

③ Группы. Подгруппа, Фактор-группа, индекс группы по подгруппе.

Теор. Лагранжа.

Группа

Непустое мн-во G с заданной на нем операцией $*$: $G \times G \mapsto G$ наз-ся группой $(G, *)$, если выполнены аксиомы: $\forall x, y, z \in G$

1) ассоциативность $(x * y) * z = x * (y * z)$

2) существование единицы $\exists e: \forall x \quad e * x = x * e = x$

3) существование обратного элемента: $\forall x \exists (y: y * x = x * y = e \quad (y = x^{-1})$

Коммутативная (абелева) группа: $a * b = b * a$

Подгруппа

Если $G = (G, *)$ -группа, H -подмн-во G , устойчивое относит. $*$, то $H = (H, *)$ -подгруппа G : $H \leq G$

Нормальная подгруппа

$N \leq G$ наз-ся нормальной, если $\forall n \in N, \forall g \in G \Rightarrow gng^{-1} \in N$. $(\forall g \in G \quad gN = Ng)$

Факторгруппа

$H \leq G$, H -нормальная подгруппа, $aH = \{ah | h \in H\}$ $\forall a$ - смежные классы.

На мн-ве классов смежности можно ввести умножение $(aH)(bH) = abH$.

Группа смежных классов группы G по нормальной подгруппе H наз-ся факторгруппой G/H .

Индекс подгруппы

Количество смежных классов группы G по подгруппе H наз-ся индексом подгруппы $(G:H)$

Теор. Лагранжа: $H \leq G$, то $|G| = (G:H) \cdot |H|$

② Циклические группы. Структура подгрупп циклической группы, порождающие элементы, их кол-во и нахождение.

Циклич. группы

$$a^0 \stackrel{\text{def}}{=} e, \quad a^n \stackrel{\text{def}}{=} \underbrace{a \cdot \dots \cdot a}_{n \text{ раз}}, \quad na \stackrel{\text{def}}{=} \underbrace{a + \dots + a}_{n \text{ раз}}$$

C -циклич. группа, если $\exists c \in C, \exists k \in \mathbb{N}: \forall x \in C \quad x = c^k \quad C = \langle c \rangle$

Порядок элемента: $\text{ord } a \stackrel{\text{def}}{=} \text{ord } \min \{a^n = e\}$

Свойства:

1) Все циклич. группы абелевы

2) Каждая циклич. группа порядка n изоморфна $\mathbb{Z}_n$, $n = \infty \Rightarrow$ изоморф. $\mathbb{Z}$.

3) Каждая подгруппа циклической группы циклическа.

4) У циклич. групп порядка n $\exists$ ровно $\varphi(n)$ порождающих элем.

φ - Ф-я Эйлера, $\varphi(n)$ = кол-во натуральных чисел, меньших n и взаимно простых с ним. $\varphi(1) \stackrel{\text{def}}{=} 1$

③ Кольца. Идеалы колец и фактор-кольца. Евклидовы кольца. Примеры

Кольцо

Кольцом R наз-ся тройка $(R, +, \cdot)$, где R - непустое мн-во (носитель); $+, \cdot: R \times R \rightarrow R$ а $\forall x, y, z \in R$ выполняются аксиомы кольца:

- 1) R - коммут. группа по сложению
- 2) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ - ассоц. умножения
- 3) дистрибутивность: $x \cdot (y + z) = x \cdot y + x \cdot z$
 $(y + z) \cdot x = y \cdot x + z \cdot x$

Кольцо с единицей - унитарное.

Коммут. кольцо: $x \cdot y = y \cdot x$

Кольцо без делителей нуля: $\forall r_1, r_2$, если $r_1 \cdot r_2 = 0 \Rightarrow \begin{cases} r_1 = 0 \\ r_2 = 0 \end{cases}$

Целостное кольцо - ассоциативно-коммутативное без делителей нуля

Идеалы колец

Подкольцо I коммутативного кольца $(R, +, \cdot)$ наз-ся его идеалом ($I \triangleleft R$), если $\forall x \in I, \forall a \in R \Rightarrow a \cdot x \in I$ и $x \cdot a \in I$

Идеал I унитарного коммут. кольца $(R, +, \cdot)$ наз-ся главным, если $\exists a \in R$:

$$I = \{a \cdot r \mid r \in R\} \quad (I = (a))$$

Кольца главных идеалов - целостные кольца, в которых все идеалы, отличные от самого кольца, главные

