, X_n}$ вкладывается в $K^{n+1} = K_{X_1, \dots, X_n, X_{n+1}}$, неприводимому многообразию $V \subseteq K_n$ соответствует неприводимое многообразие $\bar{V} \subseteq K^{n+1}$, а многообразиям $A, A_1, \dots, A_r \subseteq V$ соответствуют многообразия $\bar{A}, \bar{A}_1, \dots, \bar{A}_r \subseteq \bar{V}$. При этом $\bar{A}_2 = \dots = \bar{A}_r = \emptyset$ и $\bar{A} = \bar{A}_1$, т.е. пересечение многообразия $\bar{V}$ с гиперплоскостью $\{f = 0\}$ состоит из одной неприводимой компоненты $\bar{A} = \bar{A}_1$, которая аннулируется простым идеалом $\bar{p} := \text{rad}(f\bar{R})$. По доказанному ранее, если степень трансцендентности координатного кольца равна d , то размерность множества нулей собственного главного идеала этого кольца равна $d - 1$. После перехода к $\bar{V}$ многообразию $\bar{A}_1$ стало неприводимым подмногообразием, которое аннулируется главным идеалом кольца $\bar{R}^1$). Многообразие $\bar{A}_1 \subsetneq K^{n+1}$ рационально эквивалентно многообразию $A_1 \subsetneq K^n$, поэтому (теорема 9.7.2) $\text{trdeg}_K(R/p) = \text{trdeg}_K(\bar{R}/\bar{p})$. $\square$

Теорема 9.13.1. Пусть V и W — неприводимые многообразия в n -мерном пространстве над алгебраически замкнутым полем. Если они имеют непустое пересечение, то выполняется неравенство

$$\dim V \cap W \geq \dim V + \dim W - n.$$

Доказательство. Пусть V и W заданы в n -мерном пространстве над алгебраически замкнутыми полем K . Введем пространство $K_{X_1, \dots, X_n, Y_1, \dots, Y_n}$ и рассмотрим в нем множество

$$V \times W := \{(a_1, \dots, a_n, b_1, \dots, b_n) : (a_1, \dots, a_n) \in V, (b_1, \dots, b_n) \in W\}.$$

Нетрудно доказать, что $V \times W$ — это неприводимое многообразие размерности $d = \dim V + \dim W$.

Точка $(c_1, \dots, c_n)$ принадлежит пересечению $V \cap W$ в том и только том случае, когда $(c_1, \dots, c_n, c_1, \dots, c_n) \in V \times W$. Отсюда ясно, что размерность многообразия $V \cap W$ равна размерности многообразия Z , которое получается при пересечении $V \times W$

¹⁾ Здесь мы ясно видим смысл термина *локализация* — на заданном многообразии строится рациональное отображение, которое принимает конечные значения в каких-то точках интересующего нас неприводимого подмногообразия, а точки вне этого подмногообразия переводятся в бесконечность и тем самым исключаются из образа данного отображения.

гиперплоскостями $X_1 - Y_1 = 0, \dots, X_n - Y_n = 0$. В силу леммы 9.13.1,

$$\dim (V \times W) \cap \mathcal{V}(X_1 - Y_1) \geq d - 1.$$

Более того, при пересечении неприводимого многообразия гиперплоскостью та же оценка снизу получается для размерности любой неприводимой компоненты пересечения. Поэтому если U — любая неприводимая компонента, имеющая непустое пересечение с гиперплоскостью $X_2 - Y_2 = 0$, то еще одно применение леммы 9.13.1 дает оценку

$$\dim U \cap \mathcal{V}(X_2 - Y_2) \geq d - 2,$$

причем оценка справедлива для каждой неприводимой компоненты данного пересечения. Таким образом, мы снова имеем возможность использовать лемму 9.13.1. Ее n -кратное применение, очевидно, приведет к неравенству $\dim Z \geq d - n$. $\square$

Задача 414. Алгебраические многообразия V и W в пространстве $\mathbb{C}^n$ имеют непустое пересечение. Верно ли неравенство $\dim V \cap W \geq \dim V + \dim W - n$ в случае приводимых многообразий?

Задача 415. Пусть неприводимое многообразие V имеет размерность d . Докажите, что для любой цепочки строго вложенных непустых неприводимых подмногообразий

$$V_1 \subsetneq V_2 \subsetneq \dots \subsetneq V_s \subsetneq V$$

выполняется неравенство $s \leq d$ и существует цепочка, для которой $s = d$.

Задача 416. Докажите, что для неприводимых многообразий V и W их декартово произведение $V \times W$ является неприводимым многообразием размерности $\dim V + \dim W$.

Задача 417. В пространстве $n \times n$ -матриц с комплексными элементами выбрано произвольное подпространство L размерности $d \geq (n - r)^2 + 1$, где $1 \leq r \leq n$. Докажите, что в L содержится ненулевая матрица, ранг которой не выше r .

9.14. Комплексные многообразия

Под ε -окрестностью точки $\xi = (\xi_1, \dots, \xi_n) \in \mathbb{C}^n$ ниже понимается декартово произведение открытых кругов радиуса ε :

$$\mathcal{O}(\xi, \varepsilon) = \{\zeta = (\zeta_1, \dots, \zeta_n) : |\zeta_i - \xi_i| < \varepsilon, 1 \leq i \leq n\}.$$

Нам нужен факт непрерывной зависимости корней многочлена от коэффициентов. Вот одна из его формулировок.

Лемма 9.14.1. Пусть $a = (a_0, \dots, a_{n-1}) \in \mathbb{C}^n$ и $f_a(X) = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{C}[X]$, и пусть Z_a — множество различных корней многочлена $f_a(X)$. Тогда для любого $\varepsilon > 0$ существует $\delta > 0$ такое, что в ε -окрестности каждого корня многочлена $f_a(X)$ содержится хотя бы один корень любого многочлена $f_b(X)$ из δ -окрестности точки a : для каждой точки b из δ -окрестности точки a имеет место неравенство

$$\max_{\xi \in Z_a} \min_{\zeta \in Z_b} |\zeta - \xi| < \varepsilon,$$

Доказательство. Пусть ξ — корень многочлена $f_a(X)$, и пусть $\zeta_1, \dots, \zeta_n$ — все корни многочлена $f_b(X)$ с учетом кратностей. Рассмотрим многочлен $p(Y) := f_b(\xi + Y)$. Его корни — это разности $\zeta_1 - \xi, \dots, \zeta_n - \xi$. В силу формул Виета,

$$\prod_{i=1}^n (\zeta_i - \xi) = p(0) = f_b(\xi) \Rightarrow \min_{1 \leq i \leq n} |\zeta_i - \xi| \leq |f_b(\xi)|^{1/n}. \quad \square$$

Теорема 9.14.1. Пусть W — собственное подмногообразие неприводимого многообразия $V \subseteq \mathbb{C}^n$. Тогда в любой сколь угодно малой окрестности произвольной точки многообразия V содержится точка из множества $V \setminus W$.

Доказательство. Выберем систему координат $X_1, \dots, X_n$ в соответствии с теоремой Нётер о нормализации. Полагаем, что координатные функции $x_1, \dots, x_d$ образуют базис трансцендентности поля $\mathbb{C}(x_1, \dots, x_n)$ над $\mathbb{C}$ и кольцо $\mathbb{C}[x_1, \dots, x_n]$ цело над кольцом $\mathbb{C}[x_1, \dots, x_d]$. Мы знаем, что при проектировании $p_d(V) = \mathbb{C}^d$ и для любого собственного подмногообразия $W \subsetneq V$ его образ $p_d(W)$ является собственным подмногообразием в координатном подпространстве $\mathbb{C}^d$.

Прежде всего заметим, что теорема довольно легко доказывается в случае, когда исходное многообразие совпадает с координатным пространством. Пусть $Z \subsetneq \mathbb{C}^d$ — произвольное собственное подмногообразие в пространстве $\mathbb{C}^d$ и $\zeta \in Z$. Согласно нашим предположениям, имеется точка $\theta \in \mathbb{C}^d \setminus Z$ и существует многочлен $f(X)$, обращающийся в нуль во всех точках мно-

гоообразия Z и принимающий ненулевое значение в точке θ . Рассмотрим функцию

$$F(t) := f((1-t)\zeta + t\theta) \quad \text{при вещественных } t.$$

Будучи ненулевым многочленом от переменной t , функция $F(t)$ может обращаться в нуль лишь для конечного набора значений параметра t . Поэтому $F(t) \neq 0$ при всех $0 < t < \delta$, если только δ достаточно мало. Соответствующие точки $(1-t)\zeta + t\theta$ не принадлежат Z , а это значит, что в любой достаточно малой окрестности точки $\zeta \in Z$ есть точки из множества $\mathbb{C}^d \setminus Z$.

Условимся использовать штрих для обозначения проекции: если $\xi = (\xi_1, \dots, \xi_n)$ и $x = (x_1, \dots, x_n)$, то $\xi' = (\xi_1, \dots, \xi_d)$ и $x' = (x_1, \dots, x_d)$. Теперь возьмем произвольную точку $a \in W \subsetneq V$ и рассмотрим ее проекцию $a' = p_d(a)$. Полный прообраз $p_d^{-1}(a')$ содержит конечное число различных точек, пусть это точки $a = a_1, a_2, \dots, a_m$. Пусть $g(X) = g(X_1, \dots, X_n)$ — любой многочлен, обнуляющийся в точке $a_1 = a$ и отличный от нуля в точках $a_2, \dots, a_m$. Ключевую роль в нашем доказательстве играет приведенный минимальный многочлен $h(\lambda) \in (\mathbb{C}[x'])[\lambda]$ элемента $g(x) \neq 0$. В силу целозамкнутости кольца $\mathbb{C}[x']$ все его коэффициенты принадлежат кольцу $\mathbb{C}[x']$. Многочлен $h(\lambda) = \lambda^r + \sum_{i=0}^{r-1} h_i(x')\lambda^i$ ассоциируется с функцией

$$H(\theta, \lambda) := \lambda^r + \sum_{i=0}^{r-1} h_i(\theta)\lambda^i \in \mathbb{C}[\lambda], \quad \theta \in \mathbb{C}^d,$$

$$H(\xi', g(\xi)) = 0 \quad \forall \xi \in \mathbb{C}^n.$$

Поскольку $g(a) = 0$, получаем $h_0(a') = 0$.

