Норма на идеал. Геометричен метод

12. Норма на идеал

Нека A е пръстенът на целите алгебрични числа в крайно разширение E на полето на рационалните числа и нека $(0) \neq I \subseteq A$ е идеал в A. Тогава I и A са свободни абелеви група от ранг $n = [E : \mathbb{Q}]$, откъдето $(A : I) = |A/I| < \infty$ (виж Лема 8.1 и Твърдение 7.6).

Дефиниция 12.1 (Норма на идеал). Естественото число $(A : I) = |A/I|$ се нарича *норма* на идеала I, и се означава с $\mathrm{N}(I)$.

Лема 12.1. *Нека $(0) \neq I \subseteq A$ и $(0) \neq J \subseteq A$ са идеали в A. Тогава*

$$\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J).$$

Доказателство. Трябва да покажем, че $|A/(IJ)| = |A/I||A/J|$.
Нека $I = P_1^{e_1} \cdots P_s^{e_s}$, където $P_1, \ldots, P_s$ са два по два различни прости идеали в A и $e_1 \geq 0, \ldots, e_s \geq 0$. Тогава $A/I \cong A/P_1^{e_1} \times \cdots \times P_s^{e_s}$ (според китайската теорема за остатъците), откъдето следва, че $|A/I| = |A/P_1^{e_1}| \cdots |A/P_s^{e_s}|$. Нека $P_1 \cap \mathbb{Z} = (p_1), \ldots, P_s \cap \mathbb{Z} = (p_s)$, където $p_1, \ldots, p_s$ са прости числа в $\mathbb{Z}$, и нека $f_1, \ldots, f_s$ са степените на разклонение на простите идеали $P_1, \ldots, P_s$. Според Лема 11.3 са в сила равенствата $|A/P_1^{e_1}| = p_1^{e_1 f_1}, \ldots, |A/P_1^{e_1}| = p_s^{e_s f_s}$, откъдето

$$|A/I| = p_1^{e_1 f_1} \cdots p_s^{e_s f_s}.$$

Аналогично, нека $J = P_1^{d_1} \cdots P_s^{d_s}$, където $d_1 \geq 0, \ldots, d_s \geq 0$; както по-горе установяваме, че

$$|A/J| = p_1^{d_1 f_1} \cdots p_s^{d_s f_s}.$$

Тъй като $IJ = P_1^{e_1+d_1} \cdots P_s^{e_s+d_s}$, то

$$|A/(IJ)| = p_1^{(e_1+d_1)f_1} \cdots p_s^{(e_s+d_s)f_s} = (p_1^{e_1 f_1} \cdots p_s^{e_s f_s})(p_1^{d_1 f_1} \cdots p_s^{d_s f_s}) = |A/I||A/J|,$$

което трябваше да се докаже. □

Лема 12.2. *Нека G е свободна абелева група от краен ранг и H е подгрупа на G, такава че $\mathrm{rk}\, H = \mathrm{rk}\, G$. Нека $e_1, e_2, \ldots, e_n$ е базис на G, $f_1, f_2, \ldots, f_n$ е базис на H и нека $T \in M_n(\mathbb{Z})$ е матрицата на преход от базиса $e_1, e_2, \ldots, e_n$ на G към базиса $f_1, f_2, \ldots, f_n$ на H. Тогава $(G : H) = |\det T|$.*

Доказателство. Според основната теорема за крайнопородени абелеви групи съществуват базис $g_1, g_2, \ldots, g_n$ на G и естествени числа $m_1, m_2, \ldots, m_n$, такива че елементите $h_1 = m_1 g_1, h_2 = m_2 g_2, \ldots, h_n = m_n g_n$ са базис на H. Следователно $G/H \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$ и $(G : H) = |G/H| = m_1 m_2 \cdots m_n$.
Нека $R \in M_n(\mathbb{Z})$ е матрицата на преход от $e_1, e_2, \ldots, e_n$ към $g_1, g_2, \ldots, g_n$ и $S \in M_n(\mathbb{Z})$ е матрицата на преход от $h_1, h_2, \ldots, h_n$ към $f_1, f_2, \ldots, f_n$. Тогава

$$T = R \begin{pmatrix} m_1 & 0 & \ldots & 0 \\ 0 & m_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & m_n \end{pmatrix} S$$

и $\det T = \det R\,(m_1 m_2 \cdots m_n) \det S$. Тъй като $\det R = \pm 1$ и $\det S = \pm 1$, то $|\det T| = m_1 m_2 \cdots m_n = (G : H)$, което трябваше да се докаже. $\square$

Прилагайки горната лема към произволен идеал $(0) \neq I \subseteq A$ в пръстена A, получаваме следното твърдение:

Твърдение 12.3. *Нека $(0) \neq I \subseteq A$ е идеал в в пръстена A. Тогава*

$$\mathrm{N}(I) = |\det(T)|,$$

където $T \in M_n(\mathbb{Z})$ е матрицата на преход от някой базис $\alpha_1, \alpha_2, \ldots, \alpha_n$ на пръстена A към някой базис $\beta_1, \beta_2, \ldots, \beta_n$ на идеала I.

