Цели елементи и цели разширения

1. Цели елементи

Ще разглеждаме комутативни пръстени с неутрален елемент. Ако пръстенът R е подпръстен на пръстена S, ще предполагаме, че неутралният елемент 1_R на R съвпада с неутралния елемент 1_S на S. В този случай пръстенът S има естествена структура на R-модул и ние ще казваме, че пръстенът S е *разширение* на пръстена R.

Дефиниция 1.1 (Цели елементи). Нека пръстенът S е разширение на пръстена R. Един елемент $\alpha \in S$ е *цял* над R, когато съществува полином $f \in R[x]$ със старши коефициент, равен на 1, такъв че $f(\alpha) = 0$.

Ако $\alpha \in S$ е цял над R, пръстенът $R[\alpha] = \{\, g(\alpha) : g \in R[x]\,\}$ е крайнопороден R-модул. Наистина, тогава за всеки $g \in R[x]$ съществуват $q, r \in R[x]$, такива че

$$g = qf + r,\ \deg r < \deg f = k,\ \text{и тъй като } g(\alpha) = q(\alpha)\underbrace{f(\alpha)}_{0} + r(\alpha) = r(\alpha),$$

елементите $1, \alpha, \dots, \alpha^{k-1}$ пораждат пръстена $R[\alpha]$ като R-модул. Обратно, ако $R[\alpha]$ е крайнопороден R-модул, то както показва следващото твърдение, елементът α е цял над R.

Твърдение 1.1. *Нека пръстенът S е разширение на пръстена R. Ако S е крайнопороден R-модул, всеки елемент $\alpha \in S$ е цял над R.*

Доказателство. Нека $x_1, x_2, \dots, x_n \in S$ пораждат S като R-модул и нека $\alpha \in S$. Тогава съществуват $a_{ij} \in R$, $1 \le i, j \le n$, такива че

$$\begin{array}{l} \alpha x_1 = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ \alpha x_2 = a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \dotfill \\ \alpha x_n = a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \end{array}.$$

Нека

$$A = \begin{pmatrix} a_{11} - \alpha & a_{11} & \dots & a_{1n} \\ a_{21} & a_{22} - \alpha & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} - \alpha \end{pmatrix} \in M_n(S),\ X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in M_{n1}(S).$$

Тогава $AX = 0$ и умножавайки отляво с адюнгираната матрица $\widetilde{A} \in M_n(S)$ на A, получаваме $\det(A)X = 0$. Следователно $\det(A)x_i = 0$, $i = 1\dots, n$, откъдето следва, че $\det(A)x = 0$ за всеки $x \in S$. В частност $\det(A)\cdot 1 = 0$, т.е. $\det(A) = 0$. Остава да забележим, че $\det(A)$ е полином на α със старши коефициент ± 1 и коефициенти в R. □

Лема 1.2. *Нека пръстенът S е разширение на пръстена R и нека пръстенът T е разширение на пръстена S. Ако S е крайнопороден R-модул и T е крайнопороден S-модул, то T е крайнопороден R-модул.*

Доказателство. Нека $x_i \in S$, $i = 1, \ldots, n$, пораждат S като R-модул и нека $y_j \in T$, $j = 1, \ldots, m$, пораждат T като S-модул. Тогава $x_i y_j \in T$, $i = 1, \ldots, n$, $j = 1, \ldots, m$, пораждат пръстена T като R-модул. □

Следствие 1. *Нека пръстенът S е разширение на пръстена R. Елементите $\alpha_1, \ldots, \alpha_k \in S$ са цели над R тогава и само тогава, когато пръстенът $R[\alpha_1, \ldots, \alpha_k]$ е крайнопороден R-модул.*

Доказателство. Ако пръстенът $R[\alpha_1, \ldots, \alpha_k]$ е крайнопороден R-модул, то елементите $\alpha_1, \ldots, \alpha_k \in R[\alpha_1, \ldots, \alpha_k]$ са цели над R според Твърдение 1.1. Обратно, нека $\alpha_1, \ldots, \alpha_k \in S$ са цели елементи над R и нека $S_i = R[\alpha_1, \ldots, \alpha_i]$, $i = 1, \ldots, k$. Тогава α_i е цял над S_{i-1} и тъй като $S_i = S_{i-1}[\alpha_i]$, пръстенът S_i е крайнопороден S_{i-1}-модул, $i = 1, \ldots, k$. Сега от Лема 1.2 следва, че всеки от пръстените S_i, $i = 1, \ldots, k$, е крайнопороден R-модул. В частност $S_k = R[\alpha_1, \ldots, \alpha_k]$ е крайнопороден R-модул. □

Ако пръстенът S е разширение на пръстена R и $\alpha, \beta \in S$, то $\alpha + \beta, \alpha\beta \in R[\alpha, \beta]$. Ако α и β са цели над R, то $R[\alpha, \beta]$ е крайнопороден R-модул и всеки елемент на $R[\alpha, \beta]$ е цял над R, откъдето в частност следва, че $\alpha + \beta$ и $\alpha\beta$ са също цели елементи. *Следователно множеството $\widetilde{R}$ от всички елементи на S, които са цели над R, е подпръстен на S.* Пръстенът $\widetilde{R}$ се нарича *цяло затваряне* на R в S. Ясно е, че $\widetilde{R} \supseteq R$.

Нека R е област с поле от частни K и нека $\widetilde{R}$ е цялото затваряне на R в K.

