6. Факториальные кольца

Всюду в этой лекции A — целостное кольцо, т.е. комм. ассоц. кольцо с 1 и без делителей нуля.

Если $a, b \in A$, то $b \mid a \Longleftrightarrow (a) \subset (b)$, $a \sim b \Longleftrightarrow (a) = (b) \Longleftrightarrow \exists c \in A^*: a = cb$.

Напомним также, что ненул. необр. эл-т $p \in A$ прост, если p нельзя представить в виде $p = ab$, где a и b необратимы.

Т.1 Если A нётерово, то каждый необр. ненулевой эл-т разл. в произведение простых.

Д-во: Пусть это не так и $a_0 \in A$ необр. эл-т, который нельзя разложить в пр-е простых. Назовем эл-ты такого типа плохими. Т.к. a_0 плохой, то он не прост, а значит, $\exists\, a_1, b_1 \in A : a_0 = a_1 b_1$, где оба множителя необратимы и по крайней мере один, скажем a_1, снова плохой эл-т. Заметим, что $(a_0) \subset (a_1)$, т.к. b_1 необратим. Далее, т.к. a_1 плохой, найдутся плохой a_2 и необратимый b_2 такие, что $a_1 = a_2 b_2$ и т.д. Получаем беск. строго возр. посл-ть идеалов $(a_0) \subset (a_1) \subset (a_2) \subset \ldots$, что противоречит нётеровости кольца A ∎

Анализ д-ва единственности разложения см. Т.3.5.2 и лемму 3.5.1 из [ВиН] или Т.5.2.4 из [ВЛМ] показывает, что все упирается в след. св-во кольца A: если простой p делит произв. ab, то $p\,|\,a$ или $p\,|\,b \iff A/(p)$ нет делителей нуля, т.е. верна след. теорема:

Т.2 Если в кольце A главный идеал, порожденный любым простым элементом, прост, то любой эл-т не более чем одним способом разкл. в пр-е простых.

Зам. Если a не простой, то $a = pq \Rightarrow$ $p \notin (a)$ и $q \notin (a)$ — делители нуля в $A/(a)$ $\Rightarrow (a)$ не простой идеал.

Опр1 (Целостное!) кольцо A наз-ся **факториальным**, если каждый его необр. ненул. эл-т может единств. образом (с точностью до перестановки сомножителей и ассоциированности) быть разложен в произведение простых эл-тов из A.

Мы уже знаем, что
евклидовы $\subset PID \subseteq$ факториальные

Т.3 (св-ва факт. колец) Пусть A - факториальное кольцо. Тогда
1) $\forall a,b \in A$ $\exists$ НОД(a,b) и НОК(a,b)
2) Если эл-т α поля частных Q кольца A - корень мн-на $f(x) \in A[x]$ со ст. коэф. 1, то $\alpha \in A$.

Д-во: 1) $a = \prod p_i^{k_i}$ $b = \prod p_i^{l_i}$ $(k_i, l_i \geq 0) \Rightarrow$

$\text{НОД}(a,b) = \prod p_i^{\min\{k_i, l_i\}}$ и $\text{НОК}(a,b) = \prod p_i^{\max\{l_i, k_i\}}$.

2) Аналогично д-ву т. 3.6.1 из [ВЧН] и его сл-я для кольца $\mathbb{Z}$ и его поля частных $\mathbb{Q}$.

Опр 2 Целостное кольцо A, для которого вып-ся свойство из п. 2 т. 3 наз-ся нормальным (или целозамкнутым).

Опр 3 Для факториального кольца A назовем $f(x) \in A[x]$ примитивным, если НОД всех его коэф-тов равен 1 (аналогично кольцу $\mathbb{Z}$ см. §3.6 из [ВЧН]).

Т. 4 Если кольцо A факториально, то $A[x]$ тоже

Д-во: пусть Q — поле отношений кольца A.
Заметим, что $\forall f \in Q[x]$ $\exists \lambda \in Q^*$ и примитивный мн-н f_1 из $A[x]$: $f = \lambda f_1$.

Лемма (Гаусс) Произведение прим. мн-нов из $A[x]$ снова прим. многочлен

Д-во: аналогично д-ву для $\mathbb{Z}[x]$, см. например, в д-ве Т. 5.6.1 из [BM] $\blacksquare$

Следствие Если f из $A[x]$ неразл. в $Q[x]$, то f неразл. и в $A[x]$ (см. д-во там же)

Вернемся к g-вут-ии. Пусть $f \in A[x]$.
Т.к. $Q[x]$ – кольцо гл. идеалов, то $Q[x]$ факториально $\Rightarrow \exists\ \lambda = \frac{a}{b} \in Q^*$, $a, b \in A$ и $(a,b)=1$,
и $p_1, \ldots p_s$ – примитивные и неразл мн-ны из $A[x]$ такие, что $f = \lambda p_1 \ldots p_s$. Тогда $bf = ap_1 \ldots p_s$
Если p – простой эл-т из A: $p \mid b$, то в силу леммы Гаусса $p \mid a$, противоречие с $(a,b)=1$
$\Rightarrow f = ap_1 \ldots p_s$. Неразл прим мн-ны из $A[x]$
– простые эл-ты $A[x]$. Кроме того, A тоже факториально $\Rightarrow \exists$ простые эл-ты $q_1 \ldots q_t \in A$:

$a = q_1 \dots q_t$. Разложение $f = q_1 \dots q_t\, p_1(x) \dots p_s(x)$ — искомое. Д-но, $p_1(x) \dots p_s(x)$ — неразл. эл-ты в $\mathbb{Q}[x]$ $\Rightarrow$ опр-ны единственным образом, а $q_1 \dots q_t$ — простые эл-ты в кольце A — тоже ∎

<u>Следствие</u> Для любого поля F <u>кольцо мн-нов</u> $F[x_1 \dots x_n]$ — факториально.

$\boxed{\text{эти кольца не PID!}}$

Еще один пример $\mathbb{Z}[x]$ — факториально.

<u>Предл. 1</u> Если мн-н $f \in F[x_1 \dots x_n]$, где поле F бескон., обращается в нуль во всех точках гиперплоскости:

$$\ell := a_1 x_1 + \quad + a_n x_n + b = 0, \qquad (*)$$

то $\ell \mid f$.

Д-во: Сделав замену переменных, можем считать, что $\ell := x_1$. Тогда из условия на f $\Rightarrow$ все одночлены f содержат x_1 $\Rightarrow$ $\ell \mid f$ $\blacksquare$

Пример. Опр-ль Вандермонда $V(x_1, \dots, x_n)$ обр. в нуль при $x_i = x_j$ $\underset{\text{предл. 1}}{\Longrightarrow}$ $\prod_{i<j}(x_i - x_j) \mid V(x_1, \dots, x_n)$. Далее, сравниваем степени и старшие коэф-ты.

Вопрос, который мы рассмотрим теперь, таков. Пусть A — факториальное кольцо,

а $I = (p)$ — идеал, порождённый простым элементом. Верно ли, что A/I факториально?

Пусть $A = F[x,y,z]/(xy - z^2) = F[u,v,w]$, где $\pi(x) = u$, $\pi(y) = v$ и $\pi(z) = w$ при каноническом гом-зме $\pi: F[x,y,z] \to A$.

Тогда A — целостное нётерово кольцо, но не факториальное, т.к. $w^2 = uv$, а u, v, w — простые эл-ты этого кольца A.