За да определим норма на дробен идеал, да забележим, че всеки дробен идеал $I \in \mathrm{Div}(A)$ на A е свободна абелева група от ранг $n = [E : \mathbb{Q}]$. Наистина, тъй като $aI \subseteq A$ за някое $0 \neq a \in A$ (виж Дефиниция 9.1), то идеалът aI в A има базис $\gamma_1, \gamma_2, \ldots, \gamma_n$ над $\mathbb{Z}$; тогава числата $\beta_1 = a^{-1}\gamma_1, \beta_2 = a^{-1}\gamma_2, \ldots, \beta_n = a^{-1}\gamma_n$ са базис на I на $\mathbb{Z}$. Нека $\alpha_1, \alpha_2, \ldots, \alpha_n$ е базис на пръстена A и $\beta_1, \beta_2, \ldots, \beta_n$ е базис на дробния идеал I. Тъй като $\alpha_1, \alpha_2, \ldots, \alpha_n$ и $\beta_1, \beta_2, \ldots, \beta_n$ са също така базиси на полето E над $\mathbb{Q}$, матрицата на преход T от базиса $\alpha_1, \alpha_2, \ldots, \alpha_n$ към базиса $\beta_1, \beta_2, \ldots, \beta_n$ има рационални коефициенти и $\det T \in \mathbb{Q}$. Нека $\alpha'_1, \alpha'_2, \ldots, \alpha'_n$ (съотв. $\beta'_1, \beta'_2, \ldots, \beta'_n$) са други базиси на пръстена A (съотв. идеала I) и нека $T' \in M_n(\mathbb{Q})$ е матрицата на преход от базиса $\alpha'_1, \alpha'_2, \ldots, \alpha'_n$ към базиса $\beta'_1, \beta'_2, \ldots, \beta'_n$. Тогава $T' = R^{-1}TS$, където $R \in M_n(\mathbb{Z})$ е матрицата на преход от $\alpha_1, \alpha_2, \ldots, \alpha_n$ към $\alpha'_1, \alpha'_2, \ldots, \alpha'_n$, а $S \in M_n(\mathbb{Z})$ е матрицата на преход от $\beta_1, \beta_2, \ldots, \beta_n$ към $\beta'_1, \beta'_2, \ldots, \beta'_n$. Тъй като $\det R = \pm 1$ и $\det S = \pm 1$, то $\det T' = \pm \det T$. Следователно абсолютната стойност на детерминантата на матрицата на преход от базис на пръстена A към базис на дробния идеал I не зависи от избора на тези базиси, което ни позволява да дадем следната дефиниция на норма на дробен идеал на пръстена A:

Дефиниция 12.2 (Норма на дробен идеал). Нека $I \in \mathrm{Div}(A)$ е дробен идеал на пръстена A и нека $T \in M_n(\mathbb{Q})$ е матрицата на преход от някой базис на A към някой базис на I. Положителното рационално число $|\det T|$ се нарича *норма* на дробния идеал I и се означава с $\mathrm{N}(I)$.

Твърдение 12.3 показва, че Дефиниция 12.1 и Дефиниция 12.2 са съвместими за всеки идеал $(0) \neq I \subseteq A$ в A.

За всяко алгебрично число $0 \neq \alpha \in E$ ще означаваме с (α) (или с $A\alpha$) главния дробен идеал, породен от числото α в полето E:

$$(\alpha) = \alpha A = \{\alpha a \,:\, a \in A\}.$$

За всеки дробен идеал I на A и всяко алгебрично число $0 \neq \alpha \in E$ ще означаваме с αI произведението $(\alpha)I$ на дробните идеали (α) и I:

$$\alpha I = \{\alpha x \,:\, x \in I\}.$$

Твърдение 12.4. *Нека $0 \neq \alpha \in E$ и нека $I \in \mathrm{Div}(A)$ е дробен идеал на пръстена A. Тогава*

$$\mathrm{N}(\alpha I) = |\mathrm{N}(\alpha)|\,\mathrm{N}(I). \tag{12}$$

В частност, $\mathrm{N}(\alpha A) = |\mathrm{N}(\alpha)|$.

Доказателство. Нека $\alpha_1, \alpha_2, \ldots, \alpha_n$ е базис на пръстена A, $\beta_1, \beta_2, \ldots, \beta_n$ е базис на идеала I и нека $T \in M_n(\mathbb{Q})$ е матрицата на преход от базиса $\alpha_1, \alpha_2, \ldots, \alpha_n$ към базиса $\beta_1, \beta_2, \ldots, \beta_n$.
Нека $\varphi_\alpha : E \to E$ е линейният оператор, зададен с формулата $\varphi_\alpha(x) = \alpha x$, $x \in E$. Тогава нормата $\mathrm{N}(\alpha)$ на α е равна на детерминантата на матрицата на

φ_α в някой/всеки базис на E над $\mathbb{Q}$ (Дефиниция 6.1). Сега да забележим, че матрицата $C \in M_n(\mathbb{Q})$ на оператора в базиса $\beta_1, \beta_2, \ldots, \beta_n$ съвпада с матрицата на преход от базиса $\beta_1, \beta_2, \ldots, \beta_n$ на I към базиса $\alpha\beta_1, \alpha\beta_2, \ldots, \alpha\beta_n$ на αI. Следователно матрицата на преход от базиса $\alpha_1, \alpha_2, \ldots, \alpha_n$ на A към базиса към базиса $\alpha\beta_1, \alpha\beta_2, \ldots, \alpha\beta_n$ на αI съвпада с матрицата CT, откъдето

$$\mathrm{N}(\alpha I) = |\det(CT)| = |\det C||\det T| = |\mathrm{N}(\alpha)|\,\mathrm{N}(I).$$

За $I = A$, $\mathrm{N}(\alpha A) = |\mathrm{N}(\alpha)|\mathrm{N}(A) = |\mathrm{N}(\alpha)|$, защото $\mathrm{N}(A) = 1$. □

Твърдение 12.5 (Мултипликативност на нормата). *Нека $I, J \in \mathrm{Div}(A)$ са дробни идеали на A. Тогава*

$$\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J).$$

Доказателство. Нека числата $0 \neq \alpha \in A$, $0 \neq \beta \in A$ са такива, че $\alpha I \subseteq A$ и $\beta J \subseteq A$. Тогава $\mathrm{N}((\alpha I)(\beta J)) = \mathrm{N}(\alpha I)\mathrm{N}(\beta J)$ (Лема 12.1). Сега от равенство (12) получаваме

$$|\mathrm{N}(\alpha\beta)|\,\mathrm{N}(IJ) = |\mathrm{N}(\alpha)||\mathrm{N}(\beta)|\,\mathrm{N}(I)\mathrm{N}(J),$$

откъдето $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$, защото $|\mathrm{N}(\alpha\beta)| = |\mathrm{N}(\alpha)||\mathrm{N}(\beta)| \neq 0$. □

Последното твърдение показва, че изображението $\mathrm{Div}(A) \ni I \mapsto \mathrm{N}(I) \in \mathbb{Q}^+$ е хомоморфизъм от групата $\mathrm{Div}(A)$ в групата на положителните рационални числа $\mathbb{Q}^+$; в частност $\mathrm{N}(I^{-1}) = \mathrm{N}(I)^{-1}$ за всеки $I \in \mathrm{Div}(A)$.

