4. Целый базис и дискриминант

Т. 1 (о целом базисе) Пусть A - целозамк. обл. целостности $K = Q(A)$ - поле частных, L - кон. сепараб. расш. поля K и $B = \overline{A}^L$ - целое замыкание A в L. Тогда

(1) A нётерово $\Rightarrow$ B нётерово

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

Д-во: Напом. B - св модуль ранга n, если $\exists$ базис $x_1, \ldots, x_n \in B$: $\forall x \in B$ x единств. образом представим в виде $x = a_1 x_1 + \ldots + a_n x_n$, $a_i \in A$.

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

Можно считать, что $\forall i = 1..n$ $x_i \in B$. Д-ем это.

Пусть $x = x_i$. Т.к. L/K — конечное расш. $\Rightarrow$ L/K алгебр.

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

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

$bx \in B \Rightarrow$ меняя x на 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. 1.3.2 $\Rightarrow$ билинейная форма

$(\,,\,) : L \times L \to K$, $(x, y) = T_{L/K}(xy)$, невырождена.

Поэтому $\forall$ базиса L над K сущ. двойственный базис отн-но этой формы. В частности, для $x_1 \dots x_n \in B$

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

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 $Ky_1 + \dots + Ky_n = L$, т.к. $y_1 \dots y_n$ – 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 целозамкнутости A в силу следствия 1 т-мы 1.3.1 $\Longrightarrow \chi_{L/K}^{x_i z}(t) \in A[t] \Longrightarrow$ $\xrightarrow{\text{коэф-т!}}$

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

Разложим теперь по базису $y_1 \dots y_n$ над K:

$z = \sum \alpha_i y_i$, $\alpha_i \in K$. Имеем $(x_i, z) = \sum\limits_{j=1}^{n} \alpha_j (x_i, y_j) = \alpha_i \in A$

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

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

(1) Если A – нётерово кольцо $\Rightarrow$ M – нётеров модуль над A (как к.п. модуль над нётеровым кольцом, см., например, [ВИН, § 9,4]. $\Rightarrow$ B – нётеров модуль над A как подмодуль в M ($B \subseteq M$!)

Если $I \trianglelefteq B$, то $I \subseteq B$ – A-подмодуль $\Rightarrow$ I – к.п. над A и тем более над B $\Rightarrow$ B – нётерово кольцо.

(2) Пусть A — кольцо главных идеалов.

N и M — A-модули, порожденные $x_1 \dots x_n$ и $y_1 \dots y_n$ соот-но. Т.к. $x_1 \dots x_n$ и $y_1 \dots y_n$ лин. нез. над $K = Q(A)$ $\Rightarrow$ лин. нез. над A $\Rightarrow$ N и M — свободные A-модули ранга n. Далее, см. [Вин, §9.3]:

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

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

<u>Следствие</u> Если L — числовое алг. поле, то кольцо целых ал. чисел O_L — свободный $\mathbb{Z}$-модуль ранга $n = |L : \mathbb{Q}|$

<u>Д-во:</u> $\mathbb{Z}$ — целозам. область глав. идеалов.

Опр 1 Базис кольца $\mathcal{O}_L$ над $\mathbb{Z}$ наз-ся целым базисом поля L (или кольца $\mathcal{O}_L$)

Упр 1 а) $L = \mathbb{Q}(\sqrt{5})$. Тогда $\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}$ — целый базис L над $\mathbb{Q}$. При этом $1, \sqrt{5}$ — базис L над $\mathbb{Q}$ из целых эл-тов, но не целый базис. Найти $\mathcal{O}_L$.

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

Замечание: Если R - подкольцо кольца S и S - своб. R-модуль, то для расширения R/S корректно определены след $T_{S/R}$ и норма $N_{S/R}$.

Опр 2 Пусть S — расш. кольца R своб. как R-модуль ранга n.

