

№ 1 (1.1) Для любых  $a, b, c \in K$  выполнены равенства

$\forall a, b, c \in K$ :

а)  $a0 = 0a = 0$

►  $a0 = a(0 + 0) = a0 + a0 \Rightarrow a0 = 0$

$0a = 0$  — аналогично. ◀

б)  $a(-b) = (-a)b = -ab$

►  $0 = a0 = a(b - b) = ab + a(-b) \Rightarrow -ab = a(-b)$  ◀

с)  $(a - b)c = ac - bc$  и  $a(b - c) = ab - ac$

►  $(a - b)c + bc = (a - b + b)c = ac \Rightarrow (a - b)c = ac - bc$

$a(b - c) + ac = a(b - c + c) = ab \Rightarrow a(b - c) = ab - ac$  ◀

№ 2(1.2)

а) В кольце не может быть двух различных единиц.

►  $1_1 \underbrace{=}_{\text{т. к. } 1_2 \text{ — единица}} 1_1 \cdot 1_2 \underbrace{=}_{\text{т. к. } 1_1 \text{ — единица}} 1_2$  ◀

б) Пусть кольцо с единицей содержит не меньше двух элементов. Тогда  $1 \neq 0$ .

►  $\forall a \in K \quad a \underbrace{=}_{\text{св-во } 1} a \cdot e \underbrace{=}_{\text{св-во } 0} 0$  ◀

с) Может ли элемент ассоциативного кольца иметь более одного обратного элемента?

► Пусть  $a_1 \neq a_2$  — обратные к  $a$  элементы. Тогда  $a_1 a a_2 = \begin{cases} a_1 \cdot 1 = a_1 \\ 1 \cdot a_2 = a_2 \end{cases}$

Получается, они равны. ◀

№ 3(1.3, 2.4) Уметь отвечать на вопросы: является ли данное кольцо  $K$  коммутативным? ассоциативным? кольцом с единицей? областью целостности? полем? евклидово кольцо? Какие в  $K$  есть обратимые элементы? неразложимые? простые?

№ 4 (2.1(в)) Обратимый элемент кольца не может быть делителем нуля.

► Пусть  $a \in K$  обратим,  $\exists a^{-1} \in K : aa^{-1} = 1$ . Если  $a$  — делитель нуля, то  $\exists 0 \neq b \in K : ab = 0$ . Тогда  $a^{-1}ab = \begin{cases} a^{-1} \cdot 0 = 0 \\ 1 \cdot b = b \neq 0 \end{cases}$ . Противоречие. ◀

№ 5(2.1(д)) Если  $K$  — область целостности, то возможно сокращение: если  $ac = bc$  и  $c \neq 0$ , то  $a = b$ .

►  $ac = bc \Leftrightarrow (a - b)c = 0 \Rightarrow$  т. к. нет делителей нуля и  $c \neq 0$ , д. б.  $a - b = 0$ , т. е.  $a = b$ . ◀

№ 6(2.1(г)) В конечном коммутативном кольце если ненулевой элемент не является делителем нуля, то он обратим.

► Кольцо конечно  $\Rightarrow$  его элементы можно занумеровать:  $a_1, \dots, a_n$ . Элементы  $a \cdot a_1, \dots, a \cdot a_n$  должны быть все разные (иначе  $\forall i \neq j, a \neq 0 \quad a \cdot a_i = a \cdot a_j \Rightarrow \underbrace{a}_{\neq 0} \underbrace{(a_i - a_j)}_{\neq 0, \text{ т. к. } i \neq j} = 0$  — есть делители нуля).

Тогда  $\exists i : a \cdot a_i = 1$ , т. к.  $1 \in K$  (т. е.  $a \cdot a_1, \dots, a \cdot a_n$  —  $n$  разных элементов кольца, а в кольце всего  $n$  элементов; значит, какое-то  $a_i$  должно быть 1). ◀

№ 7 Конечная область целостности — поле.

► В области целостности нет делителей нуля, а если в конечном коммутативном кольце элемент — не делитель нуля, то он обратим (№6). Т. е. все элементы обратимы.

TODO:  $\geq 2$  эл-тов. ◀

№ 8 Множество  $K^*$  обратимых элементов кольца  $K$  является группой по умножению. Она называется мультипликативной группой, или группой обратимых элементов кольца  $K$ .

► Пусть  $K$  — кольцо,  $a, b \in K^*$ . Тогда  $\exists a^{-1}, b^{-1} \in K^*$ . Проверим групповые свойства.

1.  $a(bc) = (ab)c$  — ассоциативность в  $K^*$  следует из свойств кольца  $K$ .

