

ПРИКЛАДНАЯ АЛГЕБРА

Лекции для групп 320–328 (III-й поток)
5-й семестр








Лектор — *Гуров Сергей Исаевич*

ассистент — *Кропотов Дмитрий Александрович*

МГУ имени М.В. Ломоносова
Факультет Вычислительной математики и кибернетики
Кафедра Математических методов прогнозирования

комн. 530, 537, 682
e-mail: sgur@cs.msu.ru

Литература

-  *Воронин В.П.* Дополнительные главы дискретной математики. — М.: ф-т ВМК МГУ, 2002.
<http://padabum.com/d.php?id=10281>
-  *Гуров С.И.* Булевы алгебры, упорядоченные множества, решетки: Определения, свойства, примеры. — М.: Либроком, 2013.
-  *Журавлёв Ю.И., Флёров Ю.А., Вялый М.Н.* Дискретный анализ. Основы высшей алгебры. — М.: МЗ Пресс, 2007.
-  *Лидл Р., Нидеррайтер Г.* Конечные поля: В 2-х т. — М.: Мир, 1988.
-  *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. — М.: Связь, 1979.
-  *Нефедов В.Н., Осипова В.А.* Курс дискретной математики. — М.: Изд-во МАИ, 1992.
-  *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. — М.: Мир, 1976.

Тема 0

Группы, кольца, поля (напоминание)

Разделы

- 1 Группы
- 2 Кольца и поля
- 3 Задачи с решениями

Группы (покон Эваристу Галуа): определение и нотация

Определение

Группой \mathbf{G} называется пара $\langle G, * \rangle$, где G — непустое множество (*носитель*), а $*$ — бинарная операция на нём такая, что для любых $x, y, z \in G$ выполняются следующие *законы* или *аксиомы группы*:

G1: $(x * y) * z = x * (y * z)$ — *ассоциативность*;

G2: $\exists e \forall x : e * x = x * e = x$ — *существование единицы* (e);

G3: $\forall x \exists ! y : y * x = x * y = e$ — *существование обратного элемента* к x , символически $y = x^{-1}$.

G0: $x * y \in G$ — *устойчивость* (замкнутость) носителя.

Группы \mathbf{G} со свойством $\forall x, y \in G : x * y = y * x$ называются *коммутативными* или *абелевыми*.

Если $|\mathbf{G}| = n$, то \mathbf{G} — *конечная группа* и n — её *порядок*.

Группы: определение и нотация...

В конечной группе операцию $*$ удобно задавать *таблицей умножения* (таблицей Кэли).

Пример (Таблица умножения группы Клейна V_4)

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$$V_4 = \{e, a, b, c\}$$

— четверная группа Клейна

Часто c обозначают ab

(и $ab = ba$, т.к. группа V_4 абелева).

Мультипликативная запись групповой операции: $x \cdot y$ (или xy),

$a^0 = e$, $a^n = \underbrace{a \cdot \dots \cdot a}_{n \text{ раз}}$ и справедливы все обычные свойства

степени: $a^{m+n} = a^m \cdot a^n$, $a^{m^n} = a^{mn}$, $a^{-n} = (a^{-1})^n$, ...

Примеры групп

1. Числовые группы:

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ — абелевы группы относительно сложения. Для них используют аддитивную запись $x + y$, единичный элемент называют нулем (0), а обратный к x — противоположным ($-x$).
- Множества ненулевых элементов $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ — абелевы группы относительно умножения.

2. Бинарные наборы: элементы $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n) \in B^n$ относительно \oplus . Аддитивная запись:

$$\tilde{\alpha} \oplus \tilde{\beta} = (\alpha_1 \oplus \beta_1, \dots, \alpha_n \oplus \beta_n).$$

Нуль группы: $\tilde{0} = (0, \dots, 0)$.

Примеры групп: симметрическая группа S_n

3. Симметрическая группа S_n : все перестановки n -элементного множества $X = \{1, \dots, n\}$ относительно композиции \circ . Ясно, что $|S_n| = n!$.

Перестановки можно записывать в виде:

а) *таблицы* —

$$\pi = \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ t_1 & t_2 & \dots & t_i & \dots & t_n \end{pmatrix},$$

Пример (сначала выполняется 2-я перестановка, потом — 1-я):

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

— симметрическая группа **не абелева** при $n \geq 3$.

Примеры групп: симметрическая группа S_n ...

б) *разложения на циклы* —

$$\pi = (t_1^1 t_2^1 t_3^1 \dots t_{k_1}^1) (t_1^2 t_2^2 t_3^2 \dots t_{k_2}^2) \dots (t_1^c t_2^c t_3^c \dots t_{k_c}^c).$$

Внутри каждой пары скобок числа переставляются циклически: $\pi(t_1) = t_2, \pi(t_2) = t_3, \dots, \pi(t_k) = t_1$; в перестановке π — c циклов.

Циклы длины 1 (вида (t)) обычно опускают.

$$\left(\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{array} \right) \leftrightarrow (154)(26)$$

Пример (предыдущей композиции перестановок):

$$(123) \circ (23) = (12) \neq (13) = (23) \circ (123).$$

Примеры групп: группы симметрии объекта

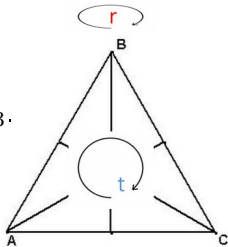
4. Группы симметрии объекта — *совокупность преобразований, совмещающих объект с самим собой.*

4.1. *Группа симметрии правильного n -угольника — группа диэдра D_n*

а) У группы D_{2k+1} , $k \in \mathbb{N}$ — две образующих: (1) **вращение** вокруг центра на $\frac{360^\circ}{2k+1}$ в выбранном направлении и (2) **симметрия** относительно оси, проходящей через выбранную вершину и середину противоположной стороны.

Пример: группа симметрии правильного треугольника $D_3 = \langle t, r \rangle = \{e, (ABC), (ACB), (A)(BC), (B)(AC), (C)(AB)\} = S_3$.

Любая перестановка вершин (сторон) описывается через образующие и имеет вид $t^m r^n$.



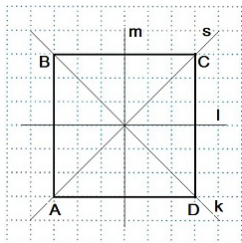
Примеры групп: группы симметрии объекта...

6) У группы D_{2k} , $k \in \mathbb{N}$ — три образующих: (1) вращение вокруг центра (в выбранном направлении) на $\frac{360^\circ}{2k}$ и две осевых симметрий — относительно фиксированных осей, проходящих через середины противоположных (2) сторон и (3) вершин.

Пример: группа симметрии квадрата

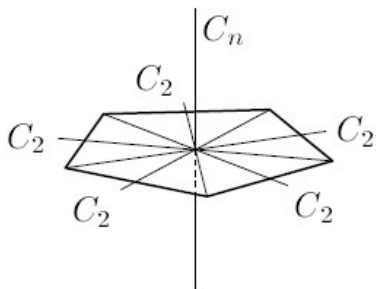
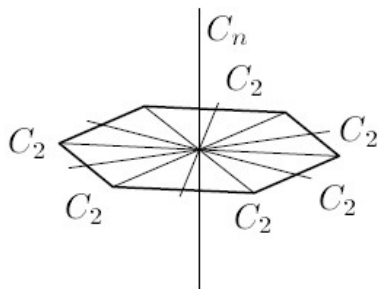
$$D_4 = \langle t, r, f \rangle = \{ e, (ABCD), (AC)(BD), (ADCB), (AD)(BC), (AB)(CD), (BD), (AC) \}.$$

Любая перестановка вершин (сторон) описывается через образующие и имеет вид $t^m r^n f^k$.



Примеры групп: группы симметрии объекта...

Пример: группы диэдра D_6 и D_5 .



