Евгений Борисович Фейгин

evgfeig@hse.ru

https://sites.google.com/view/algebra1-2020

Оценка: 0,2 ДЗ + 0,2 КР + 0,2 коллоквиум + 0,4 Экзамен

Учебники: Э. Б. Винберг „Курс Алгебры"

А. Л. Городенцов „Алгебра для ст. мат."

Делимость, алгоритм Евклида, НОД, разложение на пр. мн.

$\mathbb{Z}$ - мн-во целых чисел

$\mathbb{N}$ - мн-во натуральных чисел

Операции сложение, вычитание, деление и умножение

- $\mathbb{Z}$ и $\mathbb{N}$ замкнуты отн. слож. и умнож.
- $\mathbb{Z}$ замкнуто отн. вычитания

Элемент a обратим, если найдётся b, т.ч. $a \cdot b = 1$

Пример: в $\mathbb{N}$ обр. только 1, в $\mathbb{Z}$ ± 1.

Операции сложение и умножение коммутативные

- делить (вообще говоря) нельзя ни в $\mathbb{Z}$, ни в $\mathbb{N}$

Деление с остатком: $a, b \in \mathbb{Z}$, $b \neq 0$

$a = qb + r$, $|r| < |b|$ $\longrightarrow$

Будем считать, что $r \geq 0$

Обозначение $a \vdots b$, если $a = bq$

$b \mid a$, если $a = qb$

b делит a

Опр. Число p называется простым, если p не обратимо и из равенства $p = uv$ следует, что u или v обратимы

<u>Замечание</u>. Такой „проблемы" для $\mathbb{N}$ нет, т.к. там обратима лишь 1. $(-5 = (-1)\cdot 5 = 1\cdot(-1)\cdot 5$ и т.д.$)$

Опр. Пусть $a, b \in \mathbb{Z}$, тогда НОД(a, b) - такой делитель a и b, что он делится на любой другой общий делитель. $(a, b) \neq (0, 0)$

<u>Предложение</u> • НОД (a, b) существует.

• НОД $(a, b) = au + bv$ для некоторых целых u, v

Пример $b = 0$, $a \neq 0$, НОД $= a = a\cdot 1 + b\cdot ?$

$b \neq 0$, $b \mid a$, НОД$(a, b) = b = a\cdot b + b\cdot 1$

<u>Док-во</u>: 1) Будем считать, что $b \neq 0$ и $b \nmid a$

Поделим a на b с остатком

$a = b\cdot q_1 + r_1$, $|r_1| < |b|$

$b = r_1 q_2 + r_2$, $|r_2| < |r_1|$

$r_1 = r_2 \cdot q_3 + r_3, \quad |r_3| < |r_2|$

...

$r_{n-2} = r_{n-1} \cdot q_n + r_n, \quad |r_n| < |r_{n+1}|$

$r_{n-1} = r_n q_{n+1}, \quad r_{n+1} = 0$

покажем, что $r_n = НОД(a, b)$

- $r_{n-1} \vdots r_n$

$\Downarrow$

- $r_{n-2} \vdots r_n$

$\Downarrow$

- $r_{n-3} \vdots r_n$

по индукции: $b \vdots r_n$

Т.о. r_n действительно общий делитель a и b.

2) Хотим проверить, что $\exists\, u, v$, такие что $r_n = au + bv$

$r_1 = a - bq_1 := \underset{1}{au_1} + \underset{-q_1}{bv_1}$

$r_2 = b - r_1 \cdot q_2 = b - (au_1 + bv_1) q_2 = bv_2 + au_2$

...

$r_n = au_n + bv_n$

Т.о. мы доказали сущ. u и v, т.к. $r_n = au + bv$

3) Осталось проверить, что если d - общ. дел. a и b, то $d \mid r_n$

Мы знаем, что $r_n = au + bv \Rightarrow$ если $d \mid a$, $d \mid b \Rightarrow$ $d \mid au + bv$, т.е $d \mid r_n$

$| \ |$ "модуль": $\mathbb{Z} \to \mathbb{N} \cup \{0\}$, $|ab| = |a| \cdot |b|$

<u>Обозначение</u> Два числа a и b - вз. простые, если их НОД $= 1$.

НОД$(a, b) = (a, b)$ обозн.

Процесс постепенного деления с остатком наз-ся ал-тм Евклида

- Поиск НОД двух чисел
- Док-во того, что $(a, b) = au + bv$
- Разложение числа на простые мн-ли

Основная теорема арифметики.

Любое число может быть разложено в произведение простых и это разложение единственно с точностью до перестановки сомножителей.

Замечание: верно для нат. чисел. Для целых нужно оговаривать возможность умножения на обратные.

Лемма. Пусть p-простое число (т.е. $p=ab \Rightarrow$ ~~либо~~ a, ~~либо~~ или b обратим)

Пусть $p \mid a_1 \dots a_k$. Тогда $\exists i : p \mid a_i$

$\square$ Случай $k=2$: $p \mid a_1 a_2$, $p \nmid a_1$. Тогда

$\text{НОД}(p, a_1) = 1 \Rightarrow pu + a_1 v = 1$

$$\underline{pu a_2} + \underline{\underline{a_1 a_2 v}} = a_2 \Rightarrow a_2 \vdots p.$$

Общий случай $p \mid a_1 (a_2 \dots a_k)$ по индукции по k $\blacksquare$

Док-во теоремы: Пусть дано число n. Если n-простое, то всё, иначе $n = n_1 \cdot n_2$ и $|n_1| < n$, $|n_2| < n$. Т.о получим разложение.

Пусть есть 2 разложения:

$$p_1 \dots p_n = q_1 \dots q_m \qquad p_i,\ q_j \text{ - простые}$$

В частности $p_1 \mid q_1 \dots q_m$

$\exists i \;\; p_1 \mid q_i \Rightarrow p_1 = q_i$, сократим и уменьшим кол-во сомножителей. Далее по индукции.

<u>Следствие</u>: $a = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$, $a \vdots d \Rightarrow d = p_1^{l_1} \cdot \ldots \cdot p_s^{l_s}$

$l_i \leq k_i$

$\square$ $a = d \cdot x$ и разложение на простые в левой и правой части одинаковы $\blacksquare$

Кольцо: множество K с двумя бинарными операциями $+$ и $\times$ со след. свойствами:

1. $a + b = b + a$ ком.
2. $(a+b)+c = a+(b+c)$ ас.
3. $\forall a \in K \ \exists -a : a + (-a) = 0$
4. $\exists 0 : a + 0 = a \ \forall a$
5. $a(b+c) = ab + ac$ дист.