13. Геометрично представяне на алгебричните числа

13.1. Влагания в полето на комплексните числа. Нека $\sigma : E \to \mathbb{C}$ е влагане (инективен хомоморфизъм) на полето E в полето на комплексните числа. Тогава изображението $\overline{\sigma} : E \to \mathbb{C}$, зададено с $\overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}$, $\alpha \in E$, също е влагане на E в $\mathbb{C}$. Ще казваме, че σ е *реално* влагане на полето E, когато $\sigma = \overline{\sigma}$; в противен случай (т. е. когато $\sigma \neq \overline{\sigma}$) ще наричаме σ *комплексно* влагане на полето E. Ясно е, че σ е реално влагане точно когато $\sigma(E) \subset \mathbb{R}$. Ясно е също, че броят на различните комплексни влагания на E в $\mathbb{C}$ е четно число.
От теорията на полетата е известно, че едно крайно разширение E от степен n на полето на рационалните числа $\mathbb{Q}$ има точно n различни влагания $\sigma_1, \ldots, \sigma_n$ в полето на комплексните числа $\mathbb{C}$. Нека E има s реални влагания $\sigma_1, \ldots, \sigma_s$ и $2t$ комплексни влагания $\sigma_{s+1}, \overline{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \overline{\sigma}_{s+t}$ ($s + 2t = n$). Да определим изображение x от E в n-мерното реално линейно пространство $L^{s,t} = \mathbb{R}^s \times \mathbb{C}^t$ по следния начин

$$x(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha);\, \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha)), \qquad \alpha \in E.$$

Тогава $x(\alpha + \beta) = x(\alpha) + x(\beta)$ и $x(r\alpha) = rx(\alpha)$ за всички $\alpha, \beta \in E$ и всяко рационално число $r \in \mathbb{Q}$. Следователно x е линейно изображение на линейни пространства над полето на рационалните числа $\mathbb{Q}$. Тъй като влаганията $\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \ldots, \sigma_{s+t}$ са инективни изображения, то x също е инективно изображение.
За всяко $x = (x_1, \ldots, x_s;\, x_{s+1}, \ldots, x_{s+t}) \in L^{s,t}$ нека

$$\mathrm{N}(x) = x_1 \cdots x_s\, |x_{s+1}|^2 \cdots |x_{s+t}|^2.$$

Тогава за всяко $\alpha \in E$ е в сила равенството

$$\begin{aligned}\mathrm{N}(x(\alpha)) &= \sigma_1(\alpha) \cdots \sigma_s(\alpha)\, |\sigma_{s+1}(\alpha)|^2 \cdots |\sigma_{s+t}(\alpha)|^2 = \\ &= \sigma_1(\alpha) \cdots \sigma_s(\alpha)\, \sigma_{s+1}(\alpha)\overline{\sigma}_{s+1}(\alpha) \cdots \sigma_{s+t}(\alpha)\overline{\sigma}_{s+t}(\alpha) = \mathrm{N}(\alpha).\end{aligned}$$

Всеки вектор $x = (x_1, \ldots, x_s;\, x_{s+1}, \ldots, x_{s+t}) \in L^{s,t}$ има единствено представяне

$$\begin{aligned} x &= (x_1, \ldots, x_s;\, y_{s+1} + iz_{s+1}, \ldots, y_{s+t} + iz_{s+t}) = \\ &= x_1(1, \ldots, 0;\, 0, \ldots, 0) + \cdots + x_s(0, \ldots, 1;\, 0, \ldots, 0) + \\ &\quad + y_{s+1}(0, \ldots, 0;\, 1, \ldots, 0) + z_{s+1}(0, \ldots, 0;\, i, \ldots, 0) + \\ &\quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\quad + y_{s+t}(0, \ldots, 0;\, 0, \ldots, 1) + z_{s+t}(0, \ldots, 0;\, 0, \ldots, i), \end{aligned}$$

където $x_1, \ldots, x_s, y_{s+1}, z_{s+1}, \ldots, y_{s+t}, z_{s+t}$ са реални числа. Следователно векторите

$$\begin{aligned} v_1 &= (1, \ldots, 0;\, 0, \ldots, 0), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ v_s &= (0, \ldots, 1;\, 0, \ldots, 0), \\ v_{s+1} &= (0, \ldots, 0;\, 1, \ldots, 0), \\ v_{s+2} &= (0, \ldots, 0;\, i, \ldots, 0), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ v_{n-1} &= (0, \ldots, 0;\, 0, \ldots, 1), \\ v_n &= (0, \ldots, 0;\, 0, \ldots, i) \end{aligned} \tag{13}$$

са базис на линейното пространство $L^{s,t}$ над полето на реалните числа.

