№ 1 (1.4 [Каргальцев)] Для любого числа $u \in \mathbb{C}$ определим множество $\mathbb{Z}[u] = \cup_{n=0}^{\infty}\{a_0 + a_1u + \ldots + a_nu^n | a_0, a_1, \ldots, a_n \in \mathbb{Z}\}$.

► а) Докажите, что $\mathbb{Z}[u]$ является областью целостности.

То, что $\mathbb{Z}[u]$ кольцо проверяется непосредственно. Поскольку $\mathbb{Z}[u] \subset \mathbb{C}$ и $\mathbb{C}$ — область целостности (*потому что* $\mathbb{C}$ — *поле*), то и $\mathbb{Z}[u]$ область целостности.

б) При каких $u \in \mathbb{C}$ данное $\mathbb{Z}[u]$ "конечномерно над $\mathbb{Z}$", то есть найдётся такое N, что $\mathbb{Z}[u] = \cup_{n=0}^{\infty}\{a_0 + a_1u + \ldots + a_nu^N | a_0, a_1, \ldots, a_N \in \mathbb{Z}\}$?

Покажем, что $\mathbb{Z}[u]$ "конечномерно над $\mathbb{Z}$", $\Leftrightarrow \exists f \in \mathbb{Z}[x] : f(u) = 0$, $f \neq 0$ и старший коэффициент $f(x)$ равен 1 $(*)$.

$\Rightarrow$

Поскольку $u^{N+1} \in \mathbb{Z}[u] \Rightarrow \exists a_0, \ldots, a_N \in \mathbb{Z} : u^{N+1} = \sum\limits_0^N a_k u^k \Rightarrow u$ — корень $f(x) = x^{N+1} - \sum\limits_0^N a_k x^k$

$\Leftarrow$

Пусть u — корень многочлена $f(x) = u^N + \sum\limits_0^N a_k x^k$, удовл. условию $(*)$. Тогда u^N выражается через меньшие степени. $(u^N = -\sum\limits_0^{N-1} a_k u^k)$

Индукцией по $k \geqslant N$ легко показать, что u^k выражается через $1, u, \ldots u^{N-1}$.

$(u^{k+1} = u \cdot u^k \overset{\text{предположение индукции}}{=} u \cdot (\sum\limits_0^{N-1} b_k u^k) = (\sum\limits_1^{N-1} b_{k-1}u^k) + b_{N-1}u^N \overset{\text{база индукции}}{=} (\sum\limits_1^{N-1} b_{k-1}u^k) + b_{N-1}\sum\limits_0^{N-1} -a_k u^k$

◄

№ 2. (1.2) Для комплексного числа $z \in C$ введём норму $N(z) = |z|^2$.

а) $N(zw) = N(z)N(w)$.

Для каждого $z \in D$:

б) Верно ли, что $N(z)$ — натуральное число?

в) Верно ли, что $N(z) = 1 \Leftrightarrow z$ — обратим?

► а) Просто проверим: $N(zw) = N(a_z + b_z i)(a_w + b_w i)) = N(a_z a_w - b_z b_w + (a_z b_w + a_w b_z)i) = (a_z a_w - b_z b_w)^2 + (a_z b_w + b_z a_w)^2 =$ раскрыли скобки $= (a_z^2 + b_z^2)(a_w^2 + b_w^2) = N(z)N(w)$

б) Заметим, что $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$

Значит, $|a + bi| = a^2 + b^2 \in |N$. Аналогично:

$\mathbb{Z}[2i] = \{a + 2bi \,|\, a, b \in \mathbb{Z}\} \Rightarrow |a + 2bi| = a^2 + 4b^2 \in \mathbb{N}$

$\mathbb{Z}[\sqrt{2}i] = \{a + \sqrt{2}bi \,|\, a, b \in \mathbb{Z}\} \Rightarrow |a + \sqrt{2}bi| = a^2 + 2b^2 \in \mathbb{N}$

$\mathbb{Z}[\sqrt{3}i] = \{a + \sqrt{3}bi \,|\, a, b \in \mathbb{Z}\} \Rightarrow |a + \sqrt{3}bi| = a^2 + 3b^2 \in \mathbb{N}$

в) $\Rightarrow$

$N(z) = a^2 + b^2 = 1$

$\frac{1}{z} = \frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{a-bi}{1} = a - bi = \overline{z}$, а z и $\overline{z}$ одновременно лежат в D, значит $\exists z^{-1} = \overline{z}$.

$\Leftarrow$

$zz^{-1} = 1 \Rightarrow \begin{cases} N(zz^{-1}) = N(z)N(z^{-1}) = 1 \\ N(z) = a^2 + b^2 \geqslant 1 \end{cases} \Rightarrow N(z) = 1$

◄

№ 3 Пример нефакториального кольца вида $Z[u]$.