   $(b+c)a = ba + ca$

Кольцо называется целостным, если умн. коммут., ассоц., есть 1 и нет делителей 0.

пример. $K = 2\mathbb{Z}$ - кольцо без 1.

Элемент a кольца K называется делителем нуля, если $a \neq 0$ и $\exists b \neq$, т.ч. $ab = 0$

пример: кольцо вычетов.

Пусть $n \in \mathbb{N}_{\geq 2}$, $n = 2, 3, ..$

Кольцо вычетов $\mathbb{Z}/_{n\mathbb{Z}}$ состоит из эл. $[0]_n, \dots, [n-1]_n$

Слож умножение опр. формулами

$[a]_n + [b]_n = [a + b \mod n]_n$

$[a]_n \cdot [b]_n = [ab \mod n]_n$

Утв. Это кольцо $\square$ коммут., ассоц. и дистр. следуют из аналогичных свойств для $\mathbb{Z}$

$0 = [0]_n$, $-[a]_n = [n-a]_n$ $\boxtimes$

Легко проверить, что у делителей нуля нет обратных.

заметим $\underbrace{[1]_n + \ldots + [1]_n}_{n} = 0$

Пусть K - некоторое кольцо, пусть x - переменная

Определим $K[x] = \{a_0 + a_1 x + \ldots + a_s x^s,\ a_i \in K,\ s = 0, 1, \ldots\}$

$$a_0 + a_1 x + \ldots + a_s x^s + b_0 + b_1 x + \ldots + b_k x^k =$$

$$= \sum_{i \geq 0} (a_i + b_i) x^i, \text{ где } a_i = 0,\ i > s$$
$$b_i = 0,\ i > k$$

$$\sum_{i=0}^{s} a_i x^i \cdot \sum_{j=0}^{k} b_j x^j = \sum_{l=0}^{k+s} x^l \sum_{i+j=l} a_i b_j$$

Утв. $K[x]$ - кольцо

Утв. Если K - целостное, то $K[x]$ тоже.

Док-во $a(x) = a_0 + a_1 x + \ldots + a_n x^n$ $a_n \neq 0$

$$b(x) = b_0 + \ldots\ b_m x^m$$

$$a(x) b(x) = a_0 b_0 + \ldots + a_n b_m x^{n+m}$$

$\neq 0$, т.к. K-целостн

Пример $K[x_1, x_2] = (K[x_1])[x_2]$

Опр. целостное кольцо K называется Евклидовым, если K снабжено функцией $N : K \setminus \{0\} \to \mathbb{N} \cup \{0\}$, т.ч. 1. $N(ab) \geq N(a)$ и равенство дост. для обратимых b

2. $\forall a, b \in K \setminus \{0\}$

$\exists q, r$, т.ч. $a = bq + r$ и

$N(r) < N(b)$

Утв. ~~K-целостное~~ $\mathbb{Q}[x]$ - евклидово кольцо

Док-во: $N(ab) \geq N(a)$, где $N = \deg a(x)$

$$a(x) = a_0 + a_1 x + \ldots + a_k x^k$$

$$k \geq m$$

$$b(x) = b_0 + \ldots + b_m x^m$$

$$a(x) - b(x) \cdot \frac{a_k}{b_m} x^{k-m} = a_0' + a_1' x + \ldots + a_{k-1}' x^{k-1}$$

у разности ст. понизилось

Мы можем продолжать эту процедуру пока степень результата не $< m$.

Абелева группа

Мн-во A с одной операцией $+$ со след. свойствами

1) $a+b = b+a$, $a, b \in A$ 2) $a+(b+c) = (a+b)+c$, $a, b, c \in A$

3) $a+0 = a$ $\exists 0 \in A$ $\forall a$ 4) $\forall a \in A$ $\exists -a$: $a+(-a) = 0$

Замечание. Если операция названа $+$ $\Rightarrow$ „аддитивный вариант", иногда удобно называть операцию умножением, тогда это мультипликативный вариант. $0 \rightsquigarrow 1$, $-a \rightsquigarrow a^{-1}$

Замечание. В опр. кольца заложено понятие аб. группы по сложению

Ал 2.3. / Ал.3.1.

Опр. Поле - коммутативно, ассоциативное кольцо с единицей, у любого ненулевого элемента есть обратный по умножению.

Замечание Отсутствие делителей нуля НЕ гарантирует того, что кольцо не поле.

Опр. подгруппа B в абелевой группе A - это подмножество замкнутое относительно сложения, такое что $0 \in B$, $\forall b \in B$ $-b \in B$, т.е. тоже группа

Замечание в поле $0 \neq 1$.

Опр. подкольцо L в кольце K - подгруппа относ. сложения, т.ч. $\forall x, y \in L : x \cdot y \in L$

Опр. подполе L в поле K - подкольцо, т.ч. $1 \in L$, $\forall a \in L \setminus 0$ $a^{-1} \in L$

Поле комплексных чисел

Опр. Множество $\mathbb{C} = \{a + bi, a, b \in \mathbb{R}\}$
$= \{(a, b), a, b \in \mathbb{R}\}$

- $a + bi + c + di = a + c + (b + d)i$
- $(a + bi)(c + di) = ac - bd + (ad + bc)i$

$i \cdot i = -1$

Теорема $\mathbb{C}$-поле

□ $\mathbb{C}$ - аб. группа по сложению ✓

дистрибутивность умножения отн. сложения.

$\exists$ обратный элемент $(a+bi)\left(\frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}\right)=1$

$$a^2+b^2 \neq 0$$

$0+0i$ - нулевой

$1+0\cdot i$ - единица ■

$z = a+bi \in \mathbb{C}$ $\quad a = \operatorname{Re} z \to$ вещ.

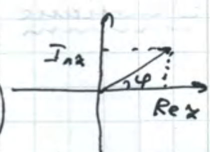
$b = \operatorname{Im} z \to$ мнимая

Опр. $|z| = \sqrt{a^2+b^2} = \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2}$

$\operatorname{Arg} z$ - угол между z и OX.

$= \{\varphi + 2\pi k,\ k \in \mathbb{Z}\}$ $\quad 0 \leq \arg z < 2\pi$.