Фактор-кольца

Класс вычетов по модулю идеала I кольца $(R, +, \cdot)$: $[r]_I = \{r + x \mid r \in R, x \in I\}$ - смежный класс по норм. подгруппе $(I, +)$ аддит. группы кольца с представителем r .
Мн-во классов вычетов - фактор-кольцо кольца R по модулю идеала I (R/I)

Евклидовы кольца

Коммутативное кольцо $(R, +, \cdot)$ наз-ся евклидовым, если:

- 1) R - целостное
- 2) $\forall r \in R \exists$ норма $N(r) \in \mathbb{N}_0$
- 3) $\forall a, \forall b \neq 0$ из $R \exists q, r: a = q \cdot b + r$ и либо $r = 0$, либо $N(r) < N(b)$
- 4) $\forall a, b \in R, a \neq 0, b \neq 0 \Rightarrow \max\{N(a), N(b)\} \leq N(a \cdot b)$

Примеры

- 1) Целостное унитарное кольцо $(\mathbb{Z}, +, \cdot)$
- 2) Кольцо классов вычетов по ~~модулю~~ модулю n : $\mathbb{Z}_n = (\{0, \dots, n-1\}, +_{\text{mod } n}, \cdot_{\text{mod } n})$
- 3) Главный идеал: $(n) = n\mathbb{Z} \triangleleft \mathbb{Z}$
- 4) Фактор-кольцо: $I = 2\mathbb{Z} \triangleleft \mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z} = \{[0]_I, [1]_I\}$
- 5) Кольцо $\mathbb{Z}$ целых чисел - евклидово

④ Поля. Характеристика поля. Построение конечных полей с помощью неприводимых мн-в. Полином. и степенное представление элем. поля. Примеры.

Поле

Поле K наз-ся тройка $(K, +, \cdot)$, где K - ненулевое мн-во, $+, \cdot: K \times K \rightarrow K$ и выполняются аксиомы поля.

- 1) K - абелева группа по сложению
- 2) $K \setminus \{0\}$ - абелева группа по умножению
- 3) $x \cdot (y+z) = x \cdot y + x \cdot z \quad \forall x, y, z \in K$

Т.е. поле - кольцо, ненулевые элем. которого образуют группу по умн-ю.

Характеристика поля

$k = \text{char } K$, k - первое k , такое что $\underbrace{1+...+1}_k = 0$.

Построение конечных полей

Неприводимые многочлены - простые (неразложимые) элементы кольца многочленов $K[x]$ над полем K .

Алгоритм построения:

- 1) Выбираем простое p и по нему поле $\mathbb{F}_p = (\{0, 1, \dots, p-1\}, +_p, \cdot_p)$.
- 2) Рассмотрим кольцо $\mathbb{F}_p[x]$
- 3) Выберем $n \in \mathbb{N}$ и неприводимый мн-н $P(x) = \sum_{i=0}^n a_i x^i \in \mathbb{F}_p[x]$
- 4) Целая $(P(x))$ порождает мн-во $\mathbb{F}_p[x]/(P(x))$, элемнты которого мн-ва мн-вом $\{R(x)\}$ остатков от деления $f(x) = Q(x) \cdot P(x) + R(x)$, $f \in \mathbb{F}_p[x]$ мн-во $\{R(x)\}$ явл. полем Галуа $GF(p^n)$

Степенное представление элем. поля

$$\mathbb{F}_p^* \cong \mathbb{F}_p \setminus \{0\}$$

α - примитивный элем, если 1) $\forall \beta \in \mathbb{F}_p^* \exists i \in \{1, \dots, p-1\}: \beta = \alpha^i$

2) $\alpha^{p-1} = 1, \alpha^i \neq 1 \text{ для } 1 \leq i \leq p-2$

$\neq$ групп элем. поля м.д. получен как α^k , где k - взаимно простое с $p-1$ (см $GF(p^n)$)

Примеры

1) Поля: $\mathbb{Q}; \mathbb{R}; \mathbb{C}; \mathbb{Z}_p$ - поле вычетов по простому модулю; $\mathbb{F}_q$, где $q = p^k$, p - простое, $k \in \mathbb{N}$; $F(x)$ - поле рац. ф-ций $f(x)/g(x)$, где f и g - мн-ны над $\mathbb{F}$, $g \neq 0$.

2) Для построения $GF(9) = GF(3^2)$ найдем мн-н степени 2, неприводимый над $\mathbb{Z}_3$ (например, x^2+1). Тогда $GF(9) = \mathbb{Z}_3[x]/(x^2+1)$. Элемнты: $0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2$.

