

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.

Часть 0

Группы, кольца, поля (напоминание)

Разделы

1 Группы

2 Кольца и поля

Группы: определение и нотация

Определение

Группой 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**;

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 носителя**.

Если $G = n$, то группа называется **конечной** и n — её **порядок**.

При **мультипликативной записи** $x \cdot y$ (или xy) единичный элемент называют **единицей** и обозначают e или 1 .

Группы: определение и нотация...

Группы со свойством $a * b = b * a$ —

- называются **коммутативными** или **абелевыми**;
- для их обозначения обычно используют **аддитивная запись** $x + y$, а единичный элемент называют **нулем** (0).

В конечной группе операцию $*$ задают **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

(и часто c обозначают ab)

Группы: примеры

1. Числовые группы: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — абелевы группы относительно сложения.

Множества ненулевых элементов $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — группы относительно умножения.

2. Бинарные наборы: элементы B^n относительно $\oplus$.

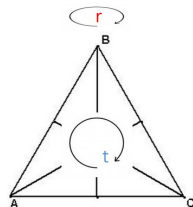
3. Симметрическая группа S_n : все перестановки n -элементного множества относительно композиции перестановок; $|S_n| = n!$.

Симметрическая группа не абелева.

Группа всех преобразований правильного треугольника в себя — симметрическая группа

$$S_3 = \langle t, r \rangle =$$

$$= \{e, (ABC), (ACB), (A)(BC), (B)(AC), (C)(AB)\}.$$



Группы: примеры...

4. Циклические группы: в них есть *порождающий элемент группы* — такой, что каждый элемент группы может быть получен многократным применением к нему групповой операции.

Обозначения:

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

и справедливы все обычные свойства степени.

C — циклическая группа:

$$\exists c \underset{C} \forall x \underset{C} \exists k \underset{\mathbb{N}} (c^k = x), \quad \langle c \rangle = C.$$

Порядок элемента: $\deg a \stackrel{\text{def}}{=} \arg \min_n \{ a^n = e \}.$

Изоморфизм групп

Определение

Пусть $G = \langle G, * \rangle$ и $G' = \langle G', \circ \rangle$ — 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 $G \cong G'$.

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 .

Подгруппы и смежные классы

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

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

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

В абелевой группе всегда $xH = Hx$.

Утверждение

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

Циклические группы: свойства

- Все циклические группы абелевы.
- Каждая конечная циклическая группа изоморфна группе $\mathbb{Z}_n = \langle \{0, 1, \dots, n-1\}, +_{\text{mod } n} \rangle$, а каждая бесконечная — изоморфна $\langle \mathbb{Z}, + \rangle$.
- Каждая подгруппа циклической группы циклическа.
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: $H = \{\dots - 6, -3, 0, 3, 6, \dots\} = 3\mathbb{Z}$.
- У циклической группы порядка n существует ровно $\varphi(n)$ порождающих элементов, где $\varphi(\cdot)$ — функция Эйлера.
Если p — простое число, то любая группа порядка p циклическая и единственна с точностью до изоморфизма.

Индекс подгруппы. Нормальные подгруппы

Количество смежных классов группы G по подгруппе H называется *индексом подгруппы*, символически $(G : H)$.

Пример

Рассмотрим подгруппу $H = \langle (12) \rangle = \{e, (12)\}$ группы $S_3 = \{e, (123), (132), (1)(23), (2)(13), (3)(12)\}$.

Разбиение G на левые смежные классы по подгруппе H :

$$H = \begin{array}{|c|c|c|} \hline e & (123) & (132) \\ \hline (3)(12) & (1)(23) & (2)(13) \\ \hline \end{array} \quad (G : H) = \frac{6}{2} = 3.$$

Подгруппа H группы G называется *нормальной*, если $\forall g \in G (gH = Hg)$, символически $H \trianglelefteq G$.

Группы можно факторизовать («делить») по нормальным подгруппам.

