Норма и следа на алгебрични числа

5. Детерминанта и следа на линеен оператор

Нека $\varphi : V \to V$ е линеен оператор в крайномерно линейно пространство V над поле k и нека

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \in M_n(k)$$

е матрицата на φ в някой базис $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ на V над k. *Следата* $\operatorname{tr}_k \varphi$ на линейния оператор φ се определя с формулата $\operatorname{tr}_k \varphi = a_{11}+a_{22}+\dots+a_{nn}$, а детерминантата $\det_k \varphi$ на линейния оператор φ се определя с формулата $\det_k \varphi = \det A$.
Нормата и следата на φ са свързани със собствените стойности $\lambda_1, \dots, \lambda_n$ на φ по следния начин:

$$\operatorname{tr}_k \varphi = \lambda_1 + \dots + \lambda_n, \tag{2}$$

$$\det_k \varphi = \lambda_1 \cdots \lambda_n. \tag{3}$$

За установим това, да забележим, че ако

$$\chi_\varphi(\lambda) = \begin{vmatrix} \lambda - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & \lambda - a_{22} & \dots & -a_{2n} \\ \dots & \dots & \dots & \dots \\ -a_{n1} & -a_{n2} & \dots & \lambda - a_{nn} \end{vmatrix} = \lambda^n + a_1\lambda^{n-1} + \dots + a_n$$

е характеристичния полином на φ, то са в сила равенствата

$$a_1 = -(a_{11} + a_{22} + \dots + a_{nn}),$$
$$a_n = \chi_\varphi(0) = \det(-A) = (-1)^n \det A.$$

Сега формули (2) и (3) следват от формулите на Виет

$$\lambda_1 + \dots + \lambda_n = -a_1,$$
$$\lambda_1 \cdots \lambda_n = (-1)^n a_n.$$

Да отбележим, че формули (2) и (3) показват, че нормата и следата на φ не зависят от избора на базиса $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ на V, т. е. $\operatorname{tr}_k \varphi$ и $\det_k \varphi$ са инварианти на оператора φ.

6. Норма и следа на алгебрично число

Нека E е крайно разширение на полето $\mathbb{Q}$ на рационалните числа и нека $\alpha \in E$ е алгебрично число. Тогава E е крайномерно линейно пространство над $\mathbb{Q}$ с размерност $[E : \mathbb{Q}]$. Да означим с $\varphi_\alpha : E \to E$ линейния оператор зададен с формулата $\varphi_\alpha(x) = \alpha x$, $x \in E$.

Дефиниция (Следа и норма на алгебрично число). Следата $\operatorname{tr}_{\mathbb{Q}} \varphi_\alpha$ на φ_α се нарича *следа на алгебричното число* α и се означава с $\operatorname{tr}_{\mathbb{Q}}^E(\alpha)$. Детерминантата $\det_{\mathbb{Q}} \varphi_\alpha$ на φ_α се нарича *норма на алгебричното число* α и се означава с $\mathrm{N}_{\mathbb{Q}}^E(\alpha)$.

Ясно, е че ако $\alpha \in \mathbb{Q}$, то $\operatorname{tr}_{\mathbb{Q}}^E(\alpha) = [E : \mathbb{Q}]\alpha$ и $\mathrm{N}_{\mathbb{Q}}^E(\alpha) = \alpha^{[E:\mathbb{Q}]}$.

Пример 6.1. Нека $E = \mathbb{Q}(i)$ и $\alpha = a + bi \in E$, $a, b \in \mathbb{Q}$. Тогава $\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha) = 2a$ и $\mathrm{N}_{\mathbb{Q}}^{E}(\alpha) = a^2 + b^2$. По-общо, ако D е свободно от квадрати рационално число и $\alpha = a + b\sqrt{D} \in E = \mathbb{Q}(\sqrt{D})$, $a, b \in \mathbb{Q}$, то $\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha) = 2a$ и $\mathrm{N}_{\mathbb{Q}}^{E}(\alpha) = a^2 - Db^2$.

