Пръстен на целите алгебрични числа в крайно разширение

3. Цели алгебрични числа в квадратично разширение на полето на рационалните числа

Ако цялото число D не се дели на квадрат на просто число, ще казваме, че D е *свободно от квадрати*. За всяко разширение E от втора степен на полето на рационалните числа съществува единствено свободно от квадрати цяло число D, такова че $E = \mathbb{Q}(\sqrt{D})$.
Нека цялото число D е свободно от квадрати и нека A е пръстенът на целите алгебрични числа в квадратичното разширение $E = \mathbb{Q}(\sqrt{D})$.

Твърдение 3.1. *Пръстенът A е свободна абелева група от ранг 2. Целите алгебрични числа $1, \sqrt{D}$ са базис на A, ако $D \equiv 2 \mod 4$ или $D \equiv 3 \mod 4$. Ако $D \equiv 1 \mod 4$, целите алгебрични числа $1, 1/2 + \sqrt{D}/2$ са базис на A.*

Доказателство. Нека $\alpha = a + b\sqrt{D} \in E$, $a, b \in \mathbb{Q}$, е цяло алгебрично число. Ако $b = 0$, то $a \in \mathbb{Q}$ е цяло алгебрично число, откъдето следва, че a е цяло число. Ако $b \neq 0$, минималният полином f на α е

$$f = (x - a - b\sqrt{D})(x - a + b\sqrt{D}) = x^2 - 2ax + a^2 - Db^2,$$

откъдето $2a$ и $a^2 - Db^2$ са цели числа. Тогава $D(2b)^2 = (2a)^2 - 4(a^2 - Db^2)$ също е цяло число и тъй като D е свободно от квадрати, то $(2b)^2$ е цяло число, което е възможно само когато числото $2b$ е цяло. Следователно $2a$ и $2b$ са цели числа и цялото число $(2a)^2 - D(2b)^2 = 4(a^2 - Db^2)$ се дели на 4, т.е

$$(2a)^2 \equiv D(2b)^2 \mod 4. \tag{1}$$

Ако $D \equiv 2 \mod 4$ или $D \equiv 3 \mod 4$, от (1) следва, че целите числа $2a$ и $2b$ се делят на 2, откъдето a и b са цели числа и $1, \sqrt{D}$ е базис на A.
Ако $D \equiv 1 \mod 4$, от (1) следва, че $2a \equiv 2b \mod 2$ и $a - b$ е винаги цяло число. Да забележим, че в този случай $1/2 + \sqrt{D}/2$ е цяло алгебрично число, защото неговият минимален полином $f = x^2 - x + (1 - D)/4$ има цели коефициенти. Освен това

$$\alpha = a + b\sqrt{D} = (a - b) \cdot 1 + (2b) \cdot (1/2 + \sqrt{D}/2),$$

откъдето следва, че $1, 1/2 + \sqrt{D}/2$ е базис на A. □

4. Цели алгебрични числа в крайно разширение на полето на рационалните числа

Нека E е крайно разширение на полето $\mathbb{Q}$ от степен $[E : \mathbb{Q}] = n$. Ще покажем, че пръстенът A на целите алгебрични числа в E е свободна абелева група от ранг n. Според теоремата за примитивния елемент, съществува алгебрично число $\alpha \in E$, такова че $E = \mathbb{Q}(\alpha)$. Следващата лема показва, че съществува *цяло* алгебрично число $\alpha \in E$, такова че $E = \mathbb{Q}(\alpha)$.

Лема 4.1. *За всяко алгебрично число α съществува цяло число $0 \neq n \in \mathbb{Z}$, такова че $n\alpha$ е цяло алгебрично число.*

Доказателство. Алгебричното число α е корен на полином с цели коефициенти:

$$a_0\alpha^k + a_1\alpha^{k-1} + \cdots + a_{k-1}\alpha + a_k = 0, \qquad a_0, a_1, \ldots, a_{k-1}, a_k \in \mathbb{Z}.$$

Нека $n = a_0$. Умножавайки горното равенство с n^{k-1} получаваме

$$(n\alpha)^k + a_1(n\alpha)^{k-1} + \cdots + a_{k-1}n^{k-2}(n\alpha) + a_k n^{k-1} = 0,$$

откъдето следва, че $n\alpha$ е цяло алгебрично число. □

Тъй като $\mathbb{Q}(\alpha) = \mathbb{Q}(n\alpha)$ за всяко цяло число $n \neq 0$, ние ще предполагаме, че $E = \mathbb{Q}(\alpha)$, където α е цяло алгебрично число. Нека

$$f = (x - \alpha_1)\cdots(x - \alpha_n) \in \mathbb{Z}[x]$$

е минималният полином на $\alpha = \alpha_1$. Ясно е, че всички спрегнати с α числа $\alpha_1, \ldots, \alpha_n$ са също цели алгебрични. Нека $E_i = \mathbb{Q}(\alpha_i)$, $i = 1, \ldots, n$. Тогава $1, \alpha_i, \ldots, \alpha_i^{n-1}$ е базис на E_i над $\mathbb{Q}$.

