Група на единиците. Теорема на Дирихле

14. Дискретни подгрупи на $\mathbb{R}^n$

Едно подмножество S на $\mathbb{R}^n$ се нарича *дискретно*, когато за всяко ограничено подмножество U на $\mathbb{R}^n$ множеството $S \cap U$ е крайно. Тъй като всеки две норми на $\mathbb{R}^n$ са еквивалентни, то е без значение коя норма на $\mathbb{R}^n$ ще използваме, за да определим ограничено подмножество на $\mathbb{R}^n$. Една подгрупа G на адитивната група на $\mathbb{R}^n$ се нарича *дискретна* подгрупа на $\mathbb{R}^n$, когато G е дискретно подмножество на $\mathbb{R}^n$.
Следващите две твърдения показват, че решетките са точно дискретните подгрупи на $\mathbb{R}^n$.

Твърдение 14.1. *Всяка решетка Λ в $\mathbb{R}^n$ е дискретна подгрупа на $\mathbb{R}^n$.*

Доказателство. Нека $e_1, \ldots, e_k$ е базис на решетката Λ над $\mathbb{Z}$. Да допълним това множество до базис $e_1, \ldots, e_k, e_{k+1}, \ldots, e_n$ на $\mathbb{R}^n$. За всеки вектор $v \in \mathbb{R}^n$ да определим норма $\|v\|$ на v по следния начин:

$$\text{ако } v = \sum_{i=1}^{n} x_i e_i, \text{ то } \|v\| = \max_{1 \le i \le n} |x_i|.$$

Нека U е ограничено подмножество на $\mathbb{R}^n$. Тогава съществува естествено число N, такова че $\|v\| \le N$ за всеки вектор $v \in U$. Ако $v \in \Lambda \cap U$, то $v = \sum_{i=1}^{k} x_i e_i$, където всички координати x_i, $i = 1, \ldots, k$, са цели числа, такива че $|x_i| \le N$ за $1 \le i \le k$. Следователно множеството $\Lambda \cap U$ съдържа не повече от $(2N+1)^k$ вектора. □

Твърдение 14.2. *Всяка дискретна подгрупа Λ на групата $\mathbb{R}^n$ е решетка.*

Доказателство. За да докажем твърдението, ще използваме индукция по размерността n на линейното пространство $\mathbb{R}^n$. Ако $n = 0$, твърдението е тривиално. Да предположим, че твърдението е доказано за всички линейни пространства $\mathbb{R}^k$, такива че $k < n$. Нека Λ е дискретна подгрупа на $\mathbb{R}^n$. Ако Λ се съдържа в собствено линейно подпространство V на $\mathbb{R}^n$, то $V \cong \mathbb{R}^k$ за някое $k < n$ и твърдението следва от индукционната хипотеза.
Ако Λ не се съдържа в собствено подпространство на $\mathbb{R}^n$, то Λ съдържа базис $e_1, \ldots, e_n$ на $\mathbb{R}^n$. Нека $\Lambda_0 \subseteq \Lambda$ е решетката, породена от векторите $e_1, \ldots, e_n$,

$$\Lambda_0 = \{k_1 e_1 + \cdots + k_n e_n \colon k_1, \ldots, k_n \in \mathbb{Z}\},$$

и нека $\mathcal{D}_0$ е следната фундаментална област на Λ_0:

$$\mathcal{D}_0 = \{x_1 e_1 + \cdots + x_n e_n \colon 0 \le x_1 < 0, \ldots, 0 \le x_n < 1\}.$$

Тогава за всеки вектор $\lambda \in \Lambda$ съществува единствен вектор $\lambda_0 \in \Lambda \cap \mathcal{D}_0$, такъв че $\lambda + \Lambda_0 = \lambda_0 + \Lambda_0$. Наистина, ако $\lambda = \sum_{i=1}^{n} \lambda_i e_i \in \Lambda$, то $\lambda_i = \lambda_i' + \lambda_i''$, където

$\lambda_i' \in \mathbb{Z}$ и $0 \leq \lambda_i'' < 1$ за $i = 1, \ldots, n$. Следователно

$$\lambda + \Lambda_0 = \sum_{i=1}^{n} (\lambda_i' + \lambda_i'') e_i + \Lambda_0 = \sum_{i=1}^{n} \lambda_i'' e_i + \sum_{i=1}^{n} \lambda_i' e_i + \Lambda_0 = \lambda_0 + \Lambda_0,$$

където $\lambda_0 = \sum\limits_{i=1}^{n} \lambda_i'' e_i \in \Lambda \cap \mathcal{D}_0$. Сега да забележим, че множеството $\mathcal{D}_0$ е ограничено — следователно множеството $\Lambda \cap \mathcal{D}_0$ е крайно. Тъй като всеки съседен клас $\lambda + \Lambda_0$, $\lambda \in \Lambda$, може да се представи като $\lambda_0 + \Lambda_0$, където $\lambda_0 \in \Lambda \cap \mathcal{D}_0$, подгрупата Λ_0 има краен брой съседни класове в групата Λ, т. е. Λ_0 *е подгрупа с краен индекс в* Λ. Нека $m = [\Lambda : \Lambda_0]$ — тогава $m\Lambda \subseteq \Lambda_0$, откъдето следва, че Λ се съдържа в решетката $\dfrac{1}{m}\Lambda_0$. Следователно Λ е решетка, защото подгрупите на решетка също са решетки. □