$x+1$ - примитивный элемент $\Rightarrow$ можно получить степенное представление

⑤ Многочлены над полем $\mathbb{F}_p$. Неприводимые мн-ны и их нахождение.
Лемма о числе неприводимых нормированных мн-в над $\mathbb{F}_p$.

Многочлены над полем $\mathbb{F}_p$

$$\mathbb{F}_p = GF(p) = \mathbb{Z}/(p) = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}, \text{ где } \begin{cases} \bar{0} = 0 + p\mathbb{Z} \\ \bar{1} = 1 + p\mathbb{Z} \\ \dots \end{cases}$$

$K[x]$ - кольцо мн-в от формальной перем. x :

$$\{p(x) = a_0 + a_1x + \dots + a_nx^n\}, a_i \in K, n \in \mathbb{N}, a_n \neq 0.$$

$K[x]$ - евклидово.

Неприводимые мн-ны

Каждый элем. евклидова кольца однозначно с точностью до перестановки разлагается в произведение простых (неразложимых) элементов.

Простые элем. $K[x]$ - неприводимые мн-ны:

- в поле $\mathbb{C}$ - только мн-ны 1-й степени
- в $\mathbb{R}$ - мн-ны 1-й степени и 2-й с $\Delta < 0$.
- в $\mathbb{Q}$ - $\exists$ неприводимые мн-ны $\forall$ $\mathbb{Q}$.

$\forall n \in \mathbb{N}, \forall p$ - простое, над $\mathbb{F}_p \exists$ неприводимый мн-н степени n .

Нет эффективных алгоритмов нахождения.

Лемма

Если d_n - число неприводимых нормированных мн-в степени n над $\mathbb{F}_p$, то $\sum_{m|n} m \cdot d_m = p^n$

$$\text{Следствия: 1) } nd_n = p^n - \sum_{k|n, k < n} kd_k \geq p^n - \sum_{k=0}^{n-1} p^k = p^n - \frac{p^n - 1}{p - 1} > 0$$

$$\Rightarrow d_n > 0$$

$$2) d_n \sim \frac{p^n}{n}, n \rightarrow \infty$$

⑥ Минимальные мн-ны над $\mathbb{F}_p$ для элем. из $\mathbb{F}_{p^n}$. Нахождение м.м.

Минимальный мн-н

$\beta \in \mathbb{F}_{p^n}$, $m_\beta(x)$ наз-ся минимальным для β , если это нормированный многочлен минимальной степени из $\mathbb{F}_p[x]$, для которого β - корень

Нахождение

Пусть задано $\mathbb{F} = \mathbb{F}_p[x]/(a(x))$, $a(x) = a_0 + a_1x + \dots + a_nx^n$ - неприводимый.

Тогда для элемента $x \in \mathbb{F}$ многочлен $a_n^{-1} \cdot a(x)$ - минимальный

⑦ Алгоритм нахождения всех корней многочлена над полем $\mathbb{F}_p$

$f(x) \in \mathbb{F}_p[x]$

1) Разложить $f(x)$ на неприводимые: $f(x) = g_1(x) \cdot \dots \cdot g_k(x)$

2) Для каждого $g_i(x), i=1, \dots, k$ рассмотреть расширение $\mathbb{F}_p[x] / (g_i(x))$ в котором он будет иметь корни $\alpha = \alpha, \alpha^p, \dots, \alpha^{p^{\deg g_i - 1}}$

Записать данные корни как многочлены из $\mathbb{F}_p[x] / (g_i(x))$.

3) Объединить все корни в один общий расширенный $\mathbb{F}_p^m$, где $m = \text{НОК}(\deg g_1, \dots, \deg g_k)$

⑧ Теорема Хэмминга. Коды Хэмминга, пример построения.

n -кодированное слово длины $n = k + m$: k инф. бит, m проверочных

или во $\{v_1, \dots, v_m\}$ всех кодированных слов длины n — (n, k) -код.

Теор. Хэмминга

n — длина кода, r — макс. допустимое число ошибок

При $2n < n$ максимальное число t кодированных слов находится в пределах:

$$\frac{2^n}{\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{2r}} \leq t \leq \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{r}}$$

Код Хэмминга

Задача плотной упаковки: при каких n и r в куб $\mathbb{B}^n$ можно уложить непересекающиеся шары радиуса r без остатка?

1) $n = 2^m - 1, r = 1 \Rightarrow$ код Хэмминга

2) $n = 23, r = 3$ — код Голая

Пример построения

$n = 7 = 2^3 - 1 \Rightarrow m = 3, r = 1$. Построим таблицу: матрица состоит из единиц, размерности $2^m - m - 1 = 4$ и из различных бинарных наборов длины m , содержащих не менее 2-х единиц.

$$\left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right]$$

$\underbrace{\hspace{4cm}}_{2^m - m - 1} \quad \underbrace{\hspace{2cm}}_m$

Складывая строки произвольным образом, получим $16 = 2^4$ возможных сообщений.