Тригонометрическая запись числа:



$z = \operatorname{Re} z + i \operatorname{Im} z = |z|(\cos\varphi + i\sin\varphi)$

Утв. $|z_1 z_2| = |z_1||z_2|$, $\operatorname{Arg}(z_1 z_2) = \operatorname{Arg} z_1 + \operatorname{Arg} z_2$

$r_1(\cos\varphi_1 + i\sin\varphi_1)\cdot r_2(\cos\varphi_2 + i\sin\varphi_2) =$

$= r_1 r_2(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2))$

$z_1/z_2 = \frac{r_1}{r_2}(\cos(\varphi_1-\varphi_2) + i\sin(\varphi_1-\varphi_2))$

Ал.3.2

Формула Муавра

$$z^n = |z|^n (\cos n \arg z + i \sin n \arg z)$$

Автоморфизм поля K: взаимно одн. отобр. $f: K \to K$, т.ч. $f(0) = 0$, $f(1) = 1$, $f(ab) = f(a) \cdot f(b)$ и $f(a+b) = f(a) + f(b)$

Автоморфизм абелевой группы и кольца опр. аналогично.

Утв. У $\mathbb{C}$ имеется автоморфизм сопряжение:

$$z \to \bar{z}$$

$$a+ib \qquad a-ib$$

Замечание рассмотрим в $\mathbb{C}$ z: $z = \bar{z}$. Т.е.

$z = a + 0 \cdot i$ – подполе $\mathbb{R} \subset \mathbb{C}$

Замечание $\overline{z + \bar{z}} = \bar{z} + \bar{\bar{z}} = \bar{z} + z \Rightarrow$

$$z + \bar{z} \in \mathbb{R}$$

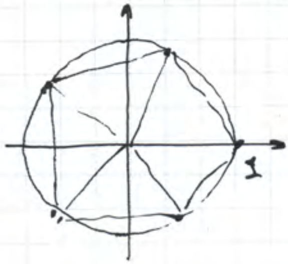
$$\overline{z\bar{z}} = \bar{z} \cdot \bar{\bar{z}} = \bar{z} z \in \mathbb{R}$$

Рассмотрим ур-е

$z^n = 1$. Т.к. $|1| = 1$, то $|z^n| = |z|^n = 1$
$\Rightarrow |z| = 1$

$(\cos\varphi + i\sin\varphi)^n = \cos n\varphi + i\sin n\varphi = 1$, т.к. $\varphi = \frac{2\pi k}{n}$

Правильный n-угольник $k = 0, \dots, n-1$



Замечание

z_1, z_2 - корни ур-е $z^n = 1$,

то $z_1 z_2$ - тоже

Кроме того 1 - корень n-ой степени. Т.о. корни n степени из 1 образуют абелеву группу C_n по умножению.

Замечание $\mathbb{Z}/n\mathbb{Z}$ - кольцо вычетов по модулю n,

изоморфна
C_n совпадает с $\mathbb{Z}/n\mathbb{Z}$ как абелева группа

$$\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} \sim [k]_n$$

"ζ_k" $\quad C_n$ абелева $\quad \mathbb{Z}/n\mathbb{Z}$

Опр. Две группы A и B наз-ся изоморфными, если $\exists$ взаимно однозн. отобр. $f: A \to B$, т.ч. $f(a * b) = f(a) * f(b)$ и нейтр. эл-т переходит в нейтральный.

Замечание $\zeta_k = \zeta_1^k$

Ал. 3.3.

Опр. Корень n-ой степени из единицы наз-ся первообр., если любой другой корень можно получить как степень нашего.

$z^n = 1$, то $z^{-1} = z^{n-1}$

Пример $n=4$ ξ_1, ξ_3 - перв.

ξ_2, ξ_0 - не перв.

$n=5$ все кроме ξ_0 перв.

Пусть n - фиксировано

$\xi_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$ Когда ξ_k явл. первообр. корн.?

тогда и только тогда когда $(k, n) = 1$.

☐ Пусть $(k,n) \neq 1$.
$= a$.

Тогда $(\xi_k)^m = \cos\frac{2\pi km}{n} + i\sin\frac{2\pi km}{n}$

$km \bmod n$ делится на a при любом m.

Т.о. $\xi_1 \neq \xi_k^m$ ни при каком m.

Пусть $(k, n) = 1$.

$ak + bn = 1 \Rightarrow \xi_k^a = \xi_{ak} = \cos\frac{2\pi ak}{n} + i\sin\frac{2\pi ak}{n} =$

$= \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} = \xi_1$

Тогда $\forall s\ \xi_s = \xi_1^{\,s} = (\xi_k^{\,a})^s$, т.е. ξ_k - первообр. корень

Замечание $n=4$, $\xi_1 \cdot \xi_3 = 1$, ~~поэтому произв.~~

т.е. первообр. корни не замкнуто отн. умножения.

индуцированного операция - операция на классах экв.

Отображение проекции (факторизации)

$\pi: M \to M/_R$, $a \mapsto R(a)$

Утв. π - сюръекция, $\pi^{-1}(x) = \{a \in M, a \sim x\}$

Теорема $\mathbb{Z}/_{n\mathbb{Z}}$ является полем $\Leftrightarrow$ n простое.

$\square$ • пусть n не простое $\Rightarrow$ $n = n_1 \cdot n_2$ и

$[n_1]_n \cdot [n_2]_n = [n]_n = 0$

• пусть n простое, ~~так~~ $m - 1, \dots, n-1 \Rightarrow$

$(m, n) = 1. \Rightarrow \exists u, v: mu + nv = 1 \Rightarrow$

$mu = 1 \pmod n$

Замечание: в кольце $\mathbb{Z}/_{n\mathbb{Z}}$ $\underbrace{[1] + \ldots + [1]}_{n} = 0$

Опр. пусть k-поле

тогда характеристика k ($\operatorname{char} k$)

наим. число p, т.ч. $\underbrace{1 + \ldots + 1}_{p} = 0$

Ал. ч. 1.

$\operatorname{char} \mathbb{Z}/_{n\mathbb{Z}} = n$ (n-простое)

<u>Ут.в.</u> Пусть k-поле, тогда $\operatorname{char} k$ - простое число или 0.

$\square$ Пусть $\operatorname{char} k = n \overset{\neq 0}{}$ - составное, т.е $n = n_1 n_2$

Тогда $\underbrace{1 + \ldots + 1}_{n} = \underbrace{(1 + \ldots + 1)}_{n_1} \cdot \underbrace{(1 + \ldots + 1)}_{n_2} \Rightarrow$

в k есть делители нуля $\Rightarrow$ k не поле. $\blacksquare$

Евклидово кольцо - целостное кольцо K с функцией нормы $N: K \setminus 0 \to \mathbb{Z}_{\geq 0}$, т.ч.

- $N(ab) \geq N(a)$ и равенство имеет место только для обратимых b
- $\forall a, b \in K, b \neq 0 \ \exists q, r \in K$ т.ч. $a = bq + r$, $N(r) < N(b)$

$F[x]$ - евклидово кольцо

$\square$ $F[x]$ - целостн. кольцо
ком., ассоц., $\exists 1$, нет дел. 0.