2.  $\exists 1 \in K^*$  (т. к.  $K^* \neq \emptyset$ ,  $\exists a \in K^*$ , по свойству обратимости  $\exists a^{-1} \in K^* : aa^{-1} = 1$  — единица в  $K$  будет являться единицей в  $K^*$ ).

3.  $(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = 1 \Rightarrow (ab)^{-1} = b^{-1}a^{-1} \in K^*$  — обратимость.

Значит,  $K^*$  — группа по умножению. ◀

№ 9(1.5-1.7) Базовые знания про комплексные числа: сложение, умножение, модуль, аргумент, извлечение корней  $n$ -ой степени.

► **Компл'ексное число**  $z$  — это выражение вида  $z = a + bi$ , где  $a$  и  $b$  — числа из  $\mathbb{R}$ , а  $i$  — **мнимая единица**. По определению  $i^2 = -1$ . Число  $a$  называют **вещественной частью** комплексного числа  $z$  (пишется  $a = \operatorname{Re}(z)$ ), а число  $b$  — **мнимой частью**  $z$  (пишется  $b = \operatorname{Im}(z)$ ). Комплексные числа можно складывать и умножать, «раскрывая скобки и приводя подобные». Множество комплексных чисел обозначают буквой  $\mathbb{C}$ .

Каждому комплексному числу  $z = a + bi$  сопоставим точку  $(a, b)$  и вектор  $(a, b)$ . Длина этого вектора называется **модулем** числа  $z$  и обозначается  $|z|$ . Пусть  $z \neq 0$ . Угол (в радианах), отсчитанный против часовой стрелки от вектора  $(1, 0)$  до вектора  $(a, b)$ , называется **аргументом** числа  $z$  и обозначается  $\operatorname{Arg}(z)$ . Аргумент определен с точностью до прибавления числа вида  $2\pi n$ , где  $n \in \mathbb{Z}$ .

**Тригонометрическая форма записи.** Для любого ненулевого комплексного числа  $z$  имеет место равенство  $z = r(\cos \varphi + i \sin \varphi)$ , где  $r = |z|$ ,  $\varphi = \operatorname{Arg}(z)$ .

Для комплексного числа  $z = r(\cos \varphi + i \sin \varphi)$  и натурального числа  $n \in \mathbb{N}$  выполнена **формула Муавра**  $z^n = r^n(\cos n\varphi + i \sin n\varphi)$ .

Для комплексного числа  $z = a + bi$ , где  $a, b \in \mathbb{R}$  число  $\bar{z} = a - bi$  называется **комплексно-сопряжённым** к  $z$ . Выполнены следующие равенства:

$$|z|^2 = z\bar{z}, \quad \overline{z+w} = \bar{z} + \bar{w}, \quad \overline{zw} = \bar{z}\bar{w}.$$

№ 10(2.2)

а) Следующие условия эквивалентны:

- (1)  $x \sim y$ ;
- (2)  $x \mid y$  и  $y \mid x$ ;
- (3) множество делителей  $x$  и множество делителей  $y$  равны.

- • (1)  $\Rightarrow$  (2) :  $\exists r \in K^* : x = ry \Rightarrow y \mid x$  по определению. Т. к.  $r \in K^*$ ,  $\exists r^{-1} \in K^* : r^{-1}x = y \Rightarrow x \mid y$  по определению.
- (2)  $\Rightarrow$  (3) :  $d \mid x \Rightarrow \exists r \in K^* : dr = x \Rightarrow$  т. к.  $y \mid x, y \mid dr$ . TODO
- (3)  $\Rightarrow$  (2) : Множества делителей  $x$  и  $y$  совпадают,  $x \mid x \Rightarrow x$  будет во множестве делителей  $y$ , т. е.  $x \mid y$ . Симметрично,  $y \mid x$ .
- (2)  $\Rightarrow$  (1) :  $\begin{cases} x \mid y \Rightarrow y = kx \\ y \mid x \Rightarrow x = ty \end{cases}$  Тогда  $y = kty \Rightarrow kt = 1$  Значит,  $k$  и  $t$  обратимы. Значит,  $x = ty, t \in K^* \Rightarrow x \sim y$  по определению.

б) Отношение  $\sim$  является отношением эквивалентности.

► 1.  $x \sim x$ , т. к.  $\exists 1 \in K^* : x = 1x$

2.  $x \sim y \Rightarrow \exists r \in K^* : x = ry \Rightarrow y = r^{-1}x \Rightarrow y \sim x$

3.  $x \sim y, y \sim z \Rightarrow \begin{cases} \exists r_1 \in K^* : x = r_1 y \\ \exists r_2 \in K^* : y = r_2 z \end{cases} \Rightarrow x = \underbrace{r_1 r_2}_{\in K^*, \text{ т. к. } (r_1 r_2)^{-1} = r_2^{-1} r_1^{-1}} z \Rightarrow x \sim z$

№ 11 (2.5) Если  $a, b, k \in \mathbb{Z}$ ,  $u \notin \mathbb{Q}$ , то  $z = a + bu \in \mathbb{Z}[u]$  делится на  $k$  тогда и только тогда, когда  $a$  и  $b$  делятся на  $k$ .

