Крайна породеност на пръстените на цели алгебрични числа

7. Локализация и цялозатвореност. Цялозатвореност на пръстените на цели алгебрични числа.

Дефиниция 7.1. Нека R е област с поле от частни K и нека $S \subset R$ е мултипликативно затворено подмножество на R. Пръстенът

$$R_S = \left\{ \frac{x}{s} \in K \ : \ x \in R, \ s \in S \right\}$$

се нарича локализация на R спрямо S.

Пример 7.1. Нека $\mathfrak{p}$ е прост идеал в R. Тогава множеството $S_{\mathfrak{p}} = R \setminus \mathfrak{p}$ е мултипликативно затворено. Локализацията на R спрямо $S_{\mathfrak{p}}$ се означава с $R_{\mathfrak{p}}$ и се нарича локализация на R спрямо $\mathfrak{p}$. Пръстенът $R_{\mathfrak{p}}$ е локален с максимален идеал

$$\mathfrak{p}R_{\mathfrak{p}} = \left\{ \frac{x}{s} \ : \ x \in \mathfrak{p}, \ s \in S \right\}.$$

Да отбележим, че полето $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ е изоморфно на полето от частни $k(\mathfrak{p})$ на областта $R/\mathfrak{p}$.

Твърдение 7.2. *Нека областта R е цяло разширение на областта T и нека S е мултипликативно затворено подмножество на T. Тогава локализацията R_S е цяло разширение на локализацията T_S.*

Доказателство. Нека $\frac{x}{s} \in R_S$. Тогава съществуват елементи $a_i \in T$, $i = 1, \dots, n$, такива че

$$x^n + \sum_{i=1}^{n} a_i x^{n-i} = 0. \tag{7.1}$$

След като умножим (7.1) с s^{-n}, получаваме равенството

$$\left(\frac{x}{s}\right)^n + \sum_{i=1}^{n} \frac{a_i}{s^i} \left(\frac{x}{s}\right)^{n-i} = 0,$$

което показва, че $\frac{x}{s}$ е цял над T_S. □

Твърдение 7.3. *Нека областта R е разширение на областта T и нека S е мултипликативно затворено подмножество на T. Да означим с $\widetilde{T}$ цялото затваряне на T в R. Тогава цялото затваряне на T_S в R_S съвпада с локализацията $\widetilde{T}_S$ на $\widetilde{T}$ спрямо S.*

Доказателство. От Твърдение 7.2 следва, че всеки елемент на $\widetilde{T}_S$ е цял над T_S. Обратно, нека $\frac{x}{s} \in R_S$ е цял над T_S. Тогава съществуват елементи $\frac{a_i}{s'} \in T_S$, $i = 1, \dots, n$, такива че

$$\left(\frac{x}{s}\right)^n + \sum_{i=1}^{n} \frac{a_i}{s'} \left(\frac{x}{s}\right)^{n-i} = 0. \tag{7.2}$$

След като умножим (7.1) с $s^n s'^n$, получаваме равенството

$$(s'x)^n + \sum_{i=1}^{n} (a_i s'^{n-1} s^i)\,(s'x)^{n-i} = 0,$$

което показва, че $s'x \in \widetilde{T}$. Следователно

$$\frac{x}{s} = \frac{s'x}{s's} \in \widetilde{T}_S. \qquad \square$$

Следствие 7.4. *Нека R е цялозатворен пръстен и S е мултипликативно затворено подмножество на R. Тогава локализацията R_S е също цялозатворен пръстен.*

Доказателство. Нека K е полето от частни на R. Според Твърдение 7.3, цялото затваряне на R_S в $K_S(=K)$ съвпада с $\widetilde{R}_S$, където $\widetilde{R}$ е цялото затваряне на R в K. Но $\widetilde{R} = R$, откъдето следва, че цялото затваряне на R_S в K е R_S. $\square$

Нека полето F е алгебрично разширение на полето $\mathbb{Q}$. Ще означаваме с D пръстена на всички цели алгебрични числа в F. Ясно е, че пръстенът D е цялото затваряне на пръстена на целите числа $\mathbb{Z}$ в полето F.

