

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

a)  $a0 = 0a = 0$

b)  $a(-b) = (-a)b = -ab$

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

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

$0a = 0$  — аналогично.

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

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

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

№ 2(1.2)

a) В кольце не может быть двух различных единиц.

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

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

►  $\forall e \neq a \in K \quad a \underbrace{=}_{\text{св-во единицы}} a \cdot e \underbrace{=}_{\text{св-во нуля}} e$

c) 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  $K$  — кольцо без делителей нуля, 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:  $a_1, \dots, a_n$ .  $\forall a \neq 0$  элементы  $a \cdot a_1, \dots, a \cdot a_n$  должны быть все разные (иначе  $\exists i \neq j : a \cdot a_i = a \cdot a_j \Rightarrow \underbrace{a}_{\neq 0} \underbrace{(a_i - a_j)}_{\neq 0, \text{ т. к. } i \neq j} = 0$ , т. е.  $a$  — делитель 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  $aa_i$  должно быть 1).

№ 7 Конечная область целостности (состоящая из более чем одного элемента) — 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.

Имеем  $\geq 2$  элементов по условию.

№ 8 Множество  $K^*$  обратимых элементов коммутативного 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.  $\exists 1 \in K^*$  (единица из  $K$  будет единицей из  $K^*$ : она лежит в  $K^*$ , т. к.  $\exists 1^{-1} = 1$ , ибо  $1 \cdot 1 = 1$ , и выполняется свойство единицы  $a1 = 1a = a$ ).

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

4.  $\forall a, b \in K^* \Leftrightarrow ab \in K^*$ , т. к.  $\exists (ab)^{-1} = b^{-1}a^{-1}$ .

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:

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

Извлекать корни можно с помощью аналога формулы Муавра. Если  $\sqrt[n]{z} = \sqrt[n]{r}(\cos \frac{\varphi}{n} + i \sin \frac{\varphi}{n})$ . Выводится из обычной формулы Муавра, расписав возведение  $z^{\frac{1}{n}}$ . ◀

**№ 10(2.2)**

а) Докажите, что для элементов  $x, y$  области целостности  $K$  следующие условия равносильны:

- (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) : Пусть  $x \mid y, x \mid x$ , т. е.  $a$  — делитель  $x$ . Тогда  $\begin{cases} \exists c : y = xc \\ \exists b : x = ab \end{cases}$  (по опр.)  $\Rightarrow y = xc = abc = a(bc) \Rightarrow y \mid a$ .

• (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.  $x \sim y, y \sim z \Rightarrow \begin{cases} \exists r_1 \in K^* : x = r_1y \\ \exists r_2 \in K^* : y = r_2z \end{cases} \Rightarrow x = \underbrace{r_1r_2}_{\substack{\in K^*, \text{ т. к. } (r_1r_2)^{-1} = r_2^{-1}r_1^{-1}}} z \Rightarrow x \sim z$

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

► •  $\Rightarrow$ :  $\begin{cases} a \div k \\ b \div k \end{cases} \Rightarrow \begin{cases} a = ka' \\ b = kb' \end{cases} \Rightarrow z = a + bu = ka' + kb'u = k(a' + b'u) \Rightarrow z \div k$

•  $\Rightarrow$ : Пусть  $z = a + bu = ka' + kb'u$ . Тогда  $(a - ka') = u(b - kb')$ .

Обе части целые  $\Rightarrow$  нули, потому что  $u$  не рациональное.

Отсюда  $\begin{cases} a = ka' \\ b = kb' \end{cases} \Rightarrow \begin{cases} a \div k \\ b \div k \end{cases}$ .

№ 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  $z \in \mathbb{Z}[u]$  с  $N(z) = p$ . Сформулируйте гипотезу о том, какие простые числа являются простыми в  $\mathbb{Z}[u]$ .

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

**Зам.** Можно опустить перебор по  $ka', kb'$  при  $k > 1$ , потому что тогда обе нормы делятся на  $k^2$ .

**Зам.** Можно брать только натуральные, т. к. для  $\mathbb{Z}[i]$  норма не поменяется вообще, а для  $\mathbb{Z}[\omega]$   $N = a^2 + ab + b^2 = a^2 - a(a+b) + (a+b)^2$ , т. е. норма элемента  $a - b\omega$  равна норме элемента  $a + (a+b)\omega$ , а такие мы уже перебрали, поскольку  $a+b$  — натуральное. Для  $a < 0$  симметрично.

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
1	4	17	13
1	5	26	21
1	6	37	31
2	2	-	-
2	3	13	7
2	4	-	-
2	5	29	19
2	6	-	-
2	7	53	39
3	3	-	-
3	4	25	13
3	5	34	19
3	6	-	-
3	7	58	37
4	4	-	-
4	5	41	21
4	6	-	-
4	7	65	37
5	5	-	-
5	6	61	31
5	7	74	39
6	6	-	-

Пользуемся №3.16 (№9 exam\_5-6): Пусть  $p$  — простое целое,  $\forall z \in \mathbb{Z}[u] : N(z) \neq p \Rightarrow p$  неразложим в  $\mathbb{Z}[u]$ .

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:

- $y \mathbb{Z}[i] - 4k + 3$
- $y \mathbb{Z}[\omega] - 3k + 2$

#### № 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:  $\forall a \in K \hookrightarrow 0a = 0 \in \{0\}$

•  $K$ :

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

2. Замкнутость относительно умножения:  $\forall a \in K, b \in I = K \hookrightarrow ab \in I = K$  — 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:  $\forall b \in K, ax \in (a) \hookrightarrow b \cdot ax = bx \cdot a \in (a)$

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
- $0 = a_1 \cdot 0 + \dots + a_n \cdot 0$  — 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  $(a) = (b)$ .