№ 12(2.9  $\Leftarrow$ )  $K$  — евклидово кольцо. Верно ли, что для  $a \neq 0, b \in K^*$  выполнено равенство  $N(ab) = N(a)$ ?

►  $b \in K^* \Rightarrow N(a) \leq N(ab) \leq N(abb^{-1}) = N(a)$

№ 13 (3.2) Для  $u = i, \omega$  и простого целого числа  $p \leq 40$  выясните, существует ли  $z \in D$  с  $N(z) = p$ . Сформулируйте гипотезу о том, какие простые целые числа являются простыми в  $D$ .

► Выпишем все варианты  $a, b$  с нормой  $\leq 40$ .

a	b	$\mathbb{Z}[i], N = a^2 + b^2$	$\mathbb{Z}[\omega], N = a^2 - ab + b^2$
1	1	2	1
1	2	5	3
1	3	10	7

a	b	$\mathbb{Z}[i], N = a^2 + b^2$	$\mathbb{Z}[\omega], N = a^2 - ab + b^2$
1	4	17	13
1	5	26	21
1	6	37	31
2	3	13	7
2	4	20	12
2	5	29	19
2	6	40	28
3	3	18	9
3	4	25	13
3	5	34	19
4	4	32	16

Выпишем все простые числа  $\leq 40$  и вычеркнем те, которые являются нормой. Берём оставшиеся.

	$\mathbb{Z}[i]$		$\mathbb{Z}[\omega]$	
	2	✗	✓	2
✓	3			3 ✗
	5	✗	✓	5
✓	7			7 ✗
✓	11		✓	11
	13	✗		13 ✗
	17	✗	✓	17
✓	19			19 ✗
✓	23		✓	23
	29	✗	✓	29
✓	31			31 ✗
	37	✗	✓	37

Гипотеза: у  $\mathbb{Z}[i]$   $4k + 3$ , у  $\mathbb{Z}[\omega]$   $3k + 2$ .

#### № 14 (3.9)

► а)  $0 \subset K, K \subset K$  — идеалы. Они называются **тривиальными**.

•  $\{0\}$ :

1. Тривиальная группа по сложению:

- Ассоциативность наследуется
- $0$  — нейтральный элемент, т. к.  $0 + a = a + 0 = 0 \forall a \in \{0\}$
- $0^{-1} = 0 = -0$

2. Замкнутость относительно умножения:  $\forall a \in K 0a = 0 \in \{0\}$

•  $K$ :

1. Тривиальная группа по сложению:

- Ассоциативность наследуется
- $0$  — нейтральный элемент, т. к.  $0 + a = a + 0 = 0 \forall a \in K$
- $a^{-1} = -a \in K$

2. Замкнутость относительно умножения:  $\forall a \in K \forall b \in I = K ab \in I = K$  — по свойству кольца

б)  $(a) = \{ax \mid x \in K\}$  — **главный идеал** или **идеал, порождённый одним элементом**

1. Подгруппа по сложению:

- $ax_1 + ax_2 = a(x_1 + x_2) \in (a)$  — замкнутость относительно сложения
- Ассоциативность наследуется
- $0$  — нейтральный элемент:  $ax + 0 = 0 + ax = ax$
- $ax + a(-x) = a(x - x) = a \cdot 0 = 0$

2. Замкнутость относительно умножения:  $\forall b \in K \forall ax \in (a) b \cdot ax = bx \cdot a \in (a)$

с)  $(a_1, \dots, a_n) = \{a_1x_1 + \dots + a_nx_n \mid x_1, \dots, x_n \in K\}$  — **конечно-порождённый идеал**, то есть идеал, порождённый конечным количеством элементов.

1. Подгруппа по сложению:

- $(a_1x_1 + \dots + a_nx_n) + (a_1y_1 + \dots + a_ny_n) = a_1(x_1 + y_1) + \dots + a_n(x_n + y_n) \in I$  — замкнутость относительно сложения
- Ассоциативность наследуется

- $0 = a_1 \cdot 0 + \dots + a_1 \cdot 0$  — нейтральный элемент:  $ax + 0 = 0 + ax = ax$
  - $(a_1x_1 + \dots + a_nx_n) + (a_1(-x_1) + \dots + a_n(-x_n)) = 0$
2. Замкнутость относительно умножения:  $\forall y \in K \ y \cdot (a_1x_1 + \dots + a_nx_n) = a_1(x_1y) + \dots + a_n(x_ny) \in I$

### № 15(3.11)

- а) Докажите, что  $(a) \subset (b)$  тогда и только тогда, когда  $b \mid a$ . б) Докажите, что  $a \sim b$  тогда и только тогда, когда  $(a) = (b)$ .