► Пример: $\mathbb{Z}[2i]$ не является факториальным кольцом, потому что $4 = 2 \cdot 2 = (2i)(-2i)$, но при этом $2 \nsim 2i$ – противоречие с единственностью разложения в факториальном кольце.

Еще пример: $\mathbb{Z}[\sqrt{3}i]$ (аналогичное рассуждение $4 = 2 \cdot 2 = (1 + \sqrt{3}i)(1 - \sqrt{3}i)$). ◄

№ 4 (2.7 [Каргальцев)] Простой элемент области целостности является неразложимым.

► Пусть p — простой и $p = xy \Rightarrow x|p \wedge y|p$. Из определения простоты $p|x \vee p|y$. Но тогда или $x|p \wedge p|x$, или $y|p \wedge p|y$. Тогда $p \sim y \vee p \sim x \Rightarrow y \in K^* \vee x \in K^*$, то есть p — неразложимый. ◄

№ 5 (2.8) В факториальном кольце любой неразложимый элемент является простым.

► Пусть $x = ab$ – неразложимый. $x = ab \Rightarrow x \,|\, ab$.

x неразложимый, значит б.о.о. $a \in K^*$. Тогда в силу единственности разложения $x = ab = ap_1 \dots p_k \Rightarrow x \sim b \Rightarrow x \,|\, b$. ◄

№ 6 (часть 2.9 [Каргальцев)] K — евклидово кольцо. Верно ли, что если для $a, b \neq 0$ выполнено равенство $N(ab) = N(a)$, то b обратим?

► Поделим a с остатком на ab:

$$a = abq + r : r = 0 \vee N(r) < N(ab)$$

.

$$r = a(1 - bq)$$

.

Если $r = 0$, то $bq = 1$ и b обратим. Иначе $N(ab) > N(r) = N(a(1 - bq)) \geqslant N(a) = N(ab)$. Противоречие. ◄

№ 7 (2.10) Геометрический способ доказательства того, что $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ — евклидово кольцо.

► ВСТАВИТЬ КАРТИНКУ Пусть $a, b \in \mathbb{Z}[i]$. Поделим a на b с остатком:

$a = pb + q$.

Надо доказать, что если $q \neq 0$, то $N(q) < N(b)$. Рассмотрим точку $\frac{a}{b}$, пусть ближайший к ней узел в решетке p, тогда $\frac{a}{b} = p + \frac{q}{b}$. Но $\frac{q}{b}$ по модулю меньше половины диагонали единичного квадрата $\left|\frac{q}{b}\right| \leqslant \left|\frac{\sqrt{2}}{2}\right| \leqslant 1$, т.е. $|q|^2 < |b|^2 \Rightarrow N(q) < N(b)$, если $\frac{q}{b}$ не совпадает с центром квадрата.

(TODO иначе)

$\mathbb{Z}[\omega]$ аналогично. ◄

№ 9 (3.1) а) Если p – простое целое число и существует такое $z \in D$, что $N(z) = p$, то z — неразложимый элемент.

б) Если p – простое целое число и не существует такого $z \in D$, что $N(z) = p$, то p – неразложимый элемент.

в) Если D – факториальное кольцо, то для любого неразложимого элемента $z \in D$ либо $N(z) = p$, либо $z \sim p$ для некоторого целого простого числа p.

► а) Имеем: $z \in D$, $N(z) = p$. Пусть $z = bc$, тогда $N(z) = N(b)N(c) = p \Rightarrow N(b) = 1$ или $N(c) = 1$, т.е $b \in D^*$ или $\in D^* \Rightarrow z$ – неразложим (исп. задачу 2в)

б) Пусть $p = bc$. Тогда $N(p) = N(b)N(c) = p^2$. Два случая:

- $N(b) = N(c) = p$ — невозможно по условию
- $N(a) = 1,\ N(b) = p^2$ или $N(a) = p^2,\ N(b) = 1 \Rightarrow b \in D^*$ или $c \in D^*$ (исп. задачу 2в).

в) $N(z) = z\overline{z} = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ (в силу факториальности кольца). z неразложим $\Rightarrow \exists i \colon p_i \vdots z \Rightarrow zk = p_i$

$N(p_i) = p_i^2 = N(z)N(k) \Rightarrow$ либо $N(z) = p_i \Rightarrow z$ – неразложим, либо $N(z) = p_i^2 \Rightarrow z \sim p_i$.

◄

№ 10 (2.7 [Каргальцев)] Если $z \in D$, $z|x$, и $N(z) = N(x)$, то $z \sim x$.

► Пусть $x = yz$. Тогда $N(yz) = N(z) \Rightarrow y$ обратим (по №6) и, значит, $x \sim z$. ◄

№ 11 (3.3 [Каргальцев)] (Простые гауссовы числа) Пусть p — простое целое число.