- а) •  $\Leftarrow: b \mid a \Rightarrow \exists c : a = cb \Rightarrow ka = (kc)b \Rightarrow (a) \subset (b)$
- $\Rightarrow: (a) \subset (b) \Rightarrow a \in (b) \Rightarrow a = cb \Rightarrow b \mid a$

б) •  $\Rightarrow: a \sim b \Rightarrow \begin{cases} a \mid b \\ b \mid a \end{cases} \Rightarrow (a) \subset (b) \subset (a) \Rightarrow (a) = (b)$

•  $\Leftarrow: (a) = (b) \Rightarrow \begin{cases} a \mid b \\ b \mid a \end{cases} \Rightarrow a \sim b$

№ 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.  $\forall a \in K \hookrightarrow a(x + y) = \underbrace{ax}_{\in I} + \underbrace{ay}_{\in J} \in I + J$

b) 1. •  $x, y \in I \cap J \Rightarrow \begin{cases} x, y \in I \\ x, y \in J \end{cases} \Rightarrow \begin{cases} x + y \in I \\ x + y \in J \end{cases} \Rightarrow x + y \in I \cap J$

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

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

№ 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 идеала  $I \subset K$  является идеалом в  $L$ ; б) прообраз идеала  $J \subset L$  является идеалом в  $K$ ?

► 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  $L$ .  $\varphi^{-1}(J) = \{a \in K : \varphi(a) \in J\}$ .

$$\forall a, b \in \varphi^{-1}(J) : \begin{cases} a + b \in \varphi^{-1}(J), \text{ т. к. } \varphi(a + b) = \varphi(a) + \varphi(b) \in J \\ \exists 1 \in \varphi^{-1}(J), \text{ т. к. } \varphi(1) = 1 \text{ по свойству гомоморфизма} \\ \exists a^{-1} \in \varphi^{-1}(J), \text{ т. к. } \varphi(a^{-1}) = (\varphi(a))^{-1} \in J \end{cases}$$

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

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

№ 19(4.2)

а) Всегда ли факторкольцо коммутативного кольца является коммутативным кольцом?

- • Ассоциативность по сложению — из ассоциативности коммутативного кольца.
- $0 \in K$  — ноль в  $K \Rightarrow 0 + I = I$  — ноль в  $K^*$ :  $(I)(a + I) = (a + I)(I) = aI + I^2 = I$ .
- Обратный по сложению:  $(a + I) + (-a + I) = (-a + I) + (a + I) = I$ .
- Дистрибутивность:  $(a + I)(b + I + c + I) = (ab + I) + (ac + I)$ .
- $1 \in K$  — единица в  $K \Rightarrow 1 + I$  — единица в  $K^*$ :  $(1 + I)(a + I) = (a + I)(1 + I) = a + I + aI + I^2 = a + I$ .
- Ассоциативность по умножению — из ассоциативности коммутативного кольца.
- $(a + I)(b + I) = ab + aI + bI + II = ab + I = ba + I = ba + bI + aI + II = (b + I)(a + I)$  — коммутативность.

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.

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

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

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

№ 21(4.6 (Lecture\_all.pdf теор. 3.2)) 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.

Рассмотрим канонический гомоморфизм  $f : K \rightarrow K/I$ . Заметим:  $f(I) = \{0\}$ ,  $f(K) = K/I$ .

**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) (можно сослаться на №18(б)) Пусть теперь  $x \in f^{-1}(J), y \in K$ . Тогда  $f(xy) = f(x)f(y) \in J$ , следовательно,  $xy \in f^{-1}(J)$ . ◀

•  $\Leftarrow$ : Пусть  $K/I$  — поле, но идеал  $I$  не максимальный. Тогда  $\exists$  нетривиальный идеал  $J \subset K : I \subset J$ . По пункту а) Леммы  $f(J)$  — идеал в  $f(K) = K/I$ . При этом  $I \subset J \Rightarrow \{0\} = f(I) \subset f(J)$ .  $f(J)$  нетривиален, ибо он не  $\{0\}$  (иначе  $J = I$ ) и не  $K/I$  (иначе  $J = K$ ). То есть, получили в поле нетривиальный идеал. Противоречие с тем, что это поле.

•  $\Rightarrow$ : Пусть идеал  $I$  максимален, но  $K/I$  — не поле. Тогда должен быть нетривиальный идеал  $L \subset K/I$ . Его прообраз  $f^{-1}(L)$  по пункту б) Леммы — идеал в  $K$ . При этом  $L \supset \{0\} \Rightarrow f^{-1}(L) \supset f^{-1}(\{0\}) = I$ . Он нетривиален, ибо его прообраз не  $I$  (иначе  $J = \{0\}$ ) и не  $K$  (иначе  $J = K/I$ ). Т. е., получили нетривиальный идеал в  $K$ , содержащий  $I$  — противоречие с максимальнойностью  $I$ . ◀

№ 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  $\exists a, b \in K \setminus I : (a+I)(b+I) = ab+I = 0+I = 0_{K/I}$ . Но тогда должно быть  $ab \in I$ , т. е. идеал не простой (вспомним, что брали  $a, b \in K \setminus I$ ). Противоречие.  
•  $\Leftarrow$ : Пусть  $I$  непростой, но  $K/I$  — область целостности. Тогда  $\exists a, b : ab \in I$ , но  $a, b \notin I$ . Рассмотрим  $(a+I)(b+I) = ab+I \underset{ab \in I}{=} I = 0_{K/I}$ , т. е.  $K/I$  — не область целостности. ◀

№ 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; д)  $F$  является коммутативным кольцом; е)  $F$  является полем; ф) существует инъекция  $K \rightarrow F$ .