№ 16(3.12) Пусть  $I, J \subset K$  — идеалы. Сумма  $I + J = \{x + y \mid x \in I, y \in J\}$  и пересечение  $I \cap J$  идеалов являются идеалами.

- а) 1. •  $(x_1 + y_1) + (x_2 + y_2) = \underbrace{(x_1 + x_2)}_{\in I} + \underbrace{(y_1 + y_2)}_{\in J} \in I + J$

- Ассоциативность следует.
- $0$  — нейтральный.
- $(x + y) + \underbrace{(-x - y)}_{\in I + J} = (x - x) + (y - y) = 0$  — обратный

$$2. \forall a \in K \hookrightarrow a(x + y) = \underbrace{ax}_{\in I} + \underbrace{ay}_{\in J} \in I + J$$

$$б) \quad 1. \bullet \ x, y \in I \cap J \Rightarrow \begin{cases} x, y \in I \\ x, y \in J \end{cases} \Rightarrow \begin{cases} x + y \in I \\ x + y \in J \end{cases} \Rightarrow x + y \in I + J$$

- Ассоциативность следует.
- $0$  — нейтральный
- $x \in I \cap J \Rightarrow \begin{cases} x \in I \\ x \in J \end{cases} \Rightarrow \begin{cases} x^{-1} \in I \\ x^{-1} \in J \end{cases} \Rightarrow x^{-1} \in I + J$  — обратный

$$2. \forall a \in K \ \forall x \in I \cap J \hookrightarrow \begin{cases} x \in I \\ x \in J \end{cases} \Rightarrow \begin{cases} ax \in I \\ ax \in J \end{cases} \Rightarrow ax \in I \cap J$$

№ 17(3.15) Пусть  $K \neq 0$ . Докажите, что  $K$  является полем тогда и только тогда, когда  $K$  не содержит нетривиальных идеалов.

- •  $\Rightarrow$ : Пусть  $K$  — поле,  $I \subset K$  — идеал.

- $x = 0 \Rightarrow (x) = \{0\}$  — тривиальный идеал.
- $\forall x \in I, x \neq 0$ ,  $x$  обратим по свойству поля, значит,  $I \supset (x) = (1) = K$ .

- $\Leftarrow$ : Пусть  $K$  — коммутативное кольцо без нетривиальных идеалов. Пусть  $x \in K, x \neq 0$ , — произвольный элемент. Тогда  $(x) \neq \{0\}$ . Значит, поскольку у нас нет нетривиальных идеалов,  $(x) = K$ .

В частности,  $1 \in (x) = K \Rightarrow \exists x^{-1}$ , т. е. элемент  $x$  обратим.

В силу произвольности  $x$ , любой ненулевой элемент обратим  $\Rightarrow K$  — поле (в  $K \geq 2$  элементов, т. к.  $0 \in K$ , и мы брали  $0 \neq x \in K$ ).

№ 18(4.1) Верно ли, что при гомоморфизме колец  $\varphi : K \rightarrow L$  а) образ; б) прообраз идеала является идеалом?

а)

- Неверно. Контрпример:  $\varphi : \mathbb{Z} \rightarrow \mathbb{Q}, \varphi(x) = x$  — поэлементное вложение.

$I = \mathbb{Z}$  в  $\mathbb{Z}$  — тривиальный идеал. Но  $\varphi(I) = \mathbb{Z}$  — не идеал в  $\mathbb{Q}$ , ибо, например,  $\underbrace{\frac{1}{2}}_{\in \mathbb{Q}} \cdot \underbrace{1}_{\in \mathbb{Z}} = \frac{1}{2} \notin \mathbb{Z}$ .

б)

- Верно. Пусть  $J$  — идеал в  $L$ .  $\varphi^{-1}(J) = \{a \in K : \varphi(a) \in J\}$ .

$$\forall a, b \in \varphi^{-1}(J) : \begin{cases} \varphi(a + b) = \varphi(a) + \varphi(b) \Rightarrow a + b \in \varphi^{-1}(J) \\ \varphi(a^{-1}) = (\varphi(a))^{-1} \in J \end{cases}$$

$$\forall x \in K \ \forall a \in \varphi^{-1}(J) \ \varphi(ax) = \varphi(a)\varphi(x) \in J.$$

Значит,  $\varphi^{-1}(J)$  — действительно идеал. ◀

№ 19(4.2)

а) Всегда ли факторкольцо коммутативного кольца является коммутативным кольцом?

$$\blacktriangleright (a+I)(b+I) = ab + aI + bI + II = ab + I = ba + I = ba + bI + aI + II = (b+I)(a+I)$$

TODO?? ◀

б) Имеется **канонический** гомоморфизм  $\varphi : K \rightarrow K/I$ , который переводит  $a \mapsto a+I$ .