► а) Если $p = 4k + 3$, то p — неразложим в $\mathbb{Z}[i]$.

Если p разложим, тогда $p = z\overline{z} = Re^2 z + Im^2 z$. Но число, дающее остаток 3 при делении на 4 не быть представлено в виде суммы двух квадратов (квадраты дают остаток 1 при делении на 4).

б) Если $p = 4k + 1$, то p — разложим в $\mathbb{Z}[i]$.

Если $p = 4k + 1$, то -1 — вычет по модулю p, т. е $\exists x \in \mathbb{Z} : p|x^2 + 1 \Rightarrow p|(x + i)(x - i)$. Если p — неразложим, тогда p — прост и либо $p|(x + i)$, либо $p|(x - i)$.

- $p|(x + i) \Rightarrow x + i = p(c + di) \Rightarrow 1 = pd \Rightarrow p \,|\, 1$ – плохо.

• $p|(x-i) \Rightarrow x-i = p(c+di) \Rightarrow -1 = pd \Rightarrow p \,|\, 1$ – плохо.

Значит, p разложим.

в) Если $p = 4k+1$, то $p = z\overline{z}$, где z — неразложим в $\mathbb{Z}[i]$.

Следует из предыдущего пункта и пункта г) предыдущей задачи.

г) Неразложимые элементы $\mathbb{Z}[i]$, не описанные в предыдущих пунктах — $\pm 1 \pm i$.

Неразложимые элементы, не описанные в предыдущих задачах могут иметь норму или 2, или 4. Норму 4 имеет только 2 и ассоциированные с ней, но $2 = (1+i)(1-i)$.

С другой стороны, $N(\pm 1 \pm i) = 2$, то есть силу пункта в) предыдущей задачи $\pm 1 \pm i$ неразложимы. ◄

№ 12 (3.10) Евклидово кольцо является кольцом главных идеалов.

► Пусть K – евклидово кольцо, $a \in K$, причем

$$N(a) = \min_{x \in K \setminus \{0\}} N(x)$$

.

Предположим, что $K \neq (a) \Rightarrow \exists b \in K \setminus (a) \Rightarrow b = aq + r$, где либо $r = 0$, либо $N(r) < N(a)$.

• $r = 0 \Rightarrow b = aq \Rightarrow b \in (a)$ – противоречие

• $N(r) < N(a) \Rightarrow r = b - aq \in I$ – противоречие с минимальностью нормы a.

◄

№ 13 (3.13) Пусть $D = \mathbb{Z}[i]$ или $\mathbb{Z}[\omega]$.

а) Верно ли, что из $a|b$ следует, что $N(a)|N(b)$?

б) Верно ли, что из НОД$(N(a), N(b)) = 1$, следует НОД$(a, b) = 1$?

в) Пусть НОД$(N(a), N(b)) = p$ – простое целое число, причём $p \not| a$, $p \not| b$. Тогда p – разложим, и если $p = z\overline{z}$, то либо z и $\overline{z}$ порождает идеал (a, b), либо z делит одно из этих чисел, а $\overline{z}$ — другое.

► а) Верно. $a \,|\, b \Rightarrow b = ak \Rightarrow N(b) = N(a)N(k)$ (по свойству нормы в D) $\Rightarrow N(a) \,|\, N(b)$

б) НОД$(N(a), N(b)) = p$

Допустим, что НОД$(a, b) = k \notin D^*$.

Тогда $a = kx, b = ky$, и

$$\left.\begin{array}{l} N(a) = N(kx) = N(k)N(x) \\ N(b) = N(ky) = N(k)N(y) \end{array}\right\} \Rightarrow \text{НОД}(N(a), N(b)) \neq 1 \tag{1}$$

– противоречие. Значит, НОД$(a, b) = 1$.

в) НОД$(N(a), N(b)) = p$

Покажем, что p – разложим. $N(a) = a\overline{a} = pt, p \not| a$, p – простое число $\Rightarrow$ допустим, что p неразложима: $p \,|\, \overline{a}$ (по свойству факториального кольца). Тогда $\overline{a} = x - iy \vdots p \Leftrightarrow x \vdots p, y \vdots p \Rightarrow a \vdots p$ – противоречие $\Rightarrow p$ – разложим.

$$\left\{\begin{array}{l} a\overline{a} = z\overline{z}k \\ b\overline{b} = z\overline{z}l \end{array}\right. \Rightarrow \left[\begin{array}{l} a \vdots z \text{ и } b \vdots \overline{z} \\ a \vdots \overline{z} \text{ и } b \vdots z \\ a \vdots z \text{ и } b \vdots z \end{array}\right. \tag{2}$$

В последнем случае идеал $(t) = (a, b) \subseteq (z, \overline{z})$ – очевидно. Докажем в обратную сторону, что $(z, \overline{z}) \subseteq (a, b)$

$z\overline{z} = a\overline{a}\xi + b\overline{b}\eta \vdots t$

◄

№ 14 (3.14) Умение находить порождающий элемент идеала в кольце $\mathbb{Z}[i]$.

