Лекция 9

Ilya Yaroshevskiy

27 октября

Содержание

1 Группы

Определение. Группа $\mathcal{G}$ – алгебра $(G, \cdot)$.

- Операция $\cdot$ ассоциативна, т.е. $\forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Существует нейтральный элемент $\mathbb{1} \in G : \forall x \in G : \mathbb{1} \cdot x = x \cdot \mathbb{1} = x$
- Существует обратный элемент $\forall x \in G \exists y : x \cdot y = y \cdot x = \mathbb{1}$

Замечание. Если $\cdot$ коммутативна, т.е. $a \cdot b = b \cdot a$, то группу называют коммутативной или абелевой. Далее все группы будем считать коммутативными

Определение. Аддитивное задание группы: $\cdot \to +, 1 \to 0$. Если вышеперечисленные свойства выполняются для некоторого $H \subset G$, замкнутого относительно операции $\cdot$, то $\mathcal{H} = (H, \cdot)$ называют подгруппой G.

Определение. Группы $\mathcal{G} = (G, \cdot)$ называется циклической, если $\exists a \in G : \forall x \in G \exists n \in \mathcal{Z} : x = a^n$

Определение.

- Порядок конечной группы – число элементов в ней, т.е. $|G|$
- Порядок элемента $a \in G$ – наименьшее положительное $n : a^n = \mathbb{1}$
- Порядок образующего элемента конечной циклической группы равен порядку самой группы

Теорема 1.1. Пусть $\mathcal{G} = (G, \cdot)$ – конечная группы и элементы $g, h \in G$ имеют порядок r, s соответственно, при чем $\gcd(r, s) = 1$. Тогда элемент gh имеет порядок rs.

Доказательство. То, что $(gh)^{rs} = \mathbb{1}$, очевидно. Следовательно, порядок p элемента gh – делитель числа rs. Пусть $p|(rs)$ и $(gh)^p = 1$. Тогда $(gh)^{pr} = h^{pr} = \mathbb{1}$. Следоваельно, $s|(pr)$, откуда $s|p$. Аналогично можно показать, что $r|p$. Т.к. $gcd(r, s) = 1$, получаем $(rs)|p$, что означает $p = rs$ □

1.1 Подгруппы и смежные классы

Определение. Смежный класс по подгруппе $\mathcal{H}$: $g\mathcal{H} = \{g \cdot h | h \in G\}, g \in G$

Определение. Отношение эквивалентности $\sim_{\mathcal{H}} = \{(a, b) \in G^2 | a\mathcal{H} = b\mathcal{H}\}$. Класс эквивалентности $[a]_{\sim_{\mathcal{H}}} = a\mathcal{H}$

Лемма 1. *Всякий смежный класс подгруппы $\mathcal{H} = (H, \cdot)$ коммутативной группы $\mathcal{G} = (G, \cdot)$ равномощен H*

Доказательство. Для $a \in G$ зададим отображение $\phi_a : H \to a\mathcal{H}$ как $\phi_a(h) = ah$. Это сюръекция, т.к. $x \in \mathcal{H} \implies \exists h \in H : x = ah = \phi_a(h)$. Это инъекция, т.к. в группе $ah_1 = ah_1 \implies h_1 = h_2$. Следовательно, $\phi_a(h)$ – биекция и $|a\mathcal{H}| = |H|$ □

Теорема 1.2 (Лагранжа)**.** Порядок конечной группы $\mathcal{G} = (G, \cdot)$ делится на порядок любой ее подгруппы

Доказательство. Смежные классы $a\mathcal{H}$ подгруппы $\mathcal{H}$ группы $\mathcal{G}$ образуют разбиение G на равномощные подмножества □

2 Конечные поля

Определение. Полем называется алгебра $(\mathbb{F}, \{+, -, \cdot, /\})$, удовлетворяющая следующим аксиомам

- $a + (b + c) = (a + b) + c$
- $a + b = b + a$
- (∃ 0∈ F: a + 0= a\)
- $\forall a \in F : \exists a' = -a \in \mathbb{F} : a + a' = \mathbb{0}$
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- $a \cdot b = b \cdot a$
- $a \cdot (b + c) + a \cdot b + a \cdot c, (b + c) \cdot a = b \cdot a + c \cdot a$
- $\exists \mathbb{1} \in \mathbb{F} \setminus \{\mathbb{0}\} : \forall a : a \cdot \mathbb{1} = \mathbb{1} \cdot a = a$
- $\forall a \neq \mathbb{0} \exists a^{-1} = \mathbb{1}/a \in \mathbb{F} : a \cdot a^{-1} = a^{-1} \cdot a = \mathbb{1}$

Замечание.