9) Систематическое кодирование. Линейные (групповые) и циклические коды: определение и свойства.

Систематическое кодирование

k бит исходного сообщения копируются в фиксированные позиции кодового слова, затем вычисляются остальные $m = n - k$ проверочных бит.

Линейные коды

Блочный (n, k) -код C наз-ся линейным, если он образует $1D$ размерности k координатного пространства $\{0, 1\}^n$

Свойства:

1) Сумма $\forall$ кодовых слов - кодовое слово

2) Кодовое расстояние $d = \min_{x \in C} \|x\|$

3) $\exists$ базис $\{g_0, \dots, g_{k-1}\}$ и $\forall v \in C \Rightarrow v = \sum_{i=0}^{k-1} u_i g_i, u_i \in \{0, 1\}$

$\Rightarrow v = G u, G_{n \times k} = [g_0, \dots, g_{k-1}]$ - порождающая матрица кода

C можно эквивалентным преобразованием: $G \mapsto \tilde{G} = \begin{bmatrix} I_k \\ P_{m \times k} \end{bmatrix}$

Тогда кодирование $v = \tilde{G} u$ - систематическое

Проверочная матрица $H_{m \times n} = \begin{bmatrix} h_0^T \\ \vdots \\ h_{m-1}^T \end{bmatrix}$, где $\{h_0, \dots, h_{m-1}\} \in \{0, 1\}^n$ - баз. $C^\perp$

Если $\tilde{G} = \begin{bmatrix} I_k \\ P_{m \times k} \end{bmatrix}$, то $H_{m \times n} = [P_{m \times k} \ I_m]$. Эти матрицы определены

с точностью до эквив. преобразований $\tilde{G}$ и строк H , но фиксированные инф. биты при систематическом кодировании задают эти матрицы однозначно.

Синдром принятого слова w : $s = H w \in \{0, 1\}^m$

Свойства синдрома:

1) $s = 0 \Rightarrow w$ - кодовое слово

2) $s = H w = H(v + e) = H e$, где e - вектор ошибок: $H e = s$

$e = \hat{e} + G u$, $\hat{e}$ - частное реш. системы $H \hat{e} = s$, u - $\forall$ вектор ошибок k .

$G u$ - решение системы $H x = 0$

Схема декодирования: $w \rightarrow s = H w \xrightarrow{H e = s} e = \hat{e} + G u \xrightarrow{\|e\| \rightarrow \min} \hat{v} = w + e$

Циклические коды

Код C наз-ся циклическим, если $\forall 0 \leq s \leq n-1 (d_0, \dots, d_{n-1}) \in C \Rightarrow (d_s, d_{s+1}, \dots, d_{n-1}, d_0, \dots, d_{s-1}) \in C$.

В кольце $\mathbb{F}_p[x]/(x^n - 1)$ есть базис $\{1, \bar{x}, \dots, \bar{x}^{n-1}\}$, в котором циклический сдвиг равносильно умножению на x .

Построение:

1) Выбираем $g(x)$ - делитель $x^n + 1$, порождающий многочлен

2) В $\mathbb{F}_2[x]/(x^n + 1)$ образуем $(g(x))$ -идеал.

3) $v = (v_0, \dots, v_{n-1})^T \leftrightarrow v(x) = v_0 + v_1 x + \dots + v_{n-1} x^{n-1}$

$v \in \{0, 1\}^n$

$v(x) \in \mathbb{F}_2[x]$

Кодирование:

1) ~~Векторное~~ Несистематическое: $v(x) = g(x)u(x)$.
В порождающей матрице $G_{n \times k} = [g_0, \dots, g_{k-1}]$ базисные векторы соотв. полиномам $x^i g(x)$, $i = \overline{0, k-1}$

2) Систематическое кодирование

~~н~~ Собразуем полином $x^m u(x)$ степени $\underbrace{m+k-1}_{\deg x^m + \deg u(x)} = n-1$.

$$x^m u(x) = g(x)q(x) + r(x), \deg r(x) < m$$

$$\Rightarrow x^m u(x) + r(x) = g(x)q(x) \in C$$

Кодирование и.д. задано как $v(x) = x^m u(x) + r(x)$, $r(x) \equiv_{g(x)} x^m u(x)$
При k старших степенях $v(x)$ имеет коэф. $u(x)$.