► Возможный вариант решения: найдем нормы двух чисел, потом найдем n – НОД этих норм. После этого переберем все числа, которые имеют норму n и проверим их на то, что они являются порождающим элементом. При этом искать можно только в первой четверти комплексной плоскости (т.к. найдя одно число, получаем сразу 4 поворотами на $\pi/2$). Если не один из них не подойдет, то проделаем то же самое со всеми делителями n в порядке уменьшения модуля, пока не дойдем до 1.

Рассмотрим пример:

3.14. Найти порождающий элемент $(11+7i, 18-i)$ в $\mathbb{Z}[i]$. *Решение.* Заметим, что $\mathbb{Z}[i]$ – евклидово кольцо, значит, оно является КГИ $\Rightarrow$ все идеалы главные $\Rightarrow$ идеал $(11+7i, 18-i)$ порождается одним элементом (t). Найдем этот элемент.

$N(11+7i) = 170$

$N(18-i) = 325$

НОД$(170, 325) = 5$.

Перебором выясняем, что в первой четверти числу с нормой 5 соответствуют два числа: $1+2i$ и $2+i$.

Заметим, что $1+2i$ не может быть порождающим элементом:

$\frac{18-i}{1+2i} = \frac{(18-i)(1-2i)}{(1+2i)(1-2i)} = \ldots = \frac{16}{5} - \frac{37}{5}i \notin \mathbb{Z}[i]$

С $2+i$ тоже плохо:

$\frac{11+7i}{2+i} = \frac{29}{5} + \frac{3}{5}i \notin \mathbb{Z}[i]$.

Следовательно, среди чисел с нормой 5 нет НОД$(a, b) \Rightarrow$ его норма $1 \Rightarrow (11+7i, 18-i) = (1)$. ◄

№ 15 Пусть $I \subset K$ является подмножеством, для которого выполнено следующее условие: для любых $a \in K$, $x \in I$, $y \in I$ верно, что $x+y \in I$, $ax \in I$. Верно ли что это условие равносильно тому, что I — идеал?

► $\Rightarrow$:

В предположении, что I непусто:

1. $(I, +) \subset (K, +)$ — подгруппа по сложению.
   - Замкнутость по сложению — дана по условию.
   - Нейтральный по сложению лежит в I: действительно, возьмем произвольный $x \in I$ и $a = 0 \in K$: тогда $0 = ax \in I$.
   - Обратный по сложению лежит в I: т.к. $-1 \in K$, то $\forall x \in I : -x = (-1) \cdot x \in I$.
2. $\forall a \in K, x \in I : ax \in I$ — дано по условию.

$\Leftarrow$:

1. $\forall x \in I, y \in I : x+y \in I$ — выполнено, т.к. идеал — подгруппа по сложению.
2. $\forall a \in K, x \in I : ax \in I$ — выполнено по определению идеала.

◄

№ 16 (3.17) а) Идеал (x, y) кольца $\mathbb{Q}[x, y]$ конечно порождён, но не является главным.

б) Приведите пример области целостности K и идеала I, который не конечно порождён.

► а) (x, y) конечно порожден по определению.

Предположим, что (x, y) — главный. Тогда $\exists f(x, y) : (x, y) = (f(x, y))$.

Т.к. $x \vdots f(x, y), y \vdots f(x, y)$, то $\deg f \leq 1$.

Если $\deg f(x, y) = 0$, то $f(x, y) \in \mathbb{Q}$: при $f(x, y) = 0$ $(f(x, y)) = 0$, при $f(x, y) \neq 0$ $(f(x, y)) = \mathbb{Q}[x, y]$. Оба случая нам не подходят.

Если $\deg f(x, y) = 1$, то $\exists a, b \in \mathbb{Q}^* : f(x, y) = ax = by$, откуда $x = a^{-1}by$, что тоже неверно.

б) $K = \mathbb{Q}[x_1, x_2, \ \ldots \ x_n, \ \ldots]$

$I = (x_1, x_2, \ \ldots \ , x_n, \ \ldots)$

Предположим, I конечно-порожден, т.е $\exists f_1, \ldots, f_t \in K : I = (f_1, \ldots, f_t)$. f_i можно представить в виде $x_1 g_i^1 + \ldots + x_{N_i} g_i^{N_i}$ для некоторого $N_i \in \mathbb{N}$, т.к. f_i лежит в идеале $(x_1, \ldots, x_n, \ldots)$. Положим $N = \max\{N_1, \ldots, N_t\}$, тогда $f_i = x_1 g_i^1 + \ldots + x_N g_i^N$.

