

6. Целый базис и дискриминант

Т.1 (о целом базисе) Пусть A - целозамк. обл. целостности

$K = \mathcal{Q}(A)$ - поле частных, L - кон. сепар. рассл. напр K
и $B = \overline{A}^L$ - целое замыкание A в L . Тогда

(1) A нётерова $\Rightarrow B$ нётерова

(2) A - обл. главных идеалов $\Rightarrow B$ - свободный модуль над A ранга $n = |L:K|$.

Л-во: Неком. B - свобод. A -модуль ранга n , если

\Rightarrow базис $x_1, \dots, x_n \in B : \forall x \in B$ x единств.

образ при скалярн в виде $x = a_1 x_1 + \dots + a_n x_n, a_i \in A$.

L — в.ч. над K и $\dim_K L = n$. Пусть x_1, \dots, x_n — базис L над K .

Можно считать, что $\forall i = 1, \dots, n$ $x_i \in B$. А — это.

Пусть $x = x_i$. Т.к. L/K — конечное расширение $\Rightarrow L/K$ алгебра.

$$\Rightarrow \exists a_i, b_i \in A; \quad x^m + \frac{a_{m-1}}{b_{m-1}} x^{m-1} + \dots + \frac{a_0}{b_0} = 0 \Rightarrow$$

$$(b = \prod_{i=1}^m b_i) \Rightarrow (bx)^m + a'_{m-1} (bx^{m-1}) + \dots + a'_0 = 0 \Rightarrow$$

$bx \in B \Rightarrow$ пусть x и bx , считаем, что $x \in B$.

Итак, пусть $x_1, \dots, x_n \in B$ — базис L над K .

Т.к. L/K сепарабельно, т. 1.5.2, \Rightarrow билинейная форма

$$(\cdot, \cdot): L \times L \rightarrow K, (x, y) = \text{Tr}_{L/K}(xy), \text{ невырождена.}$$

Пусть \mathcal{B} — базис L над K сев. двойственным базис \mathcal{B}^* — то

этой форме. В частности, для $x_1, \dots, x_n \in B$

$$\exists \text{ базис } y_1, \dots, y_n \in L : (x_i, y_j) = \delta_{ij} = \begin{cases} 1 & i=j \\ 0 & i \neq j \end{cases}$$

$$\text{Обозначим } N = \langle x_1, \dots, x_n \rangle = Ax_1 + \dots + Ax_n \subseteq B$$

$$M = \langle y_1, \dots, y_n \rangle = Ay_1 + \dots + Ay_n \subseteq L$$

при этом $Ky_1 + \dots + Ky_n = L$, где y_1, \dots, y_n - базис L/K .

Докажем, что $B \subseteq M$. Возьмем $z \in B \subseteq L$

$\forall x_i \in B, i=1..n, x_i z \in B$: Из универсальности A в смысле свойства 1 п. 1.5.1 $\xRightarrow{\text{свойство 1}} \chi_{L/K}^{x_i z}(t) \in A[t] \Rightarrow$

В частности, $(x_i, z) = T_{L/K}(x_i z) \in A$.

Различные элементы на базисе y_1, \dots, y_n над K :

$$z = \sum d_i y_i, d_i \in K. \text{ Умножим } (x_i, z) = \sum_{j=1}^n d_j (x_i, y_j) = d_i \in A$$

Значит, $z \in Ay_1 + \dots + Ay_n = M$

$$\text{Итак, } \sum_{i=1}^n Ax_i = N \subseteq B \subseteq M = \sum_{i=1}^n Ay_i$$

(1) Если A — нетривиальное кольцо $\Rightarrow M$ — нетривиальное кольцо

над A (как к.и. кольцо над нетривиальным кольцом,

см. лемма NTI или [Бук, § 9, 4]). $\Rightarrow B$ — нетривиальное

кольцо над A как подкольцо B в M ($B \subseteq M$!)

Если $I \trianglelefteq B$, то $I \subseteq B$ — A -подкольцо $\Rightarrow I$ — к.и. над A

и тем более над $B \Rightarrow B$ — нетривиальное кольцо.

(2) Пусть A — кольцо равных идеалов.