Твърдение 13.1. *Нека $\alpha_1, \ldots, \alpha_n$ е базис на E над $\mathbb{Q}$. Тогава:*

(а) *$x(\alpha_1), \ldots, x(\alpha_n)$ е базис на $L^{s,t}$ над полето на реалните числа;*
(б) *обемът на паралелепипеда със страни векторите $x(\alpha_1), \ldots, x(\alpha_n)$ е равен на $2^{-t}\sqrt{|\Delta(\alpha_1, \ldots, \alpha_n)|}$, където $\Delta(\alpha_1, \ldots, \alpha_n)$ е дискриминантата на базиса $\alpha_1, \ldots, \alpha_n$.*

Доказателство. Ясно е, че (б) влече (а). Нека

$$\begin{aligned} x(\alpha_l) &= (\sigma_1(\alpha_l), \ldots, \sigma_s(\alpha_l);\, \sigma_{s+1}(\alpha_l), \ldots, \sigma_{s+t}(\alpha_l)) = \\ &= (x_1^l, \ldots, x_s^l;\, y_{s+1}^l + iz_{s+1}^l, \ldots, y_{s+t}^l + iz_{s+t}^l) \end{aligned}$$

за $l = 1, \ldots, n$. Тогава векторът $x(\alpha_l)$ има координати

$$(x_1^l, \ldots, x_s^l, y_{s+1}^l, z_{s+1}^l, \ldots, y_{s+t}^l, z_{s+t}^l)$$

в базиса (13) на линейното пространство $L^{s,t}$ и обемът на паралелепипеда със страни векторите $x(\alpha_1), \ldots, x(\alpha_n)$ е равен на абсолютната стойност на детерминантата

$$V = \begin{vmatrix} x_1^1 & \ldots & x_s^1 & y_{s+1}^1 & z_{s+1}^1 & \ldots & y_{s+t}^1 & z_{s+t}^1 \\ x_1^2 & \ldots & x_s^2 & y_{s+1}^2 & z_{s+1}^2 & \ldots & y_{s+t}^2 & z_{s+t}^2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ x_1^n & \ldots & x_s^n & y_{s+1}^n & z_{s+1}^n & \ldots & y_{s+t}^n & z_{s+t}^n \end{vmatrix}.$$

Да сравним V с детерминантата

$$V^* = \begin{vmatrix} x_1^1 & \ldots & x_s^1 & y_{s+1}^1 + iz_{s+1}^1 & y_{s+1}^1 - iz_{s+1}^1 & \ldots & y_{s+t}^1 + iz_{s+t}^1 & y_{s+t}^1 - iz_{s+t}^1 \\ x_1^2 & \ldots & x_s^2 & y_{s+1}^2 + iz_{s+1}^2 & y_{s+1}^2 - iz_{s+1}^2 & \ldots & y_{s+t}^2 + iz_{s+t}^2 & y_{s+t}^2 - iz_{s+t}^2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ x_1^n & \ldots & x_s^n & y_{s+1}^n + iz_{s+1}^n & y_{s+1}^n - iz_{s+1}^n & \ldots & y_{s+t}^n + iz_{s+t}^n & y_{s+t}^n - iz_{s+t}^n \end{vmatrix}.$$

Изваждайки от стълбовете с номера $s+2, s+4, \ldots, s+2t$ предишните стълбове, получаваме

$$V^* = (-2i)^t \begin{vmatrix} x_1^1 & \ldots & x_s^1 & y_{s+1}^1 + iz_{s+1}^1 & z_{s+1}^1 & \ldots & y_{s+t}^1 + iz_{s+t}^1 & z_{s+t}^1 \\ x_1^2 & \ldots & x_s^2 & y_{s+1}^2 + iz_{s+1}^2 & z_{s+1}^2 & \ldots & y_{s+t}^2 + iz_{s+t}^2 & z_{s+t}^2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ x_1^n & \ldots & x_s^n & y_{s+1}^n + iz_{s+1}^n & z_{s+1}^n & \ldots & y_{s+t}^n + iz_{s+t}^n & z_{s+t}^n \end{vmatrix}.$$

Прибавяйки стълбовете с номера $s+2, s+4, \ldots, s+2t$, умножени с $-i$, към предишните стълбове, получаваме $V^* = (-2i)^t V$, откъдето $V = i^t 2^{-t} V^*$. Тъй като според Лема 7.2 е в сила равенството $(V^*)^2 = \Delta(\alpha_1, \ldots, \alpha_n)$, то

$$|V| = 2^{-t}|V^*| = 2^{-t}\sqrt{|\Delta(\alpha_1, \ldots, \alpha_n)|},$$

което трябваше да се докаже. □

13.2. Решетки в $\mathbb{R}^n$. Лема на Минковски. Ще разглеждаме линейното пространство $\mathbb{R}^n$ като абелева група относно събирането на вектори.
Ако X е (измеримо) тяло в $\mathbb{R}^n$, ще означаваме обема на X с $v(X)$.

Дефиниция 13.1 (Решетка в $\mathbb{R}^n$). Всяка крайнопородена подгрупа Λ на $\mathbb{R}^n$ се нарича *решетка* в $\mathbb{R}^n$.

Ако Λ е решетка в $\mathbb{R}^n$, то Λ притежава базис над $\mathbb{Z}$: съществуват линейно независими вектори $\lambda_1, \ldots, \lambda_k \in \Lambda$, такива че всеки вектор $\lambda \in \Lambda$ има единствено представяне

$$\lambda = m_1\lambda_1 + \cdots + m_k\lambda_k,$$

където $m_1, \ldots, m_k$ са цели числа. Всеки два базиса на Λ съдържат еднакъв брой вектори; броят на векторите във всеки базис на Λ се нарича *ранг* на Λ и се означава с $\operatorname{rk}\Lambda$. Ясно е, че $\operatorname{rk}\Lambda \leq n$ за всяка решетка Λ в $\mathbb{R}^n$.
Нека $\lambda_1, \ldots, \lambda_k$ и $\lambda'_1, \ldots, \lambda'_k$ са два базиса на решетката Λ. Нека T е матрицата на преход от базиса $\lambda_1, \ldots, \lambda_k$ към базиса $\lambda'_1, \ldots, \lambda'_k$ и нека T' е матрицата на преход от базиса $\lambda'_1, \ldots, \lambda'_k$ към базиса $\lambda_1, \ldots, \lambda_k$. Тогава елементите на матриците T и T' са цели числа и $TT' = T'T = E_k$. Следователно $(\det T)(\det T') = 1$, откъдето $\det T = \pm 1$ и $\det T' = \pm 1$. Ние доказахме следната лема:

Лема 13.2. *Ако T е матрицата на преход от един базис на Λ към друг базис на Λ, то $|\det T| = 1$.*

Нека Λ е решетка от ранг n в $\mathbb{R}^n$; тогава всеки базис на Λ над $\mathbb{Z}$ е базис на $\mathbb{R}^n$. За всеки базис $\lambda_1, \ldots, \lambda_n$ на решетката Λ, множеството

$$\mathcal{D} = \{x_1\lambda_1 + \cdots + x_n\lambda_n : 0 \leq x_1 < 1, \ldots, 0 \leq x_n < 1\}$$

се нарича *фундаментална област* на решетката Λ. Ясно е, че фундаменталната област е паралелепипед със страни векторите $\lambda_1, \ldots, \lambda_n$.
Нека $\lambda_1, \ldots, \lambda_n$ и $\lambda'_1, \ldots, \lambda'_n$ са два базиса на решетката Λ от ранг n. Да означим с D (съотв. D') обема на фундаменталната област, съответстваща на базиса $\lambda_1, \ldots, \lambda_n$ (съотв. $\lambda'_1, \ldots, \lambda'_k$). Тогава $D' = D\,|\det T|$, където T е матрицата на преход от базиса $\lambda_1, \ldots, \lambda_k$ към базиса $\lambda'_1, \ldots, \lambda'_k$. Тъй като $|\det T| = 1$ според Лема 13.2, то $D = D'$. Следователно всеки две фундаментални области на решетката Λ имат еднакъв обем.
Нека $\mathcal{D}$ е фундаментална област на решетка Λ от ранг n и нека $\mathcal{D}_\lambda$ е множеството $\lambda + \mathcal{D}$, $\lambda \in \Lambda$:

$$\mathcal{D}_\lambda = \{\lambda + x : x \in \mathcal{D}\}, \quad \lambda \in \Lambda.$$

Множествата $\mathcal{D}_\lambda$ притежават следните две свойства:

(а) $\mathcal{D}_{\lambda_1} \cap \mathcal{D}_{\lambda_2} = \emptyset$, когато $\lambda_1 \neq \lambda_2$;
(б) $\bigcup\limits_{\lambda\in\Lambda} \mathcal{D}_\lambda = \mathbb{R}^n$.

Нека X е тяло в $\mathbb{R}^n$ и нека $X_\lambda = X \cap \mathcal{D}_\lambda$, $\lambda \in \Lambda$. Тогава $X = \bigcup\limits_{\lambda\in\Lambda} X_\lambda$, като $X_{\lambda_1} \cap X_{\lambda_2} = \emptyset$ за $\lambda_1 \neq \lambda_2$. Следователно

$$v(X) = \sum_{\lambda\in\Lambda} v(X_\lambda). \tag{14}$$

Да забележим, че за всяко $\lambda \in \Lambda$ множеството $-\lambda + X_\lambda$ се съдържа във фундаменталната област $\mathcal{D}$, защото $X_\lambda \subseteq \mathcal{D}_\lambda$ и $-\lambda + X_\lambda \subseteq -\lambda + \mathcal{D}_\lambda = \mathcal{D}$. Освен това $v(-\lambda + X_\lambda) = v(X_\lambda)$, защото множеството $-\lambda + X_\lambda$ се получава от множеството X_λ чрез транслация.

Лема 13.3. *Нека Λ е решетка в $\mathbb{R}^n$ от ранг n и нека X е тяло в $\mathbb{R}^n$, такова че $v(X) > D$, където D е обемът на фундаменталната област на Λ. Тогава съществуват вектори $\lambda_1, \lambda_2 \in \Lambda$, $\lambda_1 \neq \lambda_2$, такива че $(\lambda_1 + X) \cap (\lambda_2 + X) \neq \emptyset$.*

Доказателство. Да разгледаме множествата $-\lambda + X_\lambda$, $\lambda \in \Lambda$. От равенство (14) следва, че сумата от обемите на тези множества е равна на обема $v(X)$ на X. Тъй като тези множества се съдържат във фундаменталната област $\mathcal{D}$ и тъй като $v(X) > v(\mathcal{D})$, някои две от тях имат обща точка. Следователно съществуват вектори $\lambda_1, \lambda_2 \in \Lambda$, $\lambda_1 \neq \lambda_2$, такива че $(-\lambda_1 + X_{\lambda_1}) \cap (-\lambda_2 + X_{\lambda_2}) \neq \emptyset$. Тъй като $-\lambda_1 + X_{\lambda_1} \subseteq -\lambda_1 + X$ и $-\lambda_2 + X_{\lambda_2} \subseteq -\lambda_2 + X$, то $(-\lambda_1 + X) \cap (-\lambda_2 + X) \neq \emptyset$. Лемата е доказана, защото $-\lambda_1, -\lambda_2 \in \Lambda$ и $-\lambda_1 \neq -\lambda_2$. □

Лема 13.4 (Минковски). *Нека Λ е решетка в $\mathbb{R}^n$ от ранг n и нека X е изпъкнало централно–симетрично тяло в $\mathbb{R}^n$. Тогава:*

(а) *ако $v(X) > 2^n D$, множеството X съдържа ненулева точка на решетката Λ;*

(б) *ако $v(X) \geq 2^n D$ и множеството X е компактно, то X съдържа ненулева точка на решетката Λ.*

Доказателство. (а) Нека $Y = \frac{1}{2}X$ е тялото, което се получава от X след хомотетия с коефициент $\frac{1}{2}$. Тогава $v(Y) = \frac{1}{2^n} v(X) > D$ и от предишната лема следва, че съществуват $\lambda_1, \lambda_2 \in \Lambda$, $\lambda_1 \neq \lambda_2$, такива че $(\lambda_1 + Y) \cap (\lambda_2 + Y) \neq \emptyset$. Следователно съществуват точки $x_1, x_2 \in X$, такива че

$$\frac{1}{2}x_1 + \lambda_1 = \frac{1}{2}x_2 + \lambda_2, \text{ откъдето } \frac{1}{2}x_1 + \frac{1}{2}(-x_2) = \lambda_2 - \lambda_1.$$

Тъй като тялото X е централно–симетрично, то $-x_2 \in X$, а тъй като тялото X е изпъкнало, то $\frac{1}{2}x_1 + \frac{1}{2}(-x_2) \in X$. Следователно X съдържа ненулевия вектор $\lambda_2 - \lambda_1$ от решетката Λ.