- Поля, содержащие конечное число q элементов – конечные поля или поля Галуа \(GF(q))
- Бесконечные поля называются полями характеристики нуль
- Поле является областью целостности, т.к. если допустить, что $\exists a, b \neq 0 : ab = \mathbb{0}$, то $\mathbb{0} = (((ab)b^{-1})a^{-1}) = \mathbb{1}) = 1$\)
- Простое поле $GF(p)$:
  - p – простое
  - арифметика по модулю p

2.1 Идеалы

Определение. Подмножество I кольца R называется **правым (или левым) идеалом**, если

- $(I, \{+\})$ является подгруппой $(R, \{+\})$
- $\forall r \in R, \forall x \in I : xr \in I$ (или $rx \in I$)

В коммутативных кольцах все идеалы являются двусторонними.

Определение. Если $A \subset R$, то идеалом, порождаемым A, называется нименьший идеал, содержащий A:

$$\langle A \rangle = \sum_i r_i a_i, a_i \in A, r_i \in R$$

Определение. Идеал I конечно порожден, если существует конечное множество $A : I = \langle A \rangle$

Определение. Идеал называется главным, если он порождается единственным элементом

Пример.

- Множество четных чисел является идеалом в кольце $\mathbb{Z}$, порожденным элементов 2
- Множество многочленов с вещественными коэффицентами, делащихся на $x^2 + 1$, является идеалом $\mathbb{R}[x]$
- Множество квадратных матриц, у которых последний столбец является нулевым, является левым идеалом в кольце квадратных матриц, но не является правым идеалом
- Кольцо непрерывных функций вещественного аргумента $C(\mathbb{R})$ содержит идеал непрерывных функций, таких что $f(1) = 0$
- $\{\mathbb{0}\}$ и R являются идеалами в любом кольце R
- $\langle x, y \rangle$ является идеалом, содержащим все многочлены от двух переменных с нулевым свободным членом

2.2 Максимальные идеалы

Область целостности, в которой все идеалы являются главными, называется кольцом главных идеалов

Определение. Идеал I кольца R называется максимальным, если $I \neq R$ и всякий идеал J, содержащий его, равен или I, или R

Идеал является максимальным, если он отличен от своего кольца и не содержится ни в каком ином идеале

Если $f_1, f_2, \ldots, f_n$ – система образующих масимального идеала I, то добавление в нее $f_0 \notin I$ приведет к $\langle f_0, \ldots, f_n \rangle = R$.

Пример. Идеал $\langle 7 \rangle \subset \mathbb{Z}$ является максимальным, т.к. числа, кратные 7, невозможно получить иначе как умножением 7 на целые числа

2.3 Факторкольца

Пусть дана полугруппа $\mathcal{G} = (G, \cdot)$. Бинарное отношение $\sim \subset G^2$ называется отношением конгруэнтности, если оно является эквивалентностью на G и $\forall a, b, c \in G : (a \sim b) \implies a \cdot c \sim b \cdot c$

Пример. $x \equiv y \mod n \Leftrightarrow x = qn + y$

Определение. Пусть дано кольцо R и идеал $I \subset R$. Бинарное отношение $\sim \equiv \{(a, b) \in R^2 | b - a \in I\}$ является отношением конгруэнтности. Разбиение на классы эквивалентности $[a] = a + I = a \mod I = \{a + r | r \in I\}$. Множество классов эквивалентности по отношению $\sim$ называется **факторкольцом** или кольцом вычетов R по модулю I и обозначается $R \setminus I$.