Т.к. $x_{N+1} \in I = (f_1, \ldots, f_t)$, то $\exists a_1, \ldots a_t : x_{N+1} = a_1 f_1 + \ldots a_t f_t$. Приравнивая $x_1 = \ldots = x_N = 0$ — на них все $f_1, \ldots, f_t$ равны 0 — и $x_{N+1} = 1$, приходим к противоречию.

◀

№ 17 (4.3) Умение находить факторкольца.

№ 18 (4.8) Пусть $J \subset I \subset K$ — цепочка вложенных идеалов в кольце K. Тогда кольцо $(K/J)/(I/J)$ изоморфно K/I.

▶ Рассмотрим гомоморфизм $\varphi : K/J \to K/I$, $x + J \mapsto x + I$.

Гомоморфизм корректен, т.к. независимо от выбора представителя x получим одно и то же: $x + J = y + J \Rightarrow x - y \in J \Rightarrow x - y \in I \Rightarrow x + I = y + I$.

φ — сюръекция, т.к. $\forall a + I \in K/I : \exists x = a : \varphi(a) = a + I$.

Значит, по теореме о гомоморфизме: $(K/J)/\ker\varphi \cong K/I$.

Т.к. $\ker\varphi = \{x + J : x + I = I\} = \{x + J : x \in I\} = I/J$, то $(K/I)/(I/J) \cong I/J$, ч.т.д..

◀

№ 19 (4.9) В кольце главных идеалов любой простой идеал максимален.

▶ Пусть (p) — простой идеал в КГИ K. Пусть I — идеал в K: $(p) \subset I \subset K$.

I — порожден одним элементом $\Rightarrow I = (x) \Rightarrow p \vdots x$ по задаче 15а) на 3-4.

Т.к. (p) — простой идеал, то p — простой элемент (по задаче 20 на 3-4) $\Rightarrow x \sim p$ или $x \in K^*$.

Если $x \sim p \Rightarrow I = (x) = (p)$. Если $x \in K^* \Rightarrow I = (x) = K$.

Таким образом, $\nexists I : (p) \subsetneq I \subsetneq K \Rightarrow (p)$ — максимален.

◀

№ 20 (4.10) Умение находить максимальные и простые идеалы.

▶ Для решения таких задач необходимы следующие теоремы:

- В факториальном кольце из неразложимости элемента следует его простота.
- В области целостности, $\forall p \neq 0$: (p) - простой идеал $\Leftrightarrow$ p - простой элемент

Пусть K - коммутативное кольцо, а I - идеал.

- K/I - область целостности $\Leftrightarrow$ I - простой идеал
- K/I поле $\Leftrightarrow$ идеал I максимален $\Leftrightarrow$ в K/I нет нетривиальных идеалов
- Любой максимальный идеал прост
- В КГИ простой идеал является максимальным.

◀

№ 21 (5.3) а)Верно ли, что $Quot(Quot(K)) \cong Quot(K)$?

б)Пусть $K \subset L \subset Quot(K)$ верно ли, что $Quot(K) \cong Quot(L)$?

▶ а) Пусть L - поле. Тогда $Quot(L) \cong L$.

Изоморфизм $\varphi : L \leftrightarrow Quot(L)$ выглядит как $\varphi : (a * b^{-1}) \leftrightarrow \frac{a}{b}$, где $\frac{a}{b} \in Quot(L)$.

$Quot(K)$ - поле. Тогда, в частности, $Quot(Quot(K)) \cong Quot(K)$.

б) $K \subset L \subset Quot(K) \Rightarrow Quot(K) \subset Quot(L) \subset Quot(Quot(K)) \cong Quot(K) \Rightarrow Quot(K) \cong Quot(L)$ ◀

№ 22 (5.4) Является ли кольцо $\mathbb{Z}[x]$ евклидовым?

▶ В $\mathbb{Z}[x]$ (и в $\mathbb{Z}_6[x]$, например) идеал $(2x, x^2)$ не является главным. Из евклидовости кольца следует, что оно является кольцом главных идеалов. Значит, из того, что кольцо не является кольцом главных идеалов следует, что оно не является евклидовым кольцом. ◀

№ 23 (5.5) Какие многочлены степени 0:

а) неприводимы в $\mathbb{Z}[x]$

б) являются простыми элементами в $\mathbb{Z}[x]$

► Многочлены степени 0 в $\mathbb{Z}[x]$ - это $\mathbb{Z} \subset \mathbb{Z}[x]$.

а) Составные числа являются приводимыми элементами $\mathbb{Z}[x]$ (по определению).