Лема 6.2. *Нека α е алгебрично число и $E = \mathbb{Q}(\alpha)$. Тогава характеристичният полином χ на линейния оператор $\varphi_\alpha : E \to E$ съвпада с минималния полином p на α над полето $\mathbb{Q}$.*

Доказателство. Според теоремата на Хамилтън — Кейли от курса по линейна алгебра е в сила $\chi(\varphi_\alpha) = 0$. Да забележим, че $\chi(\varphi_\alpha) = \varphi_{\chi(\alpha)}$, откъдето незабавно следва, че $\chi(\alpha) = 0$. Следователно минималният полином p дели характеристичния полином χ. Тъй като χ и p са полиноми със старши коефициент 1 от степен $[E : \mathbb{Q}]$, то $\chi = p$. □

Лема 6.2 и формули (2) и (3) показват, че за всяко алгебрично число α

$$\mathrm{tr}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)} = \alpha_1 + \cdots + \alpha_k, \tag{4}$$

$$\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)} = \alpha_1 \cdots \alpha_k, \tag{5}$$

където $\alpha_1, \ldots, \alpha_k$ са спрегнатите с α над $\mathbb{Q}$ алгебрични числа.

Нека $\mathbb{Q} \subseteq E \subseteq F$ са крайни разширения на полето на рационалните числа и нека $\alpha \in E$. Тогава умножението с α индуцира линейни оператори $E \to E$ и $F \to F$. Допускайки известна неточност, ще означаваме тези два линейни оператора с един и същи символ φ_α.

Лема 6.3. *Нека χ_E (съответно $\chi_{E'}$) е характеристичният полином на оператора $\varphi_\alpha : E \to E$ (съответно $\varphi_\alpha : E' \to E'$). Тогава $\chi_{E'} = \chi_E^{[E':E]}$.*

Доказателство. Нека $y_1, \ldots, y_m \in E'$, $m = [E' : E]$, е базис на E' над E и нека $E_1, \ldots, E_m \subseteq E'$ са множествата $y_1E, \ldots, y_mE$. Тогава $E_1, \ldots, E_m$ са линейни подпространства на E' над полето $\mathbb{Q}$ и $E' = E_1 \oplus \cdots \oplus E_m$. Тъй като

$$\varphi_\alpha(y_jE) = \alpha(y_jE) = y_j(\alpha E) \subseteq y_iE, \quad j = 1, \ldots m,$$

то всяко от подпространствата E_i е φ_α-инвариантно. Нека χ_j е характеристичният полином на линейния оператор $\varphi_\alpha|_{E_j} : E_j \to E_j$, $j = 1, \ldots m$; тогава $\chi_{E'} = \chi_1 \cdots \chi_m$. Сега да забележим, че ако $x_1, \ldots, x_k$ е базис на E над $\mathbb{Q}$, то $y_jx_1, \ldots, y_jx_k$ е базис на E_j над $\mathbb{Q}$ и матрицата на оператора $\varphi_\alpha : E \to E$ в базиса $x_1, \ldots, x_k$ съвпада с матрицата на оператора $\varphi_\alpha|_{E_j} : E_j \to E_j$ в базиса $y_jx_1, \ldots, y_jx_k$. Следователно $\chi_1 = \chi, \ldots, \chi_m = \chi$ и $\chi_{E'} = \chi_E^m$. □

Твърдение 6.4. *Нека E е крайно разширение на полето $\mathbb{Q}$ на рационалните числа и $\alpha \in E$. Нека $\alpha_1, \ldots, \alpha_k$ са спрегнатите с α над $\mathbb{Q}$ алгебрични числа. Тогава*

$$\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha) = [E : \mathbb{Q}(\alpha)](\alpha_1 + \cdots + \alpha_k), \tag{6}$$

$$\mathrm{N}_{\mathbb{Q}}^{E}(\alpha) = (\alpha_1 \cdots \alpha_k)^{[E:\mathbb{Q}(\alpha)]}. \tag{7}$$

Доказателство. Нека χ е характеристичният полином на линейния оператор $\varphi_\alpha : E \to E$ и p е минималният полином на α над $\mathbb{Q}$. Според Лема 6.3, приложена към разширенията $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq E$, е в сила $\chi = p^{[E:\mathbb{Q}(\alpha)]}$, откъдето следват формули (6) и (7). □

