

Цялозатворени пръстени. Цели разширения на пръстени.

5. Цяло затваряне. Цялозатворени пръстени.

ДЕФИНИЦИЯ 5.1. Нека пръстенът R е разширение на пръстена S . Множеството

$$\tilde{S} = \{\alpha \in R : \alpha \text{ е цял над } S\}$$

се нарича *цяло затваряне на S в R* .

ЗАБЕЛЕЖКА 5.1. Ясно е, че $S \subset \tilde{S}$,

ПРИМЕР 5.2. Цялото затваряне на пръстена на целите числа \mathbb{Z} в полето на комплексните числа \mathbb{C} е пръстенът на целите алгебрични числа.

ПРИМЕР 5.3. Цялото затваряне на пръстена на целите числа \mathbb{Z} в полето $\mathbb{Q}[i]$ е пръстенът на целите гаусови числа $\mathbb{Z}[i]$.

ТЕОРЕМА 5.4. Нека пръстенът R е разширение на пръстена S . Цялото затваряне \tilde{S} на S в R е подпръстен на R .

ДОКАЗАТЕЛСТВО. Нека $\alpha, \beta \in \tilde{S}$, т.е. α и β са цели над S . Според Твърдение 4.7 всеки елемент на пръстена $S[\alpha, \beta]$ е цял над S . Тъй като $\alpha + \beta, \alpha\beta \in S[\alpha, \beta]$, то елементите $\alpha + \beta$ и $\alpha\beta$ също са цели над S . Следователно $\alpha + \beta, \alpha\beta \in \tilde{S}$. \square

ДЕФИНИЦИЯ 5.2. Нека пръстенът R е разширение на пръстена S . Казваме, че S е *цялозатворен* в R , когато $\tilde{S} = S$.

ДЕФИНИЦИЯ 5.3. Казваме, че пръстенът R е *цялозатворен*, когато R е област и R е цялозатворен в своето поле от частни.

ТВЪРДЕНИЕ 5.5. Всеки факториален пръстен е цялозатворен.

ДОКАЗАТЕЛСТВО. Нека R е факториален пръстен с поле от частни K . Тогава всеки елемент $\alpha \in K$ се представя като

$$\alpha = \frac{a}{b}, \quad a, b \in R,$$

където a и b са взаимно прости елементи на R . Ако α е цял над R , то съществува моничен полином f с коефициенти в R ,

$$f = X^n + a_1X^{n-1} + \dots + a_{n-1}X + a_n \in R[x],$$

такъв че $f(\alpha) = 0$. Тогава

$$\begin{aligned} a^n &= -(a_1a^{n-1}b + \dots + a_{n-1}ab^{n-1} + a_nb^n) \\ &= -b(a_1a^{n-1} + \dots + a_{n-1}ab^{n-2} + a_nb^{n-1}). \end{aligned} \quad (5.1)$$

От (5.1) следва, че b дели a^n . Тъй като a^n и b са взаимно прости, то b е обратим елемент (единица) на R . Следователно $\alpha \in R$. \square

ПРИМЕР 5.6. Нека $U \neq \emptyset$ е свързано отворено подмножество на \mathbb{C} . Ще означаваме с $\mathcal{O}(U)$ пръстена на всички холоморфни функции в U . От свързаността на U следва, че $\mathcal{O}(U)$ е област. Нека $K(U)$ е полето от частни на $\mathcal{O}(U)$. Ясно е, че $K(U)$ е подполе на полето $\mathcal{M}(U)$ на всички мероморфни функции в U . От теоремата на Вайерщрас ([1], Теорема 15.11) следва, че $K(U)$ съвпада с $\mathcal{M}(U)$ ([1], Теорема 15.12).