В $G_{n \times k} = [g_0, \dots, g_{k-1}]$ базисные векторы g_i соотв. полиномам $x^{m+i} + r_i(x)$, $i = \overline{0, k-1}$

Декодирование

Синдром принятого полинома ~~н~~ $w(x)$: $S(x) \equiv_{g(x)} w(x)$

Свойства:

1) $S(x) \equiv 0 \Leftrightarrow w(x)$ - кодовое

2) $0 \leq \deg S(x) \leq m = n-k$

3) $S(x) \equiv_{g(x)} v(x) + e(x) \equiv_{g(x)} e(x) \equiv_{x^{n+1}} w(x)h(x)$

Общая схема декодирования:

1) Вычислить $S(x)$

2) Найти реш. системы $e(x) = S(x) + g(x) \cdot u(x)$ для всех 2^k возможных полиномов ~~н~~ $u(x)$ степени $k-1$

3) Полином ошибок $e(x)$ - решение с min числом ненулевых слог.

4) $u(x) = w(x) + e(x)$

10) Определение и св-ва кодов БЧХ.

$\exists$ выбраны q и $d \leq n = 2^q - 1$; d - конструктивное расстояние

Код БЧХ - циклический (n, k) -код, в котором порождающий многочлен $g(x)$ имеет корнями элементы $d, d^2, d^3, \dots, d^{d-1}$ поля $F = \mathbb{F}_2^q$, где d - генератор группы F^* , $\deg g(x) = m$ (число проверочных бит), $k = n - m$ (число инф. бит)

$$d-1 = 2^q$$

$$v(x) \in C \Leftrightarrow v(d^i) = 0, i = \overline{1, d-1}$$

Синдром принятого полинома $w(x)$: $S_i = w(d^i)$ $i = \overline{1, d-1}$

$w(x)$ - кодовое слово $\Leftrightarrow$ все синдромы равны нулю

⑪ Действие группы на множестве. Фиксатор и стабилизатор. Примеры.
 $G = (G, o, e), |G| = n$
 $T, |T| = N$

$Bij(T)$ - мн-во всех перестановок элем. T

$Symm(T)$ - симметрическая группа мн-ва T : $Symm(T) = (Bij(T), *, 1_T)$

Действие группы на множестве

1) Группа G действует на мн-ве T , если задан гомоморфизм $G \rightarrow Symm(T)$, т.е. α -действие G на T ($G \curvearrowright T$), если $\alpha \in Hom(G, Symm(T))$

2) $\alpha = (G, T; o, *, e)$

$G \times G \xrightarrow{o} G$ - групповая операция

$G \times T \xrightarrow{*} T$ - новая операция

Аксиомы:

$$e * t = t; (g \circ h) * t = h * (g * t)$$

$$g * t = g(t) = t' \Rightarrow e(t) = t, (g \circ h)(t) = h(g(t))$$

Отношение эквивалентности: $t \sim_g t' \stackrel{df}{=} \exists k: g^k(t) = t'$

g -орбиты - смежные классы эквивалентности $\sim_g$.

$C(g)$ - число всех смежных классов

$\nu_1, \dots, \nu_N$ - кол-во циклов длины $1, \dots, N$

$$Type(g) = \{\nu_1, \dots, \nu_N\}$$

$$C(g) = \sum_{k=1}^N \nu_k(g); \sum_{k=1}^N k \cdot \nu_k(g) = N$$

Отношение эквивалентности: $t \sim_G t' \stackrel{df}{=} \exists g \in G: g(t) = t'$

Орбиты - классы эквивалентности $\sim_G$

$C(G)$ - число орбит

Фиксатор:

$$Fix(g) \stackrel{df}{=} \{t \in T \mid g(t) = t\} \subseteq T$$

Стабилизатор:

$$Stab(t) \stackrel{df}{=} \{g \in G \mid g(t) = t\} \subseteq G$$

Пример:

$$T = \{1, \dots, 10\}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 6 & 1 & 8 & 5 & 2 & 7 & 10 & 3 & 4 \end{pmatrix} = (1, 9, 3)(2, 6)(4, 8, 10)(5)$$

$$Type(g) = (2, 1, 2, 0, \dots, 0); \quad \nu_1 = 2, \nu_2 = 1, \nu_3 = 2, \nu_4 = \nu_5 = \dots = \nu_{10} = 0$$

$$C(g) = 2 + 1 + 2 = 5$$

$$|T| = 2 \cdot 1 + 1 \cdot 2 + 2 \cdot 3 = 10$$

12) Лемма Бернсайда и её применение.