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

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

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

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

с) Корректность определения означает, что множество замкнуто относительно операции, и что результат её всегда определён.

- Сложение:
  - $\frac{ad+bc}{bd} \in \text{Quot}(K)$ , т. к.  $ad+bc \in K$  и  $bd \in K$  по свойствам кольца  $K$ .
  - $\nexists \frac{ad+bc}{bd} bd \neq 0$ , т. к.  $b \neq 0$  и  $d \neq 0$ .
- Умножение:
  - $\frac{ac}{bd} \in \text{Quot}(K)$ , т. к.  $a \in K$  и  $bd \in K$  по свойствам кольца  $K$ .
  - $\nexists \frac{ac}{bd} bd \neq 0$ , т. к.  $b \neq 0$  и  $d \neq 0$ .

d) • Это кольцо:

- $\frac{a}{b} + (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} + (\frac{cf+de}{df}) = \frac{adf+bcf+bde}{bdf} = \frac{ad+bc}{bd} + \frac{e}{f} = (\frac{a}{b} + \frac{c}{d}) + \frac{e}{f}$
- Ноль — элемент класса эквивалентности  $\{\frac{0}{a} \mid a \neq 0\}$ . Возьмём  $0_F := \frac{0}{1}$ . Тогда  $\frac{a}{b} + \frac{0}{1} = \frac{0}{1} + \frac{a}{b} = \frac{a}{b}$
- Для  $\frac{a}{b}$  обратный по сложению  $-\frac{a}{b} : \frac{a}{b} + -\frac{a}{b} = \frac{a-a}{b} = \frac{0}{b}$
- $\frac{a}{b}(\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} \cdot \frac{cf+de}{df} = \frac{acf+ade}{bdf} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}$

- Оно ассоциативно по умножению:  $\frac{a}{b}(\frac{c}{d} \cdot \frac{e}{f}) = \frac{a}{b}(\frac{ce}{df}) = \frac{ace}{bdf} = (\frac{ac}{bd})\frac{e}{f} = (\frac{a}{b} \cdot \frac{c}{d}) \cdot \frac{e}{f}$

- Единица — элемент класса эквивалентности  $\{\frac{a}{a} \mid a \neq 0\}$ . Возьмём  $1_F = \frac{1}{1}$ . Тогда  $\frac{a}{b} \frac{1}{1} = \frac{1}{1} \frac{a}{b} = \frac{a}{b}$

- Оно коммутативно:  $\frac{a}{b} \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \frac{a}{b}$

- e) • Каждый ненулевой элемент имеет обратный по умножению  $(\frac{a}{b})^{-1} = \frac{b}{a} : \frac{a}{b} \frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab} = \frac{1}{1}$ .
- Элементов  $\geq 2$ , т. к.  $0 \neq 1$ .

f) Возьмём  $\varphi : K \rightarrow F, \varphi(a) = \frac{a}{1}$ .

$$\text{Это гомоморфизм: } \begin{cases} \frac{ab}{1} = \varphi(ab) = \varphi(a)\varphi(b) = \frac{a}{1} \frac{b}{1} = \frac{a \cdot b}{1 \cdot 1} = \frac{ab}{1} \\ \frac{a+b}{1} = \varphi(a+b) = \varphi(a) + \varphi(b) = \frac{a}{1} + \frac{b}{1} = \frac{a \cdot 1 + 1 \cdot b}{1 \cdot 1} = \frac{a+b}{1} \end{cases}$$

Это инъекция:  $\forall a \neq b \in K \hookrightarrow \varphi(a) = \frac{a}{1} \neq \frac{b}{1} = \varphi(b)$ , ибо  $\frac{a}{1} - \frac{b}{1} = \frac{a-b}{1} \neq 0_F$ .

## № 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, напротив  $f$  не неприводим над  $\mathbb{Q}$ . Тогда существуют два таких многочлена  $g, h \in \mathbb{Q}[x]$ , что  $f = \tilde{g}\tilde{h}$  и  $\deg \tilde{g}, \deg \tilde{h} > 0$ . Положим  $d_1 = (\text{НОД знаменателей коэффициентов } \tilde{g})$  и  $d_2 = (\text{НОД знаменателей коэффициентов } \tilde{h})$ . Тогда есть разложение  $d_1 d_2 f = gh$ , где  $g, h \in \mathbb{Z}[x]$  — многочлены, полученные домножением  $\tilde{g}, \tilde{h}$  на  $d_1, d_2$  соответственно. Так как  $g$  и  $h$  примитивны, то их произведение примитивно, а значит,  $d_1 d_2 = 1$  и верно просто  $f = gh$ .

Заметим, что  $f_0 = g_0 h_0$ . Так как  $f_0$  не делится на  $p^2$ , то одно из чисел  $g_0, h_0$  не делится на  $p$ . Пусть для определенности  $h_0$  не делится на  $p$ , тогда  $g_0$  делится на  $p$ . Пусть число  $k > 0$  таково, что  $g_0, \dots, g_{k-1}$  делятся на  $p$ , а  $g_k$  не делится на  $p$ . По формуле коэффициентов для произведения многочленов  $f_k = g_k h_0 + g_{k+1} h_1 + \dots$ . Если  $k < \deg f$ , то по модулю  $p$  имеем  $0 = g_k h_0$ , где  $g_k, h_0$  не делятся на  $p$ . Значит,  $k = \deg f > \deg g$ . Это означает, что все коэффициенты  $g$  делятся на  $p$ , то есть  $g$  не примитивен. Противоречие.

## № 25(указано 6.2, но на самом деле в нём точно такого пункта нет) Многочлен $x^n - p$ ( $p$ — простое число) неприводим над $\mathbb{Q}$ .