Твърдение 6.5. *Нека E е крайно разширение на полето $\mathbb{Q}$ на рационалните числа и нека $\sigma_1, \ldots, \sigma_n : E \to \mathbb{C}$ са всички изоморфизми на E в полето $\mathbb{C}$ на комплексните числа. Тогава за всяко алгебрично число $\alpha \in E$*

$$\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha), \tag{8}$$

$$\mathrm{N}_{\mathbb{Q}}^{E}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha). \tag{9}$$

Доказателство. Нека $\tau_1, \ldots, \tau_k$ са всички изоморфизми на $\mathbb{Q}(\alpha)$ в полето $\mathbb{C}$ на комплексните числа. Тогава $\tau_1(\alpha), \ldots, \tau_k(\alpha)$ са спрегнатите с α над $\mathbb{Q}$ алгебрични числа $\alpha_1, \ldots, \alpha_k$. Тъй като всеки изоморфизъм $\tau_i\mathbb{Q}(\alpha) \to \mathbb{C}$ се продължава по точно $[E : \mathbb{Q}(\alpha)]$ различни начина до изоморфизъм $\sigma : E \to \mathbb{C}$ на E в $\mathbb{C}$, то

$$\sigma_1(\alpha) + \cdots + \sigma_n(\alpha) = [E : \mathbb{Q}(\alpha)](\alpha_1 + \cdots + \alpha_k) = \mathrm{tr}_{\mathbb{Q}}^{E}(\alpha)$$
$$\sigma_1(\alpha) \cdots \sigma_n(\alpha) = (\alpha_1 \cdots \alpha_k)^{[E:\mathbb{Q}(\alpha)]} = \mathrm{N}_{\mathbb{Q}}^{E}(\alpha),$$

според Твърдение 6.4. □

От дефиницията на следа и норма на алгебрично число α в крайно разширение E на полето на рационалните числа следва, че $\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha)$ и $\mathrm{N}_{\mathbb{Q}}^{E}(\alpha)$ са рационални числа. Ако α е цяло алгебрично число, то следата и нормата на α са цели числа.

Твърдение 6.6. *Нека E е крайно разширение на полето $\mathbb{Q}$ на рационалните числа и $\alpha \in E$ е цяло алгебрично число. Тогава* $\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha), \mathrm{N}_{\mathbb{Q}}^{E}(\alpha) \in \mathbb{Z}$.

Доказателство. Нека $f \in \mathbb{Z}[x]$ е полином със старши коефициент 1, такъв че $f(\alpha) = 0$. Тогава всички корени на f са цели алгебрични числа. Тъй като минималният полином p на α дели полинома f, то всички спрегнати с α над $\mathbb{Q}$ алгебрични числа $\alpha_1, \ldots, \alpha_k$ са цели алгебрични числа. Сега от формули (6) и (7) следва, че $\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha)$ и $\mathrm{N}_{\mathbb{Q}}^{E}(\alpha)$ са също цели алгебрични числа. Тъй като $\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha)$ и $\mathrm{N}_{\mathbb{Q}}^{E}(\alpha)$ са рационални числа, то от Твърдение 1.3 от следва, че $\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha)$ и $\mathrm{N}_{\mathbb{Q}}^{E}(\alpha)$ са цели числа. □

7. Дискриминанта

Нека E е крайно разширение на полето $\mathbb{Q}$ на рационалните числа от степен $n = [E : \mathbb{Q}]$ и нека $\alpha_1, \ldots, \alpha_n \in E$ са алгебрични числа.

Дефиниция (Дискриминанта). Детерминантата на матрицата с коефициенти $\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha_i\alpha_j)$, $1 \le i, j \le n$, се нарича *дискриминанта* на числата $\alpha_1, \ldots, \alpha_n$ и се означава с $\Delta_E(\alpha_1, \ldots, \alpha_n)$

От определението е ясно, че дискриминантата на $\alpha_1, \ldots, \alpha_n$ е рационално число. Ако $\alpha_1, \ldots, \alpha_n$ са цели алгебрични числа, то $\Delta_E(\alpha_1, \ldots, \alpha_n)$ е цяло число.