Лемма Бернсайда:

$$C(G) = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

Пример применения

Составляются слова длины $l \geq 2$ из алфавита $A = \{a_1, \dots, a_m\}$

Слова эквивалентны, если они получают одно из другого перестановкой крайних букв.

S - ? Число неэкв. слов.

T - мн-во слов длины l в A . $N = |T| = m^l$

g переставляет в слове крайние буквы; $g^2 = e \Rightarrow G = \{e, g\} \cong \mathbb{Z}_2$

$$S = C(G)$$

$$|\text{Fix}(e)| = |T| = m^l; \quad |\text{Fix}(g)| = m^{l-2}, \quad m = m^{l-1}$$

$$S = C(G) = \frac{1}{2} (m^l + m^{l-1}) = \frac{m^{l-1}(m+1)}{2}$$

13) Группы диэдра. Группы вращений правильных многогранников.

Группы диэдра

D_n - группа симметрии правильного n -угольника, включающая вращения и осевые симметрии. Правильный n -угольник имеет $2n$ различных симметрий: n поворотов и n осевых отражений.

D_n имеет элементы $R_0, \dots, R_{n-1}$ и $S_0, \dots, S_{n-1}$ - повороты на $\frac{2\pi k}{n}$ и n симметрий.

$$R_i R_j = R_{i+j}, \quad R_i S_j = S_{i+j}, \quad S_i R_j = S_{i-j}, \quad S_i S_j = R_{i-j}$$

Группы вращений правильных многогранников

1) T - группа вращений тетраэдра

$$T = \langle t, f \rangle, \quad t^3 = f^2 = e$$

t - вращ. на 120° вокруг оси, проходящей через вершину и центр

f - вращ. на 180° вокруг оси, проход. через центры противополож. ребер

$$|T| = (3-1) \cdot 4 + (2-1) \cdot 3 + 1 = 12$$



2) O - группа вращений куба

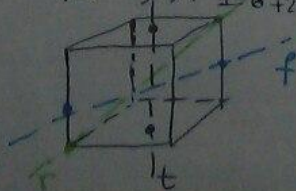
$$O = \langle t, f, r \rangle, \quad t^4 = f^2 = r^3 = e$$

t - вращ. на 90° вокруг оси, проход. через середины двух противополож. граней

f - вращ. на 180° вокруг оси, проход. через середины - " - ребер

r - вращ. на 120° вокруг оси, проход. через две противополож. вершины

$$|O| = 3 \cdot 3 + 1 \cdot 6 + 2 \cdot 4 + 1 = 24$$



14) Цикловой индекс действия группы на множ-ве.

$\text{Type}(g) = \langle \nu_1, \dots, \nu_n \rangle$; ν_i - кол-во циклов длины i .

Соотавим каждой перестановке $g \in G$ вес $w(g) = x_1^{\nu_1} \cdot x_2^{\nu_2} \cdot \dots \cdot x_n^{\nu_n}$

Цикловой индекс.

$$P(G; T, x_1, \dots, x_n) = \frac{1}{|G|} \sum_{g \in G} w(g) = P_G = P(G)$$

Свойства:

1) $G \cong G' \Rightarrow P_G = P_{G'}$, если действия определены согласовано

2) $P_G = P_{G'} \not\Rightarrow G \cong G'$

15) Теорема Пойа-Фейнмана и её применение

$T, |T| = N$; $G, |G| = n$; $G \leq T$; $R = \{c_1, \dots, c_r\}$ - множество меток ("красок")

$F = R^T$ - совокупность функций приписывания меток ("раскрашивания")

элементам T

$$R^T \times G \xrightarrow{\varphi} R^T$$

Веса элементов R : $w(c_i) = y_i$, $i = \overline{1, r}$

Теор. Пойа-Фейнмана

$$P(G; R^T) = P(G; T, x_1, \dots, x_n) \Big|_{x_k = y_1^k + \dots + y_r^k, k = \overline{1, N}}$$

Применение

Можно определить число размещений данного типа (т.е. содержаний данного кол-ва элементов конкретного цвета)

Задача об ожерельях: 5 бусин, 3 цвета (красный, зеленый, синий).

Ожерелья одинаковые, если совпадают при перевороте или повороте.