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

## № 26(6.3) Характеристика поля — простое число.

- Если  $\text{char } F = 1$ , то  $1 = 0$ , поле из одного элемента, что не является полем по нашей договорённости.

Если  $\text{char } F = mn, m, n \in \mathbb{N}, m, n > 1$ , то  $\underbrace{(1 + \dots + 1)}_m \underbrace{(1 + \dots + 1)}_n \stackrel{\text{по дистрибутивности}}{=} \underbrace{1 + \dots + 1}_{m \cdot n} = 0$ . Противоречие

с минимальностью  $\text{char } F$ .

## № 27(6.4(Lecture\_all.pdf №6.2(3))) Если существует нетривиальный гомоморфизм полей $\varphi : F \rightarrow K$ , то $\text{char}(F) = \text{char}(K)$ .

- Гомоморфизм нетривиален  $\Rightarrow$  по №29 он является инъекцией, а у инъекции  $\text{Ker } \varphi = \{0\}$  по лемме из №29. Так как  $\varphi(1) = 1$ , имеем  $\varphi(\underbrace{1 + \dots + 1}_m) = \underbrace{1 + \dots + 1}_m$ .

Если  $\underbrace{1 + \dots + 1}_m = 0$  в  $F$ , то по свойству гомоморфизма и в  $K$  тоже. Получили  $\text{char}(K) \leq \text{char}(F)$ .

Т. к.  $\text{Ker } \varphi = \{0\}$ , то только 0 переходит в 0, т. е. получив сложением единичек 0 в  $K$  знаем, что в  $F$  тоже 0. Отсюда  $\text{char}(F) \leq \text{char}(K)$ .

№ 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.

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

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

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

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

- $\Leftarrow$ : Пусть не так.  $\text{Ker } \varphi \neq \{0\} \Rightarrow \exists 0 \neq a \in \text{Ker } \varphi$ . Тогда  $\forall b \in K \hookrightarrow \varphi(b + a) = \varphi(b) + \varphi(a) = \varphi(b)$  — нарушение инъективности.

**Лемма.**  $\text{Ker } \varphi$  — идеал в  $F$

- $\text{Ker } \varphi$  — подгруппа по сложению — простая проверка.

$\forall a, b \in \text{Ker } \varphi \hookrightarrow ab \in \text{Ker } \varphi$ , т. к.  $\varphi(ab) = \varphi(a)\varphi(b) = 0 \cdot 0 = 0$  — замкнутость относительно умножения.

$\forall a \in F, x \in \text{Ker } \varphi \hookrightarrow \varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \cdot 0 = 0 \Rightarrow ax \in \text{Ker } \varphi$

В поле  $F$  идеал  $I = \begin{cases} \{0\} \\ F \end{cases}$ , т. е.  $\text{Ker } \varphi = \begin{cases} \{0\} \\ F \text{ — невозможно} \end{cases}$

(в последнем случае гомоморфизм тривиален, но у нас нетривиальный по условию).

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

- Проверка свойств. Свойства линейного пространства следуют из аксиом поля.

1.  $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$ , для любых  $\mathbf{x}, \mathbf{y} \in V$  ("коммутативность сложения");
2.  $\mathbf{x} + (\mathbf{y} + \mathbf{z}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z}$ , для любых  $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$  ("ассоциативность сложения");
3. существует такой элемент  $\mathbf{0} \in V$ , что  $\mathbf{x} + \mathbf{0} = \mathbf{x}$  для любого  $\mathbf{x} \in V$  ("существование нейтрального элемента относительно сложения"), называемый *нулевым вектором* или просто *нулём* пространства  $V$ ;
4. для любого  $\mathbf{x} \in V$  существует такой элемент  $-\mathbf{x} \in V$ , что  $\mathbf{x} + (-\mathbf{x}) = \mathbf{0}$ , называемый вектором, *противоположным* вектору  $\mathbf{x}$ ;
5.  $\alpha(\beta\mathbf{x}) = (\alpha\beta)\mathbf{x}$  ("ассоциативность умножения на скаляр");
6.  $1 \cdot \mathbf{x} = \mathbf{x}$  ("унитарность: умножение на нейтральный (по умножению) элемент поля  $F$  сохраняет вектор");
7.  $(\alpha + \beta)\mathbf{x} = \alpha\mathbf{x} + \beta\mathbf{x}$  ("дистрибутивность умножения вектора на скаляр относительно сложения скаляров");
8.  $\alpha(\mathbf{x} + \mathbf{y}) = \alpha\mathbf{x} + \alpha\mathbf{y}$  ("дистрибутивность умножения вектора на скаляр относительно сложения векторов").

№ 31(Lecture\_all.pdf утв. 6.2(2)) Любое поле  $F$  нулевой характеристики содержит  $\mathbb{Q}$  в качестве подполя.

- $\tilde{m} := \underbrace{1 + \dots + 1}_m \in F$   
 $m$  штук



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

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  $\mathbb{Z} \subset F$ .

По №5-6.21a  $\text{Quot } F = F$  для поля (подставим  $\text{Quot } F$  вместо  $F$ ).

**Лемма.** (используется для доказательства №5-6.21b) Если  $K \subset L$ , то  $\text{Quot } K \subset \text{Quot } L$  для всех колец  $K$  и  $L$ .

- $K \subset L \Rightarrow \text{Quot } K$  вложено в  $\text{Quot } L$  как множество. Инъективное отображение строится как  $\varphi : \text{Quot } K \rightarrow \text{Quot } L, \frac{a}{b} \mapsto \frac{a}{b}$ . Очевидно, это инъекция (по №3-4.23f). ◀

У нас  $\mathbb{Z} \subset F \Rightarrow \mathbb{Q} = \text{Quot } \mathbb{Z} \subset \text{Quot } F = F$ . ◀

**№ 32 (Lecture\_all.pdf утв. 6.5(2))** Пусть  $f(x)$  — неприводимый многочлен степени  $n$ , и  $K = F[x]/(f(x))$ . Тогда многочлен  $\bar{f}(x)$  имеет корень в  $K$ .

