Лекция 3 марта (первая половина)

Расширения коммутативных колец

Условимся: "кольцо" – коммутативное кольцо с единицей.

$A \subset B$ – расширение коммутативных колец,

$\mathbb{Z} \subset \mathbb{Q}$ хочется, когда $B = \mathbb{Q}$ иметь внутри B что-то типа $\mathbb{Z}$.

Лемма: следующие условия на элемент $b \in B$ эквивалентны:

(1) $b^n = a_1 b^{n-1} + \dots + a_{n-1} b + a_n$ для некоторых $a_i \in A$, $n \in \mathbb{N}$

(2) Целые неотрицательные степени $\{1, b, b^2, \dots\} = \{b^n \mid n \in \mathbb{Z}_{\geq 0}\}$ порождают конечно-порождённый A-подмодуль в B

(3) $\exists$ конечно порождённый A-подмодуль $M \subset B$: (3.1) $bM \subset M$

(3.2) $cM = 0 \Rightarrow c = 0$ $(\forall c \in B)$

$(1) \Rightarrow (2) \Rightarrow (3)$ $\quad 1 \cdot c = 0 \Rightarrow c = 0$

$(3) \Rightarrow (1)$ Пусть M порождается как A-модуль элементами $e_1, \dots, e_m$

$$(be_1, \dots, be_m) = (e_1, \dots, e_m) \cdot Y$$

$$\overset{\shortparallel}{(e_1 \dots e_m) \cdot bE} \quad \Downarrow \qquad Y \in \mathrm{Mat}_{m \times m}(A).$$

$$(e_1, \dots, e_m) \cdot (bE - Y) = 0 = (0, \dots, 0)$$

$X \in \mathrm{Mat}_m(K)$ $\quad \boxed{XX^\vee = \det(X) \cdot E}$

$X^\vee$ – присоединённая матрица

$x^\vee_{ij} = (-1)^{i+j} X_{ji}$

$$(e_1, \dots, e_m) \cdot \det(bE - Y) = 0$$

$$= \underbrace{(e_1, \dots, e_m)(bE - Y)}_{\overset{\shortparallel}{0}} \cdot (bE - Y)^\vee$$

Умножение на $\det(bE - Y)$ аннулирует M

$\Downarrow$

$\det(bE - Y) = 0$ $\quad Y \in \mathrm{Mat}_m(A)$

$\Updownarrow$

$$b^m = a_1 b^{m-1} + \ldots + a_m$$

$b \in B$ называется целым над A, если он удовлетворяет предыдущим условиям (1)–(3)

Факт: Целые над A элементы у $B \supset A$ образуют кольцо.

$$\underline{x^n = a_1 x^{n-1} + \ldots + a_n} \qquad a_i, b_i \in A$$

$$\underline{y^m = b_1 x^{m-1} + \ldots + b_m} \qquad x, y \in B$$

$$\underset{\substack{\cup\\ 1}}{M} = \operatorname{span}_A\left(x^i y^j \mid 0 \le i \le n-1,\ 0 \le j \le m-1\right)$$

$$xM \subset M \qquad yM \subset M$$

$$xyM \subset M \qquad (x+y)M \subset M.$$

xy $x+y$ целые, если x, y целые.

Факт: $A \subset B \subset C$

Пусть $\bar{A}$ – целое замыкание A в B

$$= \{b \in B \mid b \text{ цел над } A\}$$

если элемент $c \in C$ цел над $\bar{A}$, то он цел и над A.

Док-во: $c_1 : \; c_1^{n_1} = a_{1,1}c_1^{n_1-1} + \dots + a_{1,n_1}$ //

$\overline{A} \ni \; \vdots$

$c_m : \; c_m^{n_m} = a_{m,1}c_m^{n_m-1} + \dots + a_{m,n_m}$ //

$c^k = c_1 c^{k-1} + \dots + c_m$ — цел над $\overline{A}$ $\quad c_i \in \overline{A}$

$$M = \operatorname{span}\left(c^i c_1^{j_1} \cdots c_m^{j_m} \;\middle|\; \begin{matrix} 0 \le i \le k-1 \\ 0 \le j_\alpha \le n_\alpha - 1 \end{matrix} \right)$$

$cM \subset M$

Автор - Дедекинд $\quad \mathbb{Q} \subset K \quad \dim_{\mathbb{Q}} K < \infty$

$\dim_{\mathbb{Q}} K = n$

как векторного пр-ва над $\mathbb{Q}$

элементы из K наз. алгебраическими числами

$K = \mathbb{Q}[\sqrt{3}] = a + b\sqrt{3}$

$K = \mathbb{Q}[\omega] \,/\, \omega^2 + \omega + 1 = 0$

$K = \mathbb{Q}[i] \,/\, i^2 = -1$

$$\begin{array}{ccc} \mathbb{Q} & \supset & \mathbb{Z} \\ \cap & & \cap \\ K & \supset & O_K \end{array}$$

- Исходное определение Дедекинда: число $z \in K$ наз. целым если оператор $K \to K$, $x \mapsto zx$

записывается целочисленной матрицей в некотором базисе K над $\mathbb{Q}$

$$\boxed{\text{Это равносильно тому, что } z \text{ цел над } \mathbb{Z} \text{ в смысле нашего определения}}$$

$O_K \subset K$ кольцо целых над $\mathbb{Z}$ чисел (целое замыкание $\mathbb{Z}$ в $\mathbb{Q}$).