Теорема Лагранжа и следствия из неё

Теорема

Если H — подгруппа конечной группы G , то

$$|G| = (G : H) \cdot |H|.$$

Следствия

- ① Порядок любого элемента есть делитель порядка группы.
- ② Группа простого порядка:
 - циклическая и любой её отличный от единицы элемент — порождающий;
 - не имеет нетривиальных подгрупп;
 - не имеет двух подгрупп с равными индексами.

Замечание. Обращение теоремы Лагранжа **неверно**.

Разделы

1 Группы

2 Кольца и поля

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: $a \cdot (b + c) = a \cdot b + a \cdot c$; $(b + c) \cdot a = b \cdot a + c \cdot a$ — *дистрибутивность умножения относительно сложения слева и справа*.

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

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

Кольца: основные свойства, примеры

- Обратного элемента по умножению в кольце может и не быть.
В любом кольце $a \cdot 0 = 0$.
- 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*.
- Ассоциативно-коммутативное кольцо без делителей нуля — *целостное кольцо*.

Примеры колец:

1. *Классический пример* — множество целых чисел $\mathbb{Z}$ с операциями сложения и умножения. Здесь обратный элемента по умножению есть только для ± 1 .
2. $\mathbb{Z}_n \stackrel{\text{def}}{=} \langle \{0, 1, \dots, n-1\}, +_{\text{mod } n}, \cdot_{\text{mod } n} \rangle$ — *кольцо вычетов по модулю n* .
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: $\forall r_1, r_2 \in R$ имеем

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

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

Утверждение

Гомоморфная область кольца есть кольцо.

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

Идеалы колец

Определение

Подкольцо I коммутативного кольца $\langle R, +, \cdot \rangle$ называется его *идеалом*, символически $I \triangleleft R$, если

$$\forall r \in R \quad \forall x \in I \quad (a \cdot x \in I) \ \& \ (x \cdot a \in I).$$

Определение

Идеал I кольца $\langle R, +, \cdot \rangle$ называется *главным*, если найдётся элемент $a \in R$ такой, что

$$I = \{ a \cdot r \mid r \in R \},$$

символически $I = (a)$.

Пример: $(n) = n\mathbb{Z} \triangleleft \mathbb{Z}$.

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

Идеалы колец: свойства

- Само кольцо $\mathbf{R}$ и его нуль — идеалы $\mathbf{R}$, они называются *собственными*, остальные идеалы — *несобственные*.
- Если $\mathbf{R}$ — произвольное кольцо, и $n \in \mathbb{Z}$, то

$$nR = \{n \cdot x \mid x \in R\} \triangleleft \mathbf{R}.$$
- Если $\mathbf{R}$ — коммутативное кольцо, и $a_1, \dots, a_n \in R$, то

$$(a_1, \dots, a_n) = \{x_1 a_1 + \dots + x_n a_n \mid x_1, \dots, x_n \in R\} \triangleleft \mathbf{R}$$
 — *идеал, порождённый элементами $a_1, \dots, a_n$* .
- В некоммутативных кольцах различают *левые* и *правые идеалы*.
- 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 $I_1 \cdot I_2 \stackrel{\text{def}}{=} \{x_1 \cdot y_1 + \dots + x_n \cdot y_n \mid$
 $x_1 \in I_1, y_1 \in I_2, i = \overline{1, n}\} \ (n \in \mathbb{N})$,
 — 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 $I \subset I' \subset R$.

Евклидовы кольца

Определение

Коммутативное кольцо $\langle R, +, \cdot \rangle$ называется **евклидовым**, если для него выполнены следующие свойства:

E1: 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 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. Здесь норма это модуль числа.
- Евклидовы кольца — это кольца главных идеалов (обратное, вообще говоря, неверно).

Поле: определение

Определение

Поле 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 K — абелева группа;

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

K3: $a \cdot (b + c) = a \cdot b + a \cdot c$ 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 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.