Нека се убедим, че пръстенът $\mathcal{O}(U)$ не е факториален. Лесно се вижда, че неразложимите елементи в пръстена $\mathcal{O}(U)$ са холоморфните функции от вида $p(z) = u(z)(z - z_0)$, $z_0 \in U$, където $u(z)$ е обратима холоморфна функция в U . Нека $\{z_n\}_{n \in \mathbb{N}} \subset U$ е безкрайно множество от комплексни числа, което няма точка на съгъстяване в U . Според теоремата на Вайерщрас, съществува холоморфна функция $0 \neq f(z) \in \mathcal{O}(U)$, такава че $f(z_n) = 0$, $n \in \mathbb{N}$. Тъй като $f(z)$ не може да се представи като крайно произведение на неразложими елементи на $\mathcal{O}(U)$, то $\mathcal{O}(U)$ не е факториален пръстен.

Сега ще докажем, че пръстенът $\mathcal{O}(U)$ е цялозатворен. Нека $h \in \mathcal{M}(U)$ е мероморфна функция, такава че

$$h^n + a_1 h^{n-1} + \dots + a_n = 0, \quad (5.2)$$

където $a_1, \dots, a_n \in \mathcal{O}(U)$ са холоморфни функции. Да предположим, че h има полюс от ред $k > 0$ в точката $z_0 \in U$. Тогава редът на полюса на мероморфната функция $a_1 h^{n-1} + \dots + a_n$ в точката z_0 е най-много $(n-1)k$. От тук следва, че мероморфната функция $h^n + a_1 h^{n-1} + \dots + a_n$ има полюс от ред nk в точката z_0 , което очевидно противоречи на (5.2). Полученото противоречие показва, че h няма полюси в U , т.е. $h \in \mathcal{O}(U)$.

Ще използваме основната идея на Пример 5.6, за да дадем друго доказателство на Твърдение 5.5. Нека K е полето от частни на факториалния пръстен R и нека $p \in R$ е неразложим елемент. Тогава за всеки елемент $x \in K^*$ съществува представяне

$$x = \frac{a}{b} p^v, \quad a, b \in R \setminus \{0\}, v \in \mathbb{Z}, \quad (5.3)$$

такова че p не дели нито a , нито b . Нещо повече, ако

$$x = \frac{a'}{b'} p^{v'}, \quad a', b' \in R \setminus \{0\}, v' \in \mathbb{Z}, \quad (5.4)$$

е друго такова представяне, то $v = v'$. Наистина, без ограничение на общността можем да предполагаме, че $v' \geq v$. Тогава от (5.3) и (5.4) получаваме

$$p^{v'-v} a' b = a b'. \quad (5.5)$$

Тъй като p не дели нито a , нито b' , то от (5.5) следва, че $v = v'$. Това показва, че изображението $v_p : K^* \rightarrow \mathbb{Z}$, дефинирано с формулата $v_p(x) = v$, $x \in K^*$, е коректно определено. Ние ще разширим изображението v_p до изображение от K в $\mathbb{Z} \cup \{\infty\}$, като положим $v_p(0) = \infty$. Не е трудно да се провери, че така дефинираното изображение $v_p : K \rightarrow \mathbb{Z} \cup \{\infty\}$ има следните свойства:

- (i) $v_p(xy) = v_p(x) + v_p(y)$;
- (ii) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$;
- (iii) $v_p(x) = \infty \Leftrightarrow x = 0$;
- (iv) $v_p(x) \geq 0$ за всеки $x \in R$.

В следващата лема са формулирани няколко следствия от (i) - (iv).

ЛЕМА 5.7. Нека R е факториален пръстен с поле от частни K и нека p е неразложим елемент в R . Тогава:

- (i) $v_p(x^{-1}) = -v_p(x)$ за всеки $x \in K^*$; $v_p(u) = 0$ за всеки $u \in R^*$;

(ii) ако $x \in R$, то p^v дели $x \Leftrightarrow v_p(x) \geq v$;

(iii) ако x, y са елементи на K , такива че $v_p(x) \neq v_p(y)$, то

$$v_p(x + y) = \min\{v_p(x), v_p(y)\};$$

ДОКАЗАТЕЛСТВО. (i) От $v_p(1 \cdot 1) = v_p(1) + v_p(1)$ следва, че $v_p(1) = 0$. Тъй като $v_p(x^{-1}x) = v_p(1) = 0$, то $v_p(x^{-1}) = -v_p(x)$. Нека $u \in R^*$. Тогава съществува $u' \in R^*$, такъв че $uu' = 1$. Тъй като $v_p(u) + v_p(u') = v_p(1) = 0$ и $v_p(u) \geq 0$, $v_p(u') \geq 0$, то $v_p(u) = 0$.