Лема 7.5. *За всяко алгебрично число $\beta \in F$ съществува цяло число $0 \neq s \in \mathbb{Z}$, такова че $s\beta \in D$.*

Доказателство. Тъй като β е алгебрично число, то съществуват рационални числа $a_i \in \mathbb{Q}$, $i = 1, \dots k$, такива че

$$\beta^k + \sum_{i=1}^{k} a_i \beta^{k-i} = 0. \tag{7.3}$$

Нека $s \in \mathbb{Z}$ е цяло число, такова че $sa_i \in \mathbb{Z}$, $i = 1, \dots, k$. След като умножим (7.3) с s^k, получаваме

$$(s\beta)^k + \sum_{i=1}^{k} s^i a_i\,(s\beta)^{k-i} = 0,$$

откъдето следва, че $s\beta \in D$. $\square$

Забележка 7.6. Използувайки Твърдение 7.3, можем да дадем следното "идейно" доказателство на Лема 7.5:
Нека $S = \mathbb{Z} \setminus \{0\} \subset \mathbb{Z}$. Тъй като цялото затваряне на $\mathbb{Z}$ в F е пръстенът D, то цялото затваряне на $\mathbb{Z}_S(=\mathbb{Q})$ в $F_S(=F)$ е пръстенът D_S. Но цялото затваряне на $\mathbb{Q}$ в F е очевидно F, откъдето $F = D_S$.

Твърдение 7.7. *Пръстенът D е цялозатворен.*

Доказателство. От Лема 7.5 следва, че полето от частни на D съвпада с F. Нека $\alpha \in F$ е цял над D. Тогава α е цял над $\mathbb{Z}$, защото $D[\alpha]$ е цяло разширение D и D е цяло разширение на $\mathbb{Z}$ (виж Теорема 6.2). Следователно $\alpha \in D$. $\square$

8. Норма и следа

Нека числовото поле E е крайно разширение на числовото поле K и нека $\alpha \in E$. Тогава изображението $\varphi_\alpha : E \to E$, зададено с формулата $\varphi_\alpha(x) = \alpha x$, $x \in E$, е K-линеен оператор.

Дефиниция 8.1. Следата $\operatorname{Tr}\varphi_\alpha \in K$ на линейния оператор φ_α се нарича *следа на елемента* α и се означава с $\operatorname{Tr}_K^E(\alpha)$. Детерминантата $\det\varphi_\alpha$ на линейния оператор φ_α се нарича *норма на елемента* α и се означава с $N_K^E(\alpha)$.

Лема 8.1. *Нека $\alpha \in E$ и нека $\alpha_i \in \mathbb{C}$, $i = 1, \dots, k$, са всички спрегнати елементи на α над полето K. Тогава*

$$N_E^K(\alpha) = \left(\prod_{i=1}^{k} \alpha_i\right)^{[E:K(\alpha)]} \tag{8.1}$$

$$\operatorname{Tr}_E^K(\alpha) = [E : K(\alpha)] \sum_{i=1}^{k} \alpha_i. \tag{8.2}$$

Доказателство. Да означим с E_α подполето $K(\alpha)$ на E и да забележим, че E_α е φ_α-инвариантно подпространство на E с базис $1, \alpha, \dots, \alpha^{k-1}$. Нека

$$g = X^k + \sum_{i=1}^{k} a_i X^{k-i} \in K[X]$$

е минималният полином на α над полето K. Тогава матрицата A на $\varphi_\alpha|_{E_\alpha}$ спрямо базиса $1, \alpha, \dots, \alpha^{k-1}$ е

$$A = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_k \\ 1 & 0 & 0 & \dots & 0 & -a_{k-1} \\ 0 & 1 & 0 & \dots & 0 & -a_{k-2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & -a_2 \\ 0 & 0 & 0 & \dots & 1 & -a_1 \end{pmatrix}.$$

Чрез непосредствено пресмятане се проверява, че

$$\det(\varphi_\alpha|_{E_\alpha}) = \det A = (-1)^k a_k = \prod_{i=1}^{k} \alpha_i,$$

$$\operatorname{Tr}(\varphi_\alpha|_{E_\alpha}) = \operatorname{Tr} A = -a_1 = \sum_{i=1}^{k} \alpha_i.$$