(б) За всяко естествено число n нека $X_n = (1 + \frac{1}{n})X$ е тялото, което се получава от X след хомотетия с коефициент $1 + \frac{1}{n}$; тогава множеството $\bigcap\limits_{n=1}^{\infty} X_n$ е затварянето $\overline{X}$ на X в $\mathbb{R}^n$ — следователно $X = \bigcap\limits_{n=1}^{\infty} X_n$. Тъй като за всяко n е в сила неравенството $v(X_n) > 2^n D$, никое от множествата $X_n \cap \Lambda \setminus \{0\}$, $n \geq 1$, не е празно; тъй като тези множества са крайни и намаляват монотонно, тяхното пресичане също не е празното множество. За да завършим доказателството, остава да забележим, че пресичането на множествата $X_n \cap \Lambda \setminus \{0\}$, $n \geq 1$, съвпада с $X \cap \Lambda \setminus \{0\}$. □

Както показва следващото твърдение, решетки се появяват естествено в теорията на алгебричните числа.

Твърдение 13.5. *Нека $I \in \mathrm{Div}(A)$ е дробен идеал на A. Тогава:*

(а) *множеството $x(I)$ е решетка от ранг n в $L^{s,t}$;*

(б) *обемът на фундаменталната област на решетката $x(I)$ е равен на $2^{-t}\sqrt{|\Delta|}\,\mathrm{N}(I)$, където Δ е дискриминантата на пръстена A.*

Доказателство. (а) Нека числата $\beta_1, \beta_2, \ldots, \beta_n$ са базис на идеала I над $\mathbb{Z}$. Тогава числата $\beta_1, \beta_2, \ldots, \beta_n$ са базис на E над $\mathbb{Q}$ и според Твърдение 13.1 (а) векторите $x(\beta_1), x(\beta_2), \ldots, x(\beta_n)$ са базис на линейното пространство $L^{s,t}$. Тъй като изображението $x : E \to L^{s,t}$ е хомоморфизъм на абелеви групи, множеството $x(I)$ се състои от всички целочислени линейни комбинации на векторите $x(\beta_1), x(\beta_2), \ldots, x(\beta_n)$, т. е. $x(I)$ е решетка от ранг n в $L^{s,t}$.

(б) Нека числата $\alpha_1, \alpha_2, \ldots, \alpha_n$ са базис на пръстена A над $\mathbb{Z}$ и нека T е матрицата на преход от базиса $\alpha_1, \alpha_2, \ldots, \alpha_n$ на A към базиса $\beta_1, \beta_2, \ldots, \beta_n$ на I. Тогава $x(\alpha_1), x(\alpha_2), \ldots, x(\alpha_n)$ и $x(\beta_1), x(\beta_2), \ldots, x(\beta_n)$ са базиси на $L^{s,t}$, като T е матрицата на преход от базиса $x(\alpha_1), x(\alpha_2), \ldots, x(\alpha_n)$ към базиса $x(\beta_1), x(\beta_2), \ldots, x(\beta_n)$, защото изображението $x : E \to L^{s,t}$ е $\mathbb{Q}$-линейно. Тъй като обемът на паралелепипеда със страни $x(\alpha_1), x(\alpha_2), \ldots, x(\alpha_n)$ е равен на $2^{-t}\sqrt{|\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|} = 2^{-t}\sqrt{|\Delta|}$, то обемът на паралелепипеда със страни $x(\beta_1), x(\beta_2), \ldots, x(\beta_n)$ е равен на $2^{-t}\sqrt{|\Delta|}\,|\det T| = 2^{-t}\sqrt{|\Delta|}\,\mathrm{N}(I)$, което трябваше да се докаже. □

13.3. Пресмятане на един обем.

Лема 13.6. *Нека M е положително реално число и $X \subset L^{s,t}$ е множеството, състоящо се от всички точки $(x_1, \ldots, x_s; x_{s+1}, \ldots, x_{s+t}) \in L^{s,t}$, такива че*

$$|x_1| + \cdots + |x_s| + 2|x_{s+1}| + \cdots + 2|x_{s+t}| \leq M.$$

Тогава

$$v(X) = 2^s \left(\frac{\pi}{2}\right)^t \frac{M^n}{n!}. \tag{15}$$

Доказателство. Ще докажем формулата за обема на X с индукция по s и t. Да означим тялото X с $X(s,t,M)$. Нека $x_{s+1} = y_{s+1} + iz_{s+1}, \ldots, x_{s+t} = y_{s+t} + iz_{s+t}$. Тогава

$$v(X) = \int_{X(s,t,M)} \mathrm{d}x_1 \cdots \mathrm{d}x_s \mathrm{d}y_{s+1} \mathrm{d}z_{s+1} \cdots \mathrm{d}y_{s+t} \mathrm{d}z_{s+t}.$$

(а) Индукция по s: Да предположим, че формулата е в сила за $s-1$. Тогава от неравенствата

$$-M \leq x_s \leq M,$$
$$|x_1| + \cdots + |x_{s-1}| + 2|x_{s+1}| + \cdots + 2|x_{s+t}| \leq M - |x_s|$$

следва, че

$$\begin{aligned} v(X) &= \int_{-M}^{M} \left(\int_{X(s-1,t,M-|x_s|)} \mathrm{d}x_1 \cdots \mathrm{d}x_{s-1} \mathrm{d}y_{s+1} \mathrm{d}z_{s+1} \cdots \mathrm{d}y_{s+t} \mathrm{d}z_{s+t} \right) \mathrm{d}x_s = \\ &= \int_{-M}^{M} 2^{s-1} \left(\frac{\pi}{2}\right)^t \frac{(M-|x_s|)^{n-1}}{(n-1)!}\,\mathrm{d}x_s = 2\int_{0}^{M} 2^{s-1} \left(\frac{\pi}{2}\right)^t \frac{(M-x_s)^{n-1}}{(n-1)!}\,\mathrm{d}x_s = \\ &= 2^s \left(\frac{\pi}{2}\right)^t \frac{M^n}{n!}. \end{aligned}$$

Следователно, ако формула (15) е в сила за $s-1$, то тя също е в сила за s.