Дискриминант набора $\vec{x} = x_1, \dots x_n \in S$ — это

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

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

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

Упр 2 Д-те лемму 1. Указ: $T = (x_i x_j)$ $T' = (y_i y_j)$

$\Rightarrow T' = C^* T C$ (св-ва билин. формы)

Следствие Если L — алг. числовое поле, то значение дискриминант совпадает на всех целых базисах L над $\mathbb{Z}$. Д-во: $\det C = \pm 1$.

Опр 3 Если в опр 2 $\vec{x}$ - базис S над R, то дискриминантный идеал $disc(S/R) = (D(\vec{x}))$ - идеал, порожденный эл-том $D(\vec{x})$.

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

let C - обратимый эл-т кольца R. $\boxed{disc(\mathcal{O}_L/\mathbb{Z}) \in \mathbb{Z}}$.

Предл 1 Пусть A - целоз. обл. целостности

$L \supset K = Q(A)$ - кон. сеп. расш полей

$B = \overline{A}^L$ - кольцо целых над A эл-тов из L

- т.е (по т. 1) - своб. A-модуль ранга $n = |L:K|$.

и $\vec{x} = x_1 \ldots x_n \in B$ - базис L над K. Тогда

$dB \subseteq Ax_1 + \ldots + Ax_n$, где $d = D(x_1, \ldots x_n)$.

A-во: Важное зам. $x_1 \dots x_n$ – базис L над K из целых, но не базис B над A.

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

$$\overset{A}{(z, x_i)} = \left(\sum \alpha_j x_j, x_i\right) = \sum_{j=1}^{n} \overset{A}{(x_i, x_j)}\alpha_j$$

Получаем $\begin{pmatrix}(z,x_1)\\ \vdots \\ (z,x_n)\end{pmatrix} = \left(\underbrace{T_{L/K}(x_i,x_j)}_{=T}\right)\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}$, где $\det T = d$.

← система лин. ур-й отн. по $\alpha_1 \dots \alpha_n$.

Т.к. $T^{-1} = \frac{1}{d}\hat{T}$, где $\hat{T} \in M_n(A) \Rightarrow d\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix} = \hat{T}\begin{pmatrix}(z,x_1)\\ \vdots \\ (z,x_n)\end{pmatrix}$

$\Rightarrow d\alpha_i \in A$ $\forall i = 1 \dots n \Rightarrow d z = (d\alpha_1)x_1 + \dots + (d\alpha_n)x_n \in \underbrace{}_{=} A x_1 + \dots + A x_n$.

Напомним, что L/K сепар. $\Rightarrow$ $L = K(x)$ — простое, x — алг. над K

Если $f(t)$ — унит. мн-н. из $K[t]$, то $\mathrm{Dis}(f) = \prod (x_i - x_j)^2$, где x_i, $i = 1..n$ — корни $f(t)$ в алг. зам. $\overline{K}$.

<u>Теорема 2</u> (о вычислении дискриминанта). Пусть $L = K(x)$ — кон. сеп. расш. поля K степ. n, $x_1 \dots x_n$ — корни мин. мн-на $f(t) = m_K^x(t)$ в $\overline{K}$. Тогда

a) $D(1, x, \dots x^{n-1}) = \prod\limits_{i<j} (x_i - x_j)^2 = \mathrm{Dis}(f(t))$

б) $D(1, x, \dots x^{n-1}) = (-1)^{n(n-1)/2} N_{L/K}(f'(x))$.

<u>Упр 3</u> Д-ть Т. 2 (см. также лекции Губ...ва)

<u>Упр 4</u> (пример) $L = \mathbb{Q}(x)$, x — корень $f(t) = t^3 - 3t + 1$

(а) $\mathrm{Dis}(f(t)) = -4p^3 - 27q^2$ — ф-ла Кардано

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

(б) $f'(t) = 3t^2 - 3 = 3(t-1)(t+1)$

$[\rho^{x+1}]_{1,x,x^2}$ $\qquad$ $[\rho^{x-1}]_{1,x,x^2}$

$\downarrow$

$N(x+1) = -3$ $\qquad$ $N(x-1) = 1.$

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