Твърдение 7.1. *Алгебричните числа $\alpha_1, \ldots, \alpha_n \in E$ са базис на E над $\mathbb{Q}$ точно когато $\Delta_E(\alpha_1, \ldots, \alpha_n) \neq 0$.*

Доказателство. Тъй като $n = \dim_{\mathbb{Q}} E$, то е достатъчно да покажем, че алгебричните числа $\alpha_1, \ldots, \alpha_n \in E$ са линейно зависими над $\mathbb{Q}$ тогава и само тогава, когато $\Delta_E(\alpha_1, \ldots, \alpha_n) = 0$.
Ако $\alpha_1, \ldots, \alpha_n \in E$ са линейно зависими над $\mathbb{Q}$ то съществуват рационални числа $x_1, \ldots, x_n$, не всички от които са равни на 0, такива че

$$\sum_{j=1}^{n} \alpha_j x_j = 0.$$

Тогава

$$\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha_i \sum_{j=1}^{n} \alpha_j x_j) = \sum_{j=1}^{n} \mathrm{tr}_{\mathbb{Q}}^{E}(\alpha_i\alpha_j)x_j = 0, \quad i = 1, \ldots, n,$$

и ние получихме хомогенна линейна система от n уравнения за n неизвестни, която има нетривиално решение $x_1, \ldots, x_n$. Следователно матрицата от коефициенти на системата е особена, т. е. $\Delta_E(\alpha_1, \ldots, \alpha_n) = 0$.

Обратно, нека $\alpha_1, \ldots, \alpha_n \in E$ е базис на разширението E над полето на рационалните числа $\mathbb{Q}$. Ако $\Delta_E(\alpha_1, \ldots, \alpha_n) = 0$, то хомогенната линейна система

$$\sum_{j=1}^{n} \mathrm{tr}_{\mathbb{Q}}^{E}(\alpha_i \alpha_j) x_j = 0, \quad i = 1, \ldots, n, \tag{10}$$

ще има нетривиално решение $x_1, \ldots, x_n \in \mathbb{Q}$. Нека $\alpha = \sum_{j=1}^{n} \alpha_j x_j$. Тогава $\alpha \neq 0$, защото $\alpha_1, \ldots, \alpha_n$ е базис на E над $\mathbb{Q}$ и поне един от коефициентите x_j е различен от 0. Сега от (10) получаваме $\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha_i \alpha) = 0$ за $i = 1, \ldots, n$, откъдето, поради линейността на следата над $\mathbb{Q}$ следва, че $\mathrm{tr}_{\mathbb{Q}}^{E}(\beta\alpha) = 0$ за всяко $\beta \in E$. В частност, $\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha^{-1}\alpha) = 0$, което е невъзможно, защото $\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha^{-1}\alpha) = \mathrm{tr}_{\mathbb{Q}}^{E}(1) = n$. Следователно $\Delta_E(\alpha_1, \ldots, \alpha_n) \neq 0$. □

Лема 7.2. *Нека $\alpha_1, \ldots, \alpha_n$ е базис на E над $\mathbb{Q}$. Тогава*

$$\Delta_E(\beta_1, \ldots, \beta_n) = \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_n) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{vmatrix}^2, \tag{11}$$

където $\sigma_1, \ldots, \sigma_n$ са всички изоморфизми на E в $\mathbb{Q}$.

Доказателство. Нека $G = (\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha_i \alpha_j)) \in M_n(\mathbb{Q})$. Тъй като (виж формула (8))

$$\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j),$$

то е в сила равенството на матрици

$$G = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_n) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \ldots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \ldots & \sigma_n(\alpha_2) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \ldots & \sigma_n(\alpha_n) \end{pmatrix},$$

откъдето следва формула (11). □

Твърдение 7.3. *Нека $E = \mathbb{Q}[\alpha]$, където $\alpha \in \mathbb{C}$ е алгебрично число с минимален полином $f = x^n + a_1 x^n + \cdots + a_n \in \mathbb{Q}[x]$. Тогава $\Delta_E(1, \alpha, \ldots, \alpha^{n-1}) = D$, където D е дискриминантата на полинома f.*