Сколько $\exists$ различных ожерельй, содержащих 2 красные бусины?

$$x_1 = y_1 + y_2 + y_3, x_2 = y_1^2 + y_2^2 + y_3^2, \dots, x_k = y_1^k + y_2^k + y_3^k, k = \overline{1, 5}$$

$$w(\text{Red}) = y_1, w(\text{Green}) = y_2, w(\text{Blue}) = y_3$$

$$y_1 = y, y_2 = y_3 = 1 \Rightarrow x_1 = y + 2, x_2 = y^2 + 2, \dots, x_5 = y^5 + 2$$

$$P(x_1, \dots, x_5) = \frac{1}{10} (x_1^5 + 4x_5 + 5x_1x_2^2)$$

$$P(y) = \sum_{i=1}^5 u_i y^i, u_i = ?$$

$$P(y) = \frac{1}{10} (u_0 + u_1 y + u_2 y^2 + \dots + u_5 y^5) = \frac{1}{10} ((y+2)^5 + 4(y^5 + 2) + 5(y+2)(y^2 + 2)) =$$

$$= \frac{1}{10} (\dots C_5^2 2^3 y^2 + \dots + 5(y+2)(y^4 + 4y^2 + 4)) = \frac{1}{10} (\dots (10 \cdot 8 + 5 \cdot 2 \cdot 4) y^2 \dots)$$

$$\Rightarrow u_2 = \frac{80 + 40}{10} = 12$$

16 Частично упорядоченные мн-ва. Экстремальные элем, порядковые идеалы и фильтры, конусы, точные грани ч.у. множеств.

Ч.у. множества

Пара $P = (P, \leq)$, где P - непустое мн-во, $\leq$ - рефлексивное, антисимметричное транзитивное бинарное отношение на P , наз-ся ч.у. множеством.

• Рефлексивность: $x \leq x$

• Антисимм: $x \leq y, y \leq x \Rightarrow x = y$

• Транзитивность: $x \leq y, y \leq z \Rightarrow x \leq z$

Экстремальные элем.

Элем. $u \in P$ называют:

1) максимальным, если $u \leq x \Rightarrow u = x$

2) минимальным, если $u \geq x \Rightarrow u = x$

3) наибольшим, если $x \leq u \quad \forall x \in P$

4) наименьшим, если $x \geq u \quad \forall x \in P$

Порядковые идеалы и фильтры

$I \subseteq P$ наз-ся порядковым идеалом, если $\left. \begin{matrix} x \in I \\ y \leq x \end{matrix} \right\} \Rightarrow y \in I$

$F \subseteq P$ наз-ся порядковым фильтром, если $\left. \begin{matrix} x \in F \\ x \leq y \end{matrix} \right\} \Rightarrow y \in F$

$I(P)$ - мн-во всех порядковых идеалов ч.у. мн-ва P .

Конусы

$(P, \leq)$ - ч.у., $A \subseteq P$. Множества $A^+ = \{x \in P \mid \forall a \in A \Rightarrow a \leq x\}$ и $A^- = \{x \in P \mid \forall a \in A \Rightarrow x \leq a\}$ наз-ся верхним и нижним конусом, а их элементы - верхними и нижними границами.

Точные грани

$(P, \leq)$ - ч.у., $A \subseteq P$

Наименьший элем. в A^+ - точная верхняя грань - $\sup A$

Наибольший элем. в A^- - точная нижняя грань - $\inf A$

Они могут не существовать

17 Теорема Шмидта. Линейные продолжения и размерность ч.у. мн-ва

Если $x \leq y$ или $y \leq x$, то x и y сравнимы ($x \sim y$).

Полный (линейный) порядок, если $\forall x, y \Rightarrow x \sim y$

Теор. Шмидта

1) $\forall$ частичный порядок $\leq$ м.б. продолжен до линейного на том же мн-ве.

2) Каждый порядок есть пересечение всех своих линейных продолжений

$e(P)$ - мн-во всех линейных продолжений ч.у. мн-ва P .

Расширим вероятностное пр-во на мн-ве $e(P)$; E - событие вида $x \leq y$, $(x \leq y) \notin (x \leq z)$ и т.д.

$Pr[E] = \frac{\text{число линейных продолжений, в кот. имеет место } E}{|e(P)|}$

Спектр. $\text{Spec}(P) = \{P \mid \exists a \in P, a \neq 0, a \in P\}$

Размерность

$\dim(P)$ - наименьшее число линейных порядков, данных в пересечении данных ч.у. мн-во P .

(18) Решётки. Нераспределительные элем. решётки, решёточные идеалы и фильтры. Модулярные и дистрибутивные решётки, критерии модулярности и дистрибутивности.

Решётки

Ч.у. мн-во, в котором $\forall a, b \in \{a, b\}, \sup\{a, b\}$ называют решёточно упорядоченным. Решётка называется полной, если $\forall$ множество её элем. $\exists \sup$ и $\inf$.

