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

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

a) $a0 = 0a = 0$

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

$0a = 0$ — аналогично. ◄

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

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

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

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 $1 \neq 0$.

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

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 К коммутативным? ассоциативным?кольцом с единицей? область целостности? поле? евклидово кольцо? Какие в К 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: $a_1, \ldots, a_n$. Элементы $a \cdot a_1, \ldots, a \cdot a_n$ должны быть все разные (иначе $\forall i \neq j, a \neq 0\ a \cdot a_i = a \cdot a_j \Rightarrow \underbrace{a}_{\neq 0} \underbrace{(a_i - a_j)}_{\neq 0, \text{ т. к. } i \neq j} = 0$, т. е. a — делитель нуля).

Тогда $\exists i : a \cdot a_i = 1$, т. к. $1 \in K$ (т. е. $a \cdot a_1, \ldots, a \cdot a_n$ — 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 ≥ 2 элементов по условию. ◄

№ 8 Множество K^* обратимых элементов коммутативного кольца К 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 $a = \mathrm{Re}\,(z)$), а число b — **мнимой частью** z (пишется $b = \mathrm{Im}\,(z)$). 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 $\mathrm{Arg}\,(z)$. 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 $r = |z|$, $\varphi = \mathrm{Arg}\,(z)$.

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 $\overline{z} = a - bi$ называется **комплексно-сопряжённым** к z. Выполнены следующие равенства:

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

◄

№ 10(2.2)

a) Следующие условия эквивалентны:

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

► • $(1) \Rightarrow (2) : \exists r \in K^* : x = ry \Rightarrow y|x$ по определению. Т. к. $r \in K^*$, $\exists r^{-1} \in K^* : r^{-1}x = y \Rightarrow x|y$ по определению.
• $(2) \Rightarrow (3)$: Пусть $x|y, x \vdots a$. Тогда $y = xc, x = ab$ (по опр.) $\Rightarrow y = xc = abc = a(bc) \Rightarrow y \vdots a$.
• $(3) \Rightarrow (2)$: Множества делителей x и y совпадают, $x|x \Rightarrow x$ будет во множестве делителей y, т. е. $x|y$. Симметрично, $y|x$.
• $(2) \Rightarrow (1) : \begin{cases} x|y \Rightarrow y = kx \\ y|x \Rightarrow x = ty \end{cases}$ Тогда $y = kty \Rightarrow kt = 1$ Значит, k и t обратимы. Значит, $x = ty, t \in K^* \Rightarrow x \sim y$ по определению.

◄

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

◄

№ 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.

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

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

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

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

◄

№ 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 $z \in D$ с $N(z) = p$. Сформулируйте гипотезу о том, какие простые целые числа являются простыми в D.

► Выпишем все варианты a, b с нормой ≤ 40.

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

TODO: отрицательные значения.

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 утверждением с лекции: Пусть p – простое целое, $\forall z \in D : N(z) \neq p \Rightarrow$ p неразложим в D.

Выпишем все простые числа ≤ 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 $\mathbb{Z}[\omega]$ $3k + 2$ или TODO. ◄

№ 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

b) $(a) = \{ax \mid x \in K\}$ — **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: $\forall b \in K \forall ax \in (a)\ b \cdot ax = bx \cdot a \in (a)$

c) $(a_1, \ldots, a_n) = \{a_1x_1 + \ldots + a_nx_n \mid x_1, \ldots, x_n \in K\}$ — **конечно-порождённый идеал**, то есть идеал, порождённый конечным количеством элементов.
1. Подгруппа по сложению:
- $(a_1x_1 + \cdots + a_nx_n) + (a_1y_1 + \cdots + a_ny_n) = a_1(x_1 + y_1) + \cdots + a_n(x_n + y_n) \in I$ — замкнутость относительно сложения
- Ассоциативность наследуется
- $0 = a_1 \cdot 0 + \cdots + a_1 \cdot 0$ — нейтральный элемент: $ax + 0 = 0 + ax = ax$
- $(a_1x_1 + \cdots + a_nx_n) + (a_1(-x_1) + \cdots + a_n(-x_n)) = 0$
2. Замкнутость относительно умножения: $\forall y \in K\ y \cdot (a_1x_1 + \cdots + a_nx_n) = a_1(x_1y) + \cdots + a_n(x_ny) \in I$

◀

№ 15(3.11) a) Докажите, что $(a) \subset (b)$ тогда и только тогда, когда $b \mid a$.

b) Докажите, что $a \sim b$ тогда и только тогда, когда $(a) = (b)$.