Мы хотим найти последовательность точек, не принадлежащих $p_d(W) \subsetneq \mathbb{C}^d$ и таких, что последовательность сходится к точке $a' \in p_d(W)$ и при этом в полных прообразах можно выбрать точки, сходящиеся к a . Для реализации этой цели мы рассмотрим пространство $\mathbb{C}^{n+1}$ с координатами $X_1, \dots, X_d, X_0, X_{d+1}, \dots, X_n$ и алгебраическое многообразие $\bar{V} \subseteq \mathbb{C}^{n+1}$, которое порождается многочленами, определяющими исходное многообразие V , и дополнительным многочленом $X_0 - g(X_1, \dots, X_n)$. Очевидно, каждая из координатных функций $x_0, x_{d+1}, \dots, x_n$ является целым алгебраическим элементом над кольцом $\mathbb{C}[x_1, \dots, x_d]$ и $h(\lambda)$ — это минимальный

многочлен для координатной функции x_0 . Пусть π_i обозначает проекцию вида

$$\pi_i: (\xi_1, \dots, \xi_d, \xi_0, \xi_{d+1}, \dots, \xi_n) \rightarrow (\xi_1, \dots, \xi_d, \xi_0, \xi_{d+1}, \dots, \xi_i).$$

Тогда, согласно теореме 9.8.2, в пространстве $\mathbb{C}_{X_1, \dots, X_d}$ имеется собственное многообразие Z такое, что над любой точкой вне Z лежат ровно $r = \deg h$ точек многообразия $\pi_0(\bar{V}) \subseteq \mathbb{C}_{X_1, \dots, X_d, X_0}$ и над каждой из них есть точка многообразия $\bar{V}$. Рассмотрим последовательность точек

$$\theta^{(l)} \rightarrow a', \quad \theta^{(l)} \in \mathbb{C}^d \setminus (Z \cup p_d(W)),$$

и для каждого $l \rightarrow \infty$ выберем такую точку

$$\bar{\xi}^{(l)} = (\xi_1^{(l)}, \dots, \xi_d^{(l)}, \xi_0^{(l)}, \xi_{d+1}^{(l)}, \dots, \xi_n^{(l)}) \in \pi_d^{-1}(\theta^{(l)}),$$

для которой координата $\xi_0^{(l)}$ является наименьшим по модулю корнем полиномиального уравнения

$$H(\theta^{(l)}, \lambda) = 0.$$

Каждая из координатных последовательностей $\xi_i^{(l)}$ ограничена в силу целой алгебраичности координатных функций. Поэтому можно выделить сходящуюся подпоследовательность. Чтобы не усложнять индексацию, будем считать, что

$$\bar{\xi}^{(l)} \rightarrow \bar{\xi} = (\bar{\xi}_1, \dots, \bar{\xi}_d, \bar{\xi}_0, \bar{\xi}_{d+1}, \dots, \bar{\xi}_n).$$

Теперь обратимся к лемме 9.14.1. В нашем случае $H(\theta^{(l)}, \lambda) \rightarrow H(a', \lambda)$ и согласно этой лемме *каждый* из корней многочлена $H(a', \lambda)$ приближается каким-то корнем многочлена $H(\theta^{(l)}, \lambda)$. В том числе и корень $g(a') = 0$.

Значит, при выборе минимального по модулю корня мы получим последовательность корней, сходящуюся к нулю $\Rightarrow \bar{\xi}_0 = 0$. При естественной проекции

$$\bar{\xi} \rightarrow \xi = (\bar{\xi}_1, \dots, \bar{\xi}_d, \bar{\xi}_{d+1}, \dots, \bar{\xi}_n)$$

получаем $\bar{\xi}_0 = g(\xi) = 0$. Очевидно, что $\xi \in p_d^{-1}(a')$, и понятно, что есть единственная возможность $\xi = a$, так как $g(a_i) \neq 0$ при $2 \leq i \leq m$. $\square$

Следствие 9.14.1. *Для любой точки неприводимого многообразия в $\mathbb{C}^n$ в любой сколь угодно малой ее окрестности содержится регулярная точка данного многообразия.*

Теорема 9.14.2. Пусть V и W — неприводимые многообразия в $\mathbb{C}^n$. Если V и W совпадают в окрестности какой-то точки пространства $\mathbb{C}^n$, то $V = W$.

Доказательство. Согласно следствию 9.14.1, можно считать, что многообразия совпадают в окрестности точки, которая является регулярной для каждого из них. Пусть система координат $X_1, \dots, X_n$ выбрана в соответствии с теоремой Нётер о нормализации для многообразия V и $\zeta \in \mathbb{C}_d$ — проекция этой точки. От противного, допустим, что $W \neq V$. Тогда имеется ненулевой многочлен $f \in \mathcal{I}(W) \setminus \mathcal{I}(V)$ и $[f] = f(x_1, \dots, x_n)$ — целый алгебраический элемент над $\mathbb{C}(x_1, \dots, x_d)$. Пусть $[f]$ аннулируется минимальным многочленом вида

$$p(x_1, \dots, x_d, X) = \sum_{i=0}^{m-1} p_i(x_1, \dots, x_d) X^i + X^m, \quad p_i \in \mathbb{C}[X_1, \dots, X_d].$$

Тогда

$$\begin{aligned} p(x_1, \dots, x_d, f(x_1, \dots, x_n)) &= 0 \Rightarrow \\ \Rightarrow p(\xi_1, \dots, \xi_d, f(\xi_1, \dots, \xi_n)) &= 0 \quad \forall (\xi_1, \dots, \xi_n) \in V. \end{aligned}$$

Далее, для любой точки $(\xi_1, \dots, \xi_d)$ из некоторой окрестности точки $\zeta \in \mathbb{C}^d$ значения $\xi_{d+1}, \dots, \xi_n$ можно выбрать таким образом, что точка $(\xi_1, \dots, \xi_n)$ будет общей для V и W . Тогда $f(\xi_1, \dots, \xi_n) = 0$. Следовательно, $p_0(\xi_1, \dots, \xi_d) = 0$ во всех точках некоторой окрестности точки $\zeta \in \mathbb{C}^d$. Отсюда вытекает, что $p_0(X_1, \dots, X_d)$ — нулевой многочлен. Значит, $p_0(x_1, \dots, x_d) = 0$, и если $m \geq 2$, то это противоречит минимальности многочлена $p(x_1, \dots, x_d, X)$. Если $m = 1$, то $f(x_1, \dots, x_n) = 0$, и это противоречит предположению о том, что $f \notin \mathcal{I}(V)$. $\square$

Задача 418. В n -мерном пространстве дано неприводимое многообразие размерности $n - 1$. Докажите, что оно является множеством нулей одного неприводимого многочлена.

9.15. Подготовительная теорема Вейерштрасса

К комплексным многообразиям, конечно же, можно применять известные в анализе теоремы о неявной функции. Более того, у этих теорем есть и чисто алгебраические версии, которые допускают большую свободу в выборе поля.

Чтобы их изложить, нам понадобятся формальные ряды вида

$$f(X_1, \dots, X_n) = \sum_{i_1, \dots, i_n \geq 0} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n} = \sum_{l=0}^{\infty} f_l,$$

где f_l — однородный многочлен степени l . Член f_0 нулевой степени называется *свободным членом*. Сложение и умножение формальных рядов определяется естественным образом и выполняется без проблем, так как при приведении подобных членов возникают только конечные суммы. Кольцо формальных рядов с коэффициентами из поля K является целостным кольцом с единицей и обозначается $K[[X]] = K[[X_1, \dots, X_n]]$.

Ряд f называется обратимым, если для некоторого ряда g имеет место равенство $fg = 1$. Нетрудно проверить, что для обратимости ряда необходимо и достаточно, чтобы его свободный член был ненулевым.

Теорема 9.15.1 (ПОДГОТОВИТЕЛЬНАЯ ТЕОРЕМА ВЕЙЕРШТРАССА). *Предположим, что ряд $f(X_1, \dots, X_n)$ обладает нулевым свободным членом, в его составе есть одночлены вида $a_s X_1^s$, где a_s — элемент поля, и пусть $s \geq 1$ — наименьшая степень для таких одночленов. Тогда для любого ряда $g(X_1, \dots, X_n)$ существует представление*

$$g(X_1, \dots, X_n) = q(X_1, \dots, X_n) f(X_1, \dots, X_n) + \sum_{i=0}^{s-1} r_i(X_2, \dots, X_n) X_1^i,$$

в котором ряды q и $r_0, \dots, r_{s-1}$ определяются однозначно.

Доказательство. Для простоты мы приведем доказательство для случая $s = 1$. Любой ряд g можно записать в виде $g = A(g) + X_1 B(g)$, где ряд $A(g)$ не содержит буквы X_1 . Ряды $A(g)$ и $B(g)$ определяются по g однозначно, и операторы $A: g \rightarrow A(g)$ и $B: g \rightarrow B(g)$ являются линейными. Уравнение $g = qf + r$ относительно рядов q и r очевидно равносильно уравнению $B(g) = B(qf)$ относительно q . Запишем $f = A(f) + X_1 B(f)$. Тогда уравнение относительно q приобретает вид

$$B(g) = B(qA(f)) + qB(f) = p - B(hp),$$

$$p := qB(f), \quad h := -A(f)(B(f))^{-1}.$$

Обратимость ряда $B(f)$ вытекает из предположения о том, что в состав ряда f входит одночлен X_1 . Оператор $M: p \rightarrow B(hp)$ является линейным. Таким образом, для p получается линейное уравнение

$$p - Mp = b, \quad b := B(g).$$

Отсюда вытекает, что

$$p = b + Mb + M^2b + \dots + M^l b + M^{l+1}p, \quad l = 0, 1, \dots$$

Теперь для нас существенно предположение о том, что свободный член ряда f равен нулю. Из него следует, что свободный член ряда h также равен нулю. А отсюда уже нетрудно вывести, что при вычислении членов ряда

$$p := \sum_{i=0}^{\infty} M^i b$$

возникают только конечные суммы. Поэтому правая часть действительно задает некоторый формальный ряд, удовлетворяющий уравнению $p - Mp = b$. Довольно просто устанавливается также единственность решения. $\square$

Следствие 9.15.1 (АЛГЕБРАИЧЕСКАЯ ТЕОРЕМА О НЕЯВНОЙ ФУНКЦИИ). Пусть ряд $f(X_1, \dots, X_n)$ обладает нулевым свободным членом и в его составе есть одночлен X_1 . Тогда существуют обратимый ряд $q(X_1, \dots, X_n)$ и ряд $r(X_2, \dots, X_n)$ такие, что

$$f(X_1, \dots, X_n)q(X_1, \dots, X_n) = X_1 - r(X_2, \dots, X_n).$$

Доказательство. Нужно применить теорему для разложения ряда $g = X_1$. $\square$

Теорема 9.15.2. Предположим, что ряды f_i имеют вид

$$f_i(X_1, \dots, X_n) = X_i + \sum_{j=s+1}^n a_{ij} X_j + \sum_{i_1+\dots+i_n \geq 2} a_{i_1, \dots, i_n}^{(i)} X_1^{i_1} \dots X_n^{i_n},$$

$$1 \leq i \leq s. \quad (*)$$

Тогда для каждого ряда $f \in \mathbb{C}[[X_1, \dots, X_n]]$ существует представление

$$f = \sum_{i=1}^s f_i q_i + h, \quad q_1, \dots, q_r \in K[[X_1, \dots, X_n]],$$

$$h \in K[[X_{r+1}, \dots, X_n]],$$

в котором ряд h определяется однозначно.