► Проверим свойства гомоморфизма:

- $\varphi(a) + \varphi(b) = a+I + b+I = (a+b)+I = \varphi(a+b)$
- $\varphi(a)\varphi(b) = (a+I)(b+I) = ab + aI + bI + II = ab + I = \varphi(ab)$
- $\varphi(1) = 1+I = 1_{K/I}$

№ 20(4.5) Пусть  $K$  — область целостности. Идеал  $(x)$  является простым тогда и только тогда, когда  $x$  прост. ◀

$$\blacktriangleright (x) \text{ — простой} \Leftrightarrow \text{если } ab \in (x), \text{ то } \begin{cases} a \in (x) \\ b \in (x) \end{cases}$$

$$x \text{ — простой} \Leftrightarrow \text{если } ab : x, \text{ то } \begin{cases} a : x \\ b : x \end{cases}$$

Но  $ab \in (x) \Leftrightarrow ab : x$  (ибо  $(x) = \{ax \mid a \in K\}$  по определению, и  $ab \in K$ ). ◀

№ 21(4.6) Пусть  $K$  — область целостности. Нетривиальный идеал  $I$  является максимальным тогда и только тогда, когда  $K/I$  поле.

► Знаем (№17):  $K/I$  — поле  $\Leftrightarrow$  в  $K/I$  нет нетривиальных идеалов.

Пусть  $K/I$  — поле, пусть  $\exists I : I \subset J \subset K$  — нетривиальный идеал. Подействуем на него каноническим гомоморфизмом  $\varphi : K \rightarrow K/I$ .

**Лемма.** Пусть  $f : K \rightarrow L$  — гомоморфизм колец,  $I \subset K, J \subset L$  — идеалы. Тогда а)  $f(I)$  — идеал в  $f(K)$ , б)  $f^{-1}(J)$  — идеал в  $K$ .

► а) Пусть  $x \in f(I), y \in f(K)$ . Тогда найдутся такие  $x'$  и  $y'$ , где  $x' \in I, x = f(x'), y' \in K, y = f(y')$ . Имеем:  $xy = f(x')f(y') = f(x'y') \in f(I)$ , так как  $x'y' \in I$ .

б) Пусть теперь  $x \in f^{-1}(J), y \in K$ . Тогда  $f(xy) = f(x)f(y) \in J$ , следовательно,  $xy \in f^{-1}(J)$ . ◀

Из Леммы следует, что в  $K/I$  существует нетривиальный идеал  $\Leftrightarrow$ , когда существует идеал в  $K$ , содержащий  $I$ . ◀

№ 22(4.7) Пусть  $K$  — область целостности. Нетривиальный идеал  $I$  является простым тогда и только тогда, когда  $K/I$  область целостности.

► •  $\Rightarrow$ : Пусть  $I$  — простой, но  $K/I$  — не область целостности. Тогда  $\exists a, b \in K : (a+I)(b+I) = ab + I = 0 + I = 0_{K/I}$ . Но тогда должно быть  $ab \in I$ , т. е. идеал не простой. Противоречие.

•  $\Leftarrow$ : Пусть  $I$  непростой. Тогда  $\exists a, b : a, b \in I$ , но  $ab \notin I$ . Рассмотрим  $0 \neq (a+I)(b+I) = ab + \underbrace{I}_{ab \in I} = 0_{K/I}$ . ◀

№ 23(5.1, 5.2) Пусть  $K$  — область целостности. Рассмотрим множество пар  $\tilde{K} = \{a, b\}$  элементов кольца  $K$ , где  $b \neq 0$ . На этом множестве введем отношение следующим образом:  $\{a, b\} \sim \{c, d\}$ , если  $ad = bc$ .

а) Докажите, что  $\{a, b\} \sim \{ac, bc\}$ . б) Докажите, что это отношение эквивалентности.

Элемент множества классов эквивалентности  $F = \text{Quot}(K)$  будем записывать как  $\frac{a}{b}$  или  $ab^{-1}$ . Введем операции сложения и умножения на  $F = \text{Quot}(K)$ :

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Докажите, что

с) сложение и умножение корректно определено; d)  $F$  является коммутативным кольцом; e)  $F$  является полем; f) существует инъекция  $K \rightarrow F$ .