15. Логаритмично пространство на числово поле

Нека крайното разширение E на полето на рационалните числа $\mathbb{Q}$ има s реални влагания $\sigma_1, \ldots, \sigma_s$ и $2t$ комплексни влагания $\sigma_{s+1}, \overline{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \overline{\sigma}_{s+t}$ в полето на комплексните числа $\mathbb{C}$. За всяко $\alpha \in E^*$ нека

$$\begin{aligned} L_1(\alpha) &= \ln|\sigma_1(\alpha)|, & L_{s+1}(\alpha) &= \ln|\sigma_{s+1}(\alpha)|^2, \\ &\cdots\cdots\cdots\cdots & &\cdots\cdots\cdots\cdots\cdots\cdots \\ L_s(\alpha) &= \ln|\sigma_s(\alpha)|, & L_{s+t}(\alpha) &= \ln|\sigma_{s+t}(\alpha)|^2. \end{aligned}$$

Да определим изображение $L\colon E^* \to \mathbb{R}^{s+t}$ по следния начин:

$$L(\alpha) = (L_1(\alpha), \ldots, L_s(\alpha), L_{s+1}(\alpha), \ldots, L_{s+t}(\alpha)), \quad \alpha \in E^*.$$

Тъй като $L_i(\alpha_1\alpha_2) = L_i(\alpha_1) + L_i(\alpha_2)$ за всяко $\alpha \in E^*$ и всяко $i = 1, \ldots, s+t$, изображението L е *хомоморфизъм* от мултипликативната група E^* в адитивната група на линейното пространство $\mathbb{R}^{s+t}$:

$$L(\alpha_1\alpha_2) = L(\alpha_1) + L(\alpha_2), \quad \alpha_1, \alpha_2 \in E^*.$$

Ще наричаме линейното пространство $\mathbb{R}^{s+t}$ *логаритмично пространство* на числовото поле E.

Лема 15.1. *За всяко $\alpha \in E^*$ е в сила равенството*

$$\sum_{i=1}^{s+t} L_i(\alpha) = \ln|\mathrm{N}(\alpha)|. \tag{20}$$

Доказателство. От равенството

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

следва, че

$$\ln|\mathrm{N}(\alpha)| = \ln|\sigma_1(\alpha)| + \cdots + \ln|\sigma_s(\alpha)| + \ln|\sigma_{s+1}(\alpha)|^2 + \cdots + \ln|\sigma_{s+t}(\alpha)|^2,$$

което трябваше да се докаже. □

Да снабдим логаритмичното пространство $\mathbb{R}^{s+t}$ пространство със следната норма:

$$\text{за всяко } \lambda = (\lambda_1, \ldots, \lambda_{s+t}) \in \mathbb{R}^{s+t} \text{ нека } \|\lambda\| = \max_{1 \leq i \leq s+t} |\lambda_i|.$$

Нека A е пръстенът на целите алгебрични числа в числовото поле E.

Лема 15.2. *За всяко реално число $R \geq 0$ множеството*

$$A_R = \{\alpha \in A \setminus \{0\} \colon \|L(\alpha)\| \leq R\}$$

е крайно.

Доказателство. Нека $\alpha \in A_R$. Тогава от неравенствата

$$\ln|\sigma_i(\alpha)| = L_i(\alpha) \leq |L_i(\alpha)| \leq R, \quad 1 \leq i \leq s,$$
$$\ln|\sigma_i(\alpha)|^2 = L_i(\alpha) \leq |L_i(\alpha)| \leq R, \quad s+1 \leq i \leq s+t,$$

следва, че

$$\begin{aligned} |\sigma_i(\alpha)| &\leq e^R, \quad 1 \leq i \leq s, \\ |\sigma_i(\alpha)| &\leq e^{\frac{R}{2}}, \quad s+1 \leq i \leq s+t. \end{aligned} \tag{21}$$

Да разгледаме изображението $x \colon E \to L^{s,t}$, определено в параграф 13.1:

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

Неравенства (21) показват, че образът $x(A_R)$ на множеството A_R се съдържа в ограниченото подмножество

$$\{(x_1, \ldots, x_{s+t}) \in L^{s,t} \colon |x_i| \leq e^R,\ 1 \leq i \leq s;\ |x_i| \leq e^{\frac{R}{2}},\ s+1 \leq i \leq s+t\}$$

на линейното пространство $L^{s,t}$. Тъй като $x(A)$ е решетка в $L^{s,t}$ (Твърдение 13.5), множеството $x(A_R)$ е крайно, а тъй като изображението $x \colon E \to L^{s,t}$ е инективно, то множеството A_R също е крайно. □

Лема 15.3. *Множеството $L(A \setminus \{0\})$ е дискретно подмножество на $\mathbb{R}^{s+t}$.*