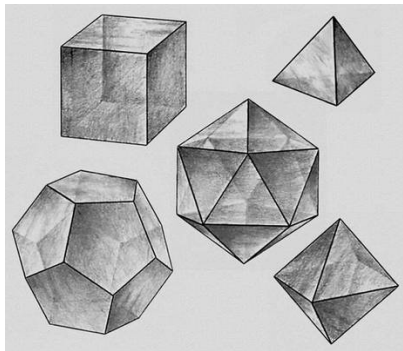
$|D_n| = 2n$: тождественная перестановка,
 $n - 1$ поворотов вокруг оси C_n и
 n отражений вокруг осей C_2 .

Примеры групп: группы симметрии объекта...

4.2. Группы вращений правильного многогранника.

Вращения — это не все симметрии многогранника, а **только повороты** (исключены зеркальные отражения).

Пять *платоновых тел* —



T — группа **тетраэдра**,

O — группа **октаэдра**
(вращение октаэдра и куба),

Y — группа **икосаэдра**
(вращение икосаэдра и додекаэдра).

Эти группы будут рассмотрены позже.

Примеры групп: вращений кубика Рубика

❶ Группа внутренних вращений кубика Рубика.

Порядок группы —

$$\begin{aligned} \frac{1}{2} \cdot 2^{11} \cdot 12! \cdot 3^7 \cdot 8! &= \\ &= 43252003274489856000 \approx \\ &\approx 4,3 \cdot 10^{19}. \end{aligned}$$



что является совсем небольшим числом по стандартам современной теории конечных групп (\approx объём Мирового океана в кубометрах).

❷ Группа внутренних вращений кубика Рубика $4 \times 4 \times 4$ (*месь Рубика*). Порядок группы —

$$\begin{aligned} \frac{3^7 \cdot 8! \cdot 24!^2}{24^7} &= \\ &= 74011968415649018698740939744985743360000000000 \approx 7,4 \cdot 10^{45}. \end{aligned}$$

Подгруппы и смежные классы

Если $\mathbf{G} = \langle G, * \rangle$ — группа, а H — подмножество G , устойчивое относительно групповой операции $*$, то $\mathbf{H} = \langle H, * \rangle$ — **подгруппа** G , символически $\mathbf{H} \leq \mathbf{G}$.

$$H \leq G, x \in G \Rightarrow xH = \{xh \mid h \in H\} \text{ и } Hx = \{hx \mid h \in H\}$$

— соответственно левый и правый **смежные классы по подгруппе H** (с представителем x).

Утверждение

Смежные классы с разными представителями либо не пересекаются, либо совпадают.

Если $\forall x \in G : xH = Hx$, то подгруппа H называется **нормальной**. Нормальность — ослабленное условие коммутативности: **в абелевой группе все подгруппы нормальны.**

Изоморфизм групп

Определение

Пусть $\mathbf{G} = \langle G, * \rangle$ и $\mathbf{G}' = \langle G', \circ \rangle$ — группы. Отображение $\varphi : G \rightarrow G'$ называется *изоморфизмом*, если оно

- 1 взаимно однозначно;
- 2 сохраняет операцию: $\forall a, b \in G: \varphi(a * b) = \varphi(a) \circ \varphi(b)$,

а такие группы — *изоморфными*, символически $\mathbf{G} \cong \mathbf{G}'$.

Свойства изоморфизма φ : $\varphi(e) = e'$ (сохранение единицы),
 $\varphi(a^{-1}) = \varphi(a)^{-1}$ (образ обратного элемента — обратный к его образу)...

Теорема (Кэли)

Любая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n .

Циклические группы

В *циклических группах* есть *порождающий элемент* (или *генератор*) — такой, что каждый элемент группы может быть получен многократным применением к нему групповой операции: C — циклическая группа, если

$$\exists c \forall x \exists k \left(c^k = x \right), \quad \langle c \rangle = C.$$

Для циклических групп возможны два случая.

1. Все степени порождающего элемента различны — тогда группа состоит из элементов: $\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots$, т.е. она изоморфна группе $\langle \mathbb{Z}, + \rangle$ целых чисел по сложению.

2. Две различные степени порождающего элемента совпадают: $a^{n+m} = a^n a^m = a^n \Rightarrow a^m = e$.

Пусть q — наименьшее натуральное m , для которого $a^m = e$. Тогда m — *порядок элемента a* , символически $\deg a$.

Циклические группы...

В рассматриваемом случае получаем:

- конечную группу;
- изоморфность любой конечной циклической группы с числом элементов n (*порядок группы*) группе

$$\mathbb{Z}_n = \langle \{0, 1, \dots, n-1\}, +_{\text{mod } n} \rangle.$$

Свойства циклических групп:

- Все циклические группы абелевы.
- Каждая подгруппа циклической группы — циклическая.
В применении к единственной бесконечной циклической группе \mathbb{Z} это даёт, что любая нетривиальная подгруппа H группы \mathbb{Z} имеет вид $H = \{mn \mid n \in \mathbb{Z}\} = m\mathbb{Z}$, где m — наименьшее положительное число из H .

Например: $H = \{\dots - 6, -3, 0, 3, 6, \dots\} = 3\mathbb{Z}$.

Генераторы конечной циклической группы

У циклической группы порядка n существует ровно $\varphi(n)$ порождающих элементов (генераторов).

Определение

$\varphi(n)$ (функция Эйлера) — количество чисел из интервала $[1, \dots, n - 1]$, взаимно простых с n

$\varphi(1) = 1$ (по определению), \dots , $\varphi(6) = |\{1, 5\}| = 2$, $\varphi(7) = 6, \dots$

Генераторы конечной циклической группы

У циклической группы порядка n существует ровно $\varphi(n)$ порождающих элементов (генераторов).

Определение

$\varphi(n)$ (функция Эйлера) — количество чисел из интервала $[1, \dots, n - 1]$, взаимно простых с n

$\varphi(1) = 1$ (по определению), \dots , $\varphi(6) = |\{1, 5\}| = 2$, $\varphi(7) = 6, \dots$

Свойства:

- $\varphi(n^m) = n^{m-1}\varphi(n)$, т.е. $\varphi(p^m) = p^{m-1}(p - 1)$,
 $\varphi(p) = p - 1$ (p — простое число).
- если m и n взаимно просты, то $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Примеры: $\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = (3 - 1)(5 - 1) = 8$,
 $\varphi(16) = \varphi(2^4) = 2^3 \cdot \varphi(2) = 8$.

Первые 99 значений $\varphi(\cdot)$

$\varphi(n)$	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Первые 99 значений $\varphi(\cdot)$

$\varphi(n)$	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Т.о. в группе $\mathbb{Z}_6 = \langle \{0, 1, 2, 3, 4, 5\}, +_6 \rangle$ $\varphi(6) = 2$ генератора. Например, $5 + 5 = 10 \equiv_6 4$, $4 + 5 = 9 \equiv_6 3$, ...

Первые 99 значений $\varphi(\cdot)$

$\varphi(n)$	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Т.о. в группе $\mathbb{Z}_6 = \langle \{0, 1, 2, 3, 4, 5\}, +_6 \rangle$ $\varphi(6) = 2$ генератора. Например, $5 + 5 = 10 \equiv_6 4$, $4 + 5 = 9 \equiv_6 3$,
Сколько генераторов в группе \mathbb{Z}_5 ?

Первые 99 значений $\varphi(\cdot)$

$\varphi(n)$	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Т.о. в группе $\mathbb{Z}_6 = \langle \{0, 1, 2, 3, 4, 5\}, +_6 \rangle$ $\varphi(6) = 2$ генератора. Например, $5 + 5 = 10 \equiv_6 4$, $4 + 5 = 9 \equiv_6 3$,
 Сколько генераторов в группе \mathbb{Z}_5 ? $\varphi(5) = 4$ — все, кроме 0.