Замечание. Факторкольцо является кольцом, если на нем определить операции следующим образом:

- $(a + I) + (b + I) = \underbrace{(a + b)}_{\in R} + I$
- $-(a + I) = (-a) + I$
- $(a + I) \cdot (b + I) = ab + I$
- Нулевой элемент $\mathbb{0} + I = I$, единичный элемент $\mathbb{1} + I$

Если R – кольцо главных идеалов, и $\langle a\rangle \in R$, то соответствующее факторкольцо обозначают R/aR

Теорема 2.1. Если $I \subset R$ является максимальным идеалом, то R/I является полем

Доказательство. Надо показать, что для всякого ненулевого $a+I \in R/I$ существует $b+I : (a+I)(b+I) = \mathbb{1}+I$. Если $a+I \neq \mathbb{0}$, то $a \notin I$
Множество $J = \{ax+m | x \in R, m \in I\}$ является идеалом, т.к. $(ax_1+m_1) \pm (ax_2+m_2) = a(x_1 \pm x_2) + (m_1 \pm m_2), (x_1 \pm x_2) \in R, (m_1 \pm m_2) \in I$ и $(ax+m)y = a(xy)+(my), xy \in R, my \in I$ при любом $y \in R$. Полагая $x = 0$ можно получить все элементы $I \implies I \subset J$.
Т.к. $a \in J, a \notin I$, а I – максимальный идеал, $J = R \implies \mathbb{1} \in J \implies \forall a \notin \mathbb{0} \exists b, m : \mathbb{1} = ab+m$, откуда $ab-1 \in I$, т.е. $(a+I)(b+I) = \mathbb{1}+I$. Т.е. для каждого ненулевого элемента факторкольца по модулю максимального идеала существует обратный элемент, т.е. оно является полем $\square$

Теорема 2.2. Пусть R – кольцо главных идеалов и p – его неприводимый элемент. Тогда факторкольцо R/pR является полем

Доказательство. Докажем, что $I = \langle p\rangle$ является масимальным. Предположим, что сущесвтует идеал $J \neq R : I \subset J$. Т.к. R – КГИ, J является главным и $\exists q \in R : J = \langle q\rangle$. Если q – обратимый элемент кольца, то $J = R$. Если $J \neq R$, то $p \in J \implies \exists s \in R : p = qs$. Но p – неприводимый элемент $\implies$ s – обратимый элемент кольца $\implies s^{-1} \in R \implies q = s^{-1}p \implies J \subset I = J$. Таким образом $\langle p\rangle = pR$ является масимальным и R/pR является полем. $\square$

В дальнейшем подобные поля будут обозначаться просто R/p

Пример.
- Пусть p – простое число. $\mathbb{Z}$ является КГИ. Тогда $\mathbb{Z}/p$ является полем и обозначается $GF(p)$
- x^2+1 неприводим над $\mathbb{R}$. $\mathbb{R}[x]$ является КГИ. Следовательно $\mathbb{R}[x]/\left\langle x^2+1\right\rangle$ является полем (комплексным чисел $\mathbb{C}$).

  $$(a+bx)(c+dx) = ac+(ab+bc)x+bdx^2 \equiv (ac-bd)+(ad+bc)x \mod (x^2+1)$$

  что соответсвует произведению комплексных чисел $a+ib$ и $c+id$, где $i = [x]_{\equiv_{x^2+1}}$. Видно, что $i \cdot i = x^2 \equiv -1 \mod (x^2+1)$
- x^2+x+1 неприводим над $GF(2)$. $GF(2)[x]$ является КГИ. Следовательно, $GF(2)/\left\langle x^2+x+1\right\rangle$ является полем и обозначается $GF(2^2)$ или $GF(4)$. Элементами $GF(4)$. Элементами $GF(4)$ являются классы вычетов многочленов $0, 1, x, x+1$ по модулю x^2+x+1. Все операции выполняются по модулю x^2+x+1. Например, $x \cdot (x+1) = x^2+x \equiv 1 \mod (x^2+x+1)$. Аналогично $\mathbb{C}$, можно ввести $\beta \in GF(2^2)$, такой что $\beta^2+\beta+1 = 0$.

2.4 Характеристика поля

Определение. Если поле кончено, то не могут быть различными все элементы $\mathbb{1}, \mathbb{1}+\mathbb{1}, \mathbb{1}+\mathbb{1}+\mathbb{1}, \ldots$. Следовательно, существует наименьшее число $p : \underbrace{\mathbb{1}+\mathbb{1}+\cdots+\mathbb{1}}_{p \text{ раз}} = \mathbb{0}$. p – **характеристика поля**

p – простое число. Если это не так, т.е. $p = st$, то

$$\mathbb{0} = \underbrace{\mathbb{1}+\mathbb{1}+\cdots+\mathbb{1}}_{st \text{ раз}} = \underbrace{\underbrace{\mathbb{1}+\mathbb{1}+\cdots+\mathbb{1}}_{s \text{ раз}}+\cdots+\underbrace{\mathbb{1}+\mathbb{1}+\cdots+\mathbb{1}}_{s \text{ раз}}}_{t \text{ раз}} =$$

$$= (\underbrace{\mathbb{1}+\mathbb{1}+\cdots+\mathbb{1}}_{s \text{ раз}})(\underbrace{\mathbb{1}+\mathbb{1}+\cdots+\mathbb{1}}_{t \text{ раз}}) \implies s = p \vee t = p$$