Дефиниция 1.2 (Целозатворен пръстен). Областта R се нарича *целозатворен* пръстен, когато $\widetilde{R} = R$.

Следващото твърдение показва, че пръстенът на целите числа е целозатворен.

Твърдение 1.3. *Всеки факториален пръстен е целозатворен.*

Доказателство. Нека елементът $\alpha = \dfrac{p}{q} \in K$, $p, q \in R$, е цял над R. Без ограничение на общността можем да предполагаме, че p и q са взаимно прости елементи на R. Тогава съществуват $a_1, \ldots, a_n \in R$, такива че

$$\left(\frac{p}{q}\right)^n + a_1 \left(\frac{p}{q}\right)^{n-1} + \cdots + a_n = 0,$$

откъдето

$$p^n = -q(a_1 p^{n-1} + \cdots + a_n q^{n-1}).$$

Следователно q дели p^n, откъдето следва, че q е обратим елемент на R, защото p и q са взаимно прости. Тъй като q е обратим в R, то $\alpha = \dfrac{p}{q} \in R$. □

От Твърдение 1.3 следва, че всяко рационално число, което е цяло над пръстена $\mathbb{Z}$ на целите числа, е цяло число.

2. Цели разширения

Нека пръстенът S е разширение на пръстена R.

Дефиниция 2.1. Казваме, че пръстенът S е *цяло разширение* на пръстена R, когато всеки елемент $\alpha \in S$ е цял над R.

Твърдение 2.1 (Транзитивност на целите разширения). *Нека пръстенът S е разширение на пръстена R и нека пръстенът T е разширение на пръстена S. Тогава T е цяло разширение на R тогава и само тогава, когато T е цяло разширение на S и S е цяло разширение на R.*

Доказателство. Ако T е цяло разширение на R, то от определението на цяло разширение следва, че T е цяло разширение на S и S е цяло разширение на R. Обратно, нека T е цяло разширение на S, S е цяло разширение на R и нека $\alpha \in T$. Тогава съществува полином $f = x^n + a_1 x^{n-1} + \cdots + a_n \in S[x]$, такъв че $f(\alpha) = 0$. Тъй като α е цял над пръстена $R[a_1, \ldots, a_n]$, то $R[a_1, \ldots, a_n, \alpha]$ е крайнопороден $R[a_1, \ldots, a_n]$-модул, а тъй като елементите $a_1, \ldots, a_n$ са цели над R, то $R[a_1, \ldots, a_n]$ е крайнопороден R-модул (Следствие 1). Следователно (виж Лема 1.2) $R[a_1, \ldots, a_n, \alpha]$ е крайнопороден R-модул, откъдето следва, че α е цял над R, според Следствие 1. □

Твърдение 2.2. *Ако полето E е цяло разширение на пръстена k, то k е поле.*

Доказателство. Нека $0 \neq \alpha \in k$ и нека $\alpha^{-1} \in E$ е обратният елемент на α. Ще покажем, че $\alpha^{-1} \in k$. Тъй като E е цяло разширение на k, съществуват $a_1, a_2, \ldots, a_n \in R$, такива че

$$(\alpha^{-1})^n + a_1(\alpha^{-1})^{n-1} + a_2(\alpha^{-1})^{n-2} + \cdots + a_n = 0,$$

откъдето $\alpha^{-1} = -(a_1 + a_2\alpha + \cdots + a_n\alpha^{n-1}) \in R$. □

Твърдение 2.3. *Ако областта E е цяло разширение на полето k, то E е поле.*

Доказателство. Нека $0 \neq \alpha \in E$. Тогава пръстенът $k[\alpha]$ е *крайномерно* линейно пространство над k и изображението $\varphi : k[\alpha] \to k[\alpha]$, зададено с $\varphi(x) = \alpha x$, $x \in k[\alpha]$, е линеен оператор в *крайномерно* линейно пространство. Ако $\varphi(x) = 0$, то $x = 0$, защото E е област. Следователно $\operatorname{Ker}\varphi = \{0\}$, откъдето $\operatorname{Im}\varphi = k[\alpha]$. В частност, съществува $x \in k[\alpha]$, такъв че $\varphi(x) = 1$, т.е. $\alpha x = 1$. □

Следствие 2.4. *Ако пръстенът S е цяло разширение на пръстена R и P е прост идеал в S, то простият идеал $\mathfrak{p} = P \cap R$ е максимален в R точно когато P е максимален в S.*

Доказателство. Ограничението на хомоморфизма на факторизация $S \to S/P$ върху R индуцира влагане на пръстени $R/\mathfrak{p} \hookrightarrow S/P$, което е цяло разширение. Тогава, според Твърдения 2.2 и 2.3, областта S/P е поле точно когато $R/\mathfrak{p}$ е поле. □

Твърдение 2.5. *Нека областта S е цяло разширение на областта R и нека $J \neq (0)$ е идеал в S. Тогава $R \cap J \neq (0)$.*

Доказателство. Нека $0 \neq \alpha \in J$. Тогава съществуват елементи $a_1, \ldots, a_n \in R$, такива че $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$. Без ограничение на общността можем да предполагаме, че $a_n \neq 0$, защото S е област и $\alpha \neq 0$. Тогава

$$R \ni a_n = -(\alpha^{n-1} + a_1\alpha^{n-2} + \cdots + a_{n-1})\alpha \in J.$$

Следователно $0 \neq a_n \in R \cap J$. □