



Лекция №1

Лектор - Гурков Сергей Исаевич
ассистент - Кропотов Дмитрий
Александрович

Литература:

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

Часть 1

Классические алгебраические структуры

Группы

Тройка $\langle G, \circ, e \rangle$, где G -кенупстое мн-во,
(коситетль), $e \in G$ - центральный элемент, а \circ -
- бинарная операция на коситеle, что
 $\forall x, y, z$ выполнено:

- $x \circ y \in G$ - устойчивость косителя
- $(x \circ y) \circ z = x \circ (y \circ z)$ - ассоциативность
- $e \circ x = x \circ e = x$ - цв-во центрального
- $\forall x \exists y: y \circ x = x \circ y = e$ - 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 чесчисл-го кольца

каз-ар ке при ведим или керазложим, есми из $p=ab \Rightarrow a$ или в одрати.

В \mathbb{Z} керазложими простие и просты в опозиците к им (только они)