



Лекция №1

Лектор - Гурков Сергей Исаевич
ассистент - Кропотов Дмитрий
Александрович

Литература:

- Абдескин, Надеждин Дискретная математика
Модульная алгебра...
- Лигал. Штедлер-Гаупт Многие поля
- Гильбертсон - Коды, исправляющие ошибки.

Часть 1

Классические алгебраические структуры

Группы

Тройка $\langle G, \circ, e \rangle$, где G -кенуство мн-во (коснтель), $e \in G$ - единицный элемент, а \circ - бинарная операция на коснеле, что

$\forall x, y, z \in G$ выполнено:

- $x \circ y \in G$ - устойчивость коснеля
- $(x \circ y) \circ z = x \circ (y \circ z)$ - ассоциативность
- $e \circ x = x \circ e = x$ - сб-во центрального элемента
- $\forall x \exists y: y \circ x = x \circ y = e$ - Задр-во элемента $\forall x \in G$

Группы \mathfrak{G} : $x \circ y = y \circ x$ абелевы

Вместо \circ пишут \cdot .

Обратный $-x^{-1}$

Нейтральный -1

Степень элемента:

$$a^0 = e, \quad a^n = \underbrace{a \cdot \dots \cdot a}_n, \quad n \in \mathbb{N}$$

Для абелевых аддитивных групп: $x + y$

Примеры

① Числовые группы

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ вtk-ко сложения
- $n\mathbb{Z} = \{0; \pm n; \pm 2n, \dots\}$
- Некоммутативные группы $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ абелевы

группы вtk-ко умножения

② Симметрическая S_n -группа всех перестановок

$|S_n| = n!$ S_n неабелева при $n > 2$

е-единичная перестановка

Число элементов группы - её порядок

Порядок элемента $a^n = e$ такое наименьшее n при $a \neq e$

$\text{ord } a$

в группе $\text{mod } 6$

$\text{ord } 1 = \text{ord } 5 = 6, \text{ord } 3 = 2$

$\text{ord } 2 = \text{ord } 4 = 3 \quad \text{ord } 0 = 1$

$\langle G, \cdot, e \rangle$ - группа $H \subset G$, являясь группой, называется подгруппой.

$E = \langle e \rangle$, все группы - тривиальные примеры
 a , $\text{ord}a=n$, то $G = \langle a \rangle$

Теорема

$$|G| = |H| \cdot [G : H]$$

Следствие

Индекс подгруппы H по группе G

Порядок \neq элементов какой группы делит порядок групп

Левые / правые смешанный класс.

xH

$$xH = \{xoh \mid h \in H\}$$

Утверждение

$$Hx = \{hox \mid h \in H\}$$

Левые смешанные классы с различными элементами либо не пересекаются, либо совпадают, в совокупности составляют всю группу.
Все левые смешанные классы равновеличины этой подгруппе.

Пример

$$G = \langle \{0, \dots, 5\}, +_6, 0 \rangle \text{ и } H = \langle \{0, 3\}, +_6, 0 \rangle$$

$$[G : H] = \frac{6}{2} = 3$$

$$\textcircled{1} \quad 0+H = \{0, 3\} = H$$

$$\textcircled{2} \quad 1+H = \{1, 4\}$$

$$\textcircled{3} \quad 2+H = \{2, 5\}$$

Если $\forall x \in G$ всегда $xH = Hx$, то H - нормальная.

В абелевой группе все подгруппы нормальны.

Если H нормальна, то кеза висима от выбора

$x \in aH$ и $y \in bH$ верно $xy^{-1} \in (aob)H$

\Rightarrow можно расширить операцию до оп-ии на смежных классах.

Оп-ие

Мн-во смежных классов с опр-ией

$$(aH) \cdot (bH) = (aob)H$$

- факторгруппа G/H

Оп-ие

$\langle G, \circ, e \rangle$ и $\langle G', \circ, e' \rangle$ отобр-ие $\varphi: G \rightarrow G'$

изоморфизм, если оно биективно и

$$\varphi(aob) = \varphi(a) \varphi(b)$$

Тогда группы изоморфны: $G \cong G'$

Теорема Кэли

\forall группа порядка n изоморфна
какой-то подгруппе S_n

Изоморфизмы без биекции - гомоморфизм.