$\forall z \in K$ $\quad 1, z, \dots, z^n$ линейно зависимы

$$a_0 z^n + a_1 z^{n-1} + \dots + a_n = 0 \qquad (n = \dim_{\mathbb{Q}} K)$$

$a_i \in \mathbb{Q} \Rightarrow$ можно считать, что $a_i \in \mathbb{Z}$ (умножим на общий знаменатель).

$\Downarrow$

$$\boxed{\text{число } a_0 z \text{ цело над } \mathbb{Z}}$$

$$a_0^n z^n + a_1 (a_0 z)^{n-1} + a_1 a_0 (a_0 z)^{n-2} + \dots + a_n a_0^{n-1}$$

$\forall$ числа $z \in K$ и для любого базиса $e_1, \dots, e_n$ поля K как векторного пр-ва над $\mathbb{Q}$

$\exists n \in \mathbb{Z} : \; nz \in O_K$, $ne_i \in O_K$ сразу для всех i

(1) K — поле частных кольца O_K

(2) O_K — свободный? $\mathbb{Z}$-модуль ранга n

$O_K \subset K \Rightarrow$ в O_K нет кручения $\Rightarrow O_K$ свободен.

любые $n+1$ векторов из O_K линейно зависимы над $\mathbb{Q}$ $\Rightarrow$ над $\mathbb{Z}$ $\quad \operatorname{rk} O_K \le n$

$\forall$ базиса $e_1, \dots, e_n$ поля K над $\mathbb{Q}$ $\exists m \in \mathbb{Z}$ $me_1, \dots, me_n \in O_K$ линейно независимы

$\operatorname{rk} O_K \ge n$

$z \in O_K \qquad zO_K \subset O_K$.

в базисе модуля O_K над $\mathbb{Z}$ (который автоматически будет базисом K над $\mathbb{Q}$) умножение на z записывается целочисленной матрицей.

G — конечная группа действует на кольце B кольцевыми автоморфизмами.

$B^G \subset B$ — подкольцо инвариантов

"

$\{b \mid gb = b \ \forall g \in G\}$

B цело над B^G $\quad \forall b \in B$ цел над B^G

Пусть G-орбита элемента b имеет вид $\{b_1, \dots, b_k\}$

$$\overset{b''}{\beta(t)} = \prod_{i=1}^{k} (t - b_i) = B^G(t)$$

$\nearrow$ $\beta(b) = 0$ $\qquad b = b_1$

многочлен со старшим к-том 1

приведённый

Лемма Гаусса (-Кронекера-Дедекинда)

$A < B$ – любое расширение колец

Пусть в $B[t]$ выполняется равенство

$f(t) = g(t) \cdot h(t)$ где f, g и h приведены.

Все к-ты f целы над A $\Longleftrightarrow$ все коэф-ты и у g и у h целы над A.

Док-во: если g и h имеют целые к-ты, то и у f целые коэф-ты

Пусть у f целые коэфф-ты.

$\exists$ кольцо $C \supset B$: в $C[t]$ и g и f полностью раскладываются на линейные множители $g(t) = \prod (t - \alpha_i)$

$h(t) = \prod (t - \beta_j)$

$\forall$ приведённого многочлена $q(t) \in B[t]$
$\exists$ кольцо $C \supset B$: $\underline{q(t) = \prod (t - \gamma_i)}$ $\gamma_i \in C$
в $C[t]$

Док-во: индукция по $\deg q$.

$$F = B[t]/q \hookleftarrow B$$

вложение констант (т.к. q приведён)

$$c_1 \neq c_2(t^4 + \dots)$$

$F \supset B$

в $F[t]$ $\quad q(t) = (t - \gamma) q_1(t)$

$$\gamma = [t]_q \in F$$

$$f = gh = \prod_i (t - \alpha_i) \prod_j (t - \beta_j)$$

к-ты f целы над $A \Rightarrow \alpha_i$ и β_j целы над целым замыканием A в $C \Rightarrow$ α_i и β_j целы над $A \Rightarrow$ к-ты у f и g целы над A