$N(f)$ - степень f

нужно проверить 2 свойства нормы

$\deg(f(x) g(x)) \geq \deg f(x)$

причём $\deg(f(x) g(x)) = \deg f(x) \Leftrightarrow$

$\Leftrightarrow \deg(g) = 0 \Leftrightarrow g = g_0 \Rightarrow g$ обратим

Деление с остатком: $f(x) = f_0 + \ldots + f_n(x^n)$

$$g(x) = g_0 + \ldots + g_m x^m$$

$$f(x) - g(x) \frac{f_n}{g_m} x^{n-m}$$

Таким образом степень уменьшается

$$f(x) = g(x)\, q(x) + r(x), \quad \deg \cancel{}\, r < \deg g$$

Следствие $f(x) = (x-c)\, q(x) + r \Rightarrow f(c) = r$, $c \in F$, $r \in F$

Многочлен $f(x) \in F[x]$ Теорема Безу

не может иметь в F больше,

чем $\deg f$ корней (попарно разл.)

Док-во Если q - корень, то $f = (x - c_1) f_1$

Если $c_1 \neq c_2$ - корень f, то $f(c_2) = (c_2 - c_1) f_1(c_2)$

$f_1(c_2) = 0 \Rightarrow f(x) = (x - c_1)(x - c_2) f_2(x)$.

Продолжаем с каждым след. новым корнем

$f(x) = (x - c_1) \ldots (x - c_m) f_m(x)$ $c_j \neq c_i$;

$\deg f_m \geq 0 \Rightarrow \deg f \geq m$

Пусть F - беск. поле. Тогда разные мн-ны определяют разные функции. Другими словами, отобр.
$F[x] \to F^F$ явл. инъект.

□ Если $f(x) \neq g(x)$, то $\deg(f(x)-g(x)) \geq 0$

Тогда кол-во корней $f(x)-g(x)$ не больше, чем $\deg(f(x)-g(x))$. Но в F бесконечное кол-во эл-тов $\Rightarrow$ все они не могут быть корнями $f(x)-g(x)$

$K[x]$ - кольцо многочленов

$\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}[x]$

$$k[x] = \{a_0 + a_1 x + \ldots + a_n x^n\}$$
$n \geq 0$, $a_i \in k$

Замечание: кольцо формальных степенных рядов (ряды Тейлора)

$$K[[x]] = \{a_0 + a_1 x + \ldots +, \ a_i \in K\}$$ - кольцо отн. естественных операций

Ряды Лорана

$$k((a)) = \{a_{-N} x^{-N} + a_{-N+1} x^{-N+1} + \ldots, N \in \mathbb{Z}, a_i \in k\}$$

$K[x]$, считаем, что k-поле

$K[x]$ - Евклидово кольцо, $N(f) = \deg f$

Обратимы ненулевые константы. для поля

для произв. кольца - все обратимые эл. кольца.

Опр. неприводимый многочлен - это простой элемент в кольце $K[x]$. Т.о. f неприводим

$f = g_1 g_2 \Rightarrow \deg g_1 = 0$ или $\deg g_2 = 0$

Факториальное кольцо — кольцо, в котором любой элемент может быть разложен в конечное произв. простых, причём это разложение единственно с точностью до перестановки сомножителей и домножения на обратимый элемент.

Евклидово кольцо является факториальным

□ • Разложение $\exists$, т.к., если $x \in K$ непрост, то $x = x_1 \cdot x_2$, $x_1 x_2$ не обр. уменьшаем норму $\Rightarrow$
$N(x) > N(x_1)$, $N(x) > N(x_2) \Rightarrow$ будет конец

• Единственность: $p_1 \cdot \ldots \cdot p_s = q_1 \cdot \ldots \cdot q_r$

Линейное представление НОД позволяет док-ть лемму: $ab \vdots q$ ← простое, $(a, q) = 1 \Rightarrow b \vdots q$

↑ кольцо факториально ☒

Следствие. $K[x]$ - факториально.

Пример. $f \in K[x]$, $\deg f = 3$, f-неприводим $\Rightarrow$ у f нет корней!

$f = g_1 \cdot g_2$, $\deg g_1 = 1$, $\deg g_2 = 2$ $\Rightarrow g_1 = x - c$,

т.е. c-корень

Класс эквивалентности обозн $\bar{x}$ или $[x]$

Рассмотрим $k[x]$ и $f \in k[x]$. Тогда
$k[x]/f$ – кольцо, соотв. отношению экв.
$R = \{(a, b) : a - b \vdots f\}$

Классы экв. состоят из многочленов вида
$a(x) + f(x)\, q(x)$

Отношение экв. R_f согласовано с умножением и сложением.

Все элементы $k[x]/f$ имеют вид $[a_0 + a_1 x + \dots + a_n x^n]_f$ для некоторых $a_i \in k$, причём все такие эл. различны

$\square$ Если $g(x)$ – произвольный многочлен, то
$g(x) = f(x)\, q(x) + r(x)$, где $\deg r < n \Rightarrow$
класс $[g(x)]_f = [r(x)]_f \Rightarrow$ любой класс экв. содержит многочлен степени не более $n-1$ $\boxtimes$

$\alpha = [x]_f \in k[x]/(f)$

$$f([x]) =$$
$$= f_0 + f_1 [x] + f_2 [x]^2 + \dots + f_n [x]^n =$$
$$= [f_0 + f_1 x + \dots + f_n x^n] = [f(x)] = 0$$

Ал.5.2

Тогда для $\forall g(x)$ в кольце $K[x]/_f$ вып. равенство

$g(\alpha) = [g(x)]$

Опр. K_1 и K_2 - кольца. Тогда $K_1 \overset{\text{изоморфны}}{\cong} K_2$, если $\exists$ биекция φ: $\varphi(a+b) = \varphi(a) + \varphi(b)$
$\varphi(ab) = \varphi(a)\varphi(b)$

Пример. $\mathbb{R}[x]/_{(x^2+1)} \cong \mathbb{C}$

$$[ax+b] \to ai + b$$

$[x^2] = -1$

$i^2 = -1$

Теорема $K[x]/_{(f)}$ - поле $\Leftrightarrow$ f-неприводимый в $K[x]$.

□ • Пусть f-приводим $\Rightarrow$

$$f = g_1 \cdot g_2, \quad \deg g_1 < \deg f, \quad \deg g_2 < \deg f$$

$[g_i]_f \neq 0$ и $[g_1]_f [g_2]_f = [f]_f = 0 \Rightarrow$

$\exists$ делители 0.

• Пусть f- неприводим. $K[x]/_{(f)}$ - поле.

Необходимо проверить $\exists$ обратного эл.