Нека e_j, $j = 1, \dots, l = [E : K(\alpha)]$ е базис на E над E_α. Да означим с E_j множеството $e_j E_\alpha$, $j = 1, \dots, l$ и да забележим, че всяко E_j е φ_α-инвариантно линейно подпространство на E с базис $e_j, e_j\alpha, \dots, e_j\alpha^{k-1}$. Тъй като елементите $e_j\alpha^i$, $i = 0, \dots, k-1$, $j = 1, \dots, l$, са линейно независими над K, то E е директна сума на подпространствата E_j, $j = 1, \dots, l$. Лесно се вижда, че матрицата на линейния оператор $\varphi_\alpha|_{E_j}$ спрямо базиса $e_j, e_j\alpha, \dots, e_j\alpha^{k-1}$ на E_j съвпада с матрицата A. От тук следва, че

$$\operatorname{Tr}(\varphi_\alpha|_{E_j}) = \operatorname{Tr}(\varphi_\alpha|_{E_\alpha}), \qquad \det(\varphi_\alpha|_{E_j}) = \det(\varphi_\alpha|_{E_\alpha}), \qquad j = 1, \dots, l.$$

Сега формули (8.1) и (8.2) следват от равенствата

$$\det \varphi_\alpha = \prod_{j=1}^{l} \det(\varphi_\alpha|_{E_j}), \qquad \operatorname{Tr} \varphi_\alpha = \sum_{j=1}^{l} \operatorname{Tr}(\varphi_\alpha|_{E_j}). \qquad \square$$

Следствие 8.2. *Нека числовото поле F е крайно разширение на полето $\mathbb{Q}$ и нека $\alpha \in F$ е цяло алгебрично число. Тогава $N_{\mathbb{Q}}^F(\alpha)$ и $\operatorname{Tr}_{\mathbb{Q}}^F(\alpha)$ са цели числа.*

Доказателство. Според Твърдение 1.7 минималният полином на α

$$g = X^k + \sum_{i=1}^{k} a_i X^{k-i}$$

има цели коефициенти. Остава да забележим (виж формули (8.1) и (8.2)), че

$$N_{\mathbb{Q}}^F(\alpha) = (-1)^{lk} (a_k)^l, \qquad \operatorname{Tr}_{\mathbb{Q}}^F(\alpha) = -la_1,$$

където $l = [F : \mathbb{Q}(\alpha)]$. $\square$

Дефиниция 8.2. Нека числовото поле E е разширение на числовото поле K. Ще казваме, че влагането $\sigma : E \to \mathbb{C}$ е *продължение* на влагането $\tau : K \to \mathbb{C}$ (или, че σ *продължава* τ), когато $\sigma|_K = \tau$.

Твърдение 8.3. *Нека числовото поле E е крайно разширение от степен n на числовото поле K, и нека $\tau : K \to \mathbb{C}$ е влагане на полето K в полето на комплексните числа $\mathbb{C}$. Тогава съществуват точно n различни влагания $\sigma_i : E \to \mathbb{C}$, $i = 1, \ldots, n$, които продължават τ.*

Доказателство. Нека $\alpha \in E$ е примитивен елемент на E над K (т.е. $E = K(\alpha)$) и нека $g = X^n + \sum_{i=1}^n a_i X^{n-i} \in K[X]$ е минималният полином на α над K. Да означим с $\tau(g)$ полинома $X^n + \sum_{i=1}^n \tau(a_i) X^{n-i} \in \tau(K)[X]$. Полиномът $\sigma(g)$ няма кратни корени, защото е неразложим над $\tau(K)[X]$. Нека $\beta_i \in \mathbb{C}$, $i = 1, \ldots, n$, са корените на $\tau(g)$. Ако $\sigma : E \to \mathbb{C}$ е продължение на τ, то $\sigma(\alpha)$ е корен на полинома $\tau(g)$, откъдето следва, че $\sigma(\alpha) = \beta_i$ за някой индекс $1 \leq i \leq n$. Нещо повече, за всеки индекс $i = 1, \ldots, n$, формулата

$$\sigma_i(e_0 + e_1\alpha + \cdots + e_{n-1}\alpha^{n-1}) = \tau(e_0) + \tau(e_1)\beta_i + \cdots + \tau(e_{n-1})\beta_i^{n-1},$$