Доказательство. Случай $s = 1$ покрывается теоремой 9.15.1. Итак, пусть

$$f = f_1 g_1 + F, \quad g_1 \in \mathbb{C}[[X_1, \dots, X_n]], \quad F \in [[X_2, \dots, X_n]].$$

Чтобы применить индукцию, найдем разложения

$$f_i = f_1 g_i + F_i, \quad g_i \in \mathbb{C}[[X_1, \dots, X_n]], \quad F_i \in \mathbb{C}[[X_2, \dots, X_n]], \\ 2 \leq i \leq s,$$

и заметим, что ряды F_i имеют такой же вид, как и исходные ряды f_i , но зависят только от переменных $X_2, \dots, X_s$. По индуктивному предположению, должно существовать разложение

$$F = \sum_{i=2}^s F_i q_i + h, \quad q_2, \dots, q_s \in \mathbb{C}[[X_2, \dots, X_n]], \\ h \in \mathbb{C}[[X_{s+1}, \dots, X_n]].$$

В итоге находим: $f = \sum_{i=1}^s f_i q_i + h$, $q_1 = g_1 - \sum_{i=2}^s g_i q_i$. Чтобы установить единственность ряда h , рассмотрим соотношение $0 = \sum_{i=1}^s f_i q_i + h$ и докажем, что $h = 0$. Это делается также по индукции. Находим $f_1 g_1 = -F$, а это равенство возможно только в случае $F = 0$, в противном случае в левой части есть моном с переменной X_1 , а в правой части такого монома заведомо нет. $\square$

Следствие 9.15.2. *Кольцо вычетов кольца $K[[X_1, \dots, X_n]]$ по идеалу, порожденному формальными рядами $f_1, \dots, f_s$ вида (*), изоморфно кольцу $K[[X_{s+1}, \dots, X_n]]$.*

В случае комплексного поля можно рассматривать сходящиеся ряды, которые являются разложениями некоторых аналитических функций. Предполагается, что ряды абсолютно сходятся в некоторой окрестности нуля. Теорема 9.15.1 применяется к абсолютно сходящимся рядам f и g и устанавливает существование абсолютно сходящихся рядов q и $r_0, \dots, r_{s-1}$. Аналогичным образом дополняется формулировка теоремы 9.15.2. В случае абсолютно сходящихся рядов следствие 9.15.1 сразу же приводит к одной из известных в анализе теорем о неявной функции.

Задача 419. *Докажите, что формальный ряд обратим в том и только том случае, когда его свободный член равен нулю.*

9.16. Применение теорем о неявной функции

Теоремы о неявной функции дают локальное представление множества решений системы уравнений в виде графика некоторой функции. Вот одна из них (доказательство можно найти во многих учебниках по математическому анализу).

Теорема 9.16.1. Пусть $f_1, \dots, f_m \in \mathbb{C}[[X_1, \dots, X_n]]$ — ряды с нулевым свободным членом и известно, что они абсолютно сходятся в некоторой окрестности нуля, и во всех точках $\xi \in \mathbb{C}^n$ этой окрестности ранг матрицы Якоби

$$J(\xi) = \begin{bmatrix} \frac{\partial f_1}{\partial X_1}(\xi) & \dots & \frac{\partial f_1}{\partial X_n}(\xi) \\ \dots & \dots & \dots \\ \frac{\partial f_m}{\partial X_1}(\xi) & \dots & \frac{\partial f_m}{\partial X_n}(\xi) \end{bmatrix}$$

имеет одно и то же значение r . Предположим, что первые r столбцов матрицы $J(0)$ содержат ненулевой минор порядка r . Тогда в некоторой окрестности нуля множество решений системы уравнений

$$f_1(X_1, \dots, X_n) = \dots = f_m(X_1, \dots, X_n) = 0$$

является графиком отображения

$$X_1 = \phi_1(X_{r+1}, \dots, X_n), \dots, X_r = \phi_r(X_{r+1}, \dots, X_n),$$

которое задано рядами $\phi_1, \dots, \phi_r$, абсолютно сходящимися в некоторой окрестности нуля.

Не ограничивая общности, будем считать, что начало координат является регулярной точкой неприводимого многообразия $V \subset \mathbb{C}_{X_1, \dots, X_n}$, которое соответствует идеалу

$$I = \mathcal{I}(V) = \langle f_1, \dots, f_m \rangle.$$

Если $d = \dim V$, то для всех точек ξ на многообразии V в некоторой окрестности регулярной точки (в данном случае это начало координат)

$$\text{rank } J(\xi) = r := n - d.$$

Здесь нужно обратить внимание на одно обстоятельство, которое *препятствует* применению теоремы 9.16.1: в ней требуется, чтобы ранг матрицы Якоби был постоянным во всех точках окрестности нуля, а мы знаем только то, что он равен r во всех ее точках, *принадлежащих* многообразию V .

Способ обойти это препятствие есть. Не ограничивая общности, будем считать, что при $\xi = 0$ ненулевой минор порядка r расположен в левом верхнем углу матрицы $J(0)$. Тогда очевидно, что этот же минор будет ненулевым во всех точках некоторой окрестности начала координат. Поэтому теорема 9.16.1 применима к первым r уравнениям, т. е. к системе уравнений

$$f_1(X_1, \dots, X_n) = \dots = f_r(X_1, \dots, X_n) = 0.$$

Теперь нам нужно понять, как связано многообразие $W = \mathcal{V}(f_1, \dots, f_r)$ с исходным неприводимым многообразием $V = \mathcal{V}(f_1, \dots, f_m)$. Очевидно, $W \supseteq V$. В действительности же каждая точка из W в окрестности начала координат принадлежит V , т. е. построенный выше график в этой окрестности состоит из точек исходного многообразия V . Тем не менее, чтобы это аккуратно доказать, требуются довольно значительные усилия.

Прежде всего заметим, что в окрестности $\mathcal{O}(0, \varepsilon)$ обнуляются также любые делители многочленов из идеала $J := \langle f_1, \dots, f_r \rangle$, которые могут получиться при делении на какой-либо многочлен g , такой что $g(0, \dots, 0) \neq 0$. Множество таких делителей можно записать в виде

$$J_0 = \left\{ f \in \mathbb{C}[X] : f = \sum_{i=1}^r f_i(h_i/g_i), \quad h_i, g_i \in \mathbb{C}[X], \quad g_i(0, \dots, 0) \neq 0 \right\}. \quad (*)$$

Легко проверяется, что J_0 есть идеал кольца $\mathbb{C}[X] = \mathbb{C}[X_1, \dots, X_n]$. При этом очевидно, что $J \subseteq J_0$, и, следовательно, $W \supseteq \supseteq W_0 := \mathcal{I}(J_0)$. Наша цель — доказать, что $W_0 = V$.

Теорема 9.16.2. Пусть многочлены $f_1, \dots, f_r \in \mathbb{C}[X_1, \dots, X_n]$ с нулевым свободным членом имеют вид

$$f_1(X_1, \dots, X_n) = a_{11}X_1 + \dots + a_{1n}X_n + \sum_{i_1 + \dots + i_n \geq 2} a_{i_1, \dots, i_n}^{(1)} X_1^{i_1} \dots X_n^{i_n},$$

.....

$$f_r(X_1, \dots, X_n) = a_{r1}X_1 + \dots + a_{rn}X_n + \sum_{i_1 + \dots + i_n \geq 2} a_{i_1, \dots, i_n}^{(r)} X_1^{i_1} \dots X_n^{i_n},$$

и пусть

$$\text{rank}[a_{ij}]_{r \times n} = r.$$

Тогда идеал J_0 вида (*) является простым, а многообразие $W = \mathcal{V}(f_1, \dots, f_r)$ представляется в виде объединения алгебраических многообразий

$$W = W_0 \cup W_1, \quad 0 \in W_0, \quad 0 \notin W_1,$$

где $W_0 = \mathcal{V}(J_0)$ — неприводимое многообразие размерности $n - r$.

Для доказательства нам нужно следующее свойство идеалов в локальных кольцах.

Теорема 9.16.3 (ТЕОРЕМА КРУЛЛЯ). Пусть M — максимальный идеал в локальном кольце R . Тогда для любого идеала $I \subseteq R$ имеет место равенство

$$\bigcap_{l=1}^{\infty} (I + M^l) = I.$$

Здесь M^l — это идеал, порожденный всеми произведениями вида $a_1 \dots a_l$ при произвольном выборе элементов $a_1, \dots, a_l \in M$.

Доказательство. Пусть $J = \bigcap_{l=1}^{\infty} M^l$. Тогда $MJ = J$ и, в силу леммы Накаямы, имеется элемент $a \in M$ такой, что $(1 - a)b = 0$ для любого $b \in J$. Докажем, что элемент $1 - a$ является обратимым. Если это не так, то он принадлежит некоторому максимальному идеалу, а поскольку в локальном кольце по определению есть только один максимальный идеал, находим: $1 - a \in M$. Отсюда $1 \in M \Rightarrow M = R$, что противоречит определению максимального идеала. Обратимость элемента $1 - a$ приводит к выводу о том, что $J = 0$. Таким образом, теорема Крулля получена в случае $I = 0$.