N и M — A -модули, порожденные элементами x_1, \dots, x_n и y_1, \dots, y_n соответственно. Т.к. x_1, \dots, x_n и y_1, \dots, y_n лев. нез. над $K = \mathbb{Q}(A)$

\Rightarrow лев. нез. над $A \Rightarrow N$ и M — свободные

A -модули ранга n . Далее, см. [Вик, § 9.3]:

B — A -подмодуль в M . $\Rightarrow B$ — свободный

N — A -подмодуль в $B \Rightarrow n = \text{rang } N \leq \text{rang } B \leq \text{rang } M = n \Rightarrow \text{rang } B = n$.

Следствие Если L — числовое алгебра, то кольцо

целых алгебраических чисел \mathcal{O}_L — свободный \mathbb{Z} -модуль ранга

$n = |L: \mathbb{Q}|$

Д-во: \mathbb{Z} -целозамкнутый не в. идеалов.

Прп 1 базис кольца \mathcal{O}_L над \mathbb{Z} наз-ся каноническим базисом
кольца \mathcal{O}_L (или рассуждениями L/K)

Прп 1 а) $L = \mathbb{Q}(\sqrt{5})$. Тогда $1, \frac{1+\sqrt{5}}{2}$ — канонич.
базис в \mathcal{O}_L . При этом $1, \sqrt{5}$ — базис L
над \mathbb{Q} из канонич. м-та, но не канонич. базис \mathcal{O}_L .

б) $L = \mathbb{Q}(\sqrt{7})$. Тогда $1, \sqrt{7}$ — канонич. базис L
над \mathbb{Q} , в частности, $\mathcal{O}_L = \mathbb{Z}[\sqrt{7}]$.

Замечание: Если R — некоторого кольца S и S — свобод. R -модуль,
то гомоморфизм R/S корректно определит
свои $T_{S/R}$ и норма $N_{S/R}$.

Опр 2 Тусло S - раск. колыа R своб. кал R -модуль. ранга n .

Дискриминант Нелора $\vec{x} = x_1, \dots, x_n \in S$ - это

$$D(\vec{x}) = D(x_1, \dots, x_n) = \det(T_{S/R}(x_i, x_j))$$

Лемма 1 Если $\vec{y} = C\vec{x}$, $C \in M_n(R)$, $\det C \neq 0$, то

$$D(\vec{y}) = \det^2(C) D(\vec{x}) \quad (*)$$

Хул 2 Δ -ге лемма 1. Уелз: $T = (x_i, x_j)$ $T' = (y_i, y_j)$

$$\Rightarrow T' = C^* T C \quad (\text{св-ва Бил. форма})$$

Следствие Если L -анг. числовое поле, то

значения дискриминанта совпадают на всех
глахх вхдущих L wg \neq . Д-во: $\det C = 1$.

Опр 3 Если в опр 2 \vec{x} -базис S над R , то
 дискриминантный элемент $\text{disc}(S/R) = (D(\vec{x}))$ -элемент,
 пропорциональный $\Delta(\vec{x})$.

Из (*) \Rightarrow Опр 3 не зависит от выбора базиса, т.к.

let C - обратимый элемент кольца R , $\boxed{\text{disc}(C\vec{x}/R) \in \mathbb{Z}}$.
 и легко $\det C \cdot \det(C^{-1}) = 1$.

Преп 1 Пусть A -элемент. Обр. ненулевых элементов,

$L \supset K = \mathbb{Q}(A)$ - кон. сеп. поле

$B = \overline{A}^L$ - кольцо целых над A в L

- т.е. (по т. 1) - с.б.б. A -модуль ранга $n = [L:K]$.

и $\vec{x} = x_1, \dots, x_n \in B$ - базис L над K , $d = D(x_1, \dots, x_n)$

Тогда $dB \subseteq Ax_1 + \dots + Ax_n \subseteq B$

Λ -во: Векторное з.м. x_1, \dots, x_n - базис L над K
 из $\mathcal{L}(A)$, но не базис B над A .