Простые числа - неприводимы: $p \in \mathbb{Z} \subset \mathbb{Z}[x] \Rightarrow p = fg \Rightarrow (deg(f) \leq 0, deg(g) \leq 0) \Rightarrow deg(f) = deg(g) = 0 \Rightarrow f \in \mathbb{Z}, g \in \mathbb{Z} \Rightarrow (f \in \mathbb{Z}^*) \vee (g \in \mathbb{Z}^*) \Rightarrow$ многочлен a неприводим.

б) Составные числа не являются простыми элементами $\mathbb{Z}[x]$. Рассмотрим $ab = x | x = ab$, где $|a| > 1, |b| > 1$. Ясно, что $(ab \not| a) \wedge (ab \not| b)$ в $\mathbb{Z}$ и в $\mathbb{Z}[x]$. Тогда это не простой элемент $\mathbb{Z}[x]$.

Простые числа являются простыми элементами $\mathbb{Z}[x]$: пусть $f(x)g(x) \vdots p$, но $(f(x) \not\vdots p) \wedge (g(x) \not\vdots p)$. Тогда хотя бы один коэффициент у каждого многочлена не делится на p. Тогда пусть $f(x) = \sum f_k x^k, g(x) = \sum g_k x^k; f(x)g(x) = \sum a_k x^k; i = max(i | f_i \not\vdots p), j = max(j | g_j \not\vdots p) \Rightarrow a_{i+j} = (f_{i+j}g_0 + f_{i+j-1}g_1 + ... + f_i g_j + ... + f_0 g_{i+j})$ Заметим, что в этой сумме все слагаемые, кроме $f_i g_j$ делятся на p т.к. по выбору i и j, один из коэффициентов имеет номер больший максимального, не делящегося. Следовательно, $a_{i+j} \not\vdots p \Rightarrow f(x)g(x) \not\vdots p$. Получено противоречие с делимостью. ◄

№ 24 (5.6) а)Примитивный многочлен $f \in \mathbb{Z}[x]$ ненулевой степени: неприводим в $\mathbb{Z}[x] \Leftrightarrow$ неприводим в $\mathbb{Q}[x]$

б)Произведение примитивных многочленов примитивно

в)Примитивный неприводимый многочлен в $f \in \mathbb{Z}[x]$ - простой элемент кольца

► Определим содержание $c(f)$ многочлена f как НОД коэффициентов многочлена.

Таким образом, многочлен f примитивен $\Leftrightarrow c(f) = 1$

Лемма Гаусса: $\forall f, g \in \mathbb{Q}[x] : c(fg) = c(f) \cdot c(g)$. Она доказывается с использованием утверждения 23.

а, $\Rightarrow$) $f \in \mathbb{Q}[x]$ неприводим $\Rightarrow f \in \mathbb{Z}[x] (\subset \mathbb{Q}[x])$ неприводим. (Если есть приведение $f = gh$ в $\mathbb{Z}[x]$, то оно есть и в $\mathbb{Q}[x]$)

а, $\Leftarrow$) пусть $f = gh$ - приведение в $\mathbb{Q}[x]$. $f = \frac{A}{B}\overline{g}\frac{C}{B}\overline{h}$, где A, C - наибольшие общие делители коэффициентов многочленов g и h соответственно. B, D - общий знаменатель коэффициентов. Таким образом, $\overline{g}$ и $\overline{h}$ - примитивные. $\Rightarrow f = \frac{AC}{BD}\overline{g}\overline{h}$, $BDf = AC\overline{g}\overline{h} \Rightarrow c(BDf) = c(BD) \cdot 1 = c(AC\overline{g}\overline{h}) = c(AC) \cdot 1 \cdot 1 \Rightarrow AC = BD \cdot u$ и $u \in \mathbb{Z}^* \Rightarrow \overline{f} = u\overline{g}\overline{h}$ в $\mathbb{Z}[x] \Rightarrow$ таким образом, из приводимости в $\mathbb{Q}[x]$, следует приводимость в $\mathbb{Z}[x]$, следовательно, из неприводимости в $\mathbb{Z}[x]$ следует неприводимость в $\mathbb{Q}[x]$

б) произведение примитивных примитивно Пусть $f = c(f)f_1$, $g = c(g)g_1$. Тогда f_1 и g_1 - примитивны. $\Rightarrow fg = c(f) \cdot c(g) \cdot f_1 \cdot g_1 = c(f)c(g)f_1 g_1$. Пусть простое число p делит fg. Тогда по утверждению в том, что простые в $\mathbb{Z}$ являются простыми в $\mathbb{Z}[x]$ имеем $p | f \vee p | g$. Но они примитивны $\Rightarrow$ противоречие.