- 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.  $f(\bar{x}) = \bar{f}(x) = 0$ . ◀

**№ 33 (Lecture\_all.pdf утв. 6.5(1))** 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.  $[K : F] = n$ . ◀

**№ 34 (7.9, 7.10)** Умение находить степень расширения и минимальный многочлен для алгебраического над полем элемента.

- Как находить минимальный многочлен  $m_\alpha$ ? Придумать многочлен, у которого  $\alpha$  является корнем, и доказать (например, по критерию Эйзенштейна из №24), что он неприводим. Тогда по СЭУ из опр. 29 минимального многочлена, это действительно минимальный многочлен.

По №7.1г(№30г exam\_5-6), степень расширения равна степени минимального многочлена.

- $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q} : m = x^2 - 2 \Rightarrow \deg = 2$
- $\mathbb{Q}(\sqrt[3]{5}) \supset \mathbb{Q} : m = x^3 - 5 \Rightarrow \deg = 3$
- $\mathbb{R}(2 - 3i) \supset \mathbb{R} : \deg = 2$   
 $m = 9x^2 + 4 = (2 - 3i)(2 + 3i)$  — сложно доказывать неприводимость, критерий Эйзенштейна не помогает.

Попробуем воспользоваться теоремой Виета:  $\begin{cases} c = (2 - 3i)(2 + 3i) = 4 + 9 = 13 \\ b = (2 - 3i) + (2 + 3i) = 4 \end{cases} \quad . \quad m = x^2 - 4x + 13$ . Тоже

неудача, критерий Эйзенштейна не помогает.

Замена  $x \mapsto x + 1$ :  $m = (x + 1)^2 - 4(x + 1) + 13 = x^2 - 2x + 10$ . Применяем критерий Эйзенштейна для  $p = 2$  и получаем, что  $m$  неприводим.

- $\mathbb{C}(2 - 3i) \supset \mathbb{C} : \deg = 1$   
 $m = x - (2 - 3i)$   
 $N(2 - 3i) = 4 + 9 = 13$  — простое число, значит,  $2 - 3i$  — простой элемент (по №3.1a(№5-6.9) знаем, что если норма — простое число, то элемент неразложим, а по №2.8(№5-6.5) в факториальном кольце простота эквивалентна неразложимости (по №7-8.7 евклидово кольцо факториально)).  
 Применяем критерий Эйзенштейна для  $p = 2 - 3i$  и получаем, что  $m$  неприводим.

- $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \supset \mathbb{Q} : \deg = 4$   
 $\alpha := \sqrt{2} + \sqrt{3} \Rightarrow \alpha^2 = 5 + 2\sqrt{6} \Rightarrow \alpha^2 - 5 = 2\sqrt{6} \Rightarrow (\alpha^2 - 5)^2 = 24$   
 $m = \alpha^4 - 10\alpha^2 + 1$

Критерий Эйзенштейна не работает. Замену подобрать не получается.

Воспользуемся эквивалентным определением минимального многочлена  $m_\alpha$ : это многочлен минимальной степени, обнуляющийся на  $\alpha$ . Разложим  $m$  на линейные множители над  $\mathbb{Q}$ .  $m = (x^2 + 2\sqrt{6} - 5)(x^2 - 2\sqrt{6} - 5) = (x - \sqrt{5 - 2\sqrt{6}})(x + \sqrt{5 - 2\sqrt{6}})(x - \sqrt{2\sqrt{6} + 5})(x + \sqrt{2\sqrt{6} + 5})$ . Минимальный многочлен должен быть произведением каких-то из этих множителей и иметь коэффициенты из  $\mathbb{Q}$ . Произведением одной или трёх

множителей он быть не может (иначе коэффициент из  $\mathbb{C}$ ), двух — тоже (коэффициент из  $\mathbb{R}$ ). Итого, надо брать все четыре множителя, т. е. наш найденный  $m$  и есть минимальный многочлен.

- $\mathbb{Q}(1 + \sqrt{2}) \supset \mathbb{Q}(\sqrt{2} + \sqrt{3})$ :  $\deg = 1$

**Лемма.**  $\mathbb{Q}[\sqrt{2} + \sqrt{3}] \cong \mathbb{Q}[\sqrt{2}, \sqrt{3}]$

►  $\subseteq$  очевидно.

⊇: Рассмотрим  $\frac{1}{\sqrt{2} + \sqrt{3}} = \frac{\sqrt{3} - \sqrt{2}}{3 - 2} = \sqrt{3} - \sqrt{2}$  — обратный к  $\sqrt{2} + \sqrt{3}$  (он есть, т. к.  $\mathbb{Q}[\sqrt{2} + \sqrt{3}] \cong \mathbb{Q}\sqrt{2} + \sqrt{3}$ ) — полю.

$(\sqrt{2} + \sqrt{3}) + (\sqrt{3} - \sqrt{2}) = 2\sqrt{3}$ , т. е.  $\sqrt{3}$  лежит в кольце. Тогда  $\sqrt{2} = (\sqrt{2} + \sqrt{3}) - \sqrt{3}$  тоже лежит в кольце. ◀

Тогда  $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \cong \mathbb{Q}(\sqrt{2})(\sqrt{3})$

$m = x - (1 + \sqrt{2})$  — степени 1, неразложимый.  $1 + \sqrt{2} \in \mathbb{Q}(\sqrt{2})(\sqrt{3})$ .