▶ a)
- $\Leftarrow$: $b|a \Rightarrow \exists c : a = cb \Rightarrow ka = (kc)b \Rightarrow (a) \subset (b)$
- $\Rightarrow$: $(a) \subset (b) \Rightarrow a \in (b) \Rightarrow a = cb \Rightarrow b|a$

b)
- $\Rightarrow$: $a \sim b \Rightarrow \begin{cases} a|b \\ b|a \end{cases} \Rightarrow (a) \subset (b) \subset (a) \Rightarrow (a) = (b)$
- $\Leftarrow$: $(a) = (b) \Rightarrow \begin{cases} a|b \\ b|a \end{cases} \Rightarrow a \sim b$

◀

№ 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.

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

◀

№ 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 ≥ 2 элементов, т. к. $0 \in K$, и мы брали $0 \neq x \in K$).

◀

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

a)

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

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

b)

► 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)

a) 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.

◀

b) Имеется **канонический** гомоморфизм $\varphi : K \to K/I$, 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 $\rightleftharpoons$ если $ab \in (x)$, то $\left[\begin{array}{l} a \in (x) \\ b \in (x) \end{array}\right.$

x — простой $\rightleftharpoons$ если $ab \;\vdots\; x$, то $\left[\begin{array}{l} a \;\vdots\; x \\ b \;\vdots\; x \end{array}\right.$

Но $ab \in (x) \Leftrightarrow ab \;\vdots\; x$ (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 $\varphi : K \to {}^{K}/_{I}$.

Лемма. Пусть $f : K \to L$ — гомоморфизм колец, $I \subset K, J \subset L$ — идеалы. Тогда a) $f(I)$ — идеал в $f(K)$, b) $f^{-1}(J)$ — идеал в K.

▶ a) 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 $x'y' \in I$.

b) 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 $0 \neq (a + I)(b + I) = ab + I \underbrace{=}_{ab \in I} I = 0_{K/I}$.

◀

№ 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 $ad = bc$.

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

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

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

Докажите, что

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

▶ 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) Корректность определения означает, что операция замкнута, и что результат её всегда определён.

- Сложение:
  - $\frac{ad+bc}{bd} \in \mathrm{Quot}(K)$, т. к. $ad + bc \in K$ и $bd \in K$ по свойствам кольца K.
  - У $\frac{ad+bc}{bd}$ $bd \neq 0$, т. к. $b \neq 0$ и $d \neq 0$.
- Умножение:
  - $\frac{ac}{bd} \in \mathrm{Quot}(K)$, т. к. $a \in K$ и $bd \in K$ по свойствам кольца K.
  - У $\frac{ac}{bd}$ $bd \neq 0$, 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 $\frac{a}{b} + \frac{0}{1} = \frac{0}{1} + \frac{a}{b} = \frac{0}{1}$
  - Для $\frac{a}{b}$ обратный по сложению $\frac{-a}{b}$: $\frac{a}{b} + \frac{-a}{b} = \frac{a-a}{b} = \frac{0}{b}$
  - $\frac{a}{b}(\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} \cdot \frac{cf+de}{df} = \frac{acf+ade}{bdf} = \frac{acbf+aebd}{bdf} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}$
- 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 ≥ 2, т. к. $0 \neq 1$.

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

Это гомоморфизм: $\frac{ab}{1} = \varphi(ab) = \varphi(a)\varphi(b) = \frac{a}{1}\frac{b}{1} = \frac{a\cdot 1+1\cdot b}{1\cdot 1} = \frac{ab}{1}$.

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 $d_1 =$ (НОД знаменателей коэффициентов $\tilde{g}$) и $d_2 =$ (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 $g_0, \ldots, g_{k-1}$ делятся на p, а g_k не делится на p. По формуле коэффициентов для произведения многочленов $f_k = g_k h_0 + g_k h_1 + \ldots$. 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 примтивен. 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: $1 \not\vdots p, -p \vdots p, -p \not\vdots p^2$, 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 $\mathrm{char}(F) = \mathrm{char}(G)$?

► Так как $\varphi(1) = 1$, имеем $\varphi(\underbrace{1 + \cdots + 1}_{m}) = \underbrace{1 + \cdots + 1}_{m}$. Т. к. $\operatorname{Ker} \varphi = \{0\}$, то $\underbrace{1 + \cdots + 1}_{m} = 0$ в K и F одновременно.

Следовательно, $\operatorname{char} F = \operatorname{char} K$. ◀

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

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

Получается, что F бесконечно. Противоречие. ◀

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

► **Лемма.** $\varphi : F \to L$ – инъекция $\Leftrightarrow \operatorname{Ker} \varphi = \{0\}$.