Циклические группы: примеры

- $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ — единственная (с точностью до изоморфизма) бесконечная циклическая группа.
- $\mathbb{Z}_n \cong \langle \{0, 1, \dots, n-1\}, +_n \rangle = \langle 1 \rangle \cong \langle \{a^0 = 1, a, a^2, \dots, a^{n-1}\}, \cdot_n \rangle = \langle a \rangle$;
- Вращения в плоскости вокруг центра правильного n -угольника, совмещающие его с собой — группа $\langle \frac{2\pi}{n} \rangle$;
- Группа n -х корней из единицы (по умножению) — $\langle e^{i\frac{2\pi}{n}} \rangle$.
- Группа *афинных преобразований* $f_{a,b} : x \mapsto ax + b$, $a, b \in \mathbb{R}$, $a \neq 0$ вещественной прямой \mathbb{R} с законом умножения $f_{a,b} \cdot f_{c,d} = f_{ac, ad+b}$ (сначала $f_{c,d}$).
Содержит подгруппы «растяжений/сжатий» ($b = 0$) и «чистых сдвигов» ($a = 1$).

Теорема Лагранжа и следствия из неё

Теорема (Лагранжа)

$$H \leq G \Rightarrow |H| \mid |G|$$

(порядок подгруппы делит порядок группы)

Следствия

- 1 Порядок любого элемента есть делитель порядка группы.
- 2 Группа G простого порядка p :
 - циклическая и любой её отличный от единицы элемент — порождающий ($\varphi(p) = p - 1$);
 - не имеет нетривиальных подгрупп, т.е. $E \stackrel{\text{def}}{=} \{e\}$ и G — единственные подгруппы G .

Замечание: обращение теоремы Лагранжа **неверно** (будет пример 60-элементной группы, не имеющей 15-элементной подгруппы).

Порядок элемента конечной группы

Лемма (о порядке элемента конечной группы)

Пусть m — максимальный порядок элемента в конечной абелевой группе $\mathbf{G} = \langle G, \circ, e \rangle$.

Тогда порядок любого элемента $x \in G$ делит m .

Порядок элемента конечной группы

Лемма (о порядке элемента конечной группы)

Пусть m — максимальный порядок элемента в конечной абелевой группе $\mathbf{G} = \langle G, \circ, e \rangle$.

Тогда порядок любого элемента $x \in G$ делит m .

Доказательство

Группа G однозначно разлагается в объединение циклических групп, порядки которых являются степенями простых чисел.

Для каждого простого делителя p_i порядка группы найдем циклическую группу максимального порядка p^{k_i} .

Обозначим произведение чисел p^{k_i} через M . Для любого $x \in G$ выполняется $x^M = e$, т.е. порядок x делит M .

Но произведение всех выбранных циклических групп имеет порядок M . Поэтому $m = M$.

Примеры

① Группа $\langle \{0, 1, 2, 3, 4, 5\}, +_6 \rangle \cong \mathbb{Z}_6$ — циклическая 6-элементная; имеет подгруппы:

- $\{0\} = \langle 0 \rangle \cong E$ — единичная, $\deg 0 = 1$, $1 \mid 6$,
- $\{0, 2, 4\} = \langle 2 \rangle = \langle 4 \rangle \cong \mathbb{Z}_3$, $\deg 2 = \deg 4 = 3$, $3 \mid 6$,
- $\{0, 3\} = \langle 3 \rangle \cong \mathbb{Z}_2$, $\deg 3 = 2$, $2 \mid 6$,
- $\{0, 1, 2, 3, 4, 5\} = \langle 1 \rangle = \langle 5 \rangle \cong \mathbb{Z}_6$ — имеет $\varphi(6) = 2$ генератора, $\deg 1 = \deg 5 = 6$, $6 \mid 6$.

Примеры

❶ Группа $\langle \{0, 1, 2, 3, 4, 5\}, +_6 \rangle \cong \mathbb{Z}_6$ — циклическая 6-элементная; имеет подгруппы:

- $\{0\} = \langle 0 \rangle \cong E$ — единичная, $\deg 0 = 1$, $1 \mid 6$,
- $\{0, 2, 4\} = \langle 2 \rangle = \langle 4 \rangle \cong \mathbb{Z}_3$, $\deg 2 = \deg 4 = 3$, $3 \mid 6$,
- $\{0, 3\} = \langle 3 \rangle \cong \mathbb{Z}_2$, $\deg 3 = 2$, $2 \mid 6$,
- $\{0, 1, 2, 3, 4, 5\} = \langle 1 \rangle = \langle 5 \rangle \cong \mathbb{Z}_6$ — имеет $\varphi(6) = 2$ генератора, $\deg 1 = \deg 5 = 6$, $6 \mid 6$.

❷ Группа $\langle \{1, 2, 3, 4, 5\}, \cdot_5 \rangle \cong \mathbb{Z}_5$ — циклическая 5-элементная; имеет подгруппы

- $\{1\} = \langle 1 \rangle \cong E$ — единичная, $\deg 1 = 1$, $1 \mid 5$,
- $\{1, 2, 3, 4, 5\} = \langle 2 \rangle = \langle 3 \rangle = \dots = \langle 5 \rangle \cong \mathbb{Z}_5$ — имеет $\varphi(5) = 4$ генератора, $\deg 2 = \dots = \deg 5 = 5$, $5 \mid 5$.

Группы: разные факты

- Симметрическая группа S_n при $n > 1$ порождается транспозициями $(1, 2), (1, 3), \dots, (1, n)$.
- Если для всех элементов a группы G выполняется тождество $a * a = e$, то группа G коммутативна.
- Порядок $\text{deg } a$ элемента a n -элементной группы G есть наименьшее натуральное k такое, что $a^k = e$.
- Всякая циклическая группа является гомоморфным образом группы \mathbb{Z} .
- Ещё пример группы — *булева группа*: множество $\mathcal{P}(A)$ всех подмножеств непустого множества A с операцией симметрической разности множеств. Здесь нейтральный элемент — \emptyset , а порядок каждого элемента — 2.

Разделы

- 1 Группы
- 2 Кольца и поля**
- 3 Задачи с решениями

Кольца: определение

Определение

Кольцом \mathbf{R} называется тройка $\langle R, +, \cdot \rangle$, где R — непустое множество (носитель), а $+$ (сложение) и \cdot (умножение) — бинарные операции на нём такие, что для любых $x, y, z \in R$ выполняются следующие *законы* или *аксиомы кольца*:

R1: относительно сложения \mathbf{R} — коммутативная группа (*аддитивная группа кольца*);

[R2: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ — *ассоциативность умножения*];

R3: $x \cdot (y + z) = x \cdot y + x \cdot z$ и $(y + z) \cdot x = y \cdot x + z \cdot x$ — *дистрибутивность слева и справа умножения относительно сложения*.

Если в R имеется единичный элемент для умножения 1 , то кольцо называется *кольцом с единицей* (*унитальным*).

Если $x \cdot y = y \cdot x$, то кольцо называется *коммутативным*.

Кольца: основные свойства, примеры

- Пример кольца без единицы — кольцо чётных чисел $2\mathbb{Z}$.
- Элемент a унитарного кольца называется *обратимым*, если существует элемент b такой, что $a \cdot b = b \cdot a = 1$.
- Если $\forall r_1, r_2 : (r_1 \cdot r_2 = 0) \Rightarrow (r_1 = 0) \vee (r_2 = 0)$ — то это кольцо *без делителей нуля*.

Унитарное ассоциативно-коммутативное кольцо без делителей нуля — *целостное кольцо*.

Примеры колец:

1. *Классический пример* — множество целых чисел \mathbb{Z} с операциями сложения и умножения (целостное кольцо). Обратимые элементы — только ± 1 .

2. $\mathbb{Z}_n \stackrel{\text{def}}{=} \langle \{0, 1, \dots, n-1\}, +_{\text{mod } n}, \cdot_{\text{mod } n} \rangle$ — *кольцо классов вычетов по модулю n (вычет = остаток)*.

3. *Кольца многочленов* — будет рассматриваться далее.

Кольца: изоморфизмы, гомоморфизмы, подкольца

Определение

Пусть $\mathbf{R} = \langle R, +, \cdot \rangle$ и $\mathbf{R}' = \langle R', \oplus, \otimes \rangle$ — кольца.

Отображение $\varphi : R \rightarrow R'$ называется *гомоморфизмом*, если оно сохраняет обе операции: $\forall r_1, r_2 \in R$ справедливо

$$\varphi(r_1 + r_2) = \varphi(r_1) \oplus \varphi(r_2), \quad \varphi(r_1 \cdot r_2) = \varphi(r_1) \otimes \varphi(r_2).$$

Взаимно однозначный гомоморфизм колец есть *изоморфизм*, символически $R \cong R'$.