- $\mathbb{Q}(\omega) \supset \mathbb{Q}$ :  $\deg = 2$

$m = x^2 + x + 1$ :  $m(\omega) = 0$  (можно понять по картинке), неприводим по критерию Эйзенштейна после замены  $x \mapsto x + 1$  для  $p = 3$ ,  $\deg m = 2$ .

- $\mathbb{Q}(\sqrt[3]{2}, \omega) \supset \mathbb{Q}$ :  $\deg = 6$

$\mathbb{Q}(\sqrt[3]{2}, \omega) \cong \mathbb{Q}[\sqrt[3]{2}][\omega]$  по №7.4а, имея в виду, что  $F[\alpha_1, \dots, \alpha_n] \cong F[\alpha_1] \dots [\alpha_n]$  — очевидно, и что  $\sqrt[3]{2}$  и  $\omega$  алгебраичны над  $\mathbb{Q}$ .

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ , т. к.  $m = x^3 - 2$  — неприводим по критерию Эйзенштейна.

$\omega \notin \mathbb{Q}(\sqrt[3]{2})$ , т. к. в  $\mathbb{Q}(\sqrt[3]{2})$  нет комплексных чисел. Значит,  $m = x^2 + x + 1$  неприводим над  $\mathbb{Q}(\sqrt[3]{2})$  по критерию Эйзенштейна.

Итого, пользуясь №7.3(№32 exam\_5-6),  $3 \cdot 2 = 6$

- $\mathbb{Q}(\sqrt[4]{2}, i) \supset \mathbb{Q}$ :  $\deg = 8$

Аналогично,  $4 \cdot 2 = 8$ .

- $\mathbb{Q}(\sqrt[5]{2}, i) \supset \mathbb{Q}$ :  $\deg = 10$

Аналогично,  $5 \cdot 2 = 10$ .

**TODO: проставить ссылки на утверждения** ◀

№ 35(6.10, 8.9а, 10.5) Умение описывать расширения степени 2: минимальный многочлен, поле разложения, нормальность, группа Галуа.

- На примере  $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ . Степень 2. Мин. многочлен  $x^2 - 2$  — степени 2.  $\mathbb{Q}(\sqrt{2})$  — поле разложения многочлена  $x^2 - 2$ , т. к. все его корни  $\sqrt{2}, -\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ . Не существует промежуточных, потому что тогда они имеют степень 1 или 2, т. е. совпадают с  $\mathbb{Q}(\sqrt{2})$  или с  $\mathbb{Q}$ .

Рассмотрим автоморфизмы  $\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$ . Их всего 2:

$$a + \sqrt{2}b \mapsto a + \sqrt{2}b$$

$$a + \sqrt{2}b \mapsto a - \sqrt{2}b$$

Других нет, т. к. достаточно рассматривать только перестановки корней минимального многочлена:

$$\sqrt{2} \mapsto \pm\sqrt{2}$$

$$-\sqrt{2} \mapsto \mp\sqrt{2}$$

Другие не рассматриваются, поскольку 1 и ЛНЗ корни многочлена образуют базис в  $\mathbb{Q}(\sqrt{2})$  как линейном пространстве над  $\mathbb{Q}$ ; 1 при этом должен перейти в 1, т. к.  $\mathbb{Q}$  сохраняется.

Таких автоморфизмов 2  $\Rightarrow$  степень расширения 2  $\Rightarrow$  это расширение Галуа. Группа из двух элементов —  $\mathbb{Z}_2$  — то группа Галуа данного расширения (других (с точностью до изоморфизма) групп из 2-х элементов не бывает). ◀

№ 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  $f(x) - f(y) = \sum_{k=1}^n a_k(x^k - y^k) = (x - y) \sum_{k=1}^n a_k(x^{k-1} + x^{k-2}y + \dots + y^{k-1}) = (x - y)\Phi(x, y)$ , где

$\Phi(x, y) = \sum_{k=1}^n a_k(x^{k-1} + x^{k-2}y + \dots + y^{k-1})$ . 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) (для  $\text{char } F = 0$ ) Многочлен  $f$  не имеет кратных корней тогда и только тогда, когда  $(f, f') = 1$ .

- Пусть  $f(x) = (x - a)^m f_1(x)$ ,  $f_1(x) \not\equiv (x - a)$ ,  $m \geq 2$ . 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  $f'(x)$ .

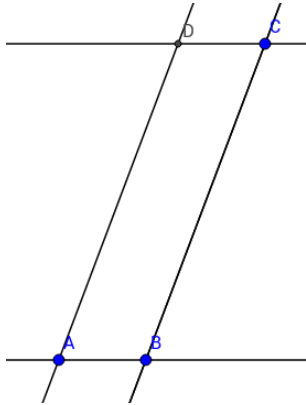
№ 38(9.6) Докажите, что можно построить

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

Если мы построили точки  $z, w$ , то можно ли построить точки с)  $\bar{z}, -z$ ? д)  $z + w, z - w$ ? е)  $z \cdot w$ ?

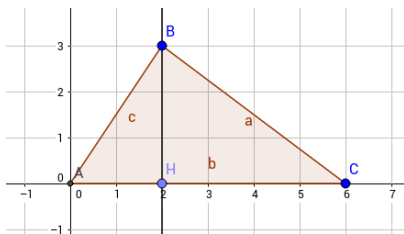
- При помощи гугла учимся строить: перпендикулярную прямую (через заданную точку), параллельную прямую (через заданную точку).

Как обосновать то, что мы можем брать раствор циркуля, равный расстоянию между какими-то двумя точками, и переносить его на другое место? Пусть есть отрезок  $AB$ , и мы хотим окружность с радиусом  $AB$  и центром в т.  $C$ .