Доказателство. За всяко $R \geq 0$, нека $U_R = \{\lambda \in \mathbb{R}^{s+t} \colon \|\lambda\| \leq R\}$ е "кълбото" с радиус R в $\mathbb{R}^{s+t}$. Да забележим, че $L(A \setminus \{0\}) \cap U_R = L(A_R)$. Тъй като A_R е крайно множество за всяко $R \geq 0$ (Лема 15.2), то $L(A \setminus \{0\}) \cap U_R$ също е крайно множество за всяко $R \geq 0$. Следователно $L(A \setminus \{0\})$ е дискретно подмножество на $\mathbb{R}^{s+t}$. □

Твърдение 15.4. *Множеството $A_0 = \{\alpha \in A \setminus \{0\} \colon L(\alpha) = 0\}$ е крайна циклична група, която се състои от всички корени на единицата в полето E.*

Доказателство. Според Лема 15.2, приложена за $R = 0$, множеството A_0 е крайно. То е мултипликативно затворено, защото от $\alpha_1, \alpha_2 \in A_0$, следва, че $L(\alpha_1\alpha_2) = L(\alpha_1) + L(\alpha_2) = 0$. Нека $\omega \in A_0$; тогава $\omega^r \in A_0$ за всяко естествено число r. Тъй като A_0 е крайно множество, съществуват естествени числа $r_1 < r_2$, такива че $\omega^{r_1} = \omega^{r_2}$, откъдето $\omega^{r_2 - r_1} = 1$, т. е. ω е корен на единицата.
Обратно, нека $\omega \in E$ е корен на единицата: $\omega^r = 1$ за някое естествено число r. Тогава $\omega \in A$, защото ω е цяло алгебрично число. Ако $\sigma \colon E \to \mathbb{C}$ е влагане на E в полето на комплексните числа $\mathbb{C}$, то $\sigma(\omega)^r = \sigma(\omega^r) = 1$, т. е. $\sigma(\omega)$ също е корен на единицата. Тъй като всички корени на единицата принадлежат на единичната окръжност на $\mathbb{C}$, то $|\sigma(\omega)| = 1$ за всяко влагане $\sigma \colon E \to \mathbb{C}$ на E в $\mathbb{C}$. Следователно $L_i(\omega) = 0$, $i = 1, \ldots, s+t$, т. е. $\omega \in A_0$.
Накрая, да забележим, че всяка крайна подгрупа W на E^* е циклична: ако $|W| = m$, то $\omega^m = 1$ за всеки $\omega \in W$, откъдето следва, че $W = C_m$. □

16. Структура на групата на единиците. Теорема на Дирихле

Дефиниция 16.1. Числото $\varepsilon \in A$ се нарича *единица* на пръстена A, когато съществува число $\varepsilon' \in A$, такова че $\varepsilon\varepsilon' = 1$.

Ще означаваме с A^* множеството от всички единици на пръстена A — ясно е, че A^* е абелева група относно операцията умножение.

Твърдение 16.1. *Съществуват единици $\varepsilon_1, \ldots, \varepsilon_k \in A^*$, такива че всяка единица $\varepsilon \in A^*$ има единствено представяне*

$$\varepsilon = \omega \varepsilon_1^{n_1} \cdots \varepsilon_k^{n_k}, \tag{22}$$

където $n_1, \ldots, n_k$ са цели числа, а ω е корен на единицата.

Доказателство. Тъй като $L\colon E^* \to \mathbb{R}^{s+t}$ е хомоморфизъм на групи и A^* е подгрупа на E^*, то $L(A^*)$ е подгрупа на $\mathbb{R}^{s+t}$, а тъй като $L(A \setminus \{0\})$ е дискретно подмножество на $\mathbb{R}^{s+t}$ (Лема 15.3), то $L(A^*)$ е дискретна подгрупа на $\mathbb{R}^{s+t}$. Следователно $L(A^*)$ е решетка в $\mathbb{R}^{s+t}$ според Твърдение 14.2.
Да изберем единици $\varepsilon_1, \ldots, \varepsilon_k \in A^*$, такива че векторите $L(\varepsilon_1), \ldots, L(\varepsilon_k)$ са базис на решетката $L(A^*)$. Ако $\varepsilon \in A^*$, то съществуват цели числа $n_1, \ldots, n_k$, такива че $L(\varepsilon) = n_1 L(\varepsilon_1) + \cdots + n_k L(\varepsilon_k)$. Тогава

$$L(\varepsilon \varepsilon_1^{-n_1} \cdots \varepsilon^{-n_k}) = L(\varepsilon) - n_1 L(\varepsilon_1) - \cdots - n_k L(\varepsilon_k) = 0,$$

откъдето следва, че $\varepsilon \varepsilon_1^{-n_1} \cdots \varepsilon^{-n_k} \in A_0$, т. е. числото $\varepsilon \varepsilon_1^{-n_1} \cdots \varepsilon^{-n_k}$ е корен на единицата (виж Твърдение 15.4). Сега да положим $\omega = \varepsilon \varepsilon_1^{-n_1} \cdots \varepsilon^{-n_k}$ — тогава $\varepsilon = \omega \varepsilon_1^{n_1} \cdots \varepsilon_k^{n_k}$, т. е. за ε съществува представяне от вида (22).
Нека

$$\varepsilon = \omega \varepsilon_1^{n_1} \cdots \varepsilon_k^{n_k} = \omega' \varepsilon_1^{m_1} \cdots \varepsilon_k^{m_k}$$