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

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

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

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

◀

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

► $\forall a \in F \forall x \in \operatorname{Ker} \varphi\ \varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \cdot 0 = 0 \Rightarrow ax \in \operatorname{Ker} \varphi$ ◀

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

◀

№ 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)) Любое поле F нулевой характеристики содержит $\mathbb{Q}$ в качестве подполя.

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

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

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

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

Получили $\mathbb{Z} \subset F$. $\mathbb{Q} = \operatorname{Quot} \mathbb{Z} \subset F$, так как если $A \subset B$, то $\operatorname{Quot} A \subset \operatorname{Quot} B$ для всех колец и $\operatorname{Quot} F = F$ для поля. У нас $\mathbb{Z} \subset F \Rightarrow \mathbb{Q} = \operatorname{Quot} \mathbb{Z} \subset \operatorname{Quot} F = F$ (используется №21 из exam_5-6).

◀

№ 32 (Lecture_all.pdf утв. 6.5(2)) Пусть $f(x)$ — неприводимый многочлен степени n, и $K = F[x]/(f(x))$. Тогда многочлен $f(x)$ имеет корень в K.

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

№ 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 $\overline{g}(x) \in K$. Рассмотрим $\overline{1}, \overline{x}, \ldots, \overline{x}^{n-1}$. Пусть они ЛЗ, т. е. $\exists \lambda_0, \lambda_1, \ldots, \lambda_{n-1} \in F : \lambda_0 \cdot \overline{1} + \lambda_1 \cdot \overline{x} + \cdots + \lambda_{n-1} \cdot \overline{x}^{n-1} = 0$. Тогда $g(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_{n-1} x^{n-1} \in (f(x))$, а по неприводимости $f(x)$ имеем $g(x) = 0$, т. е. $\lambda_0 = \lambda_1 = \cdots = \lambda_{n-1} = 0$, и данная ЛК тривиальна. Поэтому $\overline{1}, \overline{x}, \ldots, \overline{x}^{n-1}$ ЛНЗ.

$\forall$ многочлена $h(x) \in F[x]$ $\overline{h}(x)$ — образ при факторизации по идеалу $(f(x))$ — совпадает с $\overline{r}(x)$, где $r(x)$ — остаток от деления $h(x)$ на $f(x)$. Поэтому $\overline{1}, \overline{x}, \ldots, \overline{x}^{n-1}$ 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.

▶
- $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q} - 2$
- $\mathbb{Q}(\sqrt[7]{5}) \supset \mathbb{Q} - 7$
- $\mathbb{R}(2 - 3i) \supset \mathbb{R} - 2$
- $\mathbb{C}(2 - 3i) \supset \mathbb{C} - 1$
- $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \supset \mathbb{Q} - 4$
- $\mathbb{Q}(1 + \sqrt{2}) \supset \mathbb{Q}(\sqrt{2} + \sqrt{3}) - 1$
- $\mathbb{Q}(\omega) \supset \mathbb{Q} - 2$
- $\mathbb{Q}(\sqrt[3]{2}, \omega) \supset \mathbb{Q} - 6$
- $\mathbb{Q}(\sqrt[4]{2}, i) \supset \mathbb{Q} - 8$
- $\mathbb{Q}(\sqrt[5]{2}, i) \supset \mathbb{Q} - 10$

TODO: почему??? ◀

№ 6.10,8.9a,9.5) 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 $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$. 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 $b(x) = b_n x^n + \dots + b_1 x + b_0$:

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

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

Тогда имеем для $\varphi = fg$: $\varphi(x) - phi(y) = f(x)g(x) - f(y)g(y) = f(x)(g(x) - g(y)) + g(y)(f(x) - f(y)) = (x-y)[f(x)G(x,y) + g(y)\Phi(x,y)]$. 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 $f(x) = (x-a)^m f_1(x), f_1(x) \not\vdots (x-a), m \geq 2$. 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 $f'(x)$.

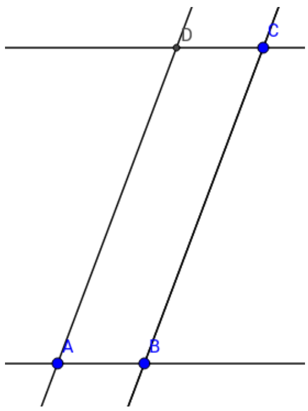
◀

№ 38(9.6) Докажите, что можно построить
a) все точки с рациональными координатами; b) ξ_n, где $n = 3, 4, 6$; c) ξ_5.

Если мы построили точки z, w, то можно ли построить точки d) $\overline{z}, -z$? e) $z + w$, $z - w$? f) $z \cdot w$, $\frac{z}{w}$ (при $w \neq 0$)? g) $\sqrt{z}$?

► 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. $CD = AB$.