в) $\mathbb{Q}[x]$ факториально $\Rightarrow$ из неприводимости следует простота

$\rho(x)h(x) \vdots f(x)$ в $\mathbb{Z}[x] \Rightarrow$ без ограничения общности $f(x) | \rho(x)$ в $\mathbb{Q}[x] \Rightarrow f(x)l(x) = \rho(x)$ в $\mathbb{Q}[x]$

$f(x)\frac{A}{B}\overline{l(x)} = \rho(x)$, $f(x)\frac{A}{B}\overline{l(x)} = c(\rho)\overline{\rho(x)} \Rightarrow Af(x)\overline{l(x)} = Bc(\rho)\overline{\rho(x)} \Rightarrow A \sim Bc(\rho)$ по лемме Гаусса $\Rightarrow A \cdot u = B \cdot c(\rho), u \in \mathbb{Z}[x]^* \Rightarrow f(x)\overline{l(x)} = u\overline{\rho(x)} \Rightarrow f(x) | \overline{\rho(x)}$ в $\mathbb{Z}[x]$, т.е. получена простота в $\mathbb{Z}[x]$ из простоты в $\mathbb{Q}[x]$

◄

№ 25 [Каргальцев] Докажите, что в кольце главных идеалов любая возрастающая цепочка идеалов

$$(a_1) \subset (a_2) \subset \ldots \subset (a_n) \subset \ldots$$

стабилизируется, то есть найдется такое k, то $(a_k) = (a_{k+1}) = \ldots$

► Поскольку $(a_i) \subset (a_{i+1}) \Rightarrow a_{i+1} | a_i$.

Возьмем $I = \cup_{k=1}^{\infty}(a_k)$. покажем, что I – идеал. Пусть $a \in I, b \in I \Rightarrow \exists k_1, k_2 : a \in (a_{k_1}), b \in (a_{k_2})$. Тогда положим $k = max(k_1, k_2)$. $a, b \in (a_k) \Rightarrow (a + b) \in (a_k)((a_k)$— идеал) $\Rightarrow (a + b) \in I$. Аналогично $\forall x \in K xa \in (a_k) \Rightarrow xa \in I$.

Поскольку K — КГИ, то существует $x : I = (x)$. $x \in I \Rightarrow \exists k : x \in (a_k)$. Но $a_k \in (x)$. Тогда $x | a_k \wedge a_k | x \Rightarrow x \sim a_k$. Но в силу вложенности это верно и для всех $j > k$, то есть $\forall j \geqslant k a_j \sim a_k \Rightarrow (a_j) = (a_k)$. То есть цепочка действительно стабилизируется. ◄

№ 26 (4.8) В КГИ из простоты идеала следует его максимальность

► Простота идеала: $\forall ab \in I \to ((a \in I) \vee (b \in I))$

От противного: пусть $I \subset J \subset K$, где $I = (p)$ - простой идеал над кольцом K. Тогда $p \in I \subset J = (x) \Rightarrow p \in J$. КГИ является факториальным кольцом (вопрос 6 на 7-8), следовательно: (p) - простой идеал $\Leftrightarrow$ p - простой элемент (задача 20 на 3-4). Тогда $x \sim p$ или $x \in K^*$ (из $p = kx$). Тогда:

- $x \sim p \Rightarrow I = J$
- $x \in K^* \Rightarrow J = (x) = (1) = K$

◄

№ 27 Любой максимальный идеал прост

► Теорема 1 (вопрос 21 (4.6) на 3-4): K/I - поле $\Leftrightarrow$ нетривиальный идеал I - максимален $\Leftrightarrow$ K/I не имеет нетривиальных идеалов

Теорема 2 (вопрос 22 (4.7) на 3-4): K/I - область целостности $\Leftrightarrow$ I - прост

Поле является областью целостности ($ab = 0 \Rightarrow a = 0 * b^{-1} = 0$ или $b = 0$). Тогда получим: I - максимален $\Rightarrow$ K/I - поле $\Rightarrow$ I - прост ◄

№ 28 Признак неприводимости Эйзенштейна для простого идеала I факториального кольца K и его поля частных F

► • Формулировка: Пусть K - факториальное кольцо, $I \subset K$ - простой идеал, $f(x) = \sum\limits_{k=0}^{n} a_k x^k \in K[x]$ - многочлен степени $n \geq 1$. Пусть $a_0 ... a_{n-1} \in I$, $a_0 \notin I^2, a_n \notin I$. Тогда $f(x)$ неприводим над $F = Quot(K)$

- Доказательство (с консультации) повторяет доказательство признака Эйзенштейна для многочленов коэффициентами из $\mathbb{Z}$ о неприводимости над $\mathbb{Q}$: пусть $f(x) = g(x)h(x), 0 < deg(g(x)) < n, 0 < deg(h(x)) < n, g(x) \in K[x], h(x) \in K[x]$.