Утверждение

Гомоморфная область кольца есть кольцо.

Подмножество $S \subseteq R$ кольца $\langle R, +, \cdot \rangle$, устойчивое относительно операций $+$ и \cdot называется *подкольцом*.

Идеалы колец

Определение

Подкольцо I коммутативного кольца \mathbf{R} называется его *идеалом* (символически $I \triangleleft \mathbf{R}$), если

$$\forall x \in I \forall r \in R : (ax \in I) \ \& \ (xa \in I).$$

Определение

Идеал I унитарного коммутативного кольца \mathbf{R} называется *главным*, если найдётся элемент $a \in R$ такой, что

$$I = \{ar \mid r \in R\},$$

символически $I = (a)$.

Пример: $(n) = n\mathbb{Z} \triangleleft \mathbb{Z}$ (ну, например, $5\mathbb{Z}$ — идеал в \mathbb{Z}).

Целостные кольца, в которых все идеалы (отличные от самого кольца) главные называются *кольцами главных идеалов* (*КГИ*).

Идеалы колец: свойства I

- Само кольцо \mathbf{R} и его нуль — идеалы \mathbf{R} , они называются *собственными*, остальные идеалы — *несобственными*.
- В кольце \mathbb{Z} целых чисел все идеалы главные и имеют вид $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$, где $n \in \mathbb{N}_0$.
- Бинарное отношение \triangleleft на множестве идеалов кольца рефлексивно, транзитивно и антисимметрично, т.е. является порядком.
- Если \mathbf{R} — произвольное кольцо, и $n \in \mathbb{Z}$, то
$$nR = \{na \mid a \in R\} \triangleleft \mathbf{R}.$$
- Если \mathbf{R} — коммутативное кольцо, и $a_1, \dots, a_n \in R$, то
$$(a_1, \dots, a_n) = \{x_1a_1 + \dots + x_na_n \mid x_1, \dots, x_n \in R\} \triangleleft \mathbf{R}$$
 — идеал, порождённый элементами a_1, \dots, a_n .

Идеалы колец: свойства II

- Если $I_1, I_2 \triangleleft \mathbf{R}$, то
 - пересечение идеалов $I_1 \cap I_2$,
 - сумма идеалов $I_1 + I_2 \stackrel{\text{def}}{=} \{x + y \mid x \in I_1, y \in I_2\}$,
 - произведение идеалов $I_1 \cdot I_2 \stackrel{\text{def}}{=} \{x_1 \cdot y_1 + \dots + x_n \cdot y_n \mid x_i \in I_1, y_i \in I_2, i = \overline{1, n}\}$,
 - идеалы \mathbf{R} .

Фактор-кольца

Классом вычетов по модулю идеала I кольца $\langle R, +, \cdot \rangle$ называется смежный класс по нормальной подгруппе $\langle I, + \rangle$ аддитивной группы кольца с некоторым представителем r :

$$\{r + x \mid r \in R, x \in I\},$$

символически $[r]_I$.

Множество классов вычетов — кольцо (вместо операндов можно брать любые элементы соответствующих классов), оно называется *фактор-кольцом кольца R по модулю идеала I* , символически R/I .

Пример: $I = 2\mathbb{Z} \triangleleft \mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} = \{[0]_I, [1]_I\}$.

Определение

Идеал I называется *максимальным* в кольце R , если не существует такого идеала I' , что $I \subset I' \subset R$.

Факториальные кольца

Определение

Целостное кольцо, в котором каждый ненулевой элемент x либо обратим, либо однозначно с точностью до перестановки сомножителей и умножения на обратимый элемент представляется в виде произведения неприводимых элементов $x = p_1 \cdot \dots \cdot p_n$, $n \geq 1$, называется **факториальным**.

- \mathbb{Z} — факториальное кольцо.
- Кольца главных идеалов факториальны.
- Кольцо $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ является факториальным (и, следовательно, областью целостности), если и только если n — простое число.

Евклидовы кольца

Определение

Кольцо $\mathbf{R} = \langle R, +, \cdot \rangle$ называется *евклидовым*, если для него выполнены следующие свойства:

E1: \mathbf{R} — целостное кольцо;

E2: для каждого ненулевого элемента $r \in R$ определена его норма $N(r) \in \mathbb{N}_0$;

E3: для любых элементов a и $b \neq 0$ кольца \mathbf{R} существуют такие элементы q и r , что

$$a = q \cdot b + r \text{ и либо } r = 0, \text{ либо } N(r) < N(b).$$

(возможность деления с остатком).

E4: норма произведения двух ненулевых сомножителей больше либо равна норме любого из сомножителей: $a, b \in R$, $a \neq 0$, $b \neq 0$ выполнено $\max \{ N(a), N(b) \} \leq N(a \cdot b)$.

Евклидовы кольца: свойства

- Возможность деления с остатком (E3) — основное свойство нормы.
- Евклидово кольцо унитарно.
- Кольцо \mathbb{Z} целых чисел евклидово (классический пример евклидова кольца).
Здесь норма — модуль числа.
- Евклидовы кольца — кольца главных идеалов (обратное, вообще говоря, неверно).
- Кольцо многочленов $k[x]$ над полем k — евклидово.
Норма — степень многочлена.

Поле: определение

Определение

Поле \mathbf{K} называется тройка $\langle K, +, \cdot \rangle$, где K — непустое множество (носитель), а $+$ (сложение) и \cdot (умножение) — бинарные операции на нём такие, что выполняются следующие *законы* или *аксиомы поля*:

K1: относительно сложения \mathbf{K} — абелева группа;

K2: относительно умножения $\mathbf{K} \setminus \{0\}$ — абелева группа (*мультипликативная группа поля*);

K3: $x \cdot (y + z) = x \cdot y + x \cdot z$ для любых $x, y, z \in K$ — *дистрибутивность умножения относительно сложения*.

Т.о. поле — кольцо, ненулевые элементы которого образуют группу относительно умножения.

Примеры бесконечных полей: числовые поля $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Группы, кольца, поля общего вида: резюме I

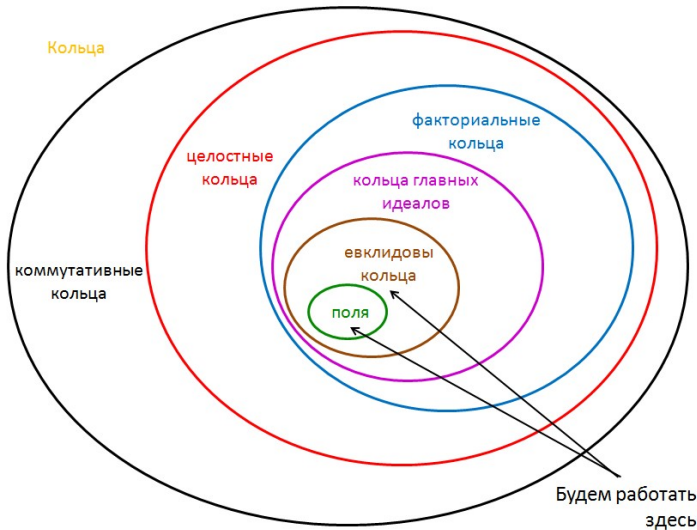
- Неформально: группа — множество с единицей, обратными элементами и устойчивое относительно ассоциативной операции.
- Неформально: кольцо — множество, устойчивое относительно сложения, вычитания и умножения с естественными аксиомами. Унитарное кольцо — с единицей по умножению.
- Унитарное ассоциативно-коммутативное (по умножению) кольцо без делителей нуля — целостное кольцо.
- Кольцо классов вычетов R/I коммутативного кольца с единицей есть поле тогда и только тогда, когда I — максимальный идеал.

Группы, кольца, поля общего вида: резюме II

- В евклидовом кольце простой элемент p порождает максимальный идеал (p) .
- Все обратимые элементы кольца с единицей образуют группу относительно умножения.
- Любая конечное целостное кольцо является полем.
- Поле, не обладающее никаким собственным подполем, называется *простым*.

