Лекция 29 октября (первая половина)

Однозначность разложения на множители

$$z = p_1 \cdots p_n = q_1 \cdots q_m$$

(1) $n = m$

(2) после надлежащей перенумерации $p_i = \pm q_i$

K - целостное (с 1 и без делителей нуля) комм. кольцо

$q \in K$ наз. неприводимым, если $q = ab \Rightarrow$ $\Rightarrow a$ или b обратим + q необратим.

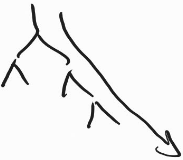
Утв: Если K нётерово, то любой необратимый элемент $a \in K$ явл. произведением конечного числа неприводимых.

Док-во: a неприводим — всё хорошо.

$a = a_1 a_2$ если a_i неприводимы

$a = b_1 b_2 b_3 b_4$ и т.д.

до тех пор пока не получим требуемое представление.



Если процесс сумеет сделать бесконечное число шагов, то можно построить возрастающую цепочку вложенных главных идеалов $(a_1) \subseteq (b_1)$

$a_1 = k b_1$

$a_1 \vdots b_1$

если k необратим, то вложение строгое.

Замечание $(a) = (b) \Longleftrightarrow a = sb$ где s обратим

Элементы a и b: $a = sb$ и $b = s^{-1}a$ где s-обратим, называются ассоциированными

$$a = sb \ \text{(и } (a) \subset (b)\text{)} \qquad b = ta \ \text{(и } (b) \subset (a)\text{)}$$

$$a = sta \Rightarrow a(1 - st) = 0 \Rightarrow st = 1$$

$(a) \subsetneq (b) \subsetneq (c) \subsetneq \dots$ что невозможно в нётеровом кольце

утв. доказано

Как понимать единственность?

$$p_1 \cdots p_m = q_1 \cdots q_n$$

одинаковые, если $m = n$ и сомножители можно перенумеровать так, что $q_i = s_i p_i$, где s_i — обратим

Что нужно для единственности? Чтобы

a или b делится

$ab \vdots p$, только если

на p.

необр.

Элемент $p \in K$ называется простым, если $ab \in (p) \Rightarrow a \in (p)$ или $b \in (p)$

Утв. Если $p_1 \dots p_n$ и $q_1 \dots q_m$ все простые и $\boxed{p_1 \dots p_n = q_1 \dots q_m}$, то $n = m$ и после надлежащей перенумерации $p_i = s_i q_i$ где s_i - обратим.

$$q_1 \dots q_m \vdots p_1 \Rightarrow \exists q_i \vdots p_1$$

пусть $i = 1$ $\quad q_1 = s p_1$

$$s p_1 q_2 \dots q_m = p_1 p_2 \dots p_n$$

кольцо целостное

$$s q_2 \dots q_m = \underbrace{p_2 \dots p_n}$$

$$q \overbrace{\text{обратим}} = p$$

$$\boxed{} = 1$$

Кольцо K (комм. целостное с единицей) наз. факториальным, если $\forall$ необратимого $a \in K$ $\exists!$ разложение на неприводимые множители $a = q_1 \dots q_m$ где все q_i - непр.

единств. в том же смысле, что выше

Утв. Нётерово кольцо K факториально $\Leftrightarrow$ все неприводимые элементы просты

Зам. Простота влечёт неприводимость

$p = km \Rightarrow$ k или m делится на p

пусть $k = sp$

$p = psm \Rightarrow 1 = sm \Rightarrow m$ - обратим

Пример: $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$

$$\mathbb{Z}[\sqrt{5}] = \frac{\mathbb{Z}[x]}{(x^2-5)} \ni 2$$

не прост!

$[a] \cdot [b] = 0$

Условие простоты: $ab \in (p) \Rightarrow a \in (p)$ или $b \in (p)$

означает что в факторе $K/(p)$ нет делителей нуля

$$\frac{\mathbb{Z}[\sqrt{5}]}{(2)} = \frac{\mathbb{Z}[x]}{(x^2-5, 2)} = \frac{\mathbb{Z}}{(2)}[x] \Big/ (x^2-5) = \frac{\mathbb{F}_2[x]}{(x^2+1)} =$$

$= \frac{\mathbb{F}_2[x]}{((x+1)^2)}$ $[x+1][x+1] = 0$ $(x+1)^2$

Упр. покажите, что 2 неприводим.

Подсказка: по аналогии с $\mathbb{C}$:

$z = a + b\sqrt{5}$ $\bar{z} = a - b\sqrt{5}$

$|z| = z\bar{z} = a^2 - 5b^2 \in \mathbb{Z}$

верно $|z_1 z_2| = |z_1| \cdot |z_2|$

$z_1\bar{z}_1 z_2\bar{z}_2$

все эл-ты нормы 1 обратимы $|z| = 1$

$z\bar{z} = 1$

$\frac{1}{z} = \bar{z}$

$\Downarrow$

$\mathbb{Z}[\sqrt{5}]$ не факториальное кольцо

$2 \cdot 2 = 4 = (\sqrt{5}+1)(\sqrt{5}-1)$

неприводимы и не ассоциированы

если все неприводимые просты, то разложение $\exists$ в силу нётеровости и единственно в силу Утв. 2 $\uparrow$

если кольцо факториально, то все неприводимые автоматом просты! q - неприводим и $\underline{ab} \vdots q$

$$a = (p_1 \ldots p_m)$$

$$b = (q_1 \ldots q_s)$$

$$ab = \underset{\approx}{p_1} \ldots \underset{\sim}{p_m} q_1 \ldots q_s \vdots q$$

$$p_1 = \varepsilon q \Rightarrow a \vdots q$$

Любое кольцо главных идеалов факториально

Целостное кольцо K наз. кольцом главных идеалов, если все идеалы в K имеют вид (a) для некоторого $a \in K$.

Утв.: В любом кольце главных идеалов следующие св-ва эл-та $a \in K$ равносильны:

(1) $K/(a)$ - поле

(2) $K/(a)$ не имеет делителей нуля (т.е. a прост)

(3) a неприводим.

$(1) \Rightarrow (2)$ тривиально и верно $\forall K$

$(2) \Rightarrow (3)$ в любом целостном кольце.

$(3) \Rightarrow (1)$ в кольце главных идеалов.

$\boxed{a = bs \text{ и } b \text{ необр.} \Rightarrow s \text{ обр.}}$

(a) максимален среди главных идеалов:

$(a) \leq (b) \Rightarrow (a) = (b)$

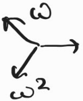
если все идеалы главные, то

a - неприв $\Leftrightarrow$ (a) максимален по включению.

$\Updownarrow$

$K/(a)$ - поле

$\mathbb{Z}$, $\mathbb{k}[x]$ где $\mathbb{k}$ - поле - факториальные кольца.

$\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ $\quad \omega^2+\omega+1=0$