  $g(x) = \sum\limits_{k=0}^{deg(g(x))} g_k x^k$, $h(x) = \sum\limits_{k=0}^{deg(h(x))} h_k x^k$. По условию $a_0 = g_0 h_0 \notin I^2 \Rightarrow (g_0 \notin I) \vee (h_0 \notin I)$. Без ограничения общности $g_0 \notin I$ и $h_0 \in I$. Пусть $h_0 ... h_k \in I, h_{k+1} \notin I$. Рассмотрим коэффициент при x^{k+1}: $a_{k+1} = g_0 h_{k+1} + g_1 h_k + ... + g_{k+1} h_0$. По предположению все слагаемые, кроме первого, лежат в I, а $g_0 h_{k+1}$ не лежит. Но тогда $a_{k+1} \notin I \Rightarrow k + 1 = n \Rightarrow deg(h(x)) \geq k + 1 = n$. Получено противоречие со степенью многочлена $h(x)$.

  Теперь, аналогично доказательству признака Эйзенштейна для $\mathbb{Z}$ и $\mathbb{Q} = Quot(\mathbb{Z})$, получим противоречие и для $g(x), h(x)$ из $F = Quot(K)$

◄

№ 29 (6.2) Умение применять признак неприводимости Эйзенштейна (в том числе, используя замену переменной)

► Для решения задач из семинарских листков было достаточно:

- посмотреть на номер и применить признак для $p = 2, 3, ...$
- сделать замену вида $x = \overline{x} + 1$ и доказать неприводимость полученного. Из приводимости $f(x)$ следует приводимость $f(x + k), k \in \mathbb{Z}$. (совершенно необязательно это будет замена именно для $k = 1$, однако её было достаточно для задач из листков)
- для многочленов от нескольких переменных, например, $f(x, y)$ был пример с заменой $y = x$ и применение признака Эйзенштейна к полученному многочлену. Из приводимости $f(x, y)$ следует приводимость $f(x, x)$

Пример, используемый в вопросе о примитивных корнях из единицы:

$\Phi_p = x^{p-1} + x^{p-2} + ... + x^2 + x + 1$, где p - простое. Вспомним, что $\Phi_p = \frac{x^p - 1}{x - 1}$. Выполним замену $x = y + 1$: $\Phi_p = \frac{x^p - 1}{x - 1}|_{x=y+1} = \frac{(y+1)^p - 1}{y} = y^{p-1} + C_p^1 y^{p-2} + ... + C_p^{p-1}$. Рассматривая все коэффициенты, получим, что $1 \not\vdots p, \forall k \in \{1, ..., p-1\} : C_p^k \vdots p$. В частности, $C_p^{p-1} = C_p^1 = p \not\vdots p^2$. Т.е. применим признак Эйзенштейна для p. Значит, Φ_p неприводим над $\mathbb{Q}[x]$ для любого простого p. ◄

№ ?? (?.?)

► ◄

№ ?? [Каргальцев]

► а) Если z — неразложимый элемент D, то существует такое простое целое число p, что $N(z) = p$ или $N(z) = p^2$

$N(z) = z\overline{z}$. Разложим $N(z)$ в произведение простых как натуральное число:

$z\overline{z} = N(z) = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$.

Так как z неразложим, а D — евклидово, то z — прост, значит $\exists k : z|p_k$.

$p_k = zu \Rightarrow p_k = \overline{p_k} = \overline{zu} \Rightarrow \overline{z}|p_k \Rightarrow N(z)|p_k^2 \Rightarrow N(z) = 1, p_k$ или p_k^2. Но так как если $N(z) = 1$, то z — обратим (а, следовательно, неразложим), то $(z) = p_k \vee N(z) = p_k^2$.

б) Если z — неразложимый элемент D и $N(z) = p^2$, то $z \sim p$.

Пусть $\overline{z} = ab \Rightarrow z = \overline{a}\overline{b} \Rightarrow \overline{z}$ — неразложим.

$z\overline{z} = N(z) = p \cdot p$. В силу единственности разложения на неразложимые, $z \sim p$.

в) Если $N(z) = p$, то z — неразложимый элемент D.

в $Da|b \Rightarrow N(a)|N(b)$.

Пусть $a|z \Rightarrow N(a)|N(z)$. В силу простоты $N(z)$ либо $N(a) = 1$ и, следовательно, a — обратимый, либо $N(a) = N(z)$ и тогда $a \sim z$. То есть z неразложим.

г) Пусть p — простое целое число. Тогда есть два варианта: либо p неразложимо в D, либо $p = z\overline{z}$, где z – неразложимо в D. Таким образом описываются все неразложимые элементы D.

Пусть p разложимо в D. Тогда найдется такой неразложимый $z : z|p$. Поскольку z не ассоциирован с p, $N(z) \neq N(p) \Rightarrow N(z) = p$. Тогда z – неразложимый и $z\overline{z} = N(z) = p$.

Любой неразложимый элемент D — либо простое целое число, либо его норма — простое целое число. ◀