Теперь рассмотрим произвольный идеал I . Если $I = R$, то утверждение очевидно. Если $I \neq R$, то I содержится в некотором максимальном идеале и, в силу его единственности, получаем $I \subseteq M$. Тогда кольцо вычетов M/I оказывается максимальным идеалом в фактор-кольце R/I и, по уже доказанному,

$$\bigcap_{l=0}^{\infty} (M/I)^l = 0.$$

Возьмем произвольный элемент a из пересечения всех идеалов вида $I + M^l$. Вычет $[a]_I$ принадлежит фактор-кольцу $M^l/I = (M/I)^l$ при всех l . Поэтому, согласно полученному выше результату о пересечении степеней вычетов, $[a]_I = 0 \Rightarrow a \in I$. Следовательно, $\bigcap_{l=1}^{\infty} (I + M^l) \subseteq I$. Противоположное включение очевидно. $\square$

Доказательство теоремы 9.16.2. Обозначим через $\mathcal{L}$ локальное кольцо, полученное при локализации кольца $\mathbb{C}[X] = \mathbb{C}[X_1, \dots, X_n]$ по идеалу $\langle X_1, \dots, X_n \rangle$, состоящему из всех многочленов f таких, что $f(0) = 0$. Напомним, что элементы $\mathcal{L}$ — это рациональные функции вида h/g , где $g(0) \neq 0$. Легко видеть, что с каждой функцией такого вида однозначно сопоставляется некоторый формальный ряд, причем суммам и произведениям будут соответствовать суммы и произведения формальных рядов. Это означает, что кольцо $\mathcal{L}$ естественным образом вкладывается в кольцо $\mathbb{C}[[X]]$. Таким образом,

$$\mathbb{C}[X] \subseteq \mathcal{L} \subseteq \mathbb{C}[[X]].$$

Обозначим через J_1 идеал, порожденный многочленами $f_1, \dots, f_r$ в кольце $\mathcal{L}$ и через J_2 — идеал, порожденный теми же многочленами в кольце $\mathbb{C}[[X]]$. Очевидно, что $J_0 \subseteq J_1 \subseteq J_2$ и $J_0 = J_1 \cap \mathbb{C}[X]$. Поэтому из простоты идеала J_1 должна следовать простота идеала J_0 .

Докажем также, что $J_1 = J_2 \cap \mathcal{L}$. Пусть $a \in J_2 \cap \mathcal{L}$. Тогда

$$a = f/g = \sum_{i=1}^r f_i G_i,$$

где f, g — многочлены с условием $g(0) \neq 0$ (поэтому ряд g обратим) и $G_1, \dots, G_r$ — какие-то формальные ряды. Каждое произведение $G_i g$ запишем в виде

$$G_i g = p_i^{(l)} + Q_i^{(l)},$$

где $p_i^{(l)}$ — многочлен степени не выше $l-1$, а $Q_i^{(l)}$ — формальная сумма одночленов степени l и выше. Тогда

$$a = A_l + B_l, \quad A_l = \sum_{i=1}^r f_i(p_i^{(l)}/g), \quad B_l = \sum_{i=1}^r f_i(Q_i^{(l)}/g),$$

где $A_l \in J_1$, а B_l есть формальная сумма одночленов степени не ниже l . Кроме того, $B_l = (f - A_l g)/g$ и поэтому $B_l \in \mathcal{L}$. Отсюда вытекает, что $B_l \in M^l$, где M — единственный максимальный идеал в локальном кольце $\mathcal{L}$, состоящий из отношений многочленов вида f/g , где $f(0) = 0$ и $g(0) \neq 0$. Таким образом, $a \in \bigcap_{l=1}^{\infty} (J_1 + M^l)$. Используя теорему Крулля, находим

$$J_1 \subseteq J_2 \cap \mathcal{L} \subseteq \bigcap_{l=1}^{\infty} (J_1 + M^l) = J_1 \quad \Rightarrow \quad J_1 = J_2 \cap \mathcal{L}.$$

Согласно следствию 9.15.2, фактор-кольцо $\mathbb{C}[[X]]/J_2$ изоморфно кольцу формальных рядов $\mathbb{C}[[X_{r+1}, \dots, X_n]]$ и поэтому является целостным. Следовательно, идеал J_2 простой. Отсюда вытекает простота идеала J_1 , а затем и простота идеала J_0 . Таким образом, простота идеала J_0 и неприводимость многообразия W_0 установлены.

Матрица Якоби идеала J_0 , конечно же, содержит строки вида (градиенты)

$$\left(\frac{\partial f_i}{\partial X_1}, \dots, \frac{\partial f_i}{\partial X_n} \right), \quad 1 \leq i \leq r.$$

Произвольная строка соответствует функции вида $f/g \in J_0$, где $f \in J$ и $g(0) \neq 0$. Применяя общеизвестные правила дифференцирования, находим

$$\frac{\partial}{\partial X_j} \left(\frac{f}{g} \right) (\xi) = \frac{1}{g(\xi)} \frac{\partial f}{\partial X_j} (\xi) - \frac{f(\xi)}{g^2(\xi)} = \frac{1}{g(\xi)} \frac{\partial f}{\partial X_j} (\xi)$$

при $\xi \in W_0 \subseteq W$.

Значит, произвольная строка матрицы Якоби для J_0 в точке нуль есть линейная комбинация градиентов функций $f_1, \dots, f_r$. Поэтому $\dim W_0 \leq n - r = d$.

Кроме того, вычеты $X_{r+1} + J_0, \dots, X_n + J_0$ координатного кольца $\mathbb{C}[V] = \mathbb{C}[X]/J_0$ алгебраически независимы над полем $\mathbb{C}$. Если это не так, то для какого-то ненулевого многочлена $f(X_{r+1}, \dots, X_n)$ получаем

$$f(X_{r+1}, \dots, X_n) \in J_0 \subseteq J_2.$$

Это означает, что вычеты вида $X_{r+1} + J_2, \dots, X_n + J_2$ алгебраически зависимы как элементы кольца $\mathbb{C}[[X]]/J_2$. В силу теоремы 9.15.2 и ее следствия 9.15.2, имеет место изоморфизм колец $\mathbb{C}[[X]]/J_2 \cong \mathbb{C}[[X_{r+1}, \dots, X_n]]$, при котором вычету

$X_{r+i} + J_2$ из кольца $\mathbb{C}[[X]]/J_2$ будет соответствовать формальный ряд $X_{r+i} \in \mathbb{C}[[X_{r+1}, \dots, X_n]]$. Значит, ряды (многочлены) $X_{r+1}, \dots, X_n$ алгебраически зависимы, а этого, конечно, быть не может. Таким образом, $\text{trdeg}(\mathbb{C}[V] : \mathbb{C}) \geq n - r = d$. В итоге $\dim W_0 = d$.

Очевидно, что $0 \in W_0$. Далее, пусть идеал J_0 порождается рациональными функциями $p_1/q_1, \dots, p_s/q_s$, где знаменатели не обращаются в нуль в точке нуль. Положим $q := q_1 \dots q_s$. Тогда для любой рациональной функции $f \in J_0$ получаем $fq \in J \Rightarrow \Rightarrow qJ_0 \subseteq J \Rightarrow W \subseteq W_0 \cup \mathcal{V}(q)$. Таким образом, $W = W_0 \cup W_1$, где $W_1 = \mathcal{V}(q) \cap W$, и наш выбор многочлена q гарантирует, что $0 \notin W_1$. $\square$

Следствие 9.16.1. *Исходное неприводимое многообразие V совпадает с W_0 .*

Теорема о неявной функции позволяет также получить практически важный результат для многообразий $V \subseteq \mathbb{C}^n$, которые получаются как алгебраическое замыкание образа пространства $\mathbb{C}^m$ при полиномиальном отображении¹⁾. Пусть отображение $p: \mathbb{C}_{Y_1, \dots, Y_m} \rightarrow \mathbb{C}_{X_1, \dots, X_n}$ определяется формулами

$$X_i = p_i(Y_1, \dots, Y_m), \quad p_i \in \mathbb{C}[Y_1, \dots, Y_m], \quad 1 \leq i \leq n,$$

и пусть его матрица Якоби в точке $\zeta = (\zeta_1, \dots, \zeta_m)$ имеет вид

$$J_p(\zeta) = \begin{bmatrix} \frac{\partial p_1}{\partial Y_1}(\zeta) & \dots & \frac{\partial p_1}{\partial Y_m}(\zeta) \\ \dots & \dots & \dots \\ \frac{\partial p_n}{\partial Y_1}(\zeta) & \dots & \frac{\partial p_n}{\partial Y_m}(\zeta) \end{bmatrix}.$$

Теорема 9.16.4. *Предположим, что максимальный ранг матрицы Якоби J_p полиномиального отображения $p: \mathbb{C}^m \rightarrow \mathbb{C}^n$ достигается в точке $\zeta \in \mathbb{C}^m$:*

$$\text{rank } J_p(\zeta) = \max_{\theta \in K^m} \text{rank } J_p(\theta).$$

Тогда точка $\xi = p(\zeta) \in \mathbb{C}^n$ является регулярной точкой алгебраического замыкания

$$V = \overline{p(\mathbb{C}^m)} \subseteq \mathbb{C}^n,$$

для которой имеет место равенство $\dim V = \text{rank } J_p(\zeta)$.

¹⁾ Легко доказывается, что V будет неприводимым.

получаем

$$\frac{\partial p_i}{\partial Y_1} \frac{\partial \phi_1}{\partial Y_j} + \dots + \frac{\partial p_i}{\partial Y_d} \frac{\partial \phi_d}{\partial Y_j} + \frac{\partial p_i}{\partial Y_j} = 0.$$

Поскольку j -й столбец матрицы J_p является линейной комбинацией первых d столбцов, то эти же равенства имеют место и при $d+1 \leq i \leq n$. Следовательно, в некоторой окрестности выполняются равенства

$$\frac{\partial X_i}{\partial Y_j} = 0, \quad d+1 \leq i \leq n, \quad d+1 \leq j \leq m.$$

В этой окрестности каждому набору значений $X_1, \dots, X_d$ соответствует только одно значение координаты X_i при $d+1 \leq i \leq n$. Значит, координатные функции $x_1, \dots, x_d, x_i$ алгебраически зависимы. $\square$

Задача 420. Алгебраическое многообразие размерности $d < n$ расположено в n -мерном пространстве. Всегда ли оно является пересечением $n-d$ гиперповерхностей?

9.17. Главные тензорные ранги трехмерных матриц

Теорема 9.16.4 — это удобный инструмент для вычисления размерности. В частности, при изучении *тензорных разложений* — специальных представлений ν -мерных матриц, т.е. таблиц, элементы которых помечены с помощью ν индексов $i_1, \dots, i_\nu$. Такие таблицы называют также *тензорами*. Точно так же, как обычные матрицы представляют линейные операторы или линейные формы при фиксированных базисах, ν -мерные матрицы представляют ν -линейные формы (часто они также называются тензорами) при фиксированных базисах.

Для простоты пусть $\nu = 3$ и заданы принадлежащие полю $\mathbb{K}$ элементы

$$a_{ijk}, \quad 1 \leq i \leq m, \quad 1 \leq j \leq n, \quad 1 \leq k \leq q.$$

Всегда можно найти какие-то элементы $u_{i\alpha}, v_{j\alpha}, w_{k\alpha} \in \mathbb{K}$ и написать разложение

$$a_{ijk} = \sum_{\alpha=1}^R u_{i\alpha} v_{j\alpha} w_{k\alpha}. \quad (*)$$

Наименьшее возможное число слагаемых R для всех разложений такого вида называется *тензорным рангом* трехмерной матрицы с элементами из поля $\mathbb{K}$.