задава влагане $\sigma_i : E \to \mathbb{C}$, което продължава τ. □

Твърдение 8.4. *Нека числовото поле E е крайно разширение на числовото поле K и нека $\sigma_i : E \to \mathbb{C}$, $i = 1, \ldots, n$, са всички различни продължения на тъждественото влагане* $\mathrm{id} : K \to \mathbb{C}$. *Тогава*

$$N_K^E(\alpha) = \prod_{i=1}^n \sigma_i(\alpha), \tag{8.3}$$

$$\mathrm{Tr}\,_K^E(\alpha) = \sum_{i=1}^n \sigma_i(\alpha), \tag{8.4}$$

за всеки елемент $\alpha \in E$.

Доказателство. Да отбележим, че елементът $\sigma_i(\alpha)$ е спрегнат с α над K, за всеки индекс $i = 1, \ldots, n$. В множеството $\{\sigma_1, \ldots, \sigma_n\}$ въвеждаме релация на еквивалентност по следния начин: $\sigma_i \sim \sigma_j \quad \Leftrightarrow \quad \sigma_i(\alpha) = \sigma_j(\alpha)$. Ясно е, че $\sigma_i \sim \sigma_j \quad \Leftrightarrow \quad \sigma_i|_{K(\alpha)} = \sigma_j|_{K(\alpha)}$. От Твърдение 8.3 следва, че всеки клас на еквивалентност съдържа точно $[E : K(\alpha)]$ влагания. Това показва, че дясната част на формули (8.3) и (8.4) е равна на дясната част на формули (8.1) и (8.2) съответно. □

Нека числовото поле F е крайно разширение на $\mathbb{Q}$. Да определим симетрична билинейна форма $\psi : F \times F \to \mathbb{Q}$ с формулата $\psi(\alpha, \beta) = \mathrm{Tr}\,_{\mathbb{Q}}^F(\alpha\beta)$, $\alpha, \beta \in F$. Ще покажем, че билинейната форма ψ е неизродена, като използваме една лема на Е. Артин. *Мултипликативен характер* от група G в поле K е всеки хомоморфизъм от G в мултипликативната група K^*.

Лема 8.5 (Е. Артин). *Ако $\chi_i : G \to K^*$, $i = 1, \ldots, n$, са различни мултипликативни характери от група G в поле K, то те са линейно независими над полето K.*

Доказателство. Ще докажем лемата с индукция по броя n на характерите χ_i. Лемата е вярна, когато $n = 1$, защото $\chi_1(e) = 1 \neq 0$. Да предположим, че лемата е доказана, когато броят на характерите е по-малък от n. Нека λ_i, $i = 1, \ldots, n$, са елементи на K, такива че

$$\lambda_1\chi_1(g) + \lambda_2\chi_2(g) + \cdots + \lambda_n\chi_n(g) = 0, \quad g \in G. \tag{8.5}$$

Тъй като $\chi_1 \neq \chi_2$, то съществува елемент $h \in G$, такъв че $\chi_1(h) \neq \chi_2(h)$. Заменяйки g с hg в (8.5), получаваме

$$\lambda_1\chi_1(h)\chi_1(g) + \lambda_2\chi_2(h)\chi_2(g) + \cdots + \lambda_n\chi_n(h)\chi_n(g) = 0, \quad g \in G. \tag{8.6}$$

Да умножим (8.5) с $\chi_1(h)$ и да го извадим от (8.6):

$$[\lambda_2\chi_2(h) - \lambda_2\chi_1(h)]\chi_2(g) + \cdots + [\lambda_n\chi_n(h) - \lambda_n\chi_1(h)]\chi_n(g) = 0, \quad g \in G.$$