(ii) Ако $x \in R$ се дели на p^v , то $x = p^v a$ за някой $a \in R$. Следователно $v_p(x) = v_p(p^v) + v_p(a) \geq v$, защото $v_p(a) \geq 0$ за всеки $a \in R$. Обратно, нека $x \in R$ и $v_p(x) \geq v$. Да представим x като $x = p^{v'} a$, където $a \in R$ и p не дели a . Тогава $v' = v_p(x) \geq v$, откъдето следва, че p^v дели a .

(iii) Можем да предполагаме без ограничение на общността, че $v_p(y) > v_p(x)$. Тогава

$$v_p(y) > v_p(x) = v_p(x + y - y) \geq \min\{v_p(x + y), v_p(-y)\} = \min\{v_p(x + y), v_p(y)\}.$$

Следователно $\min\{v_p(x + y), v_p(y)\} = v_p(x + y)$, откъдето $v_p(x) \geq v_p(x + y)$. Тъй като $v_p(x + y) \geq \min\{v_p(x), v_p(y)\} = v_p(x)$, то $v_p(x + y) = v_p(x)$. Окончателно $v_p(x + y) = v_p(x) = \min\{v_p(x), v_p(y)\}$. \square

Ако R е факториален пръстен и $x \in R$, то $v_p(x) \geq 0$ за всеки неразложим елемент $p \in R$. Обратното твърдение също е вярно:

ЛЕМА 5.8. Нека R е факториален пръстен с поле от частни K . Ако за елемента $x \in K$ е вярно, че $v_p(x) \geq 0$ за всеки неразложим елемент $p \in R$, то $x \in R$.

ДОКАЗАТЕЛСТВО. Нека $v_p(x) \geq 0$ за всеки неразложим елемент $p \in R$. Да представим x като

$$x = \frac{a}{b}, \quad a \in R, \quad b \in R \setminus \{0\}.$$

Нека $b = u \prod_{i=1}^r p_i$, $u \in R^*$ и $p_i, i = 1, \dots, r$, са неразложими елементи в R . Ще докажем, че $x \in R$, като използваме индукция по броя r на неразложимите делители на b . Ако $r = 0$, то b е обратим в R и $x \in R$. Нека $r \geq 1$. Да предположим, че твърдението е доказано за всички елементи

$$x' = \frac{a'}{b'}, \quad a' \in R, \quad b' \in R \setminus \{0\},$$

такива че $b' = u' \prod_{i=1}^s p'_i$, $s < r$, $u' \in R^*$ и $p'_i, i = 1, \dots, s$, са неразложими елементи в R . От $v_{p_1}(b) > 0$ и $v_{p_1}(a) - v_{p_1}(b) = v_{p_1}(x) \geq 0$ следва, че $v_{p_1}(a) \geq 1$. Тогава съществува елемент $a' \in R$, такъв че $a = p_1 a'$. Нека $b' = u \prod_{i=2}^r p_i$. Сега $x = \frac{a'}{b'}$ и броят на неразложимите делители на b' е $r - 1$. Следователно $x \in R$ според индукционната хипотеза. \square

Второ доказателство на Твърдение 5.5. Достатъчно е да докажем, че ако елементът $\alpha \in K$ е цял над R , то $v_p(\alpha) \geq 0$ за всеки неразложим елемент в $p \in R$ (виж Лема 5.8). Нека a_1, \dots, a_n са елементи на R , такива че

$$\alpha^n + a_1 \alpha^{n-1} + \dots + a_n = 0. \quad (5.6)$$

Да предположим, че $v_p(\alpha) = k < 0$ за някой неразложим елемент $p \in R$. Тъй като

$$v_p(a_1 \alpha^{n-1} + \dots + a_n) \geq \min\{v_p(a_1 \alpha^{n-1}), \dots, v_p(a_n)\} \geq (n-1)k,$$