Ясно, что любую трехмерную матрицу с элементами из $\mathbb{K}$ можно рассматривать как элемент пространства $\mathbb{K}^{mnq}$ и множество $\mathcal{S}_R$ всех трехмерных матриц над полем $\mathbb{K}$, для которых тензорный ранг не превосходит R , есть полиномиальный образ пространства $\mathbb{K}^{(m+n+q)R}$. Полиномиальное отображение в этом случае определяется правой частью формулы (*).

Напомним, что черта сверху означает алгебраическое замыкание множества. Натуральное число R , для которого $\overline{\mathcal{S}_R} \setminus \overline{\mathcal{S}_{R-1}} = \mathbb{K}^{mnq}$, называется *главным тензорным рангом* трехмерных матриц размера $m \times n \times q$ над полем $\mathbb{K}$. Главный ранг — в тех случаях, когда он существует, — зависит, безусловно, от m , n и q .

Теорема 9.17.1. *Для трехмерных матриц размера $m \times n \times q$ с комплексными элементами главный ранг существует и однозначно определяется по m , n и q .*

Доказательство. Очевидно, что $\overline{\mathcal{S}}_R \subseteq \overline{\mathcal{S}}_{R+1}$, и согласно теореме о размерности собственного подмногообразия при строгом включении имеет место строгое неравенство для размерностей. Поскольку размерность не может превысить mnq , при некотором R должно выполняться равенство $\overline{\mathcal{S}}_R = \overline{\mathcal{S}}_{R+1}$. Пусть R — минимальное такое значение, т.е. $\overline{\mathcal{S}}_{R-1} \neq \overline{\mathcal{S}}_R$. В случае поля $\mathbb{C}$ алгебраическое замыкание полиномиального образа совпадает с его замыканием в обычной топологии. Поэтому

$$\begin{aligned} \overline{\mathcal{S}}_{R+1} \subseteq \overline{\mathcal{S}}_{R+2} = \overline{\mathcal{S}}_{R+1} + \overline{\mathcal{S}}_1 = \overline{\mathcal{S}}_R + \overline{\mathcal{S}}_1 = \overline{\mathcal{S}}_{R+1} &\Rightarrow \\ &\Rightarrow \overline{\mathcal{S}}_{R+2} = \overline{\mathcal{S}}_{R+1} = \overline{\mathcal{S}}_R. \end{aligned}$$

Следовательно, $\overline{\mathcal{S}}_{R_1} = \overline{\mathcal{S}}_R$ для любого $R_1 \geq R$.

В силу того что *каждая* трехмерная матрица имеет какой-то тензорный ранг, получаем $\overline{\mathcal{S}}_R = \mathbb{C}^{mnq}$. Остается применить теорему 9.14.1:

$$\mathbb{C}^{mnq} = \overline{\mathcal{S}}_R = \overline{\overline{\mathcal{S}}_R \setminus \overline{\mathcal{S}}_{R-1}} = \overline{\mathcal{S}_R \setminus \overline{\mathcal{S}}_{R-1}} \subseteq \overline{\mathcal{S}_R \setminus \mathcal{S}_{R-1}} \subseteq \mathbb{C}^{mnq}.$$

В итоге находим: $\overline{\mathcal{S}_R \setminus \mathcal{S}_{R-1}} = \mathbb{C}^{mnq}$. Множество $\mathcal{S}_R$ является конструктивным (см. раздел 9.9), и поэтому $\mathbb{C}^{mnq} \setminus Z \subseteq \mathcal{S}_R \setminus \mathcal{S}_{R-1}$ для некоторого алгебраического подмногообразия $Z \subsetneq \mathbb{C}^{mnq}$. Следовательно, $\overline{\mathcal{S}_k \setminus \mathcal{S}_{k-1}} \neq \mathbb{C}^{mnq}$ при $k < R$. $\square$

Следствие 9.17.1. В любой сколь угодно малой окрестности любой трехмерной матрицы размера $m \times n \times q$ с комплексными элементами есть трехмерная матрица, тензорный ранг которой равен главному рангу для комплексных матриц размера $m \times n \times q$.

Задача 421. Докажите, что тензорный ранг любой трехмерной матрицы размера $2 \times 2 \times 2$ с комплексными элементами не больше 3. Верно ли то же самое в случае поля $\mathbb{Z}_2$?

Задача 422. Докажите, что для трехмерных матриц размера $2 \times 2 \times 2$ с вещественными элементами главный ранг не существует.

Задача 423. Докажите, что главный тензорный ранг для трехмерных комплексных матриц размера $n \times n \times 2$ равен n .

Задача 424. Докажите, что множество трехмерных комплексных матриц размера $m \times n \times q$, тензорный ранг которых не больше 1, образует неприводимое алгебраическое многообразие размерности $m + n + q - 2$.

Задача 425. Докажите, что главный тензорный ранг трехмерных комплексных матриц размера $3 \times 3 \times 3$ равен 5.

СПИСОК ЛИТЕРАТУРЫ

1. *Алексеев В. Б.* Теорема Абеля в задачах и решениях. — М.: Наука, 1978.
2. *Артамонов В. А., Латышев В. Н.* Линейная алгебра и выпуклая геометрия. — М.: Факториал Пресс, 2004.
3. *Артин Э.* Теория Галуа. — М.: МЦНМО, 2004.
4. *Атья М., Макдональд И.* Введение в коммутативную алгебру. — М.: Факториал Пресс, 2003.
5. *Беклемишев Д. В.* Курс аналитической геометрии и линейной алгебры. — М.: Физматлит, 2009.
6. *Биркгоф Г., Барти Т.* Современная прикладная алгебра. — М.: Мир, 1976.
7. *Богопольский О. В.* Введение в теорию групп, Институт компьютерных исследований — Ижевск, 2002.
8. *Ван дер Варден Б. Л.* Алгебра. — М.: Наука, 1976.
9. *Верещагин Н. К., Шень А.* Начала теории множеств. — М.: МЦНМО, 2002.
10. *Винберг Э. Б.* Курс алгебры. — М.: МЦНМО, 2013.
11. *Воеводин В. В.* Линейная алгебра. — М.: Наука, 1980.
12. *Воеводин В. В.* Вычислительные основы линейной алгебры. — М.: Наука, 1977.
13. *Воеводин В. В., Кузнецов Ю. А.* Матрицы и вычисления. — М.: Наука, 1984.
14. *Гантмахер Ф. Р.* Теория матриц. — М.: Наука, 1967.
15. *Гельфанд И. М.* Лекции по линейной алгебре. — М.: Добросвет, МЦНМО, 1998.
16. *Годунов С. К.* Современные аспекты линейной алгебры. — Новосибирск: Научная книга, 1997.
17. *Голуб Дж., Ван Лоун Ч.* Матричные вычисления. — М.: Мир, 1999.
18. *Замарашкин Н. Л.* Алгоритмы для разреженных систем линейных уравнений в $GL(2)$. — М.: Изд-во МГУ, 2014.
19. *Зарисский О., Самюэль П.* Коммутативная алгебра. Т. 1. — М.: ИЛ, 1963.
20. *Зарисский О., Самюэль П.* Коммутативная алгебра. Т. 2. — М.: ИЛ, 1963.
21. *Икрамов Х. Д.* Задачник по линейной алгебре. — М.: Наука, 1975.
22. *Икрамов Х. Д.* Численное решение матричных уравнений. — М.: Наука, 1984.
23. *Ильин В. А., Ким Г. Д.* Линейная алгебра и аналитическая геометрия. — М.: Изд-во МГУ, 1998.

24. Ильин В. П., Кузнецов Ю. И. Алгебраические основы численного анализа. — Новосибирск: Наука, Сибирское отделение, 1986.
25. Клейменов В. Ф. Жорданова форма матрицы линейного оператора. — Иркутск: Изд-во Иркутского гос. ун-та, 2009.
26. Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия и алгоритмы. — М.: Мир, 2000.
27. Кострикин А. И. Введение в алгебру. Части I, II, III. — М.: Физматлит, 2000.
28. Кострикин А. И., Манин Ю. И. Линейная алгебра и геометрия. — М.: Лань, 2008.
29. Курош А. Г. Курс высшей алгебры. — М.: Наука, 1971.
30. Курош А. Г. Лекции по общей алгебре. — М.: Наука, 1973.
31. Ленг С. Алгебра. — М.: Мир, 1968.
32. Мальцев А. И. Основы линейной алгебры. — М.: Наука, 1970.
33. Мамфорд Д. Алгебраическая геометрия. Комплексные проективные многообразия. — М.: Мир, 1979.
34. Мамфорд Д. Красная книга о многообразиях и схемах. — М.: МЦНМО, 2007.
35. Михалев А. В., Михалев А. А. Начала алгебры. Часть I. — М.: Интернет-университет информационных технологий (ИНТУИТ), 2012.
36. Постников М. М. Теория Галуа. — М.: Факториал Пресс, 2003.
37. Прасолов В. В. Многочлены. — М.: МЦНМО, 2001.
38. Прасолов В. В. Задачи и теоремы линейной алгебры. — М.: МЦНМО, 2015.
39. Проскуряков И. В. Сборник задач по линейной алгебре. — М.: Наука, 1978.
40. Рид М. Алгебраическая геометрия для всех. — М.: Мир, 1991.
41. Стрэнг Г. Линейная алгебра и ее приложения. — М.: Мир, 1980.
42. Тыртышников Е. Е. Матричный анализ и линейная алгебра. — М.: Физматлит, 2007.
43. Уилкинсон Дж. Х. Алгебраическая проблема собственных значений. — М.: Наука, 1970.
44. Фаддеев Д. К. Лекции по алгебре. — М.: Наука, 1984.
45. Фаддеев Д. К., Фаддеева В. Н. Вычислительные методы линейной алгебры. — М.: Лань, 2002.
46. Халмош П. Конечномерные векторные пространства. — М.: Физматлит, 1963.
47. Хованский А. Г. Теория Галуа, накрытия и римановы поверхности. — М.: МЦНМО, 2007.
48. Хорн Р., Джонсон Ч. Матричный анализ. — М.: Мир, 1989.
49. Шафаревич И. Р. Основы алгебраической геометрии. — М.: МЦНМО, 2007.
50. Шафаревич И. Р. Основные понятия алгебры. — Ижевск: ПХД, 2001.
51. Bhatia R. Matrix Analysis. — N. Y.: Springer-Verlag, 1997.
52. Kendig K. Elementary Algebraic Geometry. — N. Y.: Springer-Verlag, 1977.
53. Saad Y. Iterative Methods for Sparse Linear Systems. — Boston: PWS, 1996.
54. Stewart G. W. Sun Ji-guang, Matrix Perturbation Theory. — San Diego: Academic Press, 1990.
55. Strang G. Essays in Linear Algebra. — Wellesley-Cambridge Press, 2012.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Алгебраическое многообразие