Сега от индукционната хипотеза следва, че $\lambda_2\chi_2(h) - \lambda_2\chi_1(h) = 0$, откъдето $\lambda_2 = 0$. Прилагайки отново индукционната хипотеза за $\chi_1, \chi_3, \ldots, \chi_n$, получаваме $\lambda_1 = \lambda_3 = \ldots = \lambda_n = 0$. □

ТЕОРЕМА 8.6. *Нека полето F е крайно разширение на $\mathbb{Q}$. Тогава симетричната билинейна форма $\psi : F \times F \to \mathbb{Q}$, определена с формулата*

$$\psi(\alpha, \beta) = \operatorname{Tr}{}_{\mathbb{Q}}^{F}(\alpha\beta), \quad \alpha, \beta \in F,$$

е неизродена.

ДОКАЗАТЕЛСТВО. Нека α е елемент на F, такъв че $\operatorname{Tr}{}_{\mathbb{Q}}^{F}(\alpha\beta) = 0$, за всеки $\beta \in F$. Използувайки формула (8.4), получаваме

$$0 = \operatorname{Tr}{}_{\mathbb{Q}}^{F}(\alpha\beta) = \sum_{i=1}^{n} \sigma_i(\alpha\beta) = \sum_{i=1}^{n} \sigma_i(\alpha)\sigma_i(\beta), \quad \beta \in F, \tag{8.7}$$

където $\sigma_i : F \to \mathbb{C}$, $i = 1, \ldots, n$, са всички различни влагания на полето F в полето на комплексните числа $\mathbb{C}$. Сега да забележим, че $\sigma_i|_{F^*}$, $i = 1, \ldots, n$, е мултипликативен характер от групата F^* в полето $\mathbb{C}$. Затова от (8.7) и Лема 8.5 следва, че $\sigma_i(\alpha) = 0$, $i = 1, \ldots, n$, откъдето $\alpha = 0$. □

ДЕФИНИЦИЯ 8.3. Нека F е крайно разширение на $\mathbb{Q}$ и нека $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$. Детерминантата на матрицата G с коефициенти $g_{ij} = \psi(\alpha_i, \alpha_j)$, $1 \leq i, j \leq n$, се нарича *дискриминанта на* $\alpha_1, \alpha_2, \ldots, \alpha_n$ и се означава с $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

СЛЕДСТВИЕ 8.7. *Нека F е крайно разширение на $\mathbb{Q}$ от степен n. Елементите $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ образуват базис на F над $\mathbb{Q}$ тогава и само тогава, когато $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$.*

ДОКАЗАТЕЛСТВО. Нека $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Q}^n$ и нека

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n \in F.$$

Лесно се проверява, че

$$Gx = 0 \;\Leftrightarrow\; \psi(\alpha, \beta) = 0 \text{ за всеки } \beta \in F. \qquad □$$

ЗАДАЧА 8.8. Нека $F = \mathbb{Q}[\alpha]$, където $\alpha \in \mathbb{C}$ е алгебрично число с минимален полином $g \in \mathbb{Q}[x]$ от степен n. Да се докаже, че дискриминантата на елементите $1, \alpha, \ldots, \alpha^{n-1} \in F$ съвпада с дискриминантата на полинома g.

ТЕОРЕМА 8.9. *Нека полето F е крайно разширение на $\mathbb{Q}$. Тогава пръстенът D на целите алгебрични числа в F е свободна абелева група от ранг $n = [F : \mathbb{Q}]$. В частност, пръстенът D е ньотеров.*

ДОКАЗАТЕЛСТВО. От Лема 7.5 следва, че съществува базис f_j, $j = 1, \ldots, n$, на F над $\mathbb{Q}$, такъв че $f_j \in D$, $j = 1, \ldots, n$. Нека G е матрицата с коефициенти $g_{ij} = \psi(f_i, f_j)$, $1 \leq i, j \leq n$, и нека $\Delta = \det G$ е дискриминантата на $f_1, f_2, \ldots, f_n$. Коефициентите на G са цели числа, защото всички f_j, $j = 1, \ldots, n$, са цели алгебрични числа. От Следствие 8.7 знаем, че $\Delta \neq 0$. Ще покажем, че D се съдържа в абелевата група, породена от елементите $f'_j = \Delta^{-1} f_j$, $j = 1, \ldots, n$. Тъй като всяка подгрупа на свободна крайнопородена абелева група е също свободна крайнопородена абелева група, то от тук следва, че D е свободна крайнопородена абелева група.