Доказателство. Нека $\sigma_1, \ldots, \sigma_n$ са всички изоморфизми на E в $\mathbb{Q}$. Тогава $\sigma_1(\alpha) = \alpha_1, \ldots, \sigma_n(\alpha) = \alpha_n$ са всички корени на полинома f. Да означим с $W(\alpha_1, \ldots, \alpha_n)$ детерминантата на Вандермонд на числата $\alpha_1, \ldots, \alpha_n$. Използвайки формула (11) получаваме

$$\Delta_E(1, \alpha, \ldots, \alpha^{n-1}) =$$

$$= \begin{vmatrix} \sigma_1(1) & \sigma_1(\alpha) & \ldots & \sigma_1(\alpha^{n-1}) \\ \sigma_2(1) & \sigma_2(\alpha) & \ldots & \sigma_2(\alpha^{n-1}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \sigma_n(1) & \sigma_n(\alpha) & \ldots & \sigma_n(\alpha^{n-1}) \end{vmatrix}^2 = \begin{vmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \ldots & \alpha_2^{n-1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ 1 & \alpha_n & \ldots & \alpha_n^{n-1} \end{vmatrix}^2 =$$

$$= W(\alpha_1, \ldots, \alpha_n)^2 = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = D,$$

което трябваше да се докаже. □

Нека $\alpha_1, \ldots, \alpha_n$ и $\beta_1, \ldots, \beta_n$ са два базиса на E над $\mathbb{Q}$ и нека $T = (t_{ij}) \in M_n(\mathbb{Q})$ е матрицата на преход от базиса $\alpha_1, \ldots, \alpha_n$ към базиса $\beta_1, \ldots, \beta_n$:

$$\beta_j = \sum_{i=1}^{n} t_{ij} \alpha_i, \quad j = 1, \ldots, n.$$

Нека $G = (\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha_i\alpha_j)) \in M_n(\mathbb{Q})$ и $G' = (\mathrm{tr}_{\mathbb{Q}}^{E}(\beta_i\beta_j)) \in M_n(\mathbb{Q})$. Тогава според "Записки по алгебра - линейна алгебра", параграф 25, Твърдение 2 е в сила

$$G' = T^t G T,$$

откъдето

$$\det G' = (\det T)^2 \det G.$$

Горната формула показва как се променя дискриминантата при смяна на базиса на E над $\mathbb{Q}$:

Твърдение 7.4. *Нека $\alpha_1, \ldots, \alpha_n$ и $\beta_1, \ldots, \beta_n$ са два базиса на E над $\mathbb{Q}$. Тогава*

$$\Delta_E(\beta_1, \ldots, \beta_n) = (\det T)^2 \Delta_E(\alpha_1, \ldots, \alpha_n),$$

където T е матрицата на преход от базиса $\alpha_1, \ldots, \alpha_n$ към базиса $\beta_1, \ldots, \beta_n$.

Нека A е пръстенът на целите алгебрични числа в крайното разширение E на полето на рационалните числа $\mathbb{Q}$. Ще покажем, че всеки идеал $I \neq (0)$ в A е свободна абелева група от ранг $[E : \mathbb{Q}]$. Първо да забележим, че за всяко алгебрично число $x \in E$ съществува цяло число $m \neq 0$, такова че $mx \in I$. Наистина, нека $0 \neq a \in I$ — тогава $x = (x/a)a$, където $x/a \in E$. Нека $m \neq 0$ е цяло число, такова че $m(x/a) \in A$ (виж Лема 4.1). Тогава $mx = [m(x/a)]a \in I$. Ако $\alpha_1, \ldots, \alpha_n$ е базис на E над $\mathbb{Q}$, то $m_1\alpha_1, \ldots, m_n\alpha_n \in I$ за подходящи цели числа $m_1 \neq 0, \ldots, m_n \neq 0$. Ние доказахме следната лема:

Лема 7.5. *Всеки идеал $I \neq (0)$ в A съдържа базис на E над $\mathbb{Q}$.*

Да забележим, че дискриминантата на всеки базис $\alpha_1, \ldots, \alpha_n$ на E над $\mathbb{Q}$, който се съдържа в идеала I, е цяло число, защото матрицата $G = (\mathrm{tr}_{\mathbb{Q}}^{E}(\alpha_i\alpha_j))$ се състои от цели числа. Следователно съществува базис $\alpha_1, \ldots, \alpha_n \in I$ на E над $\mathbb{Q}$ с минимална абсолютна стойност на дискриминантата:

$$|\Delta_E(\alpha_1, \ldots, \alpha_n)| \leq |\Delta_E(\beta_1, \ldots, \beta_n)|$$

за всеки базис $\beta_1, \ldots, \beta_n$ на E над $\mathbb{Q}$, такъв че $\beta_1, \ldots, \beta_n \in I$.