- алгебраическая кривая 62, 414
- главная точка 400, 423
- главный тензорный ранг 447
- изоморфные многообразия 400
- касательная плоскость 422, 423
- касательное пространство 422, 423
- конечное отображение 419
- координатное кольцо 399, 400, 402, 404, 405, 407, 419, 424, 425, 430, 443
- матрица Якоби 422–425, 439, 440
- морфизм 404, 405, 419
- неприводимое 397–407, 410–414, 416, 419, 421–425, 428, 430–432, 434, 435, 439–441, 443–445, 448
- особая (сингулярная) точка 424, 425
- полиномиально эквивалентные многообразия 401
- проекции 405, 421, 433, 434
- размерность 413, 414, 421–423, 425, 430, 431
- размерность пересечения 425
- ранг точки 423
- рационально изоморфные многообразия 405

- рационально эквивалентные многообразия 404
- рациональная параметризация 405
- регулярная (неособая, гладкая, простая) точка 424
- степень 414
- тензорный ранг 71, 447, 448

Алгоритм

- арифметическая сложность 69
- Бухбергера 384
- Винограда 69, 70
- деления с остатком на системе многочленов 378
- Евклида 122, 123
- метод деления столбиком 120, 368, 409
- метод исключения элементов 68
- процесс ортогонализации Грама–Шмидта 198
- Штрассена 69, 70

Вектор

- арифметический 14–16, 32, 49–51, 53
- арифметическое пространство 14
- базис векторного (линейного) пространства 18, 19, 24, 53–55, 76, 148, 150, 151, 154, 167, 179–184, 193, 194, 198–202, 208, 210, 213, 216, 217, 219–223, 235, 237, 240, 246, 247,

- 274, 276–279, 284, 287, 293, 301, 304, 305, 308
- векторное (линейное) пространство 14, 15, 18, 48, 52, 144–148, 152, 157, 165, 166, 178, 230, 244, 248, 250, 251, 253, 258, 266, 186, 375, 425, 427
- векторное произведение 53, 54
- геометрический 15
- длина арифметического вектора 50
- длина вектора 196, 238
- кронекерово произведение 35
- линейная комбинация 15, 17, 44, 47, 114, 146, 148, 151, 154, 213, 215, 216, 237, 253, 302, 359, 397, 418, 443, 446
- линейная оболочка 15, 16, 19, 32, 43, 45, 147, 151, 157, 216, 217, 273, 274
- линейно зависимая система 16
- линейно независимая система 16
- мажоризация 289–292
- направленный отрезок 15
- нормаль 52, 53, 62
- нулевой 14, 144
- ориентация системы векторов 53, 54
- ортогональные векторы 50–54, 196–198
- ортогональный множеству 197
- радиус-вектор 16, 54
- разложение вектора по подпространствам 152
- размерность векторного (линейного) пространства 18, 45, 148, 230, 253, 273
- смешанное произведение 54
- скалярное произведение 49, 196–200, 203, 238–241, 244, 263, 269, 276–278, 280, 293
- Выпуклое множество
 - аффинная оболочка 253, 255, 271, 273, 274
 - аффинная (барицентрическая) комбинация 253
 - вершина полиэдра 273
 - внутренняя точка 257–259, 264, 273, 275
 - выпуклая комбинация 254, 256, 265, 296
 - выпуклая оболочка 255
 - выпуклое тело 257, 258, 259, 266
 - выпуклый многогранник 255
 - грань точки 273
 - двойственные задачи линейного программирования 271
 - конечнопорожденный конус 255, 270, 274
 - линейно внутренняя точка 257, 258, 268
 - линейное программирование 271
 - локально внутренняя точка 273
 - направляющее подпространство 253, 422
 - опорная гиперплоскость 264, 265
 - отрезок 254
 - плоскость 253
 - полиэдр 271–275, 291, 294
 - разделяющая гиперплоскость 264
 - размерность плоскости 253
 - ребро 273
 - симплекс 255
 - система линейных неравенств 269
 - теорема Биркгоффа 265
 - теорема Вейля 274
 - теорема Фань Цзы 273
 - теорема Фаркаша 269

- угловая (крайняя) точка 257, 259, 261, 265, 275
- функционал Минковского 258, 259

Группа

- абелева 81–85, 87, 95, 97, 102, 107–111, 144, 168, 326, 327, 340
- автоморфизм 88, 89, 95, 97, 105, 110
- аддитивная 85, 86, 89, 91, 92, 95, 107, 111, 113, 146, 338, 340, 360
- аддитивная группа поля 113
- аффинных преобразований 82, 83
- бинарная операция 79, 81, 84, 93, 111
- внутренний автоморфизм 88, 95, 96, 105
- вычетов по модулю 82, 95
- знакопеременная 91, 92, 96, 233, 235, 327
- Галуа 304, 307–314, 319, 324, 325, 330, 331
- гомоморфизм 103–106
- p -группа 109, 332
- движений плоскости 101, 102
- дробно-линейных преобразований 102, 103
- единичный элемент 86
- действие группы на множестве 98, 334
- действие сопряжением 98, 334
- изоморфизм 88, 89, 95, 97
- конечная 81, 82, 93, 96, 99
- конечно порожденная 107
- корней из единицы 89, 90, 105
- множество неподвижных точек 98
- моноид 81
- мультипликативная 86, 92, 95, 98, 105, 113
- мультипликативная группа поля 113
- коммутатор 96
- нейтральный элемент 80–86, 88
- нормализатор 95, 334
- нормальная подгруппа (нормальный делитель) 94–96, 100, 104, 105
- образ гомоморфизма 103
- обратный элемент 80–82, 86
- общая линейная группа 82
- орбита 98, 99, 334
- отображение Кэли 106
- подгруппа 91–98, 104–108, 166, 169, 232, 233, 235, 309–314, 320–322, 324, 325, 327, 330–335
- полициклический ряд 320
- полная линейная группа 82
- полугруппа 81
- порядок группы 81, 82, 84, 93, 95–100, 105–107
- примарная 109, 332
- произведение множеств 92
- прямая сумма групп 107
- прямое произведение групп 107
- симметрическая группа 82, 91, 101, 106, 310, 312, 325
- смежный класс 93, 94, 99, 104, 165, 232, 322, 333, 334
- сопряженные подгруппы 92, 94, 99, 165, 334, 335
- сопряженные элементы 92, 99, 101, 165
- специальная линейная группа 82
- стабилизатор 98, 99
- сумма множеств 92
- транзитивное действие на множестве 308
- центр 92, 95, 99, 105

Группа

- централизатор 91
- циклическая 96, 97, 105–110, 168, 169, 231–233
- фактор-группа 94, 95, 105, 323, 320–322, 324, 327, 331
- четверная группа Клейна 105, 235
- ядро гомоморфизма 103
- проблема Бернсайда 110

Зависимость

- алгебраическая 362–366
- линейная 16–19, 32, 43–48, 50, 76, 148, 150–152, 155, 157, 158, 198, 214–216, 226, 227, 235, 237, 275, 300–309, 359
- целая алгебраическая 366

Идеал

- конечно порожденный 339, 375, 377, 395
- максимальный 350–352, 359, 371, 390, 403, 441
- минимальное примарное разложение 346
- мономиальный 380
- неприводимый 342
- нильпотентный 341
- нулевой 336
- пересечение идеалов 336
- примарный 344
- p -примарный 345
- простой 342, 397
- радикальный 341–343, 387
- расширение идеала 348
- свойство поглощения 336
- символическая степень простого идеала 350
- собственный 336
- сужение идеала 348
- сумма идеалов 336
- тривиальный 336
- фактор-кольцо 337
- частное идеалов 337

Кольцо

- алгебра 230
- алгебраически зависимые элементы 362–365, 391, 422, 444
- алгебраически независимые элементы 362–365, 426, 443, 445
- ассоциативное 111
- базисы Грёбнера 378
- вычетов 112, 113, 116, 117, 129, 157, 158, 162, 165, 169, 301, 312, 318, 332, 337, 338, 341, 344, 351, 370, 390, 399, 438, 441
- гауссово 124
- гауссовых чисел 112
- гомоморфизм 114
- делитель единицы 112
- делитель нуля 111
- единичный элемент (единица) 112
- естественный гомоморфизм 348
- законы дистрибутивности 111
- идеал 336–352, 359–361, 366, 370, 371, 374–381, 394–400, 403, 404, 406, 417, 418, 422–424, 426, 428–430, 438–444
- изоморфизм 114
- коммутативное 111
- координатное 399–405, 410, 422, 425
- локальное 350, 353, 404, 441
- многочленов 118, 119, 132, 133, 142, 187, 340, 376
- модуль 340, 366, 368, 369, 371, 394, 417, 418, 420
- нётерово 339, 340, 343, 345, 347, 349, 350, 352, 376, 377, 413
- нильпотент 341, 342, 344, 347, 348, 352, 360
- нильрадикал 341
- нулевое 111

- область целостности 112
- обратимый элемент 112
- ростков 350
- с единицей 112
- разложение на неприводимые множители 124, 125, 127, 305, 312
- свойство поглощения 336
- подкольцо 120, 142, 338, 342, 365, 369, 419
- радикал идеала 341
- теорема Гильберта о базисе 375
- теорема Гильберта о нулях 394
- факториальное 124
- фактор-кольцо 337
- целое 368
- целозамкнутое 368
- целостное 112
- частных 347
- Комбинация
 - аффинная (барицентрическая) 253
 - выпуклая 254, 265
 - линейная 15–18, 44, 47, 114, 146, 148, 150, 151, 154, 157, 213, 215, 237, 253, 302, 359, 397, 418, 443
- Комплексное число
 - аргумент 75
 - вещественная и мнимая части 73
 - кватернионы 77
 - комплексная плоскость 73
 - корни из единицы 89
 - модуль 73
 - мнимая единица 74
 - первообразный корень 90
 - сопряженное число 76
 - тригонометрическая форма 75
 - функция Эйлера 90
- Кратность собственного значения
 - алгебраическая 193–195, 209, 210, 221
 - геометрическая 194, 209
- Кривая второго порядка
 - асимптотическое направление 61
 - асимптоты 60
 - гипербола 60
 - гиперболический косинус 63
 - гиперболический синус 63
 - гиперболического типа 59
 - главная ось эллипса 59
 - директрисы 59, 60
 - касательная в точке 62
 - квадрика 56
 - неасимптотическое направление 61
 - однополостный гиперболоид 63
 - оси эллипса 59
 - парабола 60
 - параметрические представления 62
 - приведенные уравнения 58
 - стереографическая проекция 63
 - фокусы 59, 60
 - хорда 61
 - центр симметрии 61
 - эксцентриситет 59, 60
 - эллипс 59
 - эллиптического типа 59
- Критерий
 - Бухбергера 382
 - неотрицательной определенности 286
 - положительной определенности (Сильвестра) 283
- Лемма
 - Гаусса 126
 - Даламбера 172
 - Диксона 380