► a)  $a \cdot bc = b \cdot ac$  — из коммутативности.

b) •  $\{a, b\} \sim \{a, b\}$ , т. к.  $ab = ab$

•  $\{a, b\} \sim \{c, d\} \Leftrightarrow ad = bc \Leftrightarrow cb = da \Leftrightarrow \{c, d\} \sim \{a, b\}$

•  $\{a, b\} \sim \{c, d\} \sim \{e, f\} \Rightarrow \begin{cases} ad = bc \\ cf = de \end{cases} \Rightarrow \begin{cases} adf = bcf \\ bcf = bde \end{cases} \Rightarrow adf = bde \Rightarrow af = be \Rightarrow \{a, b\} \sim \{e, f\}$

c) TODO TODO

## № 24(6.1) Признак неприводимости Эйзенштейна

Пусть  $f(x)$  — многочлен с целыми коэффициентами и существует такое простое число  $p$ , что:

1. старший коэффициент  $f(x)$  не делится на  $p$ ; 2. все остальные коэффициенты  $f(x)$  делятся на  $p$ ; 3. свободный член  $f(x)$  не делится на  $p^2$ .

Тогда многочлен  $f(x)$  неприводим над полем рациональных чисел.

► Пусть не так, и он приводим над  $\mathbb{Q}$ . Тогда он приводим и над  $\mathbb{Z}$  (домножим на общий знаменатель). Тогда он раскладывается в произведение двух многочленов ненулевой степени:  $f_n x^n + \dots + f_1 x + f_0 = f(x) = g(x)h(x) = (g_k x^k + \dots + g_1 x + g_0)(h_m x^m + \dots + h_1 x + h_0)$ ,  $0 < \deg g, \deg h < n$ . Возьмём всё по модулю  $p$  (если мы утверждаем, что у нас равенство выполняется в  $\mathbb{Z}$ , то оно должно выполняться и для любого натурального модуля). Тогда  $\bar{f}(x) = \bar{f}_n x^n$ .  $f(x)$  состоит из одного монома, а произведение двух многочленов будет одним мономом  $\Leftrightarrow$  оба этих

т. к. другие члены делятся на  $p$

многочлена тоже мономы. Отсюда  $\bar{f}(x) = \bar{g}(x)\bar{h}(x) = (g_k x^k)(h_m x^m)$ . Рассмотрим свободный член. Если  $k, m > 0$ , то  $a_0 = \underbrace{g_0}_{\vdots p} \underbrace{h_0}_{\vdots p} : p^2$  (свободные члены  $g(x)$  и  $h(x)$  делятся на  $p$ , т. к. они зануляются, когда мы берём по модулю  $p$ ). Противоречие.

№ 25(6.2?????) Многочлен  $x^n - p$  ( $p$  — простое число) неприводим над  $\mathbb{Q}$ .

► По критерию Эйзенштейна:  $1 \not\vdots p, -p \vdots p, -p \not\vdots p^2$ , где  $p$  — простое.

№ 26(6.3) Характеристика поля — простое число.

► Если  $k$  непростое,  $k = m \cdot n$ , то  $m \cdot n = 0$ , т. е. есть делители нуля — противоречие с тем, что у нас поле.

№ 27(6.4(Lecture\_all.pdf №6.2(3))) Пусть  $F \subset G$  — поля. Верно ли, что  $\text{char}(F) = \text{char}(G)$ ?

► Так как  $\varphi(1) = 1$ , имеем  $\varphi(\underbrace{1 + \dots + 1}_m) = \underbrace{1 + \dots + 1}_m$ . Т. к.  $\text{Ker } \varphi = \{0\}$ , то  $\underbrace{1 + \dots + 1}_m = 0$  в  $K$  и  $F$  одновременно.

Следовательно,  $\text{char } F = \text{char } K$ .

№ 28(6.5) Любое конечное поле имеет положительную характеристику.

► Пусть  $F$  конечно, а  $\text{char } F = 0$ . Тогда  $\underbrace{1 + \dots + 1}_k$  для любого  $k$  будет давать элемент поля, не совпадающий с предыдущими (иначе  $\text{char}$  была бы конечна).

Получается, что  $F$  бесконечно. Противоречие.

№ 29(№6.7) Нетривиальный гомоморфизм полей  $\varphi : F \rightarrow L$  является инъекцией.

►  $\varphi : F \rightarrow L$  — инъекция  $\Leftrightarrow \text{Ker } \varphi = \{0\}$ .

► •  $\Rightarrow$ :  $\varphi$  — инъекция  $\Rightarrow \forall a, b \in F, a \neq b, \varphi(a) \neq \varphi(b)$ .