(а) Индукция по t: Да предположим, че формулата е в сила за $t-1$. Тогава от неравенствата

$$2|x_{s+t}| = 2\sqrt{y_{s+t}^2 + z_{s+t}^2} \leq M,$$
$$|x_1| + \cdots + |x_s| + 2|x_{s+1}| + \cdots + 2|x_{s+t-1}| \leq M - 2|x_{s+t}|$$

следва, че

$$v(X) = \int_{2|x_{s+t}|\leq M} V(y_{s+t}, z_{s+t})\,\mathrm{d}y_{s+t}\mathrm{d}z_{s+t},$$

където

$$V(y_{s+t}, z_{s+t}) = \int_{X(s,t-1,M-2|x_{s+t}|)} \mathrm{d}x_1 \cdots \mathrm{d}x_s \mathrm{d}y_{s+1}\mathrm{d}z_{s+1} \cdots \mathrm{d}y_{s+t-1}\mathrm{d}z_{s+t-1} =$$
$$= 2^s \left(\frac{\pi}{2}\right)^{t-1} \frac{(M-2|x_{s+t}|)^{n-2}}{(n-2)!}.$$

Следователно

$$v(X) = \int_{2|x_{s+t}|\leq M} 2^s \left(\frac{\pi}{2}\right)^{t-1} \frac{(M-2|x_{s+t}|)^{n-2}}{(n-2)!}\,\mathrm{d}y_{s+t}\mathrm{d}z_{s+t}.$$

Преминавайки към полярни координати

$$y_{s+t} = r\cos\theta,\ z_{s+t} = r\sin\theta,\ |x_{s+t}| = r,\ \mathrm{d}y_{s+t}\mathrm{d}z_{s+t} = r\,\mathrm{d}r\mathrm{d}\theta,$$

получаваме

$$v(X) = \int_0^{2\pi} \left(\int_0^{\frac{M}{2}} 2^s \left(\frac{\pi}{2}\right)^{t-1} \frac{(M-2r)^{n-2}}{(n-2)!}\, r\,\mathrm{d}r \right) \mathrm{d}\theta =$$
$$= 2\pi \int_0^{\frac{M}{2}} 2^s \left(\frac{\pi}{2}\right)^{t-1} \frac{(M-2r)^{n-2}}{(n-2)!}\, r\,\mathrm{d}r.$$

Нека $R = M - 2r$. Тогава $r = \dfrac{M-R}{2}$, $\mathrm{d}r = -\dfrac{\mathrm{d}R}{2}$ и

$$v(X) = 2\pi \int_M^0 2^s \left(\frac{\pi}{2}\right)^{t-1} \frac{R^{n-2}}{(n-2)!} \frac{(M-R)}{2} \left(-\frac{\mathrm{d}R}{2}\right) =$$
$$= 2^s \left(\frac{\pi}{2}\right)^t \frac{1}{(n-2)!} \int_0^M R^{n-2}(M-R)\,\mathrm{d}R =$$
$$= 2^s \left(\frac{\pi}{2}\right)^t \frac{1}{(n-2)!} \left(M\int_0^M R^{n-2}\,\mathrm{d}R - \int_0^M R^{n-1}\,\mathrm{d}R \right) = 2^s \left(\frac{\pi}{2}\right)^t \frac{M^n}{n!}.$$

Следователно, ако формула (15) е в сила за $t-1$, то тя също е в сила за t. Доказателството на лемата е завършено. □

13.4. Приложения на лемата на Минковски. Нека $I \in \mathrm{Div}(A)$ е зададен дробен идеал на A — тогава обемът D на фундаменталната област на решетката $x(I)$ е $2^{-t}\sqrt{|\Delta|}\,\mathrm{N}(I)$ (виж Твърдение 13.5, (б)). Да изберем реалното число M така, че $v(X) = 2^n D$, т. е.

$$(16) \qquad 2^s \left(\frac{\pi}{2}\right)^t \frac{M^n}{n!} = 2^n(2^{-t}\sqrt{|\Delta|}\,\mathrm{N}(I)),\ \text{откъдето}\ M^n = \left(\frac{4}{\pi}\right)^t n!\sqrt{|\Delta|}\,\mathrm{N}(I).$$

Тъй като компактното множество X е изпъкнало централно–симетрично тяло, то от лемата на Минковски (Лема 13.4, (б)) следва, че X съдържа ненулева точка на решетката $x(I)$, т. е. съществува число $0 \neq \alpha \in I$, такова че

$$|\sigma_1(\alpha)| + \cdots + |\sigma_s(\alpha)| + 2|\sigma_{s+1}(\alpha)| + \cdots + 2|\sigma_{s+t}(\alpha)| \leq M.$$

Сега от неравенството между средното геометрично и средното аритметично на n положителни реални числа и от (16) получаваме

$$|\mathrm{N}(\alpha)| = |\sigma_1(\alpha)| \cdots |\sigma_s(\alpha)|\,|\sigma_{s+1}(\alpha)|^2 \cdots |\sigma_{s+t}(\alpha)|^2 \leq \frac{M^n}{n^n} = \Big(\frac{4}{\pi}\Big)^t \frac{n!}{n^n}\sqrt{|\Delta|}\,\mathrm{N}(I).$$