Лемма

- Накаямы 417
 - о разбиении группы на непесекающиеся подмножества 332, 333
 - о росте модуля многочлена 172
 - Фань Цзы 296
 - Цорна 358
- Линейное пространство
- алгебра 230
 - базис 18, 19, 24, 26, 32, 43, 45, 47–49, 51, 53–55, 76, 148, 150, 151, 154, 167, 179, 180–184, 186, 193, 194, 199, 201, 202, 208, 210, 213, 216, 217, 219–223, 235, 237, 240, 246, 274, 276–279, 284, 287, 293, 301, 304, 305, 308
 - базис Гамеля 237, 359
 - бесконечномерное 148, 241
 - гомоморфизм 147
 - изоморфизм 147
 - инвариантное подпространство 206, 207, 214, 226
 - конечномерное 148
 - пересечение подпространств 146, 151, 204, 272, 281, 288
 - подпространство 14, 145–148, 151, 152, 154, 178, 179, 194, 195, 198, 203, 206–214, 218, 221, 224, 225, 231, 232, 248, 249, 253, 254, 256, 263, 266–268, 274, 280, 281, 283–288, 398
 - пространство Крылова 213–218
 - прямая сумма подпространств 152
 - размерность 18, 32, 44, 45, 52, 76, 148, 150, 152, 153, 155, 156, 158, 162, 167, 194, 209, 211, 215–218, 221, 226, 228, 230, 301, 302, 304, 318, 325, 331, 332, 372

- сумма подпространств 152
 - теорема Грассмана 151, 204, 272, 281, 288
- Линейный оператор
- аннулирующий многочлен 188, 225
 - блочная жорданова форма 222
 - дефект 179
 - диагонализуемый 193, 195, 196, 199, 209, 228, 277, 280
 - единичный 178
 - жорданов базис 219–221
 - жорданова форма 220
 - инвариантное подпространство 206, 214, 226
 - индекс нильпотентности 210
 - индуцированный оператор 206
 - корневое разложение 209, 211, 212, 220
 - линейный функционал 177, 263, 264, 266, 268, 271, 293
 - максимальное расщепление 213
 - матрица линейного оператора 181–184, 279
 - минимальный многочлен 188, 224–228
 - неограниченный 250
 - неотрицательно определенный 277, 286
 - непрерывный 250
 - нильпотентный 210
 - нормальный 196, 276–280
 - нулевой 177
 - образ 179
 - обратимый 178
 - ограниченный 250
 - операторная норма 251
 - определитель линейного оператора 186, 427
 - положительно определенный 197, 277, 278, 280, 283
 - приведенный характеристический многочлен 184

- продолжение линейного функционала 266
- проектор 178
- произведение операторов 177
- простой структуры 193, 195, 196, 199, 209, 228, 277, 280
- пространство Крылова 213–218
- пространство образов 176
- пространство прообразов 176
- прямая сумма 207
- ранг 179
- сингулярное разложение 200–205
- скалярный 178
- след линейного оператора 185, 186
- собственное значение 193–196, 202, 208, 210, 221, 223, 278, 279
- собственное подпространство 194
- собственный вектор 193, 194
- сопряженный 276
- спектральная норма 203, 204, 252, 294, 298
- спектральный радиус 206
- сужение оператора 206
- сумма операторов 177
- теорема Кэли–Гамильтона 187, 209, 210, 212
- теорема Шура 198, 292
- характеристический многочлен 184–189, 193, 195, 208, 209, 220, 225, 226, 366
- ядро 147, 179
- вращения 57, 197, 224
- главная диагональ 36
- главный минор 184, 185, 195
- двоякостochasticкая 254, 259, 266, 289–291, 293, 296, 356
- диагонализуемая (простой структуры) 193, 195, 196, 199
- диагональная 36
- $2d + 1$ -диагональная 36
- единичная 36
- жорданова (жорданова форма) 220
- жорданова клетка (блок, ящик) 219
- закон инерции 288
- квадратная 13
- корневое разложение 209, 211
- кососимметричная 76, 224
- коэрмитова 76
- кронекерово произведение 35, 413
- линейного оператора 181
- ленточная 36
- матричная норма 252
- минимальный многочлен 188, 224–228
- минор 28–31, 38, 42–48, 66, 114, 185, 191, 195, 226, 282, 283, 286, 289, 424, 439, 440, 445
- k -я минорная 42
- невырожденная 39, 42, 44, 45, 47, 62, 66, 68, 73, 82, 87, 93, 95, 107, 182, 83, 185, 198, 201, 210, 224, 225, 286, 287
- нижняя почти треугольная 36
- нижняя треугольная 36
- нормальная 196, 199, 200, 222, 277, 280, 293, 298
- нулевая 35
- обратимая 37
- обратная 37
- операции с матрицами 31
- определитель 26

Матрица

- адамарово произведение 35
- блочная 35, 41, 70, 71, 187, 207, 208, 213, 219, 222, 224, 428
- Вандермонда 31, 137
- верхняя почти треугольная 36
- верхняя треугольная 36

Матрица

- ортогональная 76, 200, 222–224
- отражения 197
- перестановки 36
- перехода 181
- подматрица 13, 28, 35, 43, 44, 47, 85, 210, 282–285, 292, 423
- положительно определенная 197, 280, 283
- полярное разложение 295
- порядок матрицы 13
- приведенный характеристический многочлен 184
- присоединенная 38, 39, 40, 49, 188, 367, 417
- произведение 32–34
- прямая сумма 207, 218–223
- разделение переменных 46
- ранг матрицы 43, 47, 49, 203, 204, 226, 423, 425, 439, 440
- размера $m \times n$ 13
- самосопряженная 76
- Сильвестра (результант-матрица) 136
- симметричная 56, 76
- сингулярное разложение 200–205
- система линейных алгебраических уравнений 13
- скалярная 36
- скелетное разложение 47, 200
- след 185
- собственное значение 193–196, 201–206, 208–212, 220–225, 230, 277–286, 288, 289, 292–294, 296
- собственный вектор 193, 200, 277
- сопровождающая матрица 189
- сопряженная 76
- спектральная норма 203, 206, 252, 294, 298
- строго регулярная 67
- ступенчатая 64

- сумма 32
- теорема Кэли–Гамильтона 187, 209, 210, 212
- теорема Лапласа 28
- теорема Шура 198
- трехдиагональная 36
- треугольное разложение 67
- унимодулярно эквивалентные матрицы 190
- унитарная 76, 196–202, 204, 205, 275, 292–294
- Фробениуса 189
- фробениусова норма 252, 293, 294, 298
- Фурье 198, 200
- характеристический многочлен 184–189, 193, 195, 208, 209, 220, 225, 226, 427
- частичная ассоциативность 33, 34
- ширина ленты 36
- элементарная 64
- эрмитова 76

Матрицы

- конгруэнтные 287–289
- подобные 183
- унитарно подобные 196, 288
- эквивалентные 182
- эрмитово конгруэнтные 287
- унимодулярно эквивалентные 190

Минор

- алгебраическое дополнение 30
- базисный 43
- ведущий 282
- главный 184, 282
- дополнительный 30
- окаймляющий 43
- теорема Лапласа 28, 42, 55, 138

Множество

- аксиома выбора 353
- алгебраически замкнутое 388
- алгебраически открытое 388

- алгебраическое многообразие 386
- вполне упорядоченное 354, 357, 378
- выпуклое 254–260, 264–266, 268, 269, 272, 273
- выпуклое тело 257–260, 268, 269
- декартово произведение 32, 431
- замкнутое 173, 174, 244–248, 261–266
- компактное 244–249, 251, 265, 272
- лемма Цорна 267, 358
- линейно упорядоченное (цепь) 267, 353
- максимальная цепь 354
- начальный фрагмент 354
- ограниченное 173, 244
- открытое 244
- равномошные множества 356
- теорема Кантора 354
- теорема Кантора–Бернштейна–Шредера 356
- теорема Хаусдорфа 357
- теорема Цермело 354, 357
- цепь 353
- частично упорядоченное 353
- Многочлен
- алгебраическое многообразие 386
- алгоритм Бухбергера 284
- аннулирующий 188
- аннулятор множества точек 387–389, 394, 396, 397, 404, 429
- базис Грёбнера 379
- взаимно простые многочлены 122, 156, 157, 163, 164, 168, 207, 208, 225, 226
- деление с остатком 120, 121, 379
- деление с остатком на систему многочленов 379
- деление столбиком 120, 368, 409
- деления круга (круговой, цикломатический) 129, 164
- делитель 121
- дискриминант 141, 143, 164, 238, 415
- задача полиномиальной интерполяции 229
- значение многочлена 118, 134
- кольцо многочленов 118
- константа 118
- корень (нуль) многочлена 118
- кратность корня 162
- кратный корень 162
- критерий Бухбергера 382
- круговой (циклотический) 129, 164
- лемма Диксона 380
- матрица Сильвестра (результант-матрица) 136
- матрица Фробениуса (сопрядающая матрица) 189
- минимальный 155, 156, 171, 188, 224–226, 228, 230, 231, 233, 234, 316–318, 323, 330, 371, 408, 409, 415, 426–428, 433
- мономиальный идеал 380
- мультииндекс 42, 71, 133, 140
- наибольший общий делитель 121–123, 191, 317
- наилучшего приближения 248
- неполное частное 120, 368, 379
- непрерывность корней многочлена 432
- неприводимый 124–129, 134, 135, 155, 157–165, 168, 169, 171, 225, 226, 304–308, 311, 312, 314, 316, 317, 319, 322, 323, 325, 330, 331
- нетривиальный делитель 121
- нулевой 118
- общий делитель 121

Многочлен

- одночлен 118, 133
- однородный 133
- основная теорема алгебры 171
- приведенный минимальный 155
- приведенный характеристический 184
- признак Эйзенштейна 128
- произведение многочленов 119
- производная многочлена 163, 164, 168, 178, 228, 372
- простой корень 162
- равные многочлены 118, 133
- результат 136
- свободный член 118
- сепарабельный 162
- сизигии (S -многочлен) 381
- симметрический 139–142, 231, 328, 415
- словарный порядок 140, 141, 378, 385
- соотношения Ньютона 142
- сопровождающая матрица 189
- старший коэффициент 118
- степень многочлена 118, 133
- сумма многочленов 119
- суммы Ньютона 142
- теорема Гильберта о базисе 375
- теорема Гильберта о нулях 394, 395
- характеристический 184–189, 193, 195, 208, 209, 220, 225, 226, 366
- Чебышева 249
- формула Кардано 235
- формальное выражение 118
- формулы Виета 139, 328, 371, 415, 432
- элементарные многочлены Лагранжа 229
- элементарный симметрический 139