Теорема 2.3. Пусть $\mathbb{F}$ – поле из q элементов. Тогда $q = p^m$, где p – простое, а $m \in \mathbb{N}$

Доказательство. Элемент $\mathbb{1} \in \mathbb{F}$ образует аддитивную циклическую подгруппу простого порядка p оля $\mathbb{F} \implies p|q \implies GF(p) \subset \mathbb{F}$. Будем называть элементы $\alpha_1, \ldots, \alpha_m$ линейно независимыми с коэффициентами из $GF(p)$, если $\{(x_1, x_2, \ldots, x_m) \in GF(p)^m | \sum_{i+1}^m x_i\alpha_i = 0\} = \{(0, \ldots, 0)\}$. Среди всех ЛНЗ подмножеств $\mathbb{F}$ выделим подмножество $\{\alpha_1, \ldots, \alpha_m\} \subset \mathbb{F}$ с максимальным числом элементов $\implies \forall \alpha_0 \in \mathbb{F} \exists x_1, \ldots, x_m \in GF(p) : \alpha_0 = \sum_{i=1}^m x_i\alpha_i$. Различные $x_1, \ldots, x_m \in GF(p)$ приводят к различным $\alpha_0 \in \mathbb{F} \implies |\mathbb{F}| = p^m$ $\square$

Замечание.

- Поле $GF(q^m)$ образует m-мерное линейное пространство над полем $GF(q)$
- $GF(p^m), m > 1$ – расширенное конечное поле. m – степень расширения
- $GF(p^m), m > 1$ не имеет ничего общего с кольцом $\mathbb{Z}_{p^m}$ целых чисел по модулю p^m, которое полем не является

Теорема 2.4. Ненулевые элементы $GF(q)$ образует конечную циклическую группу по умножению

Доказательство.

- асиомы поля $\implies \mathbb{F} \setminus \{0\}$ образует конечную группу по умножению
- Выберем в $\mathbb{F} \setminus \{0\}$ элемента α (примитивный) с наибольшим порядком r. Пуст l – порядок некоторого другого элемента $\beta \neq 0$. Пусть π – простое число, такое что $r = \pi^a r'$ и $l = \pi^b l'$ и $\gcd(r', \pi) = \gcd(l', \pi) = 1$
- α^{π^a} имеет порядок r', а $\beta^{l'}$ имеет порядок π^b. Порядок $\gamma = \alpha^{\pi^a}\beta^{l'}$ равен $\pi^b r'$
- Т.к. r – наибольший порядок, $\pi^b r' \leq \pi^a r'$ и $b \leq a$. Это верно для всех простых $\pi \implies$ если некоторая степень простого числа является делителем l, то она является и делителем r. Следовательно, $l|r \implies$ все ненулевые элементы конечного поля удовлетворяет соотношению $x^r = 1$
- $x^r - \mathbb{1}$ принадлежит Евклидову кольцу $GF(q)[x]$ и разлагается на множители единственным образом $\implies \forall \beta \in GF(q) \setminus \{0\} : (x - \beta)|(x^n - 1)$, откуда $r \geq q - 1$
- Порядок элемента не может превышать порядка самой группы $\implies r = q - 1$

□

2.5 Свойства конечных полей

Замечание.

- Для всякого ненулевого $\beta \in GF(q)$ выполняется $\beta^{q-1} = 1$
- Все элементы поля $GF(q)$ удовлетворяют уравнению $x^q - x = 0$
- Порядок любого ненулевого $\beta \in GF(q)$ делит $q - 1$
- В поле характеристики $p > 1$ справедливо

$$(x + y)^p = x^p + y^p$$

$$(x + y)^p = \sum_{i=0}^{p} C_p^i x^i y^{p-1}; C_p^i = \frac{p!}{i!(p-i)!} \equiv 0 \mod p, 0 < i < p$$