$\text{Ker } \varphi = \{a \in F : \varphi(a) = 0_L\}$ .

Имеем  $\varphi(0) = 0$  по свойству гомоморфизма, тогда по инъективности  $\forall a \neq 0 \varphi(a) \neq \varphi(0) = 0$ , т. е.  $\text{Ker } \varphi = \{0\}$ .

•  $\Leftarrow$ :  $\text{Ker } \varphi = \{0\} \Rightarrow$

$\text{Ker } \varphi$  — идеал в  $F$

►  $\forall a \in F \forall x \in \text{Ker } \varphi \varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \cdot 0 = 0$  Then  $ax \in \text{Ker } \varphi$

В поле  $F$  идеал  $I = \begin{cases} \{0\} \\ F \end{cases}$ , т. е.  $\text{Ker } \varphi = \begin{cases} \{0\} \\ F \end{cases}$  — но в этом случае гомоморфизм тривиален, но у нас нетривиальный

№ 30(№6.8)  $K$  образует линейное пространство над  $F$ .

- Проверка свойств. Свойства линейного пространства следуют из аксиом поля. TODO: скопировать из вики свойства. ◀

№ 31(Lecture\_all.pdf утв. 6.2(2))

$$\tilde{m} := \underbrace{1 + \dots + 1}_{m \text{ штук}}$$

$$\tilde{n} := \underbrace{1 + \dots + 1}_{n \text{ штук}}$$

Для  $m \neq n$  имеем  $\tilde{m} \neq \tilde{n}$  (иначе  $\tilde{m} - \tilde{n} = 0$ , и  $\text{char } F \neq 0$ ).

Противоположный к элементу  $\tilde{m}$  обозначим  $-\tilde{m}$ .

Получили  $\mathbb{Z} \subset F$ . Значит, поле частных  $\mathbb{Q} = \text{Quot}(\mathbb{Z}) \subset F$ . TODO: почему так? ◀

№ 32 (Lecture\_all.pdf утв. 6.5(2))

- Обозначим смежный класс многочлена  $g(x) \in F$  как  $\bar{g}(x) \in K$ . Тогда имеем:  $\bar{x} \in K$  — корень многочлена  $f(x)$ , т. е.  $f(\bar{x}) = \bar{f}(\bar{x}) = 0$ . ◀

№ 33 Пусть  $f(x)$  — неприводимый многочлен степени  $n$ , и  $K = F[x]/(f(x))$ . Чему равна степень  $[K : F]$  этого расширения?

- Обозначим смежный класс многочлена  $g(x) \in F$  как  $\bar{g}(x) \in K$ . Рассмотрим  $\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}$ . Пусть они ЛЗ, т. е.  $\exists \lambda_0, \lambda_1, \dots, \lambda_{n-1} \in F : \lambda_0 \cdot \bar{1} + \lambda_1 \cdot \bar{x} + \dots + \lambda_{n-1} \cdot \bar{x}^{n-1} = 0$ . Тогда  $g(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_{n-1} x^{n-1} \in (f(x))$ , а по неприводимости  $f(x)$  имеем  $g(x) = 0$ , т. е.  $\lambda_0 = \lambda_1 = \dots = \lambda_{n-1} = 0$ , и данная ЛК тривиальна. Поэтому  $\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}$  ЛНЗ.

$\forall$  многочлена  $h(x) \in F[x]$   $\bar{h}(x)$  — образ при факторизации по идеалу  $(f(x))$  — совпадает с  $\bar{r}(x)$ , где  $r(x)$  — остаток от деления  $h(x)$  на  $f(x)$ . Поэтому  $\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}$  образуют базис  $K$  как линейного пространства над  $F$ , т. е.  $[K : F] = n$ . ◀

№ 36(9.1) Для производной выполнены формулы  $(f + g)' = f' + g'$  и  $(fg)' = f'g + fg'$ .

- Для  $f(x) = a_n x^n + \dots + a_1 x + a_0$  и  $b(x) = b_n x^n + \dots + b_1 x + b_0$ :

$$(f + g)' = n(a_n + b_n)x^{n-1} + \dots + (a_2 + b_2)x + (a_1 + b_1) = (na_n x^{n-1} + a_2 x + a_1) + (nb_n x^{n-1} + \dots + b_2 x + b_1) = f' + g'$$

Рассмотрим  $f(x) - f(y) = \sum_{k=1}^n na_k(x^k - y^k) = (x - y) \sum_{k=1}^n na_k(x^{k-1} + x^{k-2}y + \dots + y^{k-1}) = (x - y)\Phi(x, y)$ , где  $\Phi(x, y) = \sum_{k=1}^n na_k(x^{k-1} + x^{k-2}y + \dots + y^{k-1})$ . Заметим, что  $\Phi(x, x) = f'(x)$ .