са две представяния на единицата ε от вида (22). Тогава от равенството

$$L(\omega \varepsilon_1^{n_1} \cdots \varepsilon_k^{n_k}) = L(\omega' \varepsilon_1^{m_1} \cdots \varepsilon_k^{m_k})$$

получаваме

$$L(\omega) + n_1 L(\varepsilon_1) + \cdots + n_k L(\varepsilon_k) = L(\omega') + m_1 L(\varepsilon_1) + \cdots + m_k L(\varepsilon_k).$$

Тъй като ω и ω' са корени на единицата, то $L(\omega) = L(\omega') = 0$ според Твърдение 15.4. Следователно е в сила равенството

$$n_1 L(\varepsilon_1) + \cdots + n_k L(\varepsilon_k) = m_1 L(\varepsilon_1) + \cdots + m_k L(\varepsilon_k),$$

което влече $n_1 = m_1, \ldots, n_k = m_k$, защото векторите $L(\varepsilon_1), \ldots, L(\varepsilon_k)$ са базис на решетката $L(A^*)$. Сега от $\omega \varepsilon_1^{n_1} \cdots \varepsilon_k^{n_k} = \omega' \varepsilon_1^{n_1} \cdots \varepsilon_k^{n_k}$ получаваме $\omega = \omega'$. Следователно представянето на всяка единица ε на пръстена A във вида (22) е единствено. □

Забележка. Една абелева група G се нарича *крайнопородена*, когато съществуват елементи $g_1, \ldots, g_n \in G$, такива че всеки елемент $g \in G$ се представя като $g = g_1^{a_1} \cdots g_n^{a_n}$ за някои цели числа $a_1, \ldots, a_n$. От Твърдение 16.1 следва, че групата на единиците A^* е крайнопородена. Наистина, тъй като групата на корените на единицата в E е циклична (Твърдение 15.4), всеки корен на единицата $\omega \in E$ се представя като $\omega = \zeta^a$, където ζ е фиксиран корен на единицата. Следователно единиците $\zeta, \varepsilon_1, \ldots, \varepsilon_k$ пораждат групата A^*: всяка единица ε се представя като $\varepsilon = \zeta^a \varepsilon_1^{n_1} \cdots \varepsilon_k^{n_k}$.

Дефиниция 16.2 (Фундаментална система от единици). Множеството от единици $\varepsilon_1, \ldots, \varepsilon_k$ на пръстена A, се нарича *фундаментална система от единици* на пръстена A, когато за всяка единица ε на A съществува *единствено* представяне

$$\varepsilon = \omega \varepsilon_1^{n_1} \cdots \varepsilon_k^{n_k},$$

където ω е корен на единицата в E и $n_1, \ldots, n_k$ са цели числа.

От доказателството на Твърдение 16.1 е ясно, че числата $\varepsilon_1, \ldots, \varepsilon_k \in A^*$ са фундаментална система от единици на пръстена A тогава и само тогава, когато векторите $L(\varepsilon_1), \ldots, L(\varepsilon_k)$ са базис на решетката $L(A^*)$. Следователно броят на единиците във всяка система от фундаментални единици на пръстена A е равен на ранга на решетката $L(A^*)$.

Дефиниция 16.3. Броят на единиците във всяка система от фундаментални единици на пръстена A се нарича *ранг* на групата на единиците на пръстена A.

Твърдение 16.2. *Числото $\varepsilon \in A$ е единица на A точно когато $|\mathrm{N}(\varepsilon)| = 1$.*

Доказателство. От $\varepsilon\varepsilon' = 1$ следва, че $|\mathrm{N}(\varepsilon)||\mathrm{N}(\varepsilon')| = 1$. Тъй като $|\mathrm{N}(\varepsilon)$ и $|\mathrm{N}(\varepsilon')|$ са естествени числа, то $|\mathrm{N}(\varepsilon)| = |\mathrm{N}(\varepsilon')| = 1$.
Обратно, нека $|\mathrm{N}(\varepsilon)| = 1$. Тогава нормата на главния идеал (ε) е равна на 1 според Твърдение 12.4. Следователно $(\varepsilon) = A$, т. е. съществува число $\varepsilon' \in A$, такова че $\varepsilon\varepsilon' = 1$. □

Пример 16.3. Нека $D > 0$ е свободно от квадрати естествено число и нека E е мнимото квадратично поле $\mathbb{Q}(\sqrt{-D})$. Влаганията на E в $\mathbb{C}$ са тъждественото изображение и комплексното спрягане, откъдето следва, че

$$\mathrm{N}(\alpha) = \alpha\overline{\alpha} = |\alpha|^2,$$

за всяко $\alpha \in E$. Нека числата α_1, α_2 са базис на пръстена A на целите алгебрични числа в E. Тогава пръстенът A е решетката, породена от α_1 и α_2 в полето на комплексните числа: $A = \{n_1\alpha_1 + n_2\alpha_2 \colon n_1, n_2 \in \mathbb{Z}\}$. Числото $\varepsilon \in A$ е единица на A точно когато $\mathrm{N}(\varepsilon) = |\varepsilon|^2 = 1$, т. е. точно когато ε се принадлежи на единичната окръжност U на полето $\mathbb{C}$. Тъй като пресичането на решетката A и единичната окръжност U е крайно множество, групата на единиците на A е крайна и се състои от корени на единицата. Следователно рангът на групата на единиците на A е равен на 0.

