№ 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. ◄

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

► 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 $\mathbb{Z}[u] = \cup_{n=0}^{\infty}\{a_0 + a_1 u + \ldots + a_n u^N | a_0, a_1, \ldots, a_N \in \mathbb{Z}\}$?

Покажем, что $\mathbb{Z}[u]$ “конечномерно над $\mathbb{Z}$”, $\Leftrightarrow \exists f \in \mathbb{Z}[x] : f(u) = 0, f \neq 0$.

$\Rightarrow$

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 $f(x) = u^N + \sum\limits_0^N a_k x^k$ (всегда можем поделить на старший коэффициент). 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 $1, u, \ldots u^{N-1}$.

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

◄

№ 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$) \Rightarrow (a + b) \in I$. Анологично $\forall x \in K xa \in (a_k) \Rightarrow xa \in I$.

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. ◄

№ 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. ◄

№ 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, $x \sim z$. ◄

№ ?? [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. ◄

№ 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 или $p|(x + i)$, или $p|(x - i)$. В любом случае, т.к x — целое в силу задачи 18 из задач на 3-4 $p|1$, что 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. ◄