Неравенство

- Гёльдера 260
 - Вейля 292
 - Коши–Буняковского–Шварца 50, 238
 - Минковского 260
 - теорема Фаркаша 269, 275
 - треугольника 75, 236, 238, 240, 245, 260, 296
 - пара Гельдера 260
 - среднее арифметическое 257
 - среднее геометрическое 257
 - полиэдр 271
- Норма**
- абсолютная 295
 - банахово пространство 241
 - вектора 237
 - Гельдера (p -норма) 259
 - гильбертово пространство 241
 - длина 196, 238
 - дуальные нормы 251, 269, 298
 - евклидово пространство 238
 - линейного оператора 251
 - линейного функционала 251
 - матричная 252
 - метрика 237
 - метрическое пространство 237
 - нормированное пространство 231
 - операторная 251
 - подчиненная 251
 - расстояние 236
 - свойство мультипликативности 252
 - симметрическая калибровочная функция 295
 - спектральная 203, 204, 252, 294, 298
 - тождество параллелограмма 238
 - унитарно инвариантная 294, 295
 - унитарное пространство 238

- фробениусова 252, 293, 294, 298
- функционал Минковского 258
- функция Фань Цзы 295
- чебышевская (C -норма) 244
- эквивалентные нормы 247
- ядерная 296

Оболочка

- аффинная 253
- выпуклая 255
- линейная 15, 146

Определитель

- алгебраическое дополнение 30
- базисный минор 43
- Вандермонда 31
- геометрический смысл определителя 55
- дополнительный минор 30
- знакопеременная функция 24
- инверсия 21
- кососимметрическая функция 24
- n -линейная 23
- линейного оператора
- минор 28–31, 38, 42–48, 66, 114, 185, 191, 195, 226, 282, 283, 286, 289, 424, 439, 440, 445
- мультилинейная (полилинейная) функция 23
- независимые циклы 21
- объем параллелепипеда 54
- подстановка 19
- перестановка 19
- полилинейная функция 23, 114
- произведения матриц 41
- результат 136
- сопряженной матрицы 76
- теорема Лапласа 28
- транспозиция 21
- транспонированной матрицы 76
- формула Бине–Коши 40

- формулы (правило) Крамера 27
- цикл 20
- четность подстановки 22
- Отношение
- бинарное 15
- конгруэнтности 287
- мажоризации 289–293
- Рэлея 280
- эквивалентности 16, 159, 183, 190, 242, 243, 287, 309, 350
- частичного порядка 353

Подматрица

- ведущая 282
- главная 282

Подпространство

- инвариантное 206, 207, 214, 226
- Крылова 213–218, 226
- собственное 194
- сужение оператора на подпространство 206

Подстановка, перестановка

- знакопеременная группа 91, 92, 96, 231, 327
- инверсия 21
- симметрическая группа 82, 91, 101, 106, 235, 310, 312
- транспозиция 21
- цикл 20
- четность 22
- умножение подстановок 20

Поле

- автоморфизм 299
- аддитивная группа поля 113
- алгебраически замкнутое 155, 175, 360
- алгебраическое расширение 155
- алгебраическое число 155
- вычетов по простому модулю 116
- гомоморфизм 114
- конечное 166–169

Поле

- конечное расширение 153–156, 304, 313, 315, 317, 319, 323, 329
- конечное расширение Галуа 304
- координатное 403
- максимальное неподвижное 301
- малая теорема Веддерберна 117, 165
- минимальный многочлен 155, 156, 171, 316, 323, 330, 371, 373, 415, 426, 428, 435
- мультипликативная группа поля 113, 165
- нормальное (нормальное расширение) 307
- приведенный минимальный многочлен 155
- подполе 153
- поле разложения многочлена 159
- полициклическое расширение 319
- полициклический ряд 320
- примитивное расширение 315
- простое корневое расширение 317
- простое радикальное расширение 317
- размерность расширения 153
- рациональных функций 132
- резольвента Галуа 312
- резольвента Лагранжа 230
- теорема Абеля–Галуа 325, 327
- теорема Руффини 328
- характеристика поля 166
- циклическое расширение 317
- частных 130–132

Последовательность

- предел 240
- сходящаяся 240
- фундаментальная (Коши, сходящаяся в себе) 240

Произведение

- векторное 53
- естественное скалярное 197
- кронекерово 35
- линейных операторов 178
- матриц 33
- многочленов 119
- скалярное 49, 196
- смешанное 54
- тензорное 147

Пространство

- банахово 241
- гильбертово 241
- евклидово 238
- корневое 209
- Крылова 213–219
- линейное 144, 148, 152, 153, 157, 165, 168, 230, 244, 248, 266, 301, 359, 375, 427
- метрическое 236
- направляющее 253
- нормированное 237, 241, 259
- нуль-пространство (ядро) 147
- полное 241
- пополнение метрического пространства 242, 243
- сопряженное 251
- тензорное произведение 147
- унитарное 238

Система линейных алгебраических уравнений

- метод исключения элементов (метод Гаусса) 68
- нормальное псевдорешение 206
- общее решение 14
- однородная 14
- псевдорешение 206
- формулы Крамера 27
- фундаментальная система решений 49

Теорема

- Абеля–Галуа 325
 - алгебраическая теорема о неявной функции 437
 - алгоритм Евклида 122
 - Безу 121
 - Бернсайда 99
 - Бине–Коши 40
 - Биркгоффа 265
 - Больцано–Вейерштрасса 173
 - Вейерштрасса 174
 - Вейля 274
 - Виета 139
 - Виландта–Хоффмана 293
 - Гильберта о базисе 375
 - Гильберта о нулях 394
 - Грассмана 151
 - Дедекинда 312
 - Джона фон Неймана 295
 - закон инерции 288
 - Кантора 354
 - Кантора–Бернштейна–Шредера 356
 - критерий Бухбергера 382
 - критерий Сильвестра 283
 - Кронекера–Капелли 47
 - Крулля 429, 441
 - Куранта–Фишера 281
 - Кэли 106
 - Кэли–Гамильтона 187
 - Лагранжа 93
 - Лапласа 28
 - Ласкера–Нётер 345
 - лемма Цорна 358
 - Лидского 284
 - малая теорема Веддерберна 117, 165
 - малая теорема Ферма 116
 - Мирского 297
 - неравенства Вейля 292
 - неравенство Гёльдера 260
 - неравенство Минковского 260
 - неравенство Коши–Буняковского–Шварца 50, 238
 - Нётер о нормализации 391
 - обобщение основной теоремы алгебры 394
 - о базисном миноре 43
 - о наибольшем общем делителе 123
 - о перпендикуляре 198
 - основная теорема алгебры 171
 - подготовительная теорема Вейерштрасса 436
 - признак Эйзенштейна 128
 - процесс ортогонализации Грама–Шмидта 198
 - Рисса 263
 - Руффини 328
 - Силова 333
 - Фань Цзы 273
 - Фаркаша 269
 - Хана–Банаха 266
 - Хаусдорфа 357
 - Цермело 354
 - Чебышева об альтернансе 249
 - Шаля 101
 - Шура 198
- Точка**
- внутренняя 257–259
 - граничная 257
 - линейно внутренняя 257
 - локально внутренняя 273
 - предел последовательности 240
 - регулярная (неособая, гладкая, простая) 424
 - сингулярная (особая) 424
 - угловая (крайняя) 257, 265
- Ядро**
- гомоморфизма 103
 - линейного оператора 179
 - матрицы 147

Учебное издание

ТЫРТЫШНИКОВ Евгений Евгеньевич

ОСНОВЫ АЛГЕБРЫ

Редактор *Н.Б. Бартошевич-Жагель*

Оригинал-макет: *Д.В. Горбачев*

Оформление переплета: *В.Ф. Киселев*

Подписано в печать 26.01.2017. Формат 60×90/16.

Бумага офсетная. Усл. печ. л. 29.

Уч.-изд. л. 31,9. Тираж 800 экз. Заказ №1015.

Издательская фирма «Физико-математическая литература»

МАИК «Наука/Интерпериодика»

117342, г. Москва, ул. Бултерова, дом 17 Б

E-mail: porsova@fml.ru, sale@fml.ru

Сайт: <http://www.fml.ru>

Интернет-магазин: <http://www.fmlib.ru>

Отпечатано в АО «Первая Образцовая типография»

Филиал «Чеховский Печатный Двор»

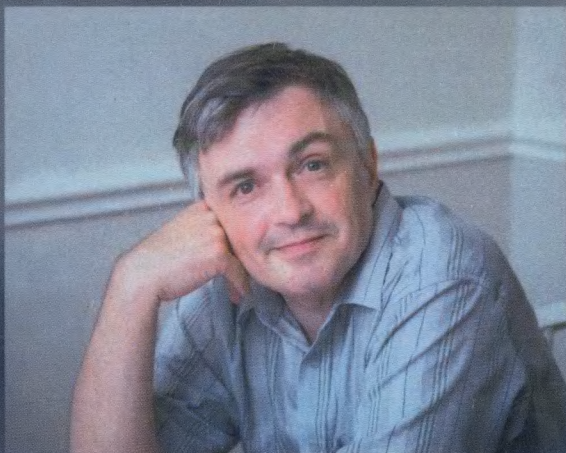
142300, Московская область, г. Чехов, ул. Полиграфистов, д. 1

Сайт: www.chpd.ru, E-mail: sales@chpd.ru, тел. 8(499)270-73-59

ISBN 978-5-9221-1728-9



9 785922 117289



Е. Е. Тыртышников

академик РАН,

директор Института вычислительной математики РАН,
профессор Московского государственного
университета им. М. В. Ломоносова
и Московского физико-технического института

Эту книгу я посвящаю тем, кто любит алгебру, и особенно тем, кто начинает изучать ее в университете, обычно на первом курсе.

Читать им лекции – особое удовольствие!

Оттого что видишь, как каждый из них искренне тянется к знанию и как зажигаются чудесные огоньки в глазах, когда возникает понимание. Уже через пару лет с горечью замечаешь, что у многих тяга к знанию ослабла и огоньков совсем мало.

Наверное, мы как-то не так учим?

Я далек от того, чтобы преувеличивать значение дидактики.

Но, согласитесь, трудный путь к пониманию очень часто освещается вдруг всего лишь одним верным словом.

Мне хотелось найти это слово.