Строим параллелограмм как на рисунке.  $CD = AB$ .

- а) Берём отрезок  $01$  и произвольную точку  $A$ , не лежащую на нём. Проводим  $0A$ . На луче  $0A$  начиная от точки  $0$  откладываем  $n$  равных отрезков произвольной длины. Пусть их концы, лежащие на  $0A$ , есть  $A_1, \dots, A_n$  (считая от точки  $0$ ). Проводим  $A_n1 = A_nB_n$  и параллельно ей  $A_{n-1}B_{n-1}, \dots, A_1B_1$ . По теореме Фалеса  $0B_1 = B_1B_2 = \dots = B_{n-1}1$ . Сделав так для любого  $n$ , получим все точки с рациональными координатами на  $01$ , разложить на ось  $OX$  тривиально, получить так же поделенную ось  $OY$  тривиально, а т. к. любая точка однозначно задаётся проекциями и мы умеем строить перпендикуляры, можем строить любую точку с рациональными координатами.
- б) Шестиугольник — откладывая на окружности хорды длиной с радиус, треугольник — по шестиугольнику, четырёхугольник — строя перпендикуляр из центра окружности, в которую он вписан.
- с) Отражение относительно осей.
- д) Тривиально.
- е) В экспоненциальной записи:  $zw = r_1 e^{i\varphi_1} r_2 e^{i\varphi_2} = (r_1 r_2) e^{i(\varphi_1 + \varphi_2)}$ . Итого, надо научиться строить сумму углов и отрезок с длиной, равной произведению двух других. Сумма углов: тривиально. Произведение: пользуемся теоремой из геометрии о соотношении высоты прямоугольного треугольника со всякими другими отрезками (та, которая выводится из подобия).



Взяв  $BH = h^2, AH = a^2, CH = b^2$ , получим  $BH^2 = AH \cdot CH \Rightarrow BH = ab$ .  
Как строить  $a^2$  и  $b^2$ ? Взяв  $BH = a^2, AH = 1, CH = x$ , получим  $a^2 = 1 \cdot x \Rightarrow x = a^2$ .

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

- Задача сводится к построению циркулем и линейкой числа  $\sqrt[3]{2}$ .

Минимальный многочлен для  $\sqrt[3]{2}$  есть  $x^3 - 2$ , неприводимый по признаку Эйзенштейна в  $\mathbb{Q}$  и потому минимальный. Значит, размерность расширения  $= 3 \Rightarrow$  не существует башни промежуточных расширений размерности  $\leq 2 \Rightarrow$

по №19 exam\_7-8 её нельзя построить.

№ 40 (10.2) Пусть  $\varphi : F \rightarrow F$  — автоморфизм поля  $F$  (изоморфизм поля на себя). а) Пусть  $\text{char} F = 0$ . Верно ли, что  $\varphi$  сохраняет  $\mathbb{Q}$ ? (то есть при  $q \in \mathbb{Q}$  выполнено равенство  $\varphi(q) = q$ ). б) Пусть  $\text{char} F = p$ . Верно ли, что  $\varphi$  сохраняет  $\mathbb{Z}_p$ ?

- а) Автоморфизм переводит единицу в единицу:  $\varphi(1) = 1$  по свойствам гомоморфизма. Тогда  $\forall p \in \mathbb{Z} \hookrightarrow \varphi(p) = \varphi(\underbrace{1 + \dots + 1}_p) = \underbrace{1 + \dots + 1}_p = p$ . Получили, что  $\mathbb{Z}$  сохраняется.

Тогда  $\varphi(2) = \varphi(1 + 1) = \varphi(1) + \varphi(1) = 1 + 1 = 2$ . И так далее. Получили, что  $\mathbb{Z}$  сохраняется.

Если какой-нибудь элемент  $\frac{a}{b} \in \mathbb{Q}$  перевёлся не в себя, то  $\varphi(\underbrace{\frac{a}{b} + \dots + \frac{a}{b}}_b) = \underbrace{\varphi(\frac{a}{b}) + \dots + \varphi(\frac{a}{b})}_b \neq a$ , т. е. в  $\mathbb{Z}$

что-то перешло не в себя. Противоречие.

- б) Да, т. к. если  $m \in \mathbb{Z}_p$ , то  $\varphi(m) = \underbrace{\varphi(1) + \dots + \varphi(1)}_m = m$

№ 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  $K \supset K^H \supset F$ .

- а) Композиция автоморфизмов, сохраняющих  $F$ , — автоморфизм, сохраняющий  $F \Rightarrow$  замкнутость.

$id$  — нейтральный элемент.

Ассоциативность следует из свойств композиции.

Обратный существует, т. к. автоморфизм — биекция. Обратный сохраняет  $F$ .

- б) Пусть  $a, b \in K^H, h \in H$ . Тогда  $h(a + b) = h(a) + h(b) = a + b$ , и поэтому  $a + b \in K^H$ . Аналогично,  $ab \in K^H$ . С другой стороны,  $h \in H \subset G$ , и поэтому  $h$  сохраняет  $F$ . Значит,  $F \subset K^H$ .  $K^H \subset K$  по определению.

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

- По №40 знаем, что автоморфизм сохраняет  $\mathbb{Q}$ . Значит, нужно смотреть только за тем, куда переходит  $\sqrt[3]{2}$ . Рассмотрим минимальный многочлен для  $\sqrt[3]{2}$ :  $m = x^3 - 2$ . Куда может перейти  $\sqrt[3]{2}$ ? В  $\sqrt[3]{2}, \underbrace{\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2}_{\notin \mathbb{Q}(\sqrt[3]{2})}$ . Значит, он

может перейти только в себя.  $\text{Aut}_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = \{id\}$ , т. к. все другие перестановки корней дают комплексные числа.