Ние доказахме следното твърдение:

Твърдение 13.7. *За всеки дробен идеал $I \in \mathrm{Div}(A)$ съществува число $\alpha \in I$, $\alpha \neq 0$, такова че*

$$|\mathrm{N}(\alpha)| \leq \Big(\frac{4}{\pi}\Big)^t \frac{n!}{n^n}\sqrt{|\Delta|}\,\mathrm{N}(I). \tag{17}$$

Следствие 13.8. *За всеки дробен идеал $I \in \mathrm{Div}(A)$ съществува идеал $J \subseteq A$, такъв че $J \sim I$ и*

$$\mathrm{N}(J) \leq \Big(\frac{4}{\pi}\Big)^t \frac{n!}{n^n}\sqrt{|\Delta|}.$$

Доказателство. Според предишното твърдение съществува число $0 \neq \alpha \in I^{-1}$, такова че

$$|\mathrm{N}(\alpha)| \leq \Big(\frac{4}{\pi}\Big)^t \frac{n!}{n^n}\sqrt{|\Delta|}\,\mathrm{N}(I^{-1}).$$

Нека $J = \alpha I$; тогава $J \sim I$. От $\alpha \in I^{-1}$ следва, че $J \subseteq A$, а от формула (12) и от горното неравенство получаваме

$$\mathrm{N}(\alpha I) = |\mathrm{N}(\alpha)|\,\mathrm{N}(I) \leq \Big(\frac{4}{\pi}\Big)^t \frac{n!}{n^n}\sqrt{|\Delta|}\,\mathrm{N}(I^{-1})\,\mathrm{N}(I) = \Big(\frac{4}{\pi}\Big)^t \frac{n!}{n^n}\sqrt{|\Delta|},$$

което трябваше да се докаже. □

С помощта на Следствие 13.8 ще покажем още веднъж, че групата от класове на идеали $\mathrm{Cl}(A)$ е крайна. За тази цел ще използваме следната лема:

Лема 13.9. *За всяко число m множеството на идеалите $J \subseteq A$, такива че $\mathrm{N}(J) \leq m$, е крайно.*

Доказателство. Достатъчно е докажем, че за всяко естествено число m множеството на идеалите $J \subseteq A$, такива че $\mathrm{N}(J) = m$, е крайно. За тази цел да забележим, че ако $K \neq (0)$ е фиксиран идеал в A, то множеството на идеалите J, такива че $K \subseteq J \subseteq A$, е крайно. Наистина, идеалите J, за които $K \subseteq J \subseteq A$, са във взаимно еднозначно съответствие с всички идеали във факторпръстена A/K, а тъй като A/K е краен пръстен (Лема 8.1), то множеството на идеалите в A/K е крайно. Ако сега $\mathrm{N}(J) = m$, то A/J е крайна група от ред m, откъдето $m(\alpha + J) = J$ за всяко $\alpha \in A$, т. е. $mA \subseteq J$. Следователно, всеки идеал J в A, такъв че $\mathrm{N}(J) = m$, съдържа идеала mA, откъдето получаваме, че множеството на тези идеали е крайно. □

Сега можем да покажем, че групата $\mathrm{Cl}(A)$ е крайна по следния начин: множеството на идеалите J в A, за които е в сила неравенството

$$\mathrm{N}(J) \leq \Big(\frac{4}{\pi}\Big)^t \frac{n!}{n^n}\sqrt{|\Delta|},$$

е крайно, а тъй като всеки дробен идеал $I \in \mathrm{Div}(A)$ е еквивалентен на идеал от това множество (Следствие 13.8), то групата $\mathrm{Cl}(A)$ също е крайна.
Неравенство (17) също ни дава долна граница за стойността на дискриминантата Δ на пръстена A.

Следствие 13.10. *Нека E е крайно разширение на полето на рационалните числа и нека Δ е дискриминантата на пръстена A на целите алгебрични числа в E. Тогава*

$$\sqrt{|\Delta|} \geq \Big(\frac{\pi}{4}\Big)^t \frac{n^n}{n!} \quad \text{и} \quad |\Delta| \geq \Big(\frac{\pi}{4}\Big)^{2t} \frac{n^{2n}}{(n!)^2}. \tag{18}$$

Доказателство. Според Твърдение 13.7 (приложено за $I = A$) съществува цяло алгебрично число $\alpha \neq 0$, такова че

$$|\mathrm{N}(\alpha)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta|}.$$

Тъй като числото $\mathrm{N}(\alpha)$ е цяло, то $|\mathrm{N}(\alpha)| \geq 1$. Следователно

$$\left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta|} \geq 1,$$

откъдето следват неравенства (18). □

В следващото доказателство ще използваме неравенството

$$\frac{n^n}{n!} \geq 2^{n-1}, \quad n \geq 1, \tag{19}$$

което се доказва с индукция по n:

$$\frac{(n+1)^{n+1}}{(n+1)!} = \frac{n^n}{n!}\,\frac{n!\,(n+1)^{n+1}}{n^n\,(n+1)!} = \frac{n^n}{n!}\left(1+\frac{1}{n}\right)^n \geq 2^{n-1}\,2 = 2^n.$$

Следствие 13.11 (Минковски). *Нека E е крайно разширение на полето на рационалните числа и нека Δ е дискриминантата на пръстена A на целите алгебрични числа в E. Ако $|\Delta| = 1$, то $E = \mathbb{Q}$.*

Доказателство. Ако $|\Delta| = 1$, то от неравенства (18) и (19) следва, че

$$1 \geq \left(\frac{\pi}{4}\right)^t \frac{n^n}{n!} \geq \left(\frac{\pi}{4}\right)^t 2^{n-1} = \left(\frac{\pi}{4}\right)^t 2^{s+2t-1} = \pi^t\,2^{s-1}.$$

Следователно $t = 0$ и $s = 1$. □