$\exists u, v : gu + fv = 1$, т.к. нод$(g, f) = 1$. $\Rightarrow$

$[gu]_f = [1]_f$

Мы знаем, что f-неприводим $\Rightarrow$ нет делителей положительной степени кроме $f(x)\cdot \mathrm{const}$.

f неприводим $\Leftrightarrow$ в $k[x]/_{(f)}$ нет дел. нуля.

$\square$ • f приводим $\Leftrightarrow \exists\, g_1, g_2,\ \deg g_i > 0$

$$g_1 \cdot g_2 = f \Rightarrow [g_1]_f [g_2]_f = 0$$

в $k[x]/_{(f)}$

• f неприводим и $\exists\, g_1, g_2 \in k[x]$

$$[g_1]_f [g_2]_f = 0 \Leftrightarrow$$

$$g_1 g_2 = fh$$

В правой части присутствует простой эл. факториального кольца $k[x] \Rightarrow$ либо $g_1 \vdots f$, либо $g_2 \vdots f \Rightarrow [g_i]_f = 0$ ■

Пример 1. $\mathbb{Q}[x]/_{x^2-2} \simeq \mathbb{Q}(\sqrt{2})$

Пример 2. $k = \mathbb{F}_p = \mathbb{Z}/_{p\mathbb{Z}}$, p-простое $\Rightarrow k$-поле

$f \in k[x]$ - многочлен степени n. $\rightsquigarrow k[x]/_{(f)}$ кольцо, состоящее из p^n эл.

Следствие: Если $\exists$ неприводимый (над $\mathbb{F}_p$) многочлен степени n, то мы построим поле из p^n элементов.

Ал. 6.1.

$\forall n$ $\exists$ неприводимый многочлен степени n над $\mathbb{F}_p$, все полученные таким образом поля из p^n эл. изоморфны

Китайская теорема об остатках.

классика: • даны натуральные числа

$n_1, \ldots, n_k$ такие, что

их НОД = 1

• даны остатки

$r_1, \ldots, r_k$, т.ч. $0 \le r_i < n_i$ $\forall i = 1$

• Тогда: • $\exists R \in \mathbb{Z}_{\ge 0}$ $R \equiv r_i \pmod{n_i}$

$i = 1, \ldots, k$.

• Если R_1 и R_2 удовл. вышепер. свойству

то $R_1 - R_2 \,\vdots\, n_1 \cdot \ldots \cdot n_k$

Алгебраическая формулировка:

Пусть $n_1, \ldots, n_k \in \mathbb{N}$: $(n_i, n_j) = 1$.

Тогда $\mathbb{Z}/_{n_1 \ldots n_k \mathbb{Z}} \simeq \bigtimes_{i=1}^{k} \mathbb{Z}/_{n_i \mathbb{Z}}$ как кольца

$[a] \mapsto (a \bmod n_1, \ldots, a \bmod n_k)$

Док-во: Заметим, что $\varphi(a+b) = \varphi(a)+\varphi(b)$

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

$$\forall a, b \in \mathbb{Z}/_{n_1 \cdots n_k}\mathbb{Z}$$

Нужно проверить инъективность и сюрь. φ

Действительно, если $\varphi(a_1) = \varphi(a_2) \Leftrightarrow$

$$a_1 \bmod n_i = a_2 \bmod n_i$$

$$\forall i = 1, \dots, k$$

$$a_1 - a_2 \vdots n_1 \cdot \ldots \cdot n_k \Rightarrow a_1 = a_2 \text{ в } \mathbb{Z}/_{n_1 \dots n_k}\mathbb{Z}$$

Сюрьект. следует из равенства мощностей $\square$

КТО для многочленов

k - поле, $f_1, \dots, f_k \in k[x]$, $(f_i, f_j) = 1$.

Тогда $k[x]/_{(f_1 \dots f_k)} \overset{\varphi}{\simeq} \prod\limits_{i=1}^{k} k[x]/_{(f_i)}$

$$\varphi([g]) = ([g]_{f_1}, \dots, [g]_{f_k})$$

Док-во: отображение φ - гомоморфизм колец, т.е. $\varphi(ab) = \varphi(a)\varphi(b)$

Инъективность $\varphi([g_1]) = \varphi([g_2]) \Leftrightarrow$ $\varphi(a+b) = \varphi(a)+\varphi(b)$

$$g_1 - g_2 \vdots f_i \; i \in 1, \dots, k$$

$$[g_1] = [g_2]$$

Ал.6.2

Сюръективность: пусть даны многочлены $r_1(x) \dots r_k(x)$

$$\deg r_i(x) < \deg f_i(x)$$

Определим $F_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^{k} f_j(x) \quad i = 1, \dots, k$

Мы знаем, что $(f_i, F_i) = 1$

$$\exists u_i, \ v_i : u_i f_i + v_i F_i = 1.$$

$$v_i F_i \equiv 1 \mod f_i$$

$$R = r_1 V_1 F_1 + r_2 V_2 F_2 + \dots + r_k V_k F_k$$

$$[R]_{f_j} = [r_j V_j F_j]_{f_j} = r_j \qquad \square$$

Док-во работает для $\forall$ евклидовых колец

В частности для целых чисел

Это док-во эффективно, т.е. с помощью Алгоритма Евклида можно явно решать систему

$$[R]_{f_1} = [r_1]_{f_1} \text{ и т.д.}$$

Группа - мн-во с одной операцией $*$ такой что

- $a*(b*c)=(a*b)*c$; • $\exists e$ т.ч. $a*e=e*a=a$ $\forall a\in G$
- $a*a^{-1}=a^{-1}*a=e$

Замечание: Как называть операцию неважно, но обычно операцию называют умножение. Если выполняется коммутативность, то часто называют сложением

Для умножения $e\sim 1$, для сложения $e\sim 0$

Опр. Абелева группа - группа, для которой операция коммутативно.

Если F-поле, то $\mathbb{F}\setminus 0=\mathbb{F}^*$ - группа по умножению (мультипликативная группа поля)

Пример: $\mathbb{Z}/n\mathbb{Z}$ - циклическая группа (по сложению, т.е аддитивная запись)

Группа преобразований мн-ва M: все вз-одн. отображения $M\to M$

Операция - композиция, e - тождественное от-е. $M\xrightarrow{id}M$

Если $|M|=n$, то такая группа наз-ся группой перестановок обозначается S_n

Опр. Гомоморфизм групп - отображение $\varphi: A \to B$,

т.ч. $\varphi(e) = e$, $\varphi(a_1 * a_2) = \varphi(a_1) * \varphi(a_2)$

Опр. Пусть $\varphi: A \to B$ - гомоморфизм абелевых групп.