Пример 16.4. Нека E е реалното квадратично поле $\mathbb{Q}(\sqrt{2})$ и нека

$$A = \mathbb{Z}[\sqrt{2}] = \{x + y\sqrt{2} \colon x, y \in \mathbb{Z}\}.$$

е пръстенът на целите алгебрични числа в E.
От $(1+\sqrt{2})(-1+\sqrt{2}) = 1$ следва, че $\varepsilon_1 = 1 + \sqrt{2}$ е единица на A. Ще покажем, че ε_1 е фундаментална единица на A.
Тъй като

$$\mathrm{N}(x + y\sqrt{2}) = (x + y\sqrt{2})(x - y\sqrt{2}) = x^2 - 2y^2,$$

то $x + y\sqrt{2} \in A$ е единица на A точно когато целите числа x и y са решения на уравнението

$$x^2 - 2y^2 = \pm 1.$$

Да забележим, че ако $\varepsilon = x + y\sqrt{2}$ е единица на A, такава че $x \geq 0$ и $y \geq 1$, то от неравенствата

$$x^2 = 2y^2 \pm 1 \geq 2y^2 - 1 \geq y^2 \text{ и } x^2 = 2y^2 \pm 1 \leq 2y^2 + 1 \leq 4y^2$$

следва, че $y \leq x \leq 2y$.
Сега нека $\varepsilon = x + y\sqrt{2}$ е единица на A, такава че $x \geq 0$ и $y \geq 0$. Да разгледаме безкрайната редица от единици на A

$$\varepsilon_m = \varepsilon(1+\sqrt{2})^{-m} = \varepsilon(-1+\sqrt{2})^m = x_m + y_m\sqrt{2}, \quad m \geq 0.$$

Тъй като редицата ε_m клони към 0 (защото $0 < -1 + \sqrt{2} < 1$), то съществува число M, такова че $\varepsilon_m = x_m + y_m\sqrt{2} < 1$ за $m > M$. Следователно за всяко $m > M$ някое от целите числа x_m и y_m е отрицателно. Нека n е най-голямото естествено число, такова че $x_n \geq 0$ и $y_n \geq 0$. Да предположим, че $y_n \geq 1$. Тогава от тъждеството

$$x_{n+1} + y_{n+1}\sqrt{2} = (x_n + y_n)(-1+\sqrt{2}) = (-x_n + 2y_n) + (x_n - y_n)\sqrt{2}$$

и от неравенствата $y_n \leq x_n \leq 2y_n$ следва, че $x_{n+1} \geq 0$ и $y_{n+1} \geq 0$, което противоречи на определението на n. Следователно $y_n = 0$, откъдето $x_n = 1$, т. е.

$\varepsilon(1+\sqrt{2})^{-n}=1$ и $\varepsilon=(1+\sqrt{2})^n$. Ние показахме, че ако $\varepsilon=x+y\sqrt{2}$ е единица на A, такава че $x\geq 0$ и $y\geq 0$, то $\varepsilon=(1+\sqrt{2})^n$ за някое $n\geq 0$.
Сега нека $\varepsilon=x+y\sqrt{2}$ е произволна единица на A. Тъй като

$$\pm\varepsilon^{\pm 1}=\pm x\pm y\sqrt{2},$$

то $\varepsilon=\pm(1+\sqrt{2})^n$ за някое цяло число n.

Твърдение 16.1 оставя отворен въпросът за ранга на групата на единиците — нашата следваща цел е да докажем, че той е равен на $s+t-1$.
От твърдение 16.2 и формула (20) следва, че числото $\varepsilon\in A\setminus\{0\}$ е единица на A точно когато $L_1(\varepsilon)+\cdots+L_{s+t}(\varepsilon)=0$. Следователно решетката $L(A^*)$ се съдържа в хипер–равнината

$$H=\{(\lambda_1,\ldots,\lambda_{s+t})\colon \lambda_1+\cdots+\lambda_{s+t}=0\}$$

на логаритмичното пространство $\mathbb{R}^{s+t}$, а тъй като размерността на H е $s+t-1$, то рангът на $L(A^*)$ е не по-голям от $s+t-1$. Ние ще установим, че рангът на $L(A^*)$ е точно $s+t-1$ с помощта на следната лема:

Лема 16.5. *Решетка Λ в n-мерно реално линейно пространство V има ранг n тогава и само тогава, когато съществува ограничено подмножество $\mathcal{U}$ на V, такова че*

$$V=\bigcup_{\lambda\in\Lambda}(\lambda+\mathcal{U}).$$

Доказателство. Ако рангът на решетката Λ е равен на n, то фундаменталната област $\mathcal{D}$ на Λ е ограничено подмножество в $\mathbb{R}^n$ и

$$V=\bigcup_{\lambda\in\Lambda}(\lambda+\mathcal{D}).$$

Обратно, нека $\mathcal{U}$ е ограничено подмножество във V и Λ е решетка от ранг $k<n$ в V. Нека векторите $e_1,\ldots,e_k$ са базис на Λ. Да допълним линейното независимото множество $e_1,\ldots,e_k$ до базис $e_1,\ldots,e_k,e_{k+1},\ldots,e_n$ на V. За всеки вектор $v\in V$ нека $x_1(v),\ldots,x_n(v)$ са координатите на v спрямо базиса $e_1,\ldots,e_n$:

$$v=x_1(v)e_1+\cdots+x_n(v)e_n.$$

Тъй като множеството $\mathcal{U}$ е ограничено, съществува константа $C>0$, такава че $|x_n(v)|<C$ за всеки вектор $v\in\mathcal{U}$.
Нека

$$\lambda=\lambda_1e_1+\cdots+\lambda_ke_k\in\Lambda \text{ и } v=x_1(v)e_1+\cdots+x_k(v)e_k+\cdots+x_n(v)e_n\in V.$$

Тогава $\lambda+v=(\lambda_1+x_1(v))e_1+\cdots+(\lambda_k+x_k(v))e_k+\cdots+x_n(v)e_n$, откъдето следва, че $x_n(\lambda+v)=x_n(v)$ за всеки вектор $\lambda\in\Lambda$ и всеки вектор $v\in V$. Сега да забележим, че ако $\lambda\in\Lambda$ и $v\in\mathcal{U}$, то $|x_n(\lambda+v)|=|x_n(v)|<C$. Следователно за всеки вектор $u\in\bigcup\limits_{\lambda\in\Lambda}(\lambda+\mathcal{U})$ е в сила неравенството $|x_n(u)|<C$, поради което $\bigcup\limits_{\lambda\in\Lambda}(\lambda+\mathcal{U})$ е собствено подмножество на V. □

Ние ще построим ограничено подмножество $\mathcal{U}$ на хипер–равнината H, такова че

$$H=\bigcup_{\varepsilon\in A^*}(L(\varepsilon)+\mathcal{U}). \tag{23}$$

За да конструираме множеството $\mathcal{U}$ и докажем (23), ще използваме следните две леми.

Лема 16.6. *Нека Δ е дискриминантата на пръстена A и нека $c_1, \dots, c_{s+t}$ са положителни реални числа, такива че*

$$c_1 \cdots c_{s+t} \geq \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}.$$

Тогава съществува цяло алгебрично число α, $\alpha \neq 0$, такова че

$$|\sigma_i(\alpha)| \leq c_i \text{ за } i = 1, \dots, s, \quad |\sigma_i(\alpha)|^2 \leq c_i \text{ за } i = s+1, \dots, s+t. \tag{24}$$

Доказателство. Да разгледаме изпъкналото централно–симетрично тяло X, което се състои от всички точки $(x_1, \dots, x_s; x_{s+1} \dots x_{s+t}) \in L^{s,t}$, такива че

$$|x_1| \leq c_1, \dots, |x_s| \leq c_s, \quad |x_{s+1}|^2 \leq c_{s+1}, \dots, |x_{s+t}|^2 \leq c_{s+t}.$$

Множеството X е директно произведение на интервалите

$$I_i = \{x_i \in \mathbb{R} \colon -c_i \leq x_i \leq c_i\}, \quad i = 1, \dots, s,$$

и дисковете

$$D_i = \{x_i \in \mathbb{C} \colon |x_i|^2 \leq c_i\}, \quad i = s+1, \dots, s+t.$$

Следователно

$$v(X) = \left(\prod_{i=1}^{s} 2c_i\right)\left(\prod_{i=s+1}^{s+t} \pi c_i\right) = 2^s \pi^t c_1 \cdots c_{s+t}.$$

Според Твърдение 13.5 фундаменталната област на решетката $x(A)$ има обем

$$D = 2^{-t}\sqrt{|\Delta|}.$$

Сега можем да приложим лемата на Минковски (Лема 13.4, (б)): тъй като

$$v(X) = 2^s \pi^t c_1 \cdots c_{s+t} \geq 2^s \pi^t \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|} = 2^{s+t}\sqrt{|\Delta|} = 2^{n-t}\sqrt{|\Delta|} = 2^n D,$$

тялото X съдържа ненулева точка от решетката $x(A)$, т. е. съществува число $0 \neq \alpha \in A$, за което са в сила неравенства (24). □

Да напомним, че два елемента $x \neq 0$ и $y \neq 0$ на област R се наричат *асоциирани*, когато главните идеали (x) и (y) съвпадат. Ако елементите x и y са асоциирани, то $x \in (y)$ и $y \in (x)$, откъдето следва, че съществуват елементи $\varepsilon, \varepsilon' \in R$, такива че $x = \varepsilon y$ и $y = \varepsilon' x$. Тогава $x = \varepsilon y = \varepsilon\varepsilon' x$, откъдето $x(1 - \varepsilon\varepsilon') = 0$. Следователно $\varepsilon\varepsilon' = 1$, защото $x \neq 0$ и R е област. Виждаме, че ако елементите $x \neq 0$ и $y \neq 0$ са асоциирани, то $x = \varepsilon y$, където ε е обратим елемент на областта R. Обратно, ако ε е обратим елемент на областта R и $x = \varepsilon y$, то $(x) = (\varepsilon y) = (\varepsilon)(y) = (y)$, защото $(\varepsilon) = A$. Следователно елементите $x \neq 0$ и $y \neq 0$ са асоциирани тогава и само тогава, когато $x = \varepsilon y$ за някой обратим елемент (единица) на областта R.