В каждом поле содержится только одно простое подполе, которое изморфно либо \mathbb{Q} , либо \mathbb{Z}_p , p — простое.

От колец к полям



Разделы

- 1 Группы
- 2 Кольца и поля
- 3 Задачи с решениями**

Задача ГКП-1

Выяснить, образуют ли группы следующие множества при указанной операции над элементами:

- 1 целые числа относительно сложения?

Задача ГКП-1

Выяснить, образуют ли группы следующие множества при указанной операции над элементами:

- ① целые числа относительно сложения? Да

Задача ГКП-1

Выяснить, образуют ли группы следующие множества при указанной операции над элементами:

- 1 целые числа относительно сложения? Да
- 2 четные числа относительно сложения?

Задача ГКП-1

Выяснить, образуют ли группы следующие множества при указанной операции над элементами:

- ① целые числа относительно сложения? Да
- ② четные числа относительно сложения? Да

Задача ГКП-1

Выяснить, образуют ли группы следующие множества при указанной операции над элементами:

- 1 целые числа относительно сложения? Да
- 2 четные числа относительно сложения? Да
- 3 целые числа, кратные данному натуральному числу n , относительно сложения?

Задача ГКП-1

Выяснить, образуют ли группы следующие множества при указанной операции над элементами:

- 1 целые числа относительно сложения? Да
- 2 четные числа относительно сложения? Да
- 3 целые числа, кратные данному натуральному числу n , относительно сложения? Да

Задача ГКП-1

Выяснить, образуют ли группы следующие множества при указанной операции над элементами:

- 1 целые числа относительно сложения? Да
- 2 четные числа относительно сложения? Да
- 3 целые числа, кратные данному натуральному числу n , относительно сложения? Да
- 4 степени данного действительного числа a , $a \neq 0, \pm 1$, с целыми показателями относительно умножения?

Задача ГКП-1

Выяснить, образуют ли группы следующие множества при указанной операции над элементами:

- 1 целые числа относительно сложения? Да
- 2 четные числа относительно сложения? Да
- 3 целые числа, кратные данному натуральному числу n , относительно сложения? Да
- 4 степени данного действительного числа a , $a \neq 0, \pm 1$, с целыми показателями относительно умножения? Да

Задача ГКП-1

Выяснить, образуют ли группы следующие множества при указанной операции над элементами:

- 1 целые числа относительно сложения? Да
- 2 четные числа относительно сложения? Да
- 3 целые числа, кратные данному натуральному числу n , относительно сложения? Да
- 4 степени данного действительного числа a , $a \neq 0, \pm 1$, с целыми показателями относительно умножения? Да
- 5 неотрицательные целые числа относительно сложения?

Задача ГКП-1

Выяснить, образуют ли группы следующие множества при указанной операции над элементами:

- 1 целые числа относительно сложения? Да
- 2 четные числа относительно сложения? Да
- 3 целые числа, кратные данному натуральному числу n , относительно сложения? Да
- 4 степени данного действительного числа a , $a \neq 0, \pm 1$, с целыми показателями относительно умножения? Да
- 5 неотрицательные целые числа относительно сложения? Нет (единицы, противоположного элемента)

Задача ГКП-1

Выяснить, образуют ли группы следующие множества при указанной операции над элементами:

- 1 целые числа относительно сложения? Да
- 2 четные числа относительно сложения? Да
- 3 целые числа, кратные данному натуральному числу n , относительно сложения? Да
- 4 степени данного действительного числа a , $a \neq 0, \pm 1$, с целыми показателями относительно умножения? Да
- 5 неотрицательные целые числа относительно сложения?
Нет (единицы, противоположного элемента)
- 6 нечетные целые числа относительно сложения?

Задача ГКП-1

Выяснить, образуют ли группы следующие множества при указанной операции над элементами:

- 1 целые числа относительно сложения? Да
- 2 четные числа относительно сложения? Да
- 3 целые числа, кратные данному натуральному числу n , относительно сложения? Да
- 4 степени данного действительного числа a , $a \neq 0, \pm 1$, с целыми показателями относительно умножения? Да
- 5 неотрицательные целые числа относительно сложения?
Нет (единицы, противоположного элемента)
- 6 нечетные целые числа относительно сложения?
Нет (устойчивости)

Задача ГКП-1...

- 7 целые числа относительно вычитания?

Задача ГКП-1...

7 целые числа относительно вычитания?

Нет (ассоциативности)

Задача ГКП-1...

- 7 целые числа относительно вычитания?
Нет (ассоциативности)
- 8 рациональные числа относительно сложения?

Задача ГКП-1...

- 7 целые числа относительно вычитания?
Нет (ассоциативности)
- 8 рациональные числа относительно сложения? Да

Задача ГКП-1...

- 7 целые числа относительно вычитания?
Нет (ассоциативности)
- 8 рациональные числа относительно сложения? Да
- 9 рациональные числа относительно умножения?

Задача ГКП-1...

- 7 целые числа относительно вычитания?
Нет (ассоциативности)
- 8 рациональные числа относительно сложения? Да
- 9 рациональные числа относительно умножения?
Нет (обратного у 0)

Задача ГКП-1...

- 7 целые числа относительно вычитания?
Нет (ассоциативности)
- 8 рациональные числа относительно сложения? Да
- 9 рациональные числа относительно умножения?
Нет (обратного у 0)
- 10 рациональные числа, отличные от нуля, относительно умножения?

Задача ГКП-1...

- 7 целые числа относительно вычитания?
Нет (ассоциативности)
- 8 рациональные числа относительно сложения? Да
- 9 рациональные числа относительно умножения?
Нет (обратного у 0)
- 10 рациональные числа, отличные от нуля, относительно умножения? Да

Задача ГКП-1...

- 7 целые числа относительно вычитания?
Нет (ассоциативности)
- 8 рациональные числа относительно сложения? Да
- 9 рациональные числа относительно умножения?
Нет (обратного у 0)
- 10 рациональные числа, отличные от нуля, относительно умножения? Да
- 11 положительные рациональные числа относительно умножения?

Задача ГКП-1...

- 7 целые числа относительно вычитания?
Нет (ассоциативности)
- 8 рациональные числа относительно сложения? Да
- 9 рациональные числа относительно умножения?
Нет (обратного у 0)
- 10 рациональные числа, отличные от нуля, относительно умножения? Да
- 11 положительные рациональные числа относительно умножения? Да

Задача ГКП-1...

- 7 целые числа относительно вычитания?
Нет (ассоциативности)
- 8 рациональные числа относительно сложения? Да
- 9 рациональные числа относительно умножения?
Нет (обратного у 0)
- 10 рациональные числа, отличные от нуля, относительно умножения? Да
- 11 положительные рациональные числа относительно умножения? Да
- 12 положительные рациональные числа относительно деления?

Задача ГКП-1...

- 7 целые числа относительно вычитания?
Нет (ассоциативности)
- 8 рациональные числа относительно сложения? Да
- 9 рациональные числа относительно умножения?
Нет (обратного у 0)
- 10 рациональные числа, отличные от нуля, относительно умножения? Да
- 11 положительные рациональные числа относительно умножения? Да
- 12 положительные рациональные числа относительно деления? Нет (ассоциативности)

Задача ГКП-1...

- 7 целые числа относительно вычитания?
Нет (ассоциативности)
- 8 рациональные числа относительно сложения? Да
- 9 рациональные числа относительно умножения?
Нет (обратного у 0)
- 10 рациональные числа, отличные от нуля, относительно умножения? Да
- 11 положительные рациональные числа относительно умножения? Да
- 12 положительные рациональные числа относительно деления? Нет (ассоциативности)

Задача ГКП-1...

- 13 корни n -й степени из единицы (как действительные, так и комплексные) относительно умножения?

Задача ГКП-1...

- 13 корни n -й степени из единицы (как действительные, так и комплексные) относительно умножения? Да

Задача ГКП-1...

- 13 корни n -й степени из единицы (как действительные, так и комплексные) относительно умножения? Да
- 14 матрицы порядка n с действительными элементами относительно умножения?