Циклическая группа

$C = \{a^n \mid a \in C, n \in \mathbb{Z}\} = \langle a \rangle$, т.о.
такая группа циклическая, a - образующий
($\forall a_1 \in C$ есть $a^{n_0} = a_1$)

Циклическая группа и её подгруппы абелевы

Пример

группа $\langle \frac{2\pi}{n} \rangle$ поворотов правильного n -угольника
на указанный угол с сохранением оси вра-
щений с центром приложения - циклическая

1. $a \in C \text{ ord } a = \infty$

$$\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots$$

тогда она изоморфна $\langle \mathbb{Z}, +, 0 \rangle$

2 ненулевых элемента: $-1, 1$.

2. $a \in C \text{ ord } a = n$

$$\langle a \rangle = C \quad \text{ord } a = |C| = n$$

изоморфна addитивной группе

$$\langle \{0, \dots, n-1\}, +, 0 \rangle \cong \mathbb{Z}_n \cong \frac{\mathbb{Z}}{n\mathbb{Z}}$$

+ no mod n

В беск. $\langle . \rangle$ группа $\cong \mathbb{Z}$

конечная $\cong \mathbb{Z}_n \Rightarrow$ все конечные цикл-ые

группы изоморфны

если \mathbb{Z}_n все элем-ты пород-ие \Rightarrow иже число
состоит с кратнами N взаимно простых с n .

(Ф-ция Эйлера $\varphi(n) =$ крат-во взаимно простых
 $(N \text{ чисел})$ $\varphi(6) = |\{1, 5\}| = 2$)

\Leftrightarrow с cond = n $\varphi(n)$ пород-иующих.

Свойства $\varphi(n)$:

- p -простые $\varphi(p) = p - 1$
- $\varphi(n^k) = n^{k-1} \varphi(n)$ $\varphi(p^k) = p^{k-1}(p-1)$
- если m и n взаимно просты
 $\varphi(mn) = \varphi(m)\varphi(n)$

Кольца

Оп-ие

$\langle R, + \rangle$

Абелева группа - кольцо, если на ней определено
умножение, связанное со слож-и дистриб. законами:

$$x \cdot (y + z) = xy + xz$$

$$(y + z)x = yx + zx$$

Обычно рассмотрим кольца ассоциативные

Если $1 \in K$, то кольцо с единицей или единичное

Тривиальное кольцо из $[0=1]$

Если \cdot - коммутативная оп-ия, то к-коммутативное.

Элемент $a \in K$ обратим, если $\exists b : ab = ba = 1$

K без делителей нуля, если $\forall r_1, r_2 \in \mathbb{R}$

$$(r_1 r_2 = 0) \Leftrightarrow \begin{cases} r_1 = 0 \\ r_2 = 0 \end{cases}$$

Определение

Челостное кольцо — кетри виальское читальское

ассоциативное — коммутативное

кольцо без делителей нуля

Примеры

① $\langle \mathbb{Z}, +, \cdot \rangle$

② K без e — $2\mathbb{Z}$

③ Z_n — кольцо классов вычетов по
модулю n (нечелостко при составки n)

Читальское $K \langle R, +, \cdot, 0, 1 \rangle$

- Все обратимые элементы R — группа по
умножению
- В \mathbb{Z} обратимы только $+1, -1$ неравда-
ющие элементы
- Z_n^* — взаимно простые с n и всего их $\varphi(n)$
Суть — ин-ое число
есть — единст-ое

Определение

Необратимый элемент р целочисл-го кольца

каз-ся кеприводимы или керазложимы, если из $p=a \cdot b \Rightarrow a$ или b обратимы.