Знаем, что любой автоморфизм задаётся перестановкой корней минимального многочлена.

Пусть  $\varphi$  — автоморфизм. Тогда  $\varphi(m_{\gamma}(\gamma)) = 0 \Rightarrow 0 = a_n \varphi(\gamma)^n + \dots + a_0 \Rightarrow \varphi(\gamma)$  — корень  $m_{\gamma} \Rightarrow$  сопряжён с  $\gamma$ .

Степень расширения равна степени минимального многочлена, т. е. 3.

№ 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)  $\mathbb{F}_2$ , б)  $\mathbb{F}_3$ .

- Выписываем все возможные многочлены и вычёркиваем те, которые разложимы. Если мы вычеркнули все разложимые (а мы умеем это делать, см. пункт а), то остались только неразложимые.

Количество  $M_k$  неприводимых многочленов степени  $k$  над  $\mathbb{Z}_p$  можно посчитать по формуле  $M_k = \frac{1}{k} \sum_{d|k} p^d \mu(\frac{k}{d})$

(теор. 11.3 из Lecture\_all), где функция Мёбиуса

$$\mu(n) = \begin{cases} 1, n \text{ свободно от квадратов и разложение } n \text{ на простые состоит из чётного числа сомножителей,} \\ -1, n \text{ свободно от квадратов и разложение } n \text{ на простые состоит из нечётного числа сомножителей,} \\ 0, n \text{ не свободно от квадратов,} \end{cases}$$

$$\mu(1) = 1.$$

Так можно проверить результат.

- a)  $\mathbb{F}_2$ : Неразложимые степени 1:  $x$  и  $x+1$ . Разложимые степени 2 — какая-то комбинация многочленов степени 1. Оставшиеся — неразложимы. Теперь смотрим всё возможные многочлены степени 3, которые можно получить, перемножая многочлены степени 1 и многочлены степени 2.

$$\deg = 2, M_2 = 1: x^2, \underbrace{x^2+1}_{(x+1)(x+1)}, x^2+x, x^2+x+1$$

$$\deg = 3, M_3 = 2: x^3, \underbrace{x^3+1}_{(x^2+1)(x^2+x+1)}, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, \underbrace{x^3+x^2+x+1}_{(x^2+1)(x+1)}$$

- b)  $\mathbb{F}_3$ : Рассуждения аналогичны.

$$\deg = 2, M_2 = 3: x^2, x^2+1, \underbrace{x^2+2}_{(2x+1)(2x+2)}, x^2+x, \underbrace{x^2+x+1}_{(x+2)^2}, x^2+x+2, x^2+2x, \underbrace{x^2+2x+1}_{(2x+2)^2}, x^2+2x+2$$

$$\deg = 3, M_3 = 8:$$

$$\begin{aligned} & x^3, \underbrace{x^3+1}_{(x^2+2x+1)(x+1)}, \underbrace{x^3+2}_{(x^2+x+1)(x+2)}, x^3+x, \underbrace{x^3+x+1}_{(x^2+x+2)(x+2)}, \underbrace{x^3+x+2}_{(x^2+2x+2)(x+1)}, x^3+2x, x^3+2x+1, x^3+2x+2, x^3+x^2, \\ & \underbrace{x^3+x^2+1}_{(x^2+2x+2)(x+2)}, x^3+x^2+2, x^3+x^2+x, \underbrace{x^3+x^2+x+1}_{(x^2+1)(x+1)}, x^3+x^2+x+2, x^3+x^2+2x, x^3+x^2+2x+1, \\ & \underbrace{x^3+x^2+2x+2}_{(x^2+2)(x+1)}, x^3+2x^2, x^3+2x^2+1, \underbrace{x^3+2x^2+2}_{(x^2+x+2)(x+1)}, x^3+2x^2+x, x^3+2x^2+x+1, \\ & \underbrace{x^3+2x^2+x+2}_{(x^2+1)(x+2)}, x^3+2x^2+2x, \underbrace{x^3+2x^2+2x+1}_{(x^2+2)(x+2)}, x^3+2x^2+2x+2 \end{aligned}$$

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

- Для  $p^n$ :  $F_{p^n} = F_p[x]/(f(x))$ , где  $f(x)$  — неприводимый многочлен степени  $n$  (пользуемся №33:  $[F[x]/(f(x)) : F] = n$ ). Итого, надо просто найти неприводимый многочлен над  $F_p$  степени  $n$ . Как искать неприводимые многочлены рассказано в №44.

Чтобы выписать элементы кольца явно, берём все возможные многочлены нужной степени над нужным полем и делим с остатком на многочлен, по которому факторизуем (факторизация в данном случае и есть деление с остатком). То есть, нужно выписать все возможные остатки при делении на наш многочлен.

Далее пишем "таблицу умножения" по модулю многочлена. Она может быть большой, посему пишем частично, чтобы показать, что можем.

- a)  $4 = 2^2 \mathbb{F}_4 = F_2[x]/(x^2+x+1) = \{0; 1; x; 1+x\}$

$\times$	0	1	$x$	$x+1$
0	0	0	0	0
1	0	1	$x$	$x+1$
$x$	0	$x$	$x^2 = x+1$	$x^2+x = 1$
$x+1$	0	$x+1$	$x^2+x = 1$	$x^2+1 = x$

- b)  $8 = 2^3 \mathbb{F}_8 = F_2[x]/(x^3+x^2+1) = \{0; 1; x; x+1; x^2; x^2+1; x^2+x; x^2+x+1\}$

- c)  $9 = 3^2 \mathbb{F}_9 = F_3[x]/(x^2+1) = \{0; 1; 2; x; x+1; x+2; 2x; 2x+1; 2x+2\}$