Задача ГКП-1...

- 13 корни n -й степени из единицы (как действительные, так и комплексные) относительно умножения? **Да**
- 14 матрицы порядка n с действительными элементами относительно умножения? **Нет** (обратных — у всех)

Задача ГКП-1...

- 13 корни n -й степени из единицы (как действительные, так и комплексные) относительно умножения? **Да**
- 14 матрицы порядка n с действительными элементами относительно умножения? **Нет** (обратных — у всех)
- 15 невырожденные матрицы порядка n с действительными элементами относительно умножения?

Задача ГКП-1...

- 13 корни n -й степени из единицы (как действительные, так и комплексные) относительно умножения? Да
- 14 матрицы порядка n с действительными элементами относительно умножения? Нет (обратных — у всех)
- 15 невырожденные матрицы порядка n с действительными элементами относительно умножения? Да

Задача ГКП-1...

- 13 корни n -й степени из единицы (как действительные, так и комплексные) относительно умножения? Да
- 14 матрицы порядка n с действительными элементами относительно умножения? Нет (обратных — у всех)
- 15 невырожденные матрицы порядка n с действительными элементами относительно умножения? Да
- 16 матрицы порядка n с целыми элементами и определителем, равным 1 относительно умножения?

Задача ГКП-1...

- 13 корни n -й степени из единицы (как действительные, так и комплексные) относительно умножения? Да
- 14 матрицы порядка n с действительными элементами относительно умножения? Нет (обратных — у всех)
- 15 невырожденные матрицы порядка n с действительными элементами относительно умножения? Да
- 16 матрицы порядка n с целыми элементами и определителем, равным 1 относительно умножения? Да

Задача ГКП-1...

- 13 корни n -й степени из единицы (как действительные, так и комплексные) относительно умножения? Да
- 14 матрицы порядка n с действительными элементами относительно умножения? Нет (обратных — у всех)
- 15 невырожденные матрицы порядка n с действительными элементами относительно умножения? Да
- 16 матрицы порядка n с целыми элементами и определителем, равным 1 относительно умножения? Да
- 17 матрицы порядка n с целыми элементами и определителем, равным ± 1 относительно умножения?

Задача ГКП-1...

- 13 корни n -й степени из единицы (как действительные, так и комплексные) относительно умножения? Да
- 14 матрицы порядка n с действительными элементами относительно умножения? Нет (обратных — у всех)
- 15 невырожденные матрицы порядка n с действительными элементами относительно умножения? Да
- 16 матрицы порядка n с целыми элементами и определителем, равным 1 относительно умножения? Да
- 17 матрицы порядка n с целыми элементами и определителем, равным ± 1 относительно умножения? Да

Задача ГКП-1...

- 13 корни n -й степени из единицы (как действительные, так и комплексные) относительно умножения? Да
- 14 матрицы порядка n с действительными элементами относительно умножения? Нет (обратных — у всех)
- 15 невырожденные матрицы порядка n с действительными элементами относительно умножения? Да
- 16 матрицы порядка n с целыми элементами и определителем, равным 1 относительно умножения? Да
- 17 матрицы порядка n с целыми элементами и определителем, равным ± 1 относительно умножения? Да
- 18 матрицы порядка n с действительными элементами относительно сложения?

Задача ГКП-1...

- 13 корни n -й степени из единицы (как действительные, так и комплексные) относительно умножения? Да
- 14 матрицы порядка n с действительными элементами относительно умножения? Нет (обратных — у всех)
- 15 невырожденные матрицы порядка n с действительными элементами относительно умножения? Да
- 16 матрицы порядка n с целыми элементами и определителем, равным 1 относительно умножения? Да
- 17 матрицы порядка n с целыми элементами и определителем, равным ± 1 относительно умножения? Да
- 18 матрицы порядка n с действительными элементами относительно сложения? Да

Задача ГКП-1...

- 13 корни n -й степени из единицы (как действительные, так и комплексные) относительно умножения? Да
- 14 матрицы порядка n с действительными элементами относительно умножения? Нет (обратных — у всех)
- 15 невырожденные матрицы порядка n с действительными элементами относительно умножения? Да
- 16 матрицы порядка n с целыми элементами и определителем, равным 1 относительно умножения? Да
- 17 матрицы порядка n с целыми элементами и определителем, равным ± 1 относительно умножения? Да
- 18 матрицы порядка n с действительными элементами относительно сложения? Да

Задача ГКП-1...

- 19 перестановки чисел $1, 2, \dots, n$ относительно композиции перестановок?

Задача ГКП-1...

- 19 перестановки чисел $1, 2, \dots, n$ относительно композиции перестановок? Да

Задача ГКП-1...

- 19 перестановки чисел $1, 2, \dots, n$ относительно композиции перестановок? Да
- 20 взаимно однозначные отображения множества натуральных чисел на себя, каждое из которых перемещает (отображает не в себя) лишь конечное число чисел, если за произведение отображений s и t принята композиция $s \circ t$ отображений (последовательное выполнение отображений t , затем s)?

Задача ГКП-1...

- 19 перестановки чисел $1, 2, \dots, n$ относительно композиции перестановок? Да
- 20 взаимно однозначные отображения множества натуральных чисел на себя, каждое из которых перемещает (отображает не в себя) лишь конечное число чисел, если за произведение отображений s и t принята композиция $s \circ t$ отображений (последовательное выполнение отображений t , затем s)? Да

Задача ГКП-1...

- 19 перестановки чисел $1, 2, \dots, n$ относительно композиции перестановок? Да
- 20 взаимно однозначные отображения множества натуральных чисел на себя, каждое из которых перемещает (отображает не в себя) лишь конечное число чисел, если за произведение отображений s и t принята композиция $s \circ t$ отображений (последовательное выполнение отображений t , затем s)? Да
- 21 преобразования множества M , т.е. взаимно однозначные отображения этого множества на себя, относительно композиции отображений?

Задача ГКП-1...

- 19 перестановки чисел $1, 2, \dots, n$ относительно композиции перестановок? Да
- 20 взаимно однозначные отображения множества натуральных чисел на себя, каждое из которых перемещает (отображает не в себя) лишь конечное число чисел, если за произведение отображений s и t принята композиция $s \circ t$ отображений (последовательное выполнение отображений t , затем s)? Да
- 21 преобразования множества M , т.е. взаимно однозначные отображения этого множества на себя, относительно композиции отображений? Да

Задача ГКП-1...

- 19 перестановки чисел $1, 2, \dots, n$ относительно композиции перестановок? Да
- 20 взаимно однозначные отображения множества натуральных чисел на себя, каждое из которых перемещает (отображает не в себя) лишь конечное число чисел, если за произведение отображений s и t принята композиция $s \circ t$ отображений (последовательное выполнение отображений t , затем s)? Да
- 21 преобразования множества M , т.е. взаимно однозначные отображения этого множества на себя, относительно композиции отображений? Да
- 22 элементы n -мерного векторного пространства \mathbb{R}^n относительно сложения?

Задача ГКП-1...

- 19 перестановки чисел $1, 2, \dots, n$ относительно композиции перестановок? Да
- 20 взаимно однозначные отображения множества натуральных чисел на себя, каждое из которых перемещает (отображает не в себя) лишь конечное число чисел, если за произведение отображений s и t принята композиция $s \circ t$ отображений (последовательное выполнение отображений t , затем s)? Да
- 21 преобразования множества M , т.е. взаимно однозначные отображения этого множества на себя, относительно композиции отображений? Да
- 22 элементы n -мерного векторного пространства \mathbb{R}^n относительно сложения? Да

Задача ГКП-1...

- 19 перестановки чисел $1, 2, \dots, n$ относительно композиции перестановок? Да
- 20 взаимно однозначные отображения множества натуральных чисел на себя, каждое из которых перемещает (отображает не в себя) лишь конечное число чисел, если за произведение отображений s и t принята композиция $s \circ t$ отображений (последовательное выполнение отображений t , затем s)? Да
- 21 преобразования множества M , т.е. взаимно однозначные отображения этого множества на себя, относительно композиции отображений? Да
- 22 элементы n -мерного векторного пространства \mathbb{R}^n относительно сложения? Да

Задача ГКП-1...

