

3. Евклидовы кольца и кольца главных идеалов

Опр 1 Кольцо ассоциативов кольца R называется **целостным** (область целостности, integral domain).

Пример \mathbb{Z} , $K[x]$ для любого целостного кольца K .
Зам не сохр. при переходе к факторкольцу!

Также как из \mathbb{Z} строится поле \mathbb{Q} , а для поля F из $F[x]$ строится поле рациональных ф-ций из любого целостн. кольца A можно построить

поле частных $\mathbb{Q}(A)$, задав отношения эквивалентности на

парах $(a, b) \sim (a', b') \Leftrightarrow ab' = a'b$ и операции на

классех эквивалентности: $\begin{bmatrix} a \\ b \end{bmatrix} + \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} ad+bc \\ bd \end{bmatrix}$ и $\begin{bmatrix} a \\ b \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} ac \\ bd \end{bmatrix}$.

см. гл. 3 § 10 из [ВУИ].

Опр 2 Пусть A — числовое кольцо. Элемент b кольца A **делит** элемент $a \in A$, если $\exists q \in A$. $a = qb$ (обозн: $b \mid a$ или $a : b$ „ a делится на b “).
 Э-ты a и b кольца A **ассоциированы**, если $a \mid b$ и $b \mid a$ (обозн: $a \sim b$)

Прелл 1 (св-ва делимости) Если A — числовое кольцо, то

- 1) $c \mid a$ и $c \mid b \Rightarrow c \mid (a+b)$;
- 2) $\forall a \in A \quad c \mid b \Rightarrow c \mid (ab)$
- 3) a и b ассоциированы $\Leftrightarrow \exists c \in A^* : a = cb$ * — нн-во обр. э-та

Опр 3 Необратимый ненулевой э-т p целого кольца A наз-ся **простым**, если он не может быть представл. в виде $p = ab$, где a и b — обратимые э-ты.

Опр 4 Число называется нормой A наз-ся **евклидовой**,
если сущ-т ф-ция $N: A \setminus \{0\} \rightarrow \mathbb{N}_0$

(называемая **нормой**), удовл. след. условиям:

- 1) $N(ab) \geq N(a)$ и рав-во имеет место $\Leftrightarrow b \in A^*$,
- 2) $\forall a, b \in A, b \neq 0, \exists q, r \in A: a = qb + r$
и мнб $r \neq 0$, мб $N(r) < N(b)$.

Зам. В 2) не требуется единств. q и r . В 1) второе
можно вывести из ост. условий

Примеры 1. $A = \mathbb{Z}, N(a) = |a|$
2. $A = F[x], N(f) = \deg f$ } о сн. сур-мерн
см. ч 3, § 5 пр. 1 [Вик]

3. Кольцо $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i - \text{мнимая единица}\}$

целых гауссовых чисел отн-но нормы $N(a + bi) = a^2 + b^2$

Опр 5 Наибольшим общим делителем элементов a и b в коммутативном кольце A называется элемент $d \in A$:

- 1) $d \mid a$ и $d \mid b$ (d — общий делитель a и b);
- 2) если $d' \in A$: $d' \mid a$ и $d' \mid b$, то $d' \mid d$.

Обозн. $d = (a, b)$.

Т. 1 Если A — евкл. кольцо. Тогда для любых $a, b \in A$

существует наиб. общий делитель $d = (a, b)$ и

найдётся $u, v \in A$: $d = au + bv$. (Д-во: см. [ВАН] Т. 3.5.1)

Опр 6 Элементы a и b в евкл. кольце A называются

взаимно простыми, если $(a, b) = 1$.

Следствие (критерий взаимной простоты)

$$(a, b) = 1 \Leftrightarrow \exists u, v \in A : au + bv = 1.$$

+ Теорема
о разложении
в простые
элементы
Т. 3.5.2
из [ВАН]

Опр 7 Унитарное кольцо, в котором все
узлы идеалы, наз-ся **кольцом ПИД**
узлов (Principle Integral Domain = PID).

Примеры 1) F -поле 2) \mathbb{Z} , но не \mathbb{Z}_n в случае
составн
т.к там есть делители.

3) Которое евкл. кольцо — PID
(см. Т. 9.2.2 из [Вик])

4) Существоют неевкл. PID: например,
 $A = \{a + b\sqrt{-19} \mid a, b \in \mathbb{Z} + \frac{1}{2}\}$ — кольцо в \mathbb{C}
— неевклидово кольцо главных идеалов.

Т.2 В кооме н. идеалов A $\forall x, y \in A$ существует их наиб. общий делитель d и он может быть представлен в виде $d = ax + by$, где $a, b \in A$.

Л-во: 1-м и ин-во $I = \{ax + by \mid a, b \in A\}$.

В силу предл. 2.4 — это идеал, порож. x и y .
т.к. A — PID, то $\exists u \in A : I = (u)$.

Этот u — наибольший \square

Мы будем часто обозн. $I = (x, y) \equiv (d)$.

Т-ма о св-х и единств. разл. тоже сохр для PID
Отсюда следует (см. § 3.10 след. из предл. 1), что в поле
частных коомов н. идеалов есть однознач. запись в виде несокр-
грозди.

Т. 3 Пусть n — ненулевой делитель n — числа главных идеалов A . Фактор-кольцо $A/(n)$ является полем $\Leftrightarrow n$ — простой делитель n — числа A .

Д-во. см. Т. 9.2.4 из [ВЧН],

Т. 4 Пусть m, n — взаимно простые делители n — числа главных идеалов A . Тогда

$$A/(mn) \cong A/(m) \oplus A/(n).$$

Д-во: см. Т. 9.2.5 из [ВЧН] | $\frac{\text{ЧКЗ. } \varphi: A \rightarrow A/(m) + A/(n)}{a \mapsto (a + (m), a + (n))}$
и Т. 1 о том-значении.

Примеры 1) $\mathbb{Z}_n \simeq \mathbb{Z}_k \oplus \mathbb{Z}_l \Leftrightarrow n=kl$ и $(k,l)=1$.

2) $f(x) = (x-c_1) \cdot \dots \cdot (x-c_n)$, где c_1, \dots, c_n — разл.

$$\Rightarrow K[x]/(f) \simeq K[x]/(x-c_1) \oplus \dots \oplus K[x]/(x-c_n) \simeq K \oplus \dots \oplus K = K^n.$$

Т.5 (о форме Санта мы из PID). М-я из под коэрн А п. идеалов приводится к нормальной форме Санта.

Д-во: Смысл: нет алгоритма Евклида.

Назовем квазиэлементарными преобразованиями следующие операции (сдвиги) x_1, \dots, x_m заменим

перн эн-ров x_i и x_j нэ $ax_i + bx_j, cx_i + dx_j$, згел
 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ - обратная м-ца с эн-ми из A (она обратна
 $\Leftrightarrow \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \in A^\times$). Пр.-е, обратное

к КБАЗ эн-ментарному — КБАЗ эн-ментарному.
Пару эн-ров $\{x, y\}$ коорд. A можно кбаз эн-ент.
Пр.-е, условие к базису $\{d, 0\}$, згел $d = \{a, b\}$.
 A -но, по т. 2 $\exists a, b \in A: ax + by = d$. Тогда
м-ца $\begin{pmatrix} a & b \\ -y/d & x/d \end{pmatrix}$ обратна (ее инв-т = $\mathbf{1}$).

Коорд. кбаз эн-ент. пр.-е преобраз $\{x, y\}$ в $\{d, 0\}$.

Восстанови г-во преобраз так же как и
Док-во т. 1.2 из АТ 1н. \square