Разложим $z \in B$ по базису \vec{x} : $z = \sum_{j=1}^n d_j x_j, d_j \in K$

$$(z, x_i) = \left(\sum_{j=1}^n d_j x_j, x_i \right) = \sum_{j=1}^n (x_j, x_i) d_j$$

Получаем $\begin{pmatrix} (z, x_1) \\ \vdots \\ (z, x_n) \end{pmatrix} = \begin{pmatrix} T_{S/K}(x_1, x_j) \\ \vdots \\ T_{S/K}(x_i, x_j) \end{pmatrix} \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$, где $\det T = d$.

← смена мест.
 $x_1 \dots x_n$ - по $d_1 \dots d_n$.

$$T \cdot K \cdot T^{-1} = \frac{1}{d} \hat{T}, \text{ где } \hat{T} \in M_n(A) \Rightarrow d \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} = \hat{T} \begin{pmatrix} (z, x_1) \\ \vdots \\ (z, x_n) \end{pmatrix}$$

$$\Rightarrow d d_i \in A \quad \forall i = 1 \dots n \Rightarrow d \cdot z = (d d_1) x_1 + \dots + (d d_n) x_n \in$$

$A x_1 + \dots + A x_n$ \square

В случае, когда L — кон. сепрб. расщепиме поле K ,
то для $x_1, \dots, x_n \in L$ можно задать еще одно
определение дискриминанта.

Пример 2 Пусть L/K — кон. сеп. расщ. поле, $[L:K] = n$
и $\sigma_1, \dots, \sigma_n$ — разн. K -вложения L в \bar{K} . Тогда $\forall x_1, \dots, x_n \in L$

$$D(x_1, \dots, x_n) = \det^2 (\sigma_i(x_j))_{i,j=1, \dots, n}$$

Лемма Т.ч. L/K — сеп., то по определ. 1.8.3 имеем

$$T_{L/K}(x_i x_j) = \sum_{k=1}^n \sigma_k(x_i x_j) = \sum_{k=1}^n \sigma_k(x_i) \sigma_k(x_j).$$

$$\text{Пусть } C = (\sigma_k(x_i))_{k,i} \in M_n(K). \text{ Тогда } (T_{L/K}(x_i x_j))_{i,j} = \\ = C^T \cdot C \Rightarrow D(x_1, \dots, x_n) = \det^2 C \quad \square$$

Теорема, что L/K сепар. $\Rightarrow L = K(\alpha)$ - простое
 α -зар. над K

Если $f(t)$ - густ. мн-н. $\exists K[t]$, то $\text{Dis}(f) = \prod (x_i - x_j)^2$,
где $x_i, i=1, \dots, n$ - корни $f(t)$ в алг. зам. \bar{K} .

Теорема 2 (о вычислении дискриминанта). Пусть

$L = K(\alpha) = K(\alpha)$ сеп. расщ. над K ст. n , x_1, \dots, x_n - корни

мн-н. $f(t) = M_K^{\alpha}(t)$ в \bar{K} . Тогда

$$a) \text{D}(1, \alpha, \dots, \alpha^{n-1}) = \prod_{i < j} (x_i - x_j)^2 = \text{Dis}(f(t))$$

$$b) \text{D}(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{n(n-1)/2} N_L (f'(\alpha)).$$

Упр 3 Δ - то 7.2, см. упр. 2. \bar{K}
(см. также задачу 7.6.1)

Упр 4 (упрощен) $L = \mathbb{Q}(x)$, x — корень $f(t) = t^3 - 3t + 1$

(a) $\text{Dis}(f(t)) = -4p^3 - 27q^2 = \Delta$ — дискриминант

$$\Rightarrow \Delta(1, x, x^2) = +4 \cdot 3^3 - 27 = 81$$

(b) $f'(t) = 3t^2 - 3 = 3(t-1)(t+1)$

$$\left[p^{x+1} \right]_{1, x, x^2}$$

$$\left[p^{x-1} \right]_{1, x, x^2}$$



$$N(x+1) = -3$$

$$N(x-1) = 1.$$

$$\Rightarrow \Delta(1, x, x^2) = f(1)^{3 \cdot 2/2} \underset{\substack{1 \\ 27}}{N(3)} (-3) (1) = 81.$$