- 28 параллельные переносы трехмерного пространства \mathbb{R}^3 относительно композиции движений?

Задача ГКП-1...

- 28 параллельные переносы трехмерного пространства \mathbb{R}^3 относительно композиции движений? Да

Задача ГКП-1...

- 28 параллельные переносы трехмерного пространства \mathbb{R}^3 относительно композиции движений? Да
- 29 повороты трехмерного пространства \mathbb{R}^n вокруг прямых, проходящих через данную точку O относительно композиции движений?

Задача ГКП-1...

- 28 параллельные переносы трехмерного пространства \mathbb{R}^3 относительно композиции движений? Да
- 29 повороты трехмерного пространства \mathbb{R}^n вокруг прямых, проходящих через данную точку O относительно композиции движений? Да

Задача ГКП-1...

- 28 параллельные переносы трехмерного пространства \mathbb{R}^3 относительно композиции движений? Да
- 29 повороты трехмерного пространства \mathbb{R}^n вокруг прямых, проходящих через данную точку O относительно композиции движений? Да
- 30 все движения трехмерного пространства \mathbb{R}^n относительно композиции движений?

Задача ГКП-1...

- 28 параллельные переносы трехмерного пространства \mathbb{R}^3 относительно композиции движений? Да
- 29 повороты трехмерного пространства \mathbb{R}^n вокруг прямых, проходящих через данную точку O относительно композиции движений? Да
- 30 все движения трехмерного пространства \mathbb{R}^n относительно композиции движений? Да

Задача ГКП-1...

- 28 параллельные переносы трехмерного пространства \mathbb{R}^3 относительно композиции движений? Да
- 29 повороты трехмерного пространства \mathbb{R}^n вокруг прямых, проходящих через данную точку O относительно композиции движений? Да
- 30 все движения трехмерного пространства \mathbb{R}^n относительно композиции движений? Да
- 31 действительные многочлены степени не выше n от неизвестного x и нулевой многочлен относительно сложения?

Задача ГКП-1...

- 28 параллельные переносы трехмерного пространства \mathbb{R}^3 относительно композиции движений? Да
- 29 повороты трехмерного пространства \mathbb{R}^n вокруг прямых, проходящих через данную точку O относительно композиции движений? Да
- 30 все движения трехмерного пространства \mathbb{R}^n относительно композиции движений? Да
- 31 действительные многочлены степени не выше n от неизвестного x и нулевой многочлен относительно сложения? Да

Задача ГКП-1...

- 28 параллельные переносы трехмерного пространства \mathbb{R}^3 относительно композиции движений? Да
- 29 повороты трехмерного пространства \mathbb{R}^n вокруг прямых, проходящих через данную точку O относительно композиции движений? Да
- 30 все движения трехмерного пространства \mathbb{R}^n относительно композиции движений? Да
- 31 действительные многочлены степени не выше n от неизвестного x и нулевой многочлен относительно сложения? Да
- 32 действительные многочлены любых степеней (включая 0) от переменной x относительно сложения?

Задача ГКП-1...

- 28 параллельные переносы трехмерного пространства \mathbb{R}^3 относительно композиции движений? Да
- 29 повороты трехмерного пространства \mathbb{R}^n вокруг прямых, проходящих через данную точку O относительно композиции движений? Да
- 30 все движения трехмерного пространства \mathbb{R}^n относительно композиции движений? Да
- 31 действительные многочлены степени не выше n от неизвестного x и нулевой многочлен относительно сложения? Да
- 32 действительные многочлены любых степеней (включая 0) от переменной x относительно сложения? Да

Задача ГКП-1...

- 28 параллельные переносы трехмерного пространства \mathbb{R}^3 относительно композиции движений? Да
- 29 повороты трехмерного пространства \mathbb{R}^n вокруг прямых, проходящих через данную точку O относительно композиции движений? Да
- 30 все движения трехмерного пространства \mathbb{R}^n относительно композиции движений? Да
- 31 действительные многочлены степени не выше n от неизвестного x и нулевой многочлен относительно сложения? Да
- 32 действительные многочлены любых степеней (включая 0) от переменной x относительно сложения? Да

Задача ГКП-2

В циклической группе $\langle a \rangle$ порядка n найти все генераторы и элементы g порядка k , удовлетворяющие условию $g^k = e$ при

- 1. $n = 24, k = 6,$*
- 2. $n = 100, k = 20,$*
- 3. $n = 100, k = 5$*

Задача ГКП-2

В циклической группе $\langle a \rangle$ порядка n найти все генераторы и элементы g порядка k , удовлетворяющие условию $g^k = e$ при

1. $n = 24, k = 6$, 2. $n = 100, k = 20$, 3. $n = 100, k = 5$

Решение. Порядок любого элемента делит порядок группы.

Элемент $g = a^m$ циклической группы

$C(n) = \{a^0 = 1, a^1, a^2, \dots, a^{n-1}\}$ будет удовлетворять условию $g^k = e = 1$, если $m = \frac{n}{k} \cdot l$, $l = 1, \dots, k - 1$. При $l = 5$ получаем тривиальное решение $m = 0, g = 1$.

$g = a^m$ — генератор $C(n)$, если m взаимно просто с n .

① $n = 24, k = 6$

Группа имеет $\varphi(24) = \varphi(2^3 \cdot 3) = 2^2 \varphi(2) \cdot \varphi(3) = 8$

генераторов: a^m — генератор, если

$m = 1, 5, 7, 11, 13, 17, 19, 23$.

$a^m = g, g^6 = e$, если $m = \frac{24}{6} \cdot l, l = 1, \dots, 5$,

$m = 4, 8, 12, 16, 20$.

Задача ГКП-2...

$$\textcircled{2} \quad \underline{n = 100, k = 20}$$

Группа имеет

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = 2^1 \cdot \varphi(2) \cdot 5^1 \cdot \varphi(5) = 2 \cdot 1 \cdot 5 \cdot 4 = 40$$

генераторов: a^m — генератор, если

$$m = 1, 3, 7, 9, 11, 13, \dots, 99.$$

$$a^m = g, g^{20} = e, \text{ если } m = \frac{100}{20} \cdot l, l = 1, \dots, 19:$$

$$m = 0, 5, 10, 15, 20, \dots, 5 \cdot 19 = 95.$$

$$\textcircled{3} \quad \underline{n = 100, k = 5}$$

Группа — та же, что и в предыдущей задаче, и генераторы — те же.

$$a^m = g, g^5 = e, \text{ если } m = \frac{100}{5} \cdot l, l = 1, \dots, 4:$$

$$m = 0, 20, 40, 60, 80.$$

Задача ГКП-3

Показать, что

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right),$$

если $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ — примарное разложение n .

Задача ГКП-3

Показать, что

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right),$$

если $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ — примарное разложение n .

Решение

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1}) \cdot \dots \cdot \varphi(p_k^{\alpha_k}) = p_1^{\alpha_1-1} \varphi(p_1) \cdot \dots \cdot p_k^{\alpha_k-1} \varphi(p_k) = \\ &= \frac{n}{p_1 \cdot \dots \cdot p_k} (p_1-1) \cdot \dots \cdot (p_k-1) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

Задача ГКП-4

Найти все подгруппы циклической группы порядка 24.

Задача ГКП-4

Найти все подгруппы циклической группы порядка 24.

Решение. Циклическая 24-элементная группа $C = \{a^0 = 1, a^1, a^2, \dots, a^{23}\}$ имеет (циклические) подгруппы, генераторами которых будут элементы a^m , где $m \mid n$, т.е. $m = 1, 2, 3, 4, 6, 8, 12, 22$.