Лема 16.7. *За всяко реално число $Q \geq 1$ съществува крайно множество от цели алгебрични числа $\{\alpha_1, \dots, \alpha_k\} \subset A \setminus \{0\}$, такова че:*

(а) $|\mathrm{N}(\alpha_j)| \leq Q$, $j = 1, \dots, k$;

(б) *всяко цяло алгебрично число $\alpha \in A$, $\alpha \neq 0$, такова че $|\mathrm{N}(\alpha)| \leq Q$, е асоциирано с някое число от множеството $\{\alpha_1, \dots, \alpha_k\}$.*

Доказателство. За всяко цяло алгебрично число $\alpha \neq 0$ нормата на главния идеал $(\alpha) = \alpha A$ е равна на $|\mathrm{N}(\alpha)|$ (виж Твърдение 12.4). Според Твърдение 13.9 множеството на идеалите $(0) \neq I \subseteq A$, такива че $\mathrm{N}(I) \leq Q$, е крайно. Нека $(\alpha_1), \dots, (\alpha_k)$ са всички ненулеви главни идеали в пръстена A, чиято норма не надминава Q. Ако $\alpha \in A$, $\alpha \neq 0$ и $|\mathrm{N}(\alpha)| \leq Q$, то главният идеал (α) съвпада с някой от идеалите $(\alpha_1), \dots, (\alpha_k)$ — следователно числото α е асоциирано с някое от числата $\alpha_1, \dots, \alpha_k$. □

Твърдение 16.8. *Рангът на решетката $L(A^*)$ е равен на $s + t - 1$.*

Доказателство. За всяко реално число $Q \geq 1$ нека H_Q е афинната хипер–равнина

$$H_Q = \{(\lambda_1, \ldots, \lambda_{s+t})\colon \lambda_1 + \cdots + \lambda_{s+t} = \ln Q\}$$

в логаритмичното пространство $\mathbb{R}^{s+t}$. Ясно е, че хипер–равнината H_Q се получава от хипер–равнината H чрез транслация — например чрез транслация с вектора

$$v_Q = \left(\frac{\ln Q}{s+t}, \ldots, \frac{\ln Q}{s+t}\right).$$

Ако ε е единица на A, то $L(\varepsilon) + H_Q = H_Q$, защото $L(\varepsilon) \in H$.

За всяко число $\alpha \in A$, $\alpha \neq 0$, нека $l(\alpha)$ е следното подмножество на H_Q:

$$l(\alpha) = \{\lambda = (\lambda_1, \ldots, \lambda_{s+t}) \in H_Q\colon \lambda_i \geq L_i(\alpha),\ i = 1, \ldots, s+t\}.$$

Нека ε е единица на A и $\alpha \in A$, $\alpha \neq 0$. Да сравним множествата $l(\alpha)$ и $l(\varepsilon\alpha)$:

$$\lambda \in l(\alpha) \quad \Leftrightarrow \quad \lambda_i \geq L_i(\varepsilon\alpha) = L(\alpha), \qquad i = 1, \ldots, s+t, \tag{25}$$

$$\lambda \in l(\varepsilon\alpha) \quad \Leftrightarrow \quad \lambda_i \geq L_i(\varepsilon\alpha) = L_i(\varepsilon) + L(\alpha), \qquad i = 1, \ldots, s+t. \tag{26}$$

От (25) и (26) следва, че

$$l(\varepsilon\alpha) = L(\varepsilon) + l(\alpha),$$

за всяка единица ε на A и всяко число $\alpha \in A$, $\alpha \neq 0$.

Всяко множество $l(\alpha)$ е ограничено, защото ако $(\lambda_1, \ldots, \lambda_{s+t}) \in l(\alpha)$, то

$$L_i(\alpha) \leq \lambda_i = \ln Q - \sum_{j \neq i} \lambda_j \leq \ln Q - \sum_{j \neq i} L(\alpha_j), \quad i = 1, \ldots, s+t.$$

Да докажем, че множествата $l(\alpha)$ покриват хипер–равнината H_Q, когато

$$Q \geq \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}. \tag{27}$$

Нека $(\lambda_1, \ldots, \lambda_{s+t}) \in H_Q$ и нека $c_1 = e^{\lambda_1}, \ldots, c_{s+t} = e^{\lambda_{s+t}}$. Тъй като

$$c_1 \cdots c_{s+t} = e^{\lambda_1} \cdots e^{\lambda_{s+t}} = e^{\lambda_1 + \cdots + \lambda_{s+t}} = e^{\ln Q} = Q \geq \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|},$$

то, според Лема 16.6, съществува число $\alpha \in A$, $\alpha \neq 0$, такова че

$$|\sigma_i(\alpha)| \leq c_i \text{ за } i = 1, \ldots, s, \quad |\sigma_i(\alpha)|^2 \leq c_i \text{ за } i = s+1, \ldots, s+t.$$