Лема 4.2. *Изображението $\sigma_i : E \to E_i$, зададено с*

$$\sigma_i(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\alpha_i + \cdots + c_{n-1}\alpha_i^{n-1},$$

е изоморфизъм на полета за всяко $i = 1, \ldots, n$.

Доказателство. Нека $\varphi_i : \mathbb{Q}[x] \to E_i$ е хомоморфизмът на пръстени, зададен с $\varphi(g) = g(\alpha_i)$, $g \in \mathbb{Q}[x]$. Тогава $\ker\varphi_i = (f)$ φ_i и според теоремата за хомоморфизмите φ_i индуцира изоморфизъм на полета $\psi_i : \mathbb{Q}[x]/(f) \to E_i$. Тъй като като $\psi_i = \sigma_i\psi_1$, то $\sigma_i = \psi_i\psi_1^{-1}$ е изоморфизъм на полета. □

Забележете, че от дефиницията на σ_i следва, че $\sigma_i|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$, $i = 1, \ldots, n$.

Лема 4.3. *Нека $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} \in E$ е цяло алгебрично число. Тогава $\beta_i = b_0 + b_1\alpha_i + \cdots + b_{n-1}\alpha_i^{n-1} \in E_i$ също е цяло алгебрично число.*

Доказателство. Нека $a_1, \ldots, a_k$ са цели числа, такива че

$$\beta^k + a_1\beta^{k-1} + \cdots + a_{k-1}\beta + a_k = 0.$$

Тогава

$$\sigma_i(\beta^k + a_1\beta^{k-1} + \cdots + a_{k-1}\beta + a_k) = \sigma_i(\beta)^k + a_1\sigma_i(\beta)^{k-1} + \cdots + a_{k-1}\sigma_i(\beta) + a_k = 0,$$

т.е. $\sigma_i(\beta) = \beta_i = b_0 + b_1\alpha_i + \cdots + b_{n-1}\alpha_i^{n-1}$ е цяло алгебрично число. □

Лема 4.4. *Нека $D \in \mathbb{Z}$ е дискриминантата на минималния полином на α. Ако $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} \in E$ е цяло алгебрично число, то $Db_0, Db_1, \ldots, Db_{n-1}$ са цели числа.*

Доказателство. Нека $\beta_i = b_0 + b_1\alpha_i + \cdots + b_{n-1}\alpha_i^{n-1}$, $i = 1, \ldots, n$. Прилагайки формулите на Крамер към линейната система

$$b_0 + \alpha_i b_1 + \cdots + \alpha_i^{n-1} b_{n-1} = \beta_i, \quad i = 1, \ldots, n,$$

получаваме $b_i = \Delta_i/\Delta$, $i = 0, \ldots, n-1$, където

$$\Delta_i = \det\begin{pmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{i-1} & \beta_1 & \alpha_1^{i+1} & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \ldots & \alpha_2^{i-1} & \beta_2 & \alpha_2^{i+1} & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \ldots & \alpha_n^{i-1} & \beta_n & \alpha_n^{i+1} & \ldots & \alpha_n^{n-1} \end{pmatrix},$$

$$\Delta = W(\alpha_1, \alpha_2, \ldots, \alpha_n) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j).$$

Следователно $Db_i = \Delta\Delta_i$, $i = 0, \ldots, n-1$, защото $D = \Delta^2$. Тъй като $\alpha_1, \ldots, \alpha_n$ и $\beta_1, \ldots, \beta_n$ са цели алгебрични числа, то Db_i, $i = 0, \ldots, n-1$, също са цели алгебрични числа. Но Db_i, $i = 0, \ldots, n-1$, са рационални числа, откъдето следва, че $Db_i \in \mathbb{Z}$, $i = 0, \ldots, n-1$. □

ТЕОРЕМА 4.5. *Пръстенът A на целите алгебрични числа в $E = \mathbb{Q}(\alpha)$ е свободна абелева група от ранг $n = [E : \mathbb{Q}]$.*

ДОКАЗАТЕЛСТВО. Според предишната лема пръстенът A е подгрупа на крайнопородената абелева група $\mathbb{Z} \cdot D^{-1} + \mathbb{Z} \cdot \alpha D^{-1} + \cdots + \mathbb{Z} \cdot \alpha^{n-1} D^{-1}$. Следователно A е крайнопородена абелева група, а тъй като A очевидно няма торзионни елементи, то A е свободна абелева група от краен ранг. Освен това, всеки базис на A над $\mathbb{Z}$ е също така базис на E над $\mathbb{Q}$, откъдето следва, че рангът на A е точно $n = [E : \mathbb{Q}]$. □