Тогда имеем для  $\varphi = fg$ :  $\varphi(x) - \varphi(y) = f(x)g(x) - f(y)g(y) = f(x)(g(x) - g(y)) + g(y)(f(x) - f(y)) = (x - y)[f(x)G(x, y) + g(y)\Phi(x, y)]$ . Отсюда  $\varphi' = f(x)G(x, x) + g(x)\Phi(x, x) = f(x)g'(x) + g(x)f'(x)$ . ◀

№ 37 (9.2) Многочлен  $f$  не имеет кратных корней тогда и только тогда, когда  $(f, f') = 1$ .

- Пусть  $f(x) = (x - a)^m f_1(x)$ ,  $f_1(x) \not\equiv 0 \pmod{x - a}$ ,  $m \geq 2$ . Тогда  $f'(x) = m(x - a)^{m-1} f_1(x) + (x - a)^m f_1'(x)$ .
  - Если  $m > 1$ , то  $f'(a) = 0$ .
  - Если  $m = 1$ , то  $f'(x) = (x - a)f_1'(x) + f_1(x) \Rightarrow f'(a) = f_1(a) \neq 0 \Rightarrow f(x)$  имеет кратные корни  $\Leftrightarrow$  эти корни являются корнями  $f'(x)$ .

№ 38(9.6) Докажите, что можно построить

а) все точки с рациональными координатами; б)  $\xi_n$ , где  $n = 3, 4, 6$ ; в)  $\xi_5$ .

Если мы построили точки  $z, w$ , то можно ли построить точки d)  $\bar{z}, -z$ ? е)  $z + w, z - w$ ? f)  $z \cdot w, \frac{z}{w}$  (при  $w \neq 0$ )? г)

$\sqrt{z}$ ?

- TODO ◀

№ 39 (9.12a) Докажите невозможность удвоения куба, то есть построение куба объёма 2, имея куб объёма 1 с помощью циркуля и линейки.

- TODO ◀

№ 40 (10.2)

- TODO ◀

№ 41 (10.4 (Lectures\_all.pdf задача 9.1, утв. 9.1)) Пусть  $F \subset K$  — расширение полей. Множество автоморфизмов  $K$ , оставляющих  $F$  на месте, является группой и называется группой автоморфизмов и обозначается  $\text{Aut}_F(K) = \text{Aut}([K : F])$ . а)  $\text{Aut}_F(K)$  — группа. б) Пусть  $H \subset \text{Aut}_F(K)$  — подгруппа. Тогда

$K^H = \{x \in K \mid \forall h \in H \hookrightarrow h(x) = x\}$  является полем, причём  $K \supset K^H \supset F$ .

- b) Действительно, если  $a, b \in K^H, h \in H$  то  $h(a+b) = h(a) + h(b) = a + b$ , и поэтому  $a + b \in K^H$ . Аналогично,  $ab \in K^H$ . С другой стороны,  $h \in H \subset G$ , и поэтому  $h(x) = x \ \forall x \in F$ . Значит,  $F \subset K^H$ .

◀

**№ 42 (10.5)** Опишите группы автоморфизмов  $\mathbb{Q}(\sqrt[3]{2})$ .

► TODO

◀

**№ 43 (11.1 (Lectures\_all.pdf теор. 11.1))** а) Конечное поле характеристики  $p$  состоит из  $p^n$  элементов. б) Поле  $F$  является полем разложения многочлена  $x^{p^n} - x$ . с) Существует единственное поле из  $p^n$  элементов.

- а) Так как  $K$  — конечное расширение поля  $\mathbb{Z}_p$ , то  $K$  является  $n$ -мерным линейным пространством над  $\mathbb{Z}_p$ , и поэтому состоит из  $p^n$  элементов. б) Пусть  $\alpha \in K, \alpha \neq 0$ . Тогда  $\alpha^{p^n-1} = 1$ . Следовательно,  $\alpha$  является корнем многочлена  $f$ . Степень многочлена  $f$  равна  $p^n$ , все элементы  $K$  являются его корнями. Ясно, что  $K$  — минимальное поле, в котором  $f$  раскладывается на линейные множители. Следовательно,  $K$  — его поле разложения. с) Поле разложение многочлена  $f$  единственно с точностью до изоморфизма.

◀

**№ 44 (11.2)** Найдите все неприводимые многочлены (со стар. коэффициент 1) степени 2, 3 над полем а)  $F_2$ , б)  $F_3$ .

► TODO

◀

**№ 45 (11.3)** Постройте поле из а) 4; б) 8; с) 9 элементов.

► TODO

◀