Тогда $\ker\varphi = \{a \in A : \varphi(a) = 0\}$ - ядро φ.

Св-ва: • $\ker\varphi$ - подгруппа: если $a_1 \in \ker\varphi$, $a_2 \in \ker\varphi$, то

$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2) = 0$

• Пусть $b \in B$. Тогда либо $\varphi^{-1}(b) = \varnothing$,

либо $\varphi^{-1}(b) = a + \ker\varphi = \{a + a', a' \in \ker\varphi\}$

$\square$ пусть $\varphi(b)^{-1} = a$. Тогда $\varphi(a_1) = b \Leftrightarrow$

$\varphi(a_1) = \varphi(a) \Leftrightarrow \varphi(a_1 - a) = 0 \Leftrightarrow$

$a_1 - a \in \ker\varphi$ $\blacksquare$

Следствие: $\ker\varphi = 0 \Leftrightarrow \varphi$ - вложение (инъекция)

Замечание Пусть A и B - две группы. Обозначим через

$\mathrm{Hom}(A,B)$ множество всех гомоморфизмов $A \to B$.

Тогда $\mathrm{Hom}(A,B)$ обладает структурой группы.

$(\varphi_1 + \varphi_2)(a) = \varphi_1(a) + \varphi_2(a)$

Нейтральный: $\varphi(a) = 0$

Противоположный: $(-\varphi)(a) = -\varphi(a)$

Опр. Порядок элемента a в группе A - мин. число k такое, что если применить операцию к элементу a $k-1$ раз, то получим нейтральный эл-т. Обозн $\operatorname{ord}(a)$

Опр. $\varphi: A \to B$ - гомом. $\operatorname{Im}\varphi = \{b \in B : \exists a \in A \ \varphi(a) = b\}$

Замечание $\operatorname{Im}\varphi$ - подгруппа B.

$$\varphi(e) = e, \ \varphi(a^{-1}) = \varphi(a)^{-1}, \ \varphi(a * b) = \varphi(a) * \varphi(b)$$

Опр. Пусть $A_1 \ldots A_k$ - группы. Тогда прямое произведение $A_1 \times \ldots \times A_k$ - группа, состоящая из элементов $(a_1, \ldots, a_k)$ $a_i \in A_i$.

Пусть k_1 k_2 - кольца $\varphi: k_1 \to k_2$ - гомоморфизм. Тогда φ - гомоморфизм абелевых групп по сложению. В частности, φ - инъекция $\Rightarrow \ker\varphi = 0$

Замечание $\varphi: k_1 \to k_2$, тогда $\varphi(1) = 1$ не всегда.

Утв. Пусть $\varphi: k_1 \to k_2$ - гомоморфизм колец, положим k_1 - целостное. Тогда либо $\varphi = 0$, либо $\varphi(1) = 1$.

$\square$ $\varphi(1 \cdot 1) = \varphi(1)\varphi(1) \Rightarrow \varphi(1)(\varphi(1) - 1) = 0$

Ал. 7.2.

т.к. K_2 - целостное, то либо $\varphi(1)=0$, либо $\varphi(1)=1$.

Если $\varphi(1)=0$, то $\forall a \in K_1$ $\varphi(a)=\varphi(a\cdot 1)=0$.

$\mathbb{F}$ - поле, $\mathbb{F}^* = \mathbb{F}\setminus\{0\}$ - мультиплик. группа поля (по умножению)

Теорема. Пусть $A \subset \mathbb{F}^*$ - произвольная конечная подгруппа. Тогда A - циклическая.

Лемма. Пусть A - коммутативная группа, $b_1, b_2 \in A$, т.ч. $\operatorname{ord} b_1 = m_1$, $\operatorname{ord} b_2 = m_2$ $(m_1, m_2)=1$. Тогда $\operatorname{ord}(b_1 b_2) = m_1 m_2$

$\square$ $(b_1 b_2)^s = e \Rightarrow s \vdots m_1$?

$b_1^s = b_2^{-s}$ $\qquad \operatorname{ord} b^{-1} = \operatorname{ord} b$, т.к. $b^k = 1 \Leftrightarrow$

$\Downarrow$

$b_1^{sm_2} = b_2^{-sm_2} = e$ $\qquad (b^k)^{-1} = 1 \Leftrightarrow (b^{-1})^k = 1$.

$\Downarrow$

$sm_2 \vdots m_1$

$\Downarrow$

$s \vdots m_1$. Аналогично $s \vdots m_2 \Rightarrow s = m_1 m_2$

$\blacksquare$

Док-во теоремы

Для того, чтобы доказать, что группа цикл., достаточно проверить, что если m - max порядок элементов из A, то m делится на порядок любого другого элемента

$a \in A$, $ord(a)$, $m = \max\limits_{a \in A} ord(a)$

Если $ord\, a \mid m$ $\forall a \in A$, то $a^m = 1$ $\forall a \in A$.

$x^m - 1 = 0$ - все эл. A являются корнем $\Rightarrow m \geq |A|$

Пусть $|A| = n$. Пусть $m = \max\limits_{a \in A} \{ord\, a\}$. Хотим доказать, что $m = n$. Достаточно проверить, что $\forall a \in A$ $ord\, a \mid m$. Действительно, в этом случае многочлен $x^m - 1|_A = 0$, но у этого мн-на не больше m различных корней $\Rightarrow n \leq m$

Пусть a_1 и a_2 - эл. A, т.ч. $ord\, a_1 = m_1$, $ord\, a_2 = m_2$

Нам достаточно предъявить a_3 из A такой что $ord\, a_3 = \text{НОК}(m_1, m_2)$

Например, если $(m_1, m_2) = 1$, то подойдёт $a_3 = a_1 a_2$.

Общий случай: $m_1 = p_1^{u_1} p_2^{u_2} \ldots p_s^{u_s}$ $\quad$ p_i - попарно разл. прост. $u_i, v_i \in \mathbb{Z}_{\geq 0}$

$m_2 = p_1^{v_1} p_2^{v_2} \ldots p_s^{v_s}$

$l_1 = \prod\limits_{i : v_i \leq u_i} p_i^{u_i}$ $\qquad$ $l_2 = \prod\limits_{i : u_i \leq v_i} p_i^{v_i}$

Получаем: $m_1 = l_1 k_1$, $m_2 = l_2 \cdot k_2$

$(l_1, l_2) = 1$

Ал.8.1.

НОК $(m_1, m_2) = l_1 l_2$.