Тогава

$$\ln|\sigma_i(\alpha)| \leq \lambda_i \text{ за } i = 1, \ldots, s, \quad \ln|\sigma_i(\alpha)|^2 \leq \lambda_i \text{ за } i = s+1, \ldots, s+t,$$

което означава, че $(\lambda_1, \ldots, \lambda_{s+t}) \in l(\alpha)$. Следователно, ако Q удовлетворява неравенство (27), то

$$H_Q = \bigcup_{\alpha \in A \setminus \{0\}} l(\alpha).$$

Да забележим, че $l(\alpha) = \emptyset$, когато $|\mathrm{N}(\alpha)| > Q$. Наистина, ако $l(\alpha) \neq \emptyset$, то съществува точка $(\lambda_1, \ldots, \lambda_{s+t}) \in H_Q$, такава че $L_i(\alpha) \leq \lambda_i$ за $i = 1, \ldots, s+t$. Сумирайки неравенствата и прилагайки формула (20) получаваме

$$\ln|\mathrm{N}(\alpha)| = L_1(\alpha) + \cdots + L_{s+t}(\alpha) \leq \lambda_1 + \cdots + \lambda_{s+t} = \ln Q,$$

т. е. ако $l(\alpha) \neq \emptyset$, то $|\mathrm{N}(\alpha)| \leq Q$. Следователно, ако Q удовлетворява неравенство (27), то

$$H_Q = \bigcup_{\substack{\alpha \in A \setminus \{0\} \\ \mathrm{N}(\alpha) \leq Q}} l(\alpha).$$

Сега да изберем реално число Q, което удовлетворява неравенство (27). Нека $\{\alpha_1, \ldots, \alpha_k\} \subset A \setminus \{0\}$ е крайното множество, определено в Лема 16.7, и нека $\mathcal{U}_Q$ е ограниченото множество

$$\mathcal{U}_Q = \bigcup_{j=1}^{k} l(\alpha_j) \subset H_Q.$$

Ние твърдим, че

$$H_Q = \bigcup_{\varepsilon \in A^*} (L(\varepsilon) + \mathcal{U}_Q). \tag{28}$$

Наистина, нека $\lambda \in H_Q$. Тогава $\lambda \in l(\alpha)$ за някое число $\alpha \in A$, $\alpha \neq 0$, такова че $|\mathrm{N}(\alpha)| \leq Q$. Сега от Лема 16.7 следва, че $\alpha = \varepsilon\alpha_j$ за някое $1 \leq j \leq k$ и някоя единица ε на A, откъдето $\alpha \in l(\alpha) = l(\varepsilon\alpha_j) = L(\varepsilon) + l(\alpha_j) \subseteq L(\varepsilon) + \mathcal{U}_Q$.
Нека $\mathcal{U} = -v_Q + \mathcal{U}_Q$; ясно е, че множеството $\mathcal{U}$ е ограничено и се съдържа в H. Тъй като $H = -v_Q + H_Q$, то от (28) следва, че

$$H = \bigcup_{\varepsilon \in A^*} (L(\varepsilon) + \mathcal{U}).$$

Следователно рангът на решетката $L(A^*)$ е равен на $s + t - 1$, защото според Лема 16.5 рангът на $L(A^*)$ е равен на размерността на хипер–равнината H. □

Тъй като броят на единиците във всяка система от фундаментални единици на пръстена A е равен на ранга на решетката $L(A^*)$, то от Твърдение 16.1 и Твърдение 16.8 получаваме следното описание на групата от единиците на пръстена A:

Теорема 16.9 (Дирихле). *Съществуват единици $\varepsilon_1, \ldots, \varepsilon_{s+t-1} \in A^*$, такива че всяка единица $\varepsilon \in A^*$ има единствено представяне*

$$\varepsilon = \omega\varepsilon_1^{n_1} \cdots \varepsilon_{s+t-1}^{n_{s+t-1}},$$

където $n_1, \ldots, n_{s+t-1}$ са цели числа, а ω е корен на единицата.

Пример 16.10. Нека $D > 1$ е свободно от квадрати естествено число и E е реалното квадратично поле

$$\mathbb{Q}(\sqrt{D}) = \{x + y\sqrt{D} \colon x, y \in \mathbb{Q}\}.$$

Нека A е пръстенът на целите алгебрични числа в E.
Ако $\sigma : E \to \mathbb{C}$ е влагане на E в полето на комплексните числа, то от равенството

$$\sigma\big(\sqrt{D}\big)^2 = \sigma\big(\sqrt{D}^2\big) = \sigma(D) = D$$

следва, че $\sigma(\sqrt{D}) = \pm\sqrt{D}$. Тогава $\sigma(x + y\sqrt{D}) = a \pm b\sqrt{D}$, $x, y \in \mathbb{Q}$, което показва, че E има само реални влагания в полето на комплексните числа. Тъй като $s = 2$ и $t = 0$, то рангът на групата на единиците на A е равен на 1: съществува фундаментална единица $\varepsilon_1 \in A$, такава, че всяка единица $\varepsilon \in A$ се представя като $\varepsilon = \pm\varepsilon_1^n$ за някое $n \in \mathbb{Z}$.