Нека $\alpha \in D$ и нека x_j, $j = 1, \ldots, n$, са рационални числа, такива че

$$\sum_{j=1}^{n} x_j f_j = \alpha.$$

Тогава

$$\sum_{j=1}^{n} g_{ij}x_j = \psi(\alpha, f_i), \quad i = 1, \ldots, n. \tag{8.8}$$

Нека $x = (x_1, \ldots, x_n) \in \mathbb{Q}^n$ и нека $b = (\psi(\alpha, f_1), \ldots, \psi(\alpha, f_n)) \in \mathbb{Z}^n$. Уравнения (8.8) показват, че векторът x е решение на линейната система $Gx = b$. Умножавайки тази система отляво с присъединената матрица $\widetilde{G}$, получаваме $\Delta x = \widetilde{G}b$. Тъй като $\widetilde{G} \in M_{n\times n}(\mathbb{Z})$ и $b \in \mathbb{Z}^n$, то $\Delta x \in \mathbb{Z}^n$. Следователно

$$\alpha = \sum_{j=1}^{n} x_j f_j = \sum_{j=1}^{n} (\Delta x_j) f'_j \in \sum_{j=1}^{n} \mathbb{Z} f'_j.$$

Рангът на D е равен на n, защото D поражда n-мерното векторно пространство F над $\mathbb{Q}$ (виж Лема 7.5). За да завършим доказателството, нека забележим, че ако един пръстен е крайнопородена абелева група, то той е ньотеров. □

Задача 8.10. Нека D е пръстенът на целите алгебрични числа в едно крайно разширение F на $\mathbb{Q}$ и нека $\omega_1, \omega_2, \ldots, \omega_n$ и $\omega'_1, \omega'_2, \ldots, \omega'_n$ са два базиса на свободната абелева група D. Да се докаже, че

$$\Delta(\omega_1, \omega_2, \ldots, \omega_n) = \Delta(\omega'_1, \omega'_2, \ldots, \omega'_n).$$

Заключението на Задача 8.10 показва, че следващата дефиниция е коректна.

Дефиниция 8.4. Нека D е пръстенът на целите алгебрични числа в едно крайно разширение F на $\mathbb{Q}$ и нека $\omega_1, \omega_2, \ldots, \omega_n$ е базис на свободната абелева група D. Дискриминантата $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ на елементите $\omega_1, \omega_2, \ldots, \omega_n$ се нарича *дискриминанта на полето* F и се означава с δ_F.

Задача 8.11. Нека $g \in \mathbb{Z}[X]$ е неразложим над $\mathbb{Q}$ моничен полином от степен n и нека $\alpha \in \mathbb{C}$ е корен на g. Да се докаже, че ако дискриминантата на полинома g е свободна от квадрати, то елементите $1, \alpha, \ldots, \alpha^{n-1}$ образуват базис на пръстена D на целите алгебрични числа в полето $F = \mathbb{Q}(\alpha)$. В този случай дискриминантата δ_F на полето F съвпада с дискриминантата на полинома g.

Задача 8.12. Нека цялото число d е свободно от квадрати и нека D е пръстенът на целите алгебрични числа в квадратичното разширение $F = \mathbb{Q}(\sqrt{d})$. Да се докаже, че

$$D = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & \text{когато } d \equiv 2, 3 \mod 4, \\ \mathbb{Z} + \mathbb{Z}\,\dfrac{-1+\sqrt{d}}{2} & \text{когато } d \equiv 1 \mod 4. \end{cases}$$

Задача 8.13. Нека цялото число d е свободно от квадрати и нека $F = \mathbb{Q}(\sqrt{d})$. Да се докаже, че

$$\delta_F = \begin{cases} 4d & \text{когато } d \equiv 2, 3 \mod 4, \\ d & \text{когато } d \equiv 1 \mod 4. \end{cases}$$