$a_3 = a_1^{k_1} a_2^{k_2}$ порядок $l_1 l_2 =$ НОК (m_1, m_2)

Действительно, $ord\, a_1^{k_1} = l_1$, $ord\, a_2^{k_2} = l_2$, $(l_1, l_2) = 1 \Rightarrow$

$ord\, a_3 = l_1 l_2$

Примеры циклич. $\mathbb{Z}$ по сложению, $\mathbb{Z}/n\mathbb{Z}$ по сложе.

Замечание: любая циклическая группа изоморфна

$\mathbb{Z}$ или $\mathbb{Z}/n\mathbb{Z}$

Пример: пусть K - конечное поле. Тогда K^* циклична

(мультипликативная группа поля)

Пример Группа S_n-перестановки n-элементов, то

есть $S_n = \{ f : \{1, \dots, n\} \to \{1, \dots, n\} \}$

Является ли S_n циклической?

Порядок

$$n = 3: \quad \overset{1}{e}, \ \overset{2}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}}, \ \overset{2}{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}}, \ \overset{3}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}$$

$$\overset{2}{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}} \quad \overset{3}{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}}$$

Нет эл. порядка $6 \Rightarrow$ не цикл.

Пример. Пусть X - произвольное мн-во $G = \{ f : X \to X \}$ биекции

Эта группа называется группа преобразований X

Лемма. Пусть G - циклическая группа, $H < G$ - подгруппа. Тогда H тоже цикл.

<u>Опр.</u> $H < G$ наз. подгруппой, если

$\cdot\, e \in H$

$\cdot\, g_1, g_2 \in H \Rightarrow g_1 g_2 \in H$

$\cdot\, g \in H \Rightarrow g^{-1} \in H$

$\square$ $G = \{a^n, n \in \mathbb{Z}\}$. a - фикс. эл-т из G.

Пусть $h \in H$ - такой элемент, что $h = a^k$, $k > 0$, k - мин. с таким свойством.

Докажем, что H порождена h, т.е. $H = \{h^n, n \in \mathbb{Z}\}$

Пусть $h_1 \in H$, т.ч. $h_1 = a^m$, $m > k$

Тогда поделим с остатком:

$m = kr + q$, $q < k \Rightarrow$

$a^m = a^{kr} \cdot a^q \Leftrightarrow h_1 = h^r \cdot a^q \Rightarrow$

$a^q = \frac{h_1}{\cancel{h}} \cdot h^{-r} \in H$, но

$q < k$, что противоречит

минимальности при выборе k

$\blacksquare$

G - циклическая тогда обозначение $\langle a \rangle$, $a \in G$ образующая

Ан. 8. 2.

Пример. Пусть V - векторное пр-во. $G = \{t_a, (a \in V), t_a(x) = x + a\}$

Тогда G - группа по сложению и $G \simeq V$ по сл-ю

$t_a \mapsto a$

Изоморфизм групп - биекция, сохраняющая умножение и взятие обратного

Пример. Пусть V - векторное пр-во, $Hom(V, V)$ - все линейные от-я из $V \to V$ $\overset{\text{"}}{End}(V)$

Является ли $End(V)$ группой по умножению

нет, т.к. не у всех эл-тов есть обратный

Опр. $GL(V)$ - группа всех обратимых (вз. одн.) элементов $End(V)$

Элементы $GL(V)$ наз-ся изоморфизмами.

Пусть на $\mathbb{R}^2$ задано обычное расстояние: $(x, y) \to \sqrt{x^2+y^2}$

Пусть $O(\mathbb{R}^2)$ - все ~~[illegible]~~ линейные обратимые преобр. $GL(\mathbb{R}^2)$ $\mathbb{R}^2$, сохраняющие длину векторов.

Утв. $\forall$ эл-т из $O(\mathbb{R}^2)$ имеет вид: $\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$

либо $\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$

Симметрические группы

S_n - группа перестановок n элементов

$$S_n = \{ f: \{1, .., n\} \to \{1, ..., n\} \}$$

S_n не циклическая

Группы преобразований

X - произв. мн-во

$$G = \{ f : X \xrightarrow{\text{биекция}} X \}$$

Группа обратимых линейных отображений

V - векторное пространство, $Hom(V, V)$ - все лин. отобр. $V \to V$ $= End(V)$

$GL(V)$ - группа всех обр. (вз. однозн.) элементов $End(V)$

Элементы $GL(V)$ - изоморфизмы

Группа преобразований двумерного пр-ва, сохраняющих длины векторов.

На $\mathbb{R}^2$ задано расстояние $(x, y) \rightsquigarrow \sqrt{x^2 + y^2}$

$O(\mathbb{R}^2)$ - все лин. преобр $\mathbb{R}^2$, сохр. дл. векторов.

$GL(\mathbb{R}^2)$

$\forall$ эл. из $O(\mathbb{R}^2)$ имеет вид $\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ или $\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$

$\square \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$

$$x^2+y^2 = (ax+by)^2 + (cx+dy)^2$$

$$\begin{cases} a^2+c^2=1 & a=\cos\alpha,\ c=\sin\alpha \\ b^2+d^2=1 & b=\pm\sin\alpha,\ d=\pm\cos\alpha \\ ab+cd=0 & \boxtimes \end{cases}$$

Определители 1 и -1.

$$O(\mathbb{R}^2) = O_+(\mathbb{R}^2) \sqcup O_-(\mathbb{R}^2)$$

$E \in O_+(\mathbb{R}^2)$, $O_+(\mathbb{R}^2)$ - подгруппа в $O(\mathbb{R}^2)$

Специальная ортогональная группа

$O_+(\mathbb{R}^2)$ или SO_2 или $SO(\mathbb{R}^2)$

$$SO_2 \simeq \{z \in \mathbb{C};\ |z|=1\} \simeq S^1$$

Д-во: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$

Мы хотим: $x^2+y^2 = (ax+by)^2+(cx+dy)^2$

$$\begin{cases} a^2+c^2=1 \\ b^2+d^2=1 \\ ab+cd=0 \end{cases} \Rightarrow \begin{cases} a=\cos\alpha, \; c=\sin\alpha \\ b=\mp\sin\alpha, \; d=\pm\cos\alpha \end{cases}$$

$O(\mathbb{R}^2) = O_+(\mathbb{R}^2) \sqcup O_-(\mathbb{R}^2)$, $O_\pm(\mathbb{R}^2) = \{g : \det g = \pm 1\}$

не связное объединение

Замечание: $E \in O_+(\mathbb{R}^2)$

$O_+(\mathbb{R}^2)$ - подгруппа в $O(\mathbb{R}^2)$

если $x, y \in O_-(\mathbb{R}^2)$, то $xy \in O_+(\mathbb{R}^2)$

Обозначение $O_+(\mathbb{R}^2)$ обозн. SO_2 или $SO(\mathbb{R}^2)$

Замечание: $SO_2 \simeq \{z \in \mathbb{C} : |z| = 1\} \simeq S^1$

K - кольцо, комм., ассоц.