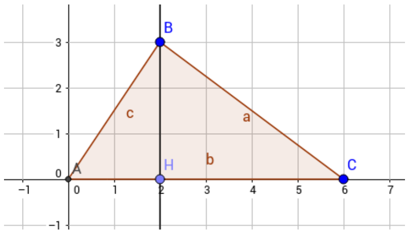
a) Берём отрезок 01 и произвольную точку A, не лежащую на нём. Проводим $0A$. На луче $0A$ начиная от точки 0 откладываем n равных отрезков произвольной длины. Пусть их концы, лежащие на $0A$, есть $A_1, \dots, A_n$ (считая от точки 0). Проводим $A_n 1 =: A_n B_n$ и параллельно ей $A_{n-1}B_{n-1}, \dots, A_1 B_1$. По теореме Фалеса $0B_1 = B_1 B_2 = \dots = B_{n-1}1$. Сделав так для любого n, получим все точки с рациональными координатами на 01, размножить 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.

b) Шестиугольник — откладывая на окружности хорды длиной с радиус, треугольник — по шестиугольнику, четырёхугольник — строя перпендикуляр из центра окружности, в которую он вписан.

c) Отражение относительно осей.

d) Тривиально.

e) В экспоненциальной записи: $z\omega = r_1 e^{i\varphi_1} r_2 e^{i\varphi_2} = (r_1 r_2) e^{i(\varphi_1+\varphi_2}$. 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=aˆ2, CH=bˆ2$, 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 $\sqrt[3]{2}$. Но $\mathbb{Q}(\sqrt[3]{2})$ — расширение степени 3 над $\mathbb{Q}$, поэтому не существует башни промежуточных расширений размерности 2.

TODO: Больше объяснений! ◀

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

▶ a) 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. Имеем: $\frac{p}{q} \underbrace{\sim}_{\text{определение экв-ти}} \frac{pq^{-1}}{1} \underbrace{\sim}_{\text{изоморфизм}} pq^{-1}$ $\varphi(\frac{p}{a}) = \varphi(pa^{-1}) = \varphi(p) \underbrace{[\varphi(a)]^{-1}}_{\text{свойство гомоморфизма}} = pa^{-1} = \frac{p}{a}$ b) 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 $\mathrm{Aut}_F(K) = \mathrm{Aut}([K : F])$. a) $\mathrm{Aut}_F(K)$ — группа. b) Пусть $H \subset \mathrm{Aut}_F(K)$ — подгруппа. Тогда $K^H = \{x \in K \mid \forall h \in H \hookrightarrow h(x) = x\}$ является полем, причём $K \supset K^H \supset F$.

▶ a) 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. b) 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 $\mathbb{Q}(\sqrt[3]{2})$.

▶ $\mathbb{Q}(\sqrt[3]{2}$ — группа $\{id\}$, т. к. все другие перестановки корней дают комплексные числа.

Знаем, что любой автоморфизм задаётся перестановкой корней минимального многочлена.

Пусть φ — авторморфизм. Тогда $\varphi(m_\gamma(\gamma)) = 0 \Rightarrow 0 = a_n \varphi(\gamma)^m + \dots + a_0 \Rightarrow \varphi(\gamma)$ — корень $m_\gamma \Rightarrow$ сопряжён с γ. ◀

№ 43 (11.1 (Lectures_all.pdf теор. 11.1)) a) Конечное поле характеристики p состоит из p^n элементов. b) Поле F является полем разложения многочлена $x^{p^n} - x$. c) Существует единственное поле из p^n элементов.

▶ a) 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. b) Пусть $\alpha \in K, \alpha \neq 0$. Тогда $\alpha^{p^n - 1} = 1$. Следовательно, α 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. c) 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 a) $\mathbb{F}_2$, b) $\mathbb{F}_3$.

▶ Выписываем все возможные многочлены и вычёркиваем те, которые разложимы.

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: $\cancel{x^2}$, $\underbrace{\cancel{x^2+1}}_{(x+1)(x+1)}$, $\cancel{x^2+x}$, x^2+x+1

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

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

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

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

◀

№ 45 (11.3) Постройте поле из a) 4; b) 8; c) 9 элементов.

► Для p^n: $F_{p^n} = {}^{F_p[x]}/_{(f(x))}$, где $f(x)$ — примитивный многочлен степени n. Итого, надо просто найти многочлен над F_p степени n.

a) $4 = 2^2$ $\mathbb{F}_4 = {}^{F_2[x]}/_{(x^2+x+1)} = \{0; 1; x; 1+x\}$
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) $9 = 3^2$ $\mathbb{F}_9 = {}^{F_3[x]}/_{(x^3+2x+2)}$

TODO: почему так? Как явно выписывать?

◀