то $v_p(\alpha^n) = nk < v_p(a_1 \alpha^{n-1} + \dots + a_n)$. Сега от Лема 5.7 (iii) следва, че

$$v_p(\alpha^n + a_1 \alpha^{n-1} + \dots + a_n) = \min\{v_p(\alpha^n), v_p(a_1 \alpha^{n-1} + \dots + a_n)\} = nk,$$

което очевидно противоречи на (5.6). \square

6. Цели разширения на пръстени

Дефиниция. Казваме, че разширението R на пръстена S е *цяло разширение* на S , когато всеки елемент на R е цял над S .

ЗАБЕЛЕЖКА 6.1. Ако пръстенът R е крайнопороден S -модул, то R е цяло разширение на S (виж Теорема 4.6). Пръстенът на целите алгебрични числа е цяло разширение на пръстена на целите числа \mathbb{Z} , което не е крайнопороден \mathbb{Z} -модул.

ТВЪРДЕНИЕ 6.2 (транзитивност). *Нека $T \subset S \subset R$ са разширения на пръстени. Разширението $T \subset R$ е цяло тогава и само тогава, когато разширенията $T \subset S$ и $S \subset R$ са цели.*

ДОКАЗАТЕЛСТВО. От дефиницията на цял елемент е ясно, че ако $\alpha \in R$ е цял над T , то α е цял и над S . От тук следва, че ако $T \subset R$ е цяло разширение, то разширенията $T \subset S$ и $S \subset R$ също са цели.

Обратно, да предположим, че $T \subset S$ и $S \subset R$ са цели разширения. Нека $\alpha \in R$ и нека $f = X^n + a_1 X^{n-1} + \dots + a_n \in S[X]$ е моничен полином, такъв че $f(\alpha) = 0$. Да забележим, че пръстенът $S_0 = T[a_1, \dots, a_n]$ е крайнопороден T -модул, защото елементите $a_1, \dots, a_n \in S$ са цели над T . Освен това, тъй като $f \in S_0[X]$, елементът α е цял над S_0 и затова пръстенът $S_0[\alpha]$ е крайнопороден S_0 -модул. Сега Лема 6.2 влече, че $S_0[\alpha]$ е крайнопороден T -модул, откъдето следва, че α е цял над T . \square

ТВЪРДЕНИЕ 6.3. *Ако областта R е цяло разширение на пръстена S , то R е поле тогава и само тогава, когато S е поле.*

ДОКАЗАТЕЛСТВО. Да припомним, че един линеен оператор $\varphi : V \rightarrow V$ в крайномерно векторно пространство V е сюрективен, тогава и само тогава, когато е инжективен (по друг начин: $\text{im } \varphi = V \Leftrightarrow \text{ker } \varphi = \{0\}$).

Ако S е поле и $0 \neq \alpha \in R$, то пръстенът $R_0 = S[\alpha]$ е крайномерно векторно пространство над S . Нека $\varphi_\alpha : R_0 \rightarrow R_0$ е изображението, определено с формулата $\varphi_\alpha(r) = \alpha r$, $r \in R_0$. Тогава φ_α е линеен оператор, който е инжективен, защото R_0 е област. Според горната забележка съществува елемент $\beta \in R_0$, такъв че $\varphi_\alpha(\beta) = 1$, т.е. $\alpha\beta = 1$. Следователно всеки елемент $0 \neq \alpha \in R$ има обратен и R е поле.

Обратно, нека R е поле и нека $0 \neq s \in S$. Тъй като s е обратим в R , то съществува елемент $s^{-1} \in R$, такъв че $s^{-1}s = 1$. Тъй като s^{-1} е цял над S , то съществува моничен полином $f = X^n + a_1 X^{n-1} + \dots + a_n \in S[X]$, такъв че $f(s^{-1}) = 0$, т.е.

$$s^{-n} + a_1 s^{-n+1} + \dots + a_n = 0, \quad a_1, \dots, a_n \in S. \quad (6.1)$$

Умножавайки (6.1) по