Фактор кольцо отн. эквивалентности

$\sim$ - отношение экв. согласовано с опер. сложения и умножения, если $\forall$

$a_1 \sim b_1,\ a_2 \sim b_2 \Rightarrow a_1 + a_2 \sim b_1 + b_2$

$a_1 a_2 \sim b_1 b_2$

<u>Утв.</u> Если отн. экв. согласовано с операциями, то на мн-ве классов имеется структура кольца.

<u>Опр.</u> Подмн-во I кольца k наз-ся идеалом, если

- I - подкольцо
- $\forall i \in I,\ a \in k \to ai \in I$

<u>Пример</u>: Тривиальные идеалы $I = 0$, $I = k$

<u>Пример</u>:
- $K = \mathbb{Z}$, $I = n\mathbb{Z} = \{k \in \mathbb{Z} : n \mid k\}$
- $K = \mathbb{R}[x]$, k-поле, $I = \{g(x) : f \mid g\}$, $f \in K[x]$

Сравнение с отн. экв-ти

Пусть I - произвольный идеал в k,

$a \underset{I}{\sim} b$, если $a - b \in I$

Ал. 9.1.

Утв. Это отн. экв. согл. с умножением и сложением.

$\square$ $\left.\begin{array}{l} a_1 \sim b_1 \\ a_2 \sim b_2 \end{array}\right| \Rightarrow \begin{array}{l} a_1 = b_1 + i_1 \\ a_2 = b_2 + i_2 \end{array}$ $i_1, i_2 \in I$

$$a_1 a_2 = b_1 b_2 + i_2 b_1 + b_2 i_1 + i_1 i_2 \Rightarrow$$

$$a_1 a_2 - b_1 b_2 \in I.$$

$$a_1 + a_2 = b_1 + b_2 + i_1 + i_2 \Rightarrow a_1 + a_2 \sim b_1 + b_2$$

Пример ~~подкольцо~~

$\mathbb{Z} \subset \mathbb{Q}$ подкольцо, но НЕ идеал

Следствие из утв.

$K/_I$ обладает ест. естественной структурой кольца (ком. и асс.)

Замечание Брать фактор можно только по идеалу, а не по произвольному кольцу.

Пример $I = 0 \Rightarrow K/_I \simeq K$; $I = K \Rightarrow K/_I \simeq 0$

Пример. Пусть K является полем

Лемма В поле имеются только тривиальные идеалы.

$\square$ Пусть $I \subset k$ какой-то ненулевой идеал. Пусть $x \in I$ - ненулевой эл. Т.к. k - поле, то $\exists x^{-1} \Rightarrow x \cdot x^{-1} = 1 \in I \Rightarrow \forall y \in k \; y \cdot 1 \in I$ $\blacksquare$

Следствие Для произвольного кольца k с 1, если $1 \in I$ - идеал k, то $I = K$.

Пример Все идеалы в $\mathbb{Z}$ имеют вид $n\mathbb{Z}$

Док-во. Пусть I - идеал в $\mathbb{Z}$, $I \neq 0$.

Рассмотрим $m \in \mathbb{Z}_{>0}$ - мин. полож. элемент I

Тогда хотим проверить, что $\forall k \in I \; k \,\vdots\, m$.

Действительно, будем считать, что $k > 0$ (иначе умножим на -1)

$k = mq + r \quad 0 \le r \le m$ Тогда $r = \underset{I}{k} - \underset{I}{mq} \Rightarrow$

$r \in I$, т.е. $r = 0 \Rightarrow k \,\vdots\, m$. $\blacksquare$

Пример $\hat{I} = 2\mathbb{Z} \cup 3\mathbb{Z}$ $\quad 3 - 2 = 1$.

Опр. Пусть K - кольцо, $I \in K$ - идеал.

Тогда I наз. главным, если $\exists a \in K$, т.ч. $I = \{ax, x \in K\}$

В этом случае $I = (a)$

Замечание. $\forall a \in K$ мн-во эл-тов вида $\{ax, x \in K\}$ является идеалом.

Все идеалы $\mathbb{Z}$ - главные.

Опр. Кольцо k наз-ся кольцом главных идеалов, если все идеалы k - главные.

Теорема $\forall$ Евклидово кольцо является кольцом главных идеалов. (КГИ)

$\square$ На евклидовом кольце задана норма

$N : K \setminus 0 \to \mathbb{Z}_{\geq 0}$

Если I - идеал в K, то если $I \neq 0$, то $\exists$ эл-нт m в I с наименьшей нормой.

Тогда $\forall k \in I$ $k \vdots m$ (деление с остатком)

$\blacksquare$

Следствие k - поле $\Rightarrow K[x]$ - КГИ

Пример $K = k[x, y]$, $I = \{ f(x,y) : f(0,0) = 0 \}$

$f(x,y) = \sum a_{ij} x^i y^j$

$a_{00} = 0$

Ал. 9.3

I - идеал, но не главный, т.к. $x, y \in I$,

но $\nexists f \in I : x \vdots f, y \vdots f$.

<u>Утв.</u> K - произвольное кольцо.

$f_1, \ldots, f_n \in K$, $f_i \neq 0$

Тогда $I = \{x_1 f_1 + \ldots + x_n f_n,\ x_i \in K\}$ - идеал.

<u>Опр</u> $I = (f_1, \ldots, f_n)$ - идеал, порождённый $f_1, \ldots, f_n$ (с образующими $f_1, \ldots, f_n$).

<u>Пример</u> $I = (x^2, xy, y^2) = \{f(x,y) = \sum a_{ij} x^i y^j : a_{00} = a_{10} = a_{01} = 0\}$

Тогда I - идеал и нетрудно проверить, что I нельзя породить меньше, чем тремя эл-тами.

Мы везде предполагали, что K - коммутативное кольцо. Если кольцо не ком., то тогда определяют левый и правый идеал.

$(i \in I,\ x \in K \Rightarrow xi \in I$ или $ix \in I)$

Если $\mathcal{I}$ правый и левый, то он наз-ся двуст.

Пример Пусть G-конечная группа, K-поле, тогда $K[G]$-групповое кольцо группы G состоит из выражений вида $\sum\limits_{g\in G} a_g \bar{g}$, где $a_g \in K$, $\bar{g}$ - формальные символы.

$$\sum a_g \bar{g} + \sum b_g \bar{g} = \sum (a_g + b_g) \cdot \bar{g}$$

$$\bar{g_1} \cdot \bar{g_2} = \overline{g_1 g_2}$$