Алгебраическая решётка - тройка $L = \langle L, \cup, \cap \rangle$, где L - непустое мн-во; $\cup$ - объединение, $\cap$ - пересечение - бинарные операции.

$$x \cup y = y \cup x; \quad x \cap y = y \cap x$$

$$x \cup (y \cap z) = (x \cup y) \cap z; \quad x \cap (y \cup z) = (x \cap y) \cup z$$

$$x \cup x = x; \quad x \cap x = x$$

$$x \cap (x \cup y) = x; \quad x \cup (x \cap y) = x$$

~~Идеалы и фильтры~~

Универсальные грани решётки: ноль - наименьший элем; единица - наибольший. Элем $a \neq 0$ решётки L с нулём 0 наз-ся атомом, если $\forall x \in L$

$$a \cap x = \begin{cases} 0, & \text{если } x \text{ не содержит атом } a \\ a, & \text{если } x \text{ содержит атом } a \end{cases}$$

Решёточный идеал

$I \subseteq L$ наз-ся идеалом, если: 1) $\forall x \in I, y \in L \Rightarrow x \cap y \in I$ 2) $\forall x, y \in I \Rightarrow x \cup y \in I$

Решёточный фильтр

$F \subseteq L$ наз-ся решёточным фильтром, если: 1) $\forall x \in F, y \in L \Rightarrow x \cap y \in F$ 2) $\forall x, y \in F \Rightarrow x \cup y \in F$

Модулярные решётки

Решётка $\langle L, \cup, \cap \rangle$ наз-ся модулярной, если $\forall x, y, z \in L$ выполняется модулярный закон

$$\text{Mod: } x \leq y \Rightarrow x \cup (y \cap z) = y \cap (x \cup z)$$

Критерий модулярности: решётка модулярна $\Leftrightarrow$ никакая её подрешётка не изоморфна N_5 .

Дистрибутивные решётки

Решётка $\langle L, \cup, \cap \rangle$ наз-ся дистрибутивной, если в ней выполняются дистрибутивные законы:

$$(x \cup y) \cap z = (x \cap z) \cup (y \cap z)$$

$$(x \cap y) \cup z = (x \cup z) \cap (y \cup z)$$

Критерий дистрибутивности: решётка дистрибутивна $\Leftrightarrow$ никакая её подрешётка не изоморфна ни N_5 , ни M_3 .

Неразложимые элементы

Элем $z \neq 0$ наз-ся неразложимым, если из $z = x \cup y$ следует $z = x$, либо $z = y$.

$\text{Irr } L$ - мн-во неразложимых в объединение элем. L .

$$\text{Irr}(x) = \{y \in \text{Irr } L \mid y \leq x\}$$

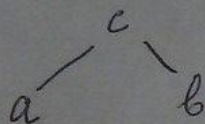
$$\forall x \neq 0 \Rightarrow x = \bigcup_{a \in \text{Irr}(x)} a$$

①⑨ Решётка порядковых идеалов ч.у. множества.

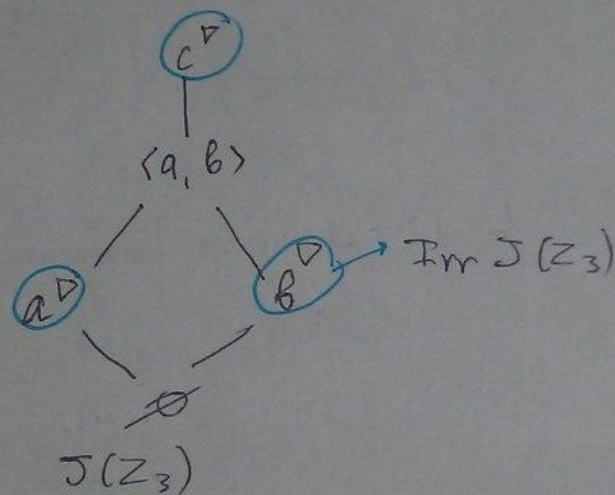
$\mathcal{I}(P)$ - мн-во всех порядковых идеалов ч.у. мн-ва P .

$$\text{Irr } \mathcal{I}(P) \cong P$$

Пример:



$\mathbb{Z}_3$



②⑩ Фундаментальная теорема о конечных дистрибутивных решётках

Теор. ФТКАР

✓ конечная дистрибутивная решётка L изоморфна решётке порядковых идеалов ч.у. мн-ва её неразложимых элем: $L \cong \mathcal{I}(\text{Irr } L)$