\exists керазложимы простые и просты во пологиске к ими (только они)

Лекция №2

Опр

Ненулевой элемент p целостного кольца кеприводимый или керазложимый, если $p = a \cdot b \Rightarrow$ либо a , либо b обратим.

Например, простые числа в кольце \mathbb{Z}

Опр.

Целостное кольцо, в котором каждыи ненулевой элемент

1) обратим

либо

2) однозначно представляется в

виде произведения кеприводимых элементов

каз-ся факториальными или

кольцом с однозначным разложением.

Пример : \mathbb{Z}

$$\mathbb{Z}[\sqrt{-3}] = \{m + n\sqrt{-3} \mid m, n \in \mathbb{Z}\}$$

не факториально:

$$4 = 2 \cdot 2 = (\pm 1 + \sqrt{-3})(\pm 1 - \sqrt{-3})$$

Идеалы колца

Подкольцо $I \leq R$

$I \in$ подкольцам

Подкольцо собственное, если не совпадает
со всем кольцом.

Опр

Подкольцо $I \leq R$ коммутивного кольца
каждое (из строк или) идеалом,
если $\forall i \in I \quad \forall r \in R: i \cdot r \in I$

$I \trianglelefteq R$

Примеры:

• $2\mathbb{Z} \trianglelefteq \mathbb{Z}$

- Само кольцо и 0 - триivialные идеалы
- Идеалы, не совпадающие со всем кольцом - собственные

Опр

Идеал $I \trianglelefteq R$ главный и порождённый
элементом $a \in R$, если
 $I = \{a \cdot r \mid r \in R\} \stackrel{\text{def}}{=} (a)$

Целостное кольцо, в котором все идеалы
 главные, наз-ся кольцом главных идеалов

Примеры:

- \mathbb{Z}
- $\mathbb{Z}_n - A \trianglelefteq \mathbb{Z}_n$ содержит
мног своих левых элементов
 и им порождается

Все КГИ факториальны

Опр

Максимальный идеал коммутативного кольца
 наз-ся собственный идеал, строго же
 содержащийся в каком-либо

свойства идеала.

В четырех-м коммутативном кольце \exists максимальный идеал.

Пример:

- $b \in \mathbb{Z} \setminus \{2, 3, 5, \dots\}$ — главные
- (6) не максимальен

УПВ.

Максимальные идеалы в \mathbb{Z} есть (p) , где p — простое число.

D-60:

[$\exists p$ — простое, но (p) — не максимальный]

$\Rightarrow b \in \mathbb{Z} \setminus$ собственных идеалов $I \supset (p)$.

$\mathbb{Z} - \text{кру} \Rightarrow \exists i: 0 < i < p, \text{т.к. } I = (i) \Rightarrow$

$\Rightarrow p : i \Rightarrow \left[\begin{array}{l} i=1 \\ i=p-? \end{array} \right] \rightarrow \text{т.к. } (1) = \mathbb{Z} - \text{не}$

собственных.

[$m = n \cdot k, n, k \in \mathbb{N} \Rightarrow I(m) = m \in \mathbb{Z} \subset I(n) =$

$= n \in \mathbb{Z} \Rightarrow I(m) — \text{максимальный.}$ изг

Опр

Класс вычетов по модулю идеала I коммутативного кольца $\langle R, +, \cdot, 0 \rangle$ с представителями r , называемый ик-бо

$$r+I = \{r+i \mid r \in R, i \in I\} \stackrel{\text{def}}{=} \overline{r}_I$$

Пример:

- $(n) \leq \mathbb{Z}$ с предст-и n :

$$\overline{r} = r+n\mathbb{Z} = \{r, r \pm n, r \pm 2n, \dots\}$$

r — остаток от деления целого на n ,
 $0 \leq r < n$

$$n=5, r=3: \quad \overline{3} = \{3, 3 \pm 5, 3 \pm 10, \dots\} = 3+5\mathbb{Z}$$

Совокупность всех вычетов R по модулю $I \trianglelefteq R$ образуют факторкольцо R/I

$$\mathbb{Z}_n \cong \mathbb{Z}/(n) \quad \{0, 1\} = \mathbb{Z}_2 \cong \mathbb{Z}/(2) = \{\overline{0}, \overline{1}\}$$