Твърдение 7.6. *Нека $\alpha_1, \ldots, \alpha_n \in I$ е базис на E над $\mathbb{Q}$ с минимална абсолютна стойност на дискриминантата $\Delta_E(\alpha_1, \ldots, \alpha_n)$. Тогава $\alpha_1, \ldots, \alpha_n$ е базис на I над пръстена на целите числа $\mathbb{Z}$, т. е. за всяко число $\alpha \in I$ съществуват единствени цели числа $m_1, \ldots, m_n$, такива че*

$$\alpha = m_1\alpha_1 + \cdots + m_n\alpha_n.$$

Доказателство. Тъй като $\alpha_1, \ldots, \alpha_n$ е базис на E над $\mathbb{Q}$, то всяко число $x \in I$ има единствено представяне

$$\alpha = m_1\alpha_1 + \cdots + m_n\alpha_n,$$

където $m_1, \ldots, m_n$ са рационални числа. Да предположим, че някое от числата $m_1, \ldots, m_n$ не е цяло — без ограничение на общността можем да предположим, че $m_1 \notin \mathbb{Z}$. Тогава $m_1 = n_1 + \theta$, където $n_1 \in \mathbb{Z}$, а $0 < \theta < 1$, откъдето

$$\alpha - n_1\alpha_1 = \theta\alpha_1 + m_2\alpha_2 + \cdots + m_n\alpha_n.$$

Нека $\beta_1 = \alpha - n_1\alpha_1, \beta_2 = \alpha_2, \ldots, \beta_n = \alpha_n$. Тогава $\beta_1, \ldots, \beta_n \in I$ е базис на E над $\mathbb{Q}$ и матрицата на преход T от базиса $\alpha_1, \ldots, \alpha_n$ към базиса $\beta_1, \ldots, \beta_n$ е

$$T = \begin{pmatrix} \theta & 0 & \ldots & 0 \\ m_2 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ m_n & 0 & \ldots & 1 \end{pmatrix}.$$

Сега, прилагайки Твърдение 7.4, получаваме

$$|\Delta_E(\beta_1,\ldots,\beta_n)| = \theta^2|\Delta_E(\alpha_1,\ldots,\alpha_n)| < |\Delta_E(\alpha_1,\ldots,\alpha_n)|,$$

което противоречи на избора на базиса $\alpha_1,\ldots,\alpha_n \in I$. Следователно $m_1,\ldots,m_n$ са цели числа и $\alpha_1,\ldots,\alpha_n \in I$ е базис на I над $\mathbb{Z}$. □

Нека $\alpha_1,\ldots,\alpha_n$ и $\beta_1,\ldots,\beta_n$ са два базиса на идеала $I \neq (0)$ над пръстена на целите числа $\mathbb{Z}$ и нека $T \in M_n(\mathbb{Z})$ е матрицата на преход от $\alpha_1,\ldots,\alpha_n$ към $\beta_1,\ldots,\beta_n$. Тогава $T^{-1} \in M_n(\mathbb{Z})$ е матрицата на преход от $\beta_1,\ldots,\beta_n$ към $\alpha_1,\ldots,\alpha_n$ и от $\det(T)\det(T^{-1}) = 1$, следва че $\det T = \pm 1$.

Твърдение 7.7. *Нека $\alpha_1,\ldots,\alpha_n$ и $\beta_1,\ldots,\beta_n$ са два базиса на идеала $I \neq (0)$ над пръстена на целите числа $\mathbb{Z}$. Тогава*

$$\Delta_E(\beta_1,\ldots,\beta_n) = \Delta_E(\alpha_1,\ldots,\alpha_n).$$

Доказателство. Следва от равенството

$$\Delta_E(\beta_1,\ldots,\beta_n) = (\det T)^2\Delta_E(\alpha_1,\ldots,\alpha_n).$$

Дефиниция (Дискриминанта на идеал). Нека $I \neq (0)$ е идеал в A и нека $\alpha_1,\ldots,\alpha_n \in I$ е базис на I над $\mathbb{Z}$. Цялото число $\Delta_E(\alpha_1,\ldots,\alpha_n)$ се нарича *дискриминанта на I* и се означава с $\Delta_E(I)$.