Порядок соответствующей подгруппы — n/m .

$$m = 1 : \{1, a^1, a^2, \dots, a^{24}\} = \langle a^1 \rangle = C \cong \mathbb{Z}_{24};$$

$$m = 2 : \{1, a^2, a^4, a^6, \dots, a^{22}\} = \langle a^2 \rangle \cong \mathbb{Z}_{12};$$

$$m = 3 : \{1, a^3, a^6, a^9, \dots, a^{21}\} = \langle a^3 \rangle \cong \mathbb{Z}_8;$$

$$m = 4 : \{1, a^4, a^8, a^{12}, \dots, a^{20}\} = \langle a^4 \rangle \cong \mathbb{Z}_6;$$

$$m = 6 : \{1, a^6, a^{12}, a^{18}\} = \langle a^6 \rangle \cong \mathbb{Z}_4;$$

$$m = 8 : \{1, a^8, a^{16}\} = \langle a^8 \rangle \cong \mathbb{Z}_3;$$

$$m = 12 : \{1, a^{12}\} = \langle a^{12} \rangle \cong \mathbb{Z}_2;$$

$$m = 24 : \{1\} = \langle 1 \rangle \cong E \text{ — единичная.}$$

Задача ГКП-5

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

- 1 целые числа \mathbb{Z} ?

Задача ГКП-5

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

- 1 целые числа \mathbb{Z} ? **Кольцо.**

Задача ГКП-5

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

- 1 целые числа \mathbb{Z} ? **Кольцо.**
- 2 четные числа ($2\mathbb{Z}$)?

Задача ГКП-5

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

- 1 целые числа \mathbb{Z} ? Кольцо.
- 2 четные числа $(2\mathbb{Z})$? Кольцо.

Задача ГКП-5

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

- 1 целые числа \mathbb{Z} ? Кольцо.
- 2 четные числа $(2\mathbb{Z})$? Кольцо.
- 3 целые $d\mathbb{Z}$, $d > 0$?

Задача ГКП-5

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

- 1 целые числа \mathbb{Z} ? Кольцо.
- 2 четные числа $(2\mathbb{Z})$? Кольцо.
- 3 целые $d\mathbb{Z}$, $d > 0$? Кольцо.

Задача ГКП-5

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

- 1 целые числа \mathbb{Z} ? Кольцо.
- 2 четные числа $(2\mathbb{Z})$? Кольцо.
- 3 целые $d\mathbb{Z}$, $d > 0$? Кольцо.
- 4 рациональные числа \mathbb{Q} ?

Задача ГКП-5

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

- 1 целые числа \mathbb{Z} ? Кольцо.
- 2 четные числа $(2\mathbb{Z})$? Кольцо.
- 3 целые $d\mathbb{Z}$, $d > 0$? Кольцо.
- 4 рациональные числа \mathbb{Q} ? Поле.

Задача ГКП-5

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

- 1 целые числа \mathbb{Z} ? Кольцо.
- 2 четные числа $(2\mathbb{Z})$? Кольцо.
- 3 целые $d\mathbb{Z}$, $d > 0$? Кольцо.
- 4 рациональные числа \mathbb{Q} ? Поле.
- 5 действительные числа \mathbb{R} ?

Задача ГКП-5

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

- 1 целые числа \mathbb{Z} ? Кольцо.
- 2 четные числа $(2\mathbb{Z})$? Кольцо.
- 3 целые $d\mathbb{Z}$, $d > 0$? Кольцо.
- 4 рациональные числа \mathbb{Q} ? Поле.
- 5 действительные числа \mathbb{R} ? Поле.

Задача ГКП-5

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

- 1 целые числа \mathbb{Z} ? Кольцо.
- 2 четные числа $(2\mathbb{Z})$? Кольцо.
- 3 целые $d\mathbb{Z}$, $d > 0$? Кольцо.
- 4 рациональные числа \mathbb{Q} ? Поле.
- 5 действительные числа \mathbb{R} ? Поле.
- 6 комплексные числа \mathbb{C} ?

Задача ГКП-5

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

- 1 целые числа \mathbb{Z} ? Кольцо.
- 2 четные числа $(2\mathbb{Z})$? Кольцо.
- 3 целые $d\mathbb{Z}$, $d > 0$? Кольцо.
- 4 рациональные числа \mathbb{Q} ? Поле.
- 5 действительные числа \mathbb{R} ? Поле.
- 6 комплексные числа \mathbb{C} ? Поле.

Задача ГКП-5

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

- 1 целые числа \mathbb{Z} ? **Кольцо.**
- 2 четные числа $(2\mathbb{Z})$? **Кольцо.**
- 3 целые $d\mathbb{Z}$, $d > 0$? **Кольцо.**
- 4 рациональные числа \mathbb{Q} ? **Поле.**
- 5 действительные числа \mathbb{R} ? **Поле.**
- 6 комплексные числа \mathbb{C} ? **Поле.**

Задача ГКП-5...

- 7 матрицы порядка n с целыми элементами относительно сложения и умножения матриц?

Задача ГКП-5...

- 7 матрицы порядка n с целыми элементами относительно сложения и умножения матриц?
Кольцо (обратной матрицы может не быть).

Задача ГКП-5...

- 7 матрицы порядка n с целыми элементами относительно сложения и умножения матриц?
Кольцо (обратной матрицы может не быть).
- 8 матрицы порядка n с действительными элементами относительно сложения и умножения матриц?

Задача ГКП-5...

- 7 матрицы порядка n с целыми элементами относительно сложения и умножения матриц?
Кольцо (обратной матрицы может не быть).
- 8 матрицы порядка n с действительными элементами относительно сложения и умножения матриц?
Кольцо (обратной матрицы может не быть).

Задача ГКП-5...

- 7 матрицы порядка n с целыми элементами относительно сложения и умножения матриц?
Кольцо (обратной матрицы может не быть).
- 8 матрицы порядка n с действительными элементами относительно сложения и умножения матриц?
Кольцо (обратной матрицы может не быть).
- 9 многочлены от одного неизвестного x с целыми коэффициентами относительно обычных операций сложения и умножения?

Задача ГКП-5...

- 7 матрицы порядка n с целыми элементами относительно сложения и умножения матриц?
Кольцо (обратной матрицы может не быть).
- 8 матрицы порядка n с действительными элементами относительно сложения и умножения матриц?
Кольцо (обратной матрицы может не быть).
- 9 многочлены от одного неизвестного x с целыми коэффициентами относительно обычных операций сложения и умножения?
Кольцо (многочлены $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ в случае $a_0 = 0$ необратимы).

Задача ГКП-5...

- 7 матрицы порядка n с целыми элементами относительно сложения и умножения матриц?
Кольцо (обратной матрицы может не быть).
- 8 матрицы порядка n с действительными элементами относительно сложения и умножения матриц?
Кольцо (обратной матрицы может не быть).
- 9 многочлены от одного неизвестного x с целыми коэффициентами относительно обычных операций сложения и умножения?
Кольцо (многочлены $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ в случае $a_0 = 0$ необратимы).
- 10 многочлены от одного неизвестного x с действительными коэффициентами относительно обычных операций?

Задача ГКП-5...

- 7 матрицы порядка n с целыми элементами относительно сложения и умножения матриц?

Кольцо (обратной матрицы может не быть).

- 8 матрицы порядка n с действительными элементами относительно сложения и умножения матриц?

Кольцо (обратной матрицы может не быть).

- 9 многочлены от одного неизвестного x с целыми коэффициентами относительно обычных операций сложения и умножения?

Кольцо (многочлены $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ в случае $a_0 = 0$ необратимы).

- 10 многочлены от одного неизвестного x с действительными коэффициентами относительно обычных операций?

Кольцо (многочлены $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ в случае $a_0 = 0$ необратимы).

Задача ГКП-5...

- 7 матрицы порядка n с целыми элементами относительно сложения и умножения матриц?

Кольцо (обратной матрицы может не быть).

- 8 матрицы порядка n с действительными элементами относительно сложения и умножения матриц?

Кольцо (обратной матрицы может не быть).

- 9 многочлены от одного неизвестного x с целыми коэффициентами относительно обычных операций сложения и умножения?

Кольцо (многочлены $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ в случае $a_0 = 0$ необратимы).

- 10 многочлены от одного неизвестного x с действительными коэффициентами относительно обычных операций?

Кольцо (многочлены $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ в случае $a_0 = 0$ необратимы).