Факторкольцо по максимальному идеалу — поле

Опн

Челостное кольцо - евклидово, если $\forall a \neq 0$

\exists корни $N(a) \in \mathbb{N}_0$

$\forall b \neq 0 \quad \exists q, r : a = qb + r$ и либо $r=0$,
либо $N(r) < N(b)$

Пример:

- $\mathbb{Z} \quad N=1 \cdot 1$
- кольцо многочленов, $N=\deg$.
- кольцо целых гауссовых чисел

$$\mathbb{Z}[\sqrt{-1}] = \{m + n\sqrt{-1}\}, m, n \in \mathbb{Z}$$

$$N(m+ni) = m^2 + n^2$$

$K\Gamma U \{ m+n \frac{1+\sqrt{-1}g}{2} \mid m, n \in \mathbb{Z} \}$ кеевклидово

Все евклидовы кольца - $K\Gamma U$.

Опн

Челостное кольцо, в котором все
некудлевые элементы обратимы - поле.

2 результата поля - абелевы группы (по + и по $*$)

CB-Ba:

- K^* - мультипликативная группа пол

- R/I — поле $\Leftrightarrow I \trianglelefteq R$ — главный.

Подполе собственное, если $K' \neq K$

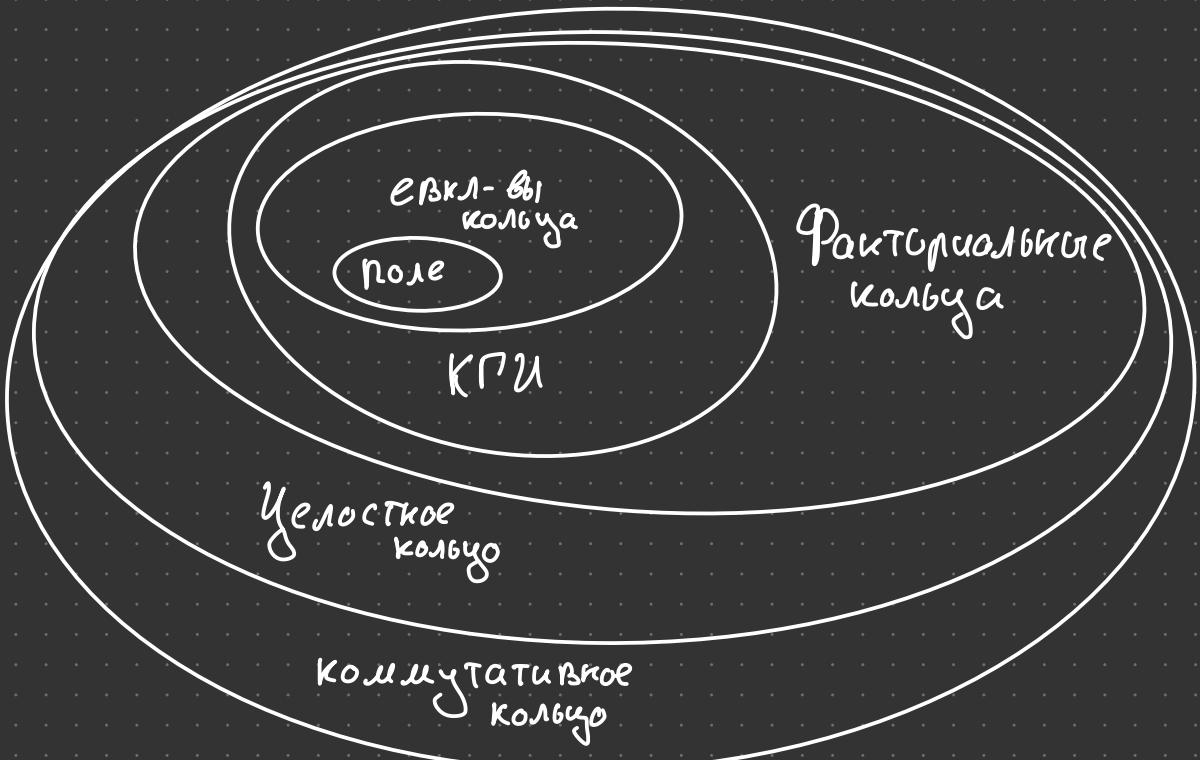
Примеры:

- $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ — бесконечное
- конечно \mathbb{Z}_p , p — простое

Поле без собственных подполей — простое

Теорема (Фробениус)

В \mathbb{F} поле $\exists!$ простое подполе $\cong \begin{cases} \mathbb{Q} & \text{или} \\ \mathbb{Z}_p, p - \text{прост.} \end{cases}$



Опн

Абстрактное векторное пространство над полем $K = \{k, \lambda, \beta, \dots\}$ — это алгебраическая система $\langle V, k, +, \cdot \rangle$, где

- $V = \{v_0, v_1, \dots\}$ — мн-во векторов — абелево¹ группой по $+$
- \cdot — бинарная операция умножения элемента из k на вектор из V : $K \times V \rightarrow V$

причём $+$ и \cdot удовл-т аксиомы:

- 1) $\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$
 $(\lambda_1 + \lambda_2)v = \lambda_1 v + \lambda_2 v$
- 2) $\lambda(\beta v) = (\lambda\beta)v$
- 3) $1 \cdot v = v$

$\boxed{V = k^n}$; $+$ — подвекторное

такая структура — линейное векторное пр-во

(n -мерное координатное пр-во
над полем K)

$$\forall x \in V \exists! \lambda_i : x = \sum_{i=1}^n \lambda_i e_i$$

Удаляем e_n из базиса, получаем лин-ое подпр-во

Если в опр-ии поле $K \rightarrow$ кольцо K , то опр-ие модуль.

$$\psi: A \rightarrow B \quad \text{ker } \psi = \{a \mid a \in A; \psi(a) = 0 \in B\}$$

$$\text{Im } \psi = \{b \mid b \in B; \exists a \in A, \psi(a) = b\}$$

Сюръективный изоморфизм — автоморфизм
Биективный — изоморфизм

Изоморфизм в седе — автоморфизм.

Св-ва сравнивания по модулю:

- $a \equiv_m b \Leftrightarrow \text{HOD}(a, m) = 1 \Rightarrow a \equiv_m b$
- $a \cdot c \equiv_m b \cdot c \Rightarrow a \equiv_m b$

Кократные классы и поля

Простые поля Галуа — поля классов вычетов

Поле из 4-х элементов:

- расширение пр-ва для \uparrow числа элем-ов.

Характ-ка поля:

$$\underbrace{1 + \dots + 1}_p = 0 \quad p = \text{char } K$$

$\text{char } K$ — простое, иначе $uv: (u \cdot 1)v = 0 \Rightarrow$
 $\Rightarrow uv = 0 - ?!$

Если $1 + 1 + \dots + 1 + \dots \neq 0 \Rightarrow \text{char } K = 0$

$\{0, 1, \dots, p-1\} \cong \mathbb{Z}_p$ - минимальное подполе \mathbb{F} поля
к характеристики $p > 0$.

поле \mathbb{F}_p - с дробными квадратами
- беск. поле пологости-ой характеристики

$\sim \mathbb{Q}$ с операциями

$] K = \mathbb{F}_p$, тогда $\mathbb{F}_p(\alpha)$ - беск. поле
характеристики $p > 0$

Теорема (Торсг-Во Родбекуса)

В поле характеристики $p > 0$ выполнено
Торсг-Во $(a+b)^p = a^p + b^p$

Д-бо:

b & коммутативная калькуляция
формула степени бинома:

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \dots + b^p$$
$$\binom{p}{i} = \frac{p!}{(p-i)! i!} : p \Rightarrow = 0 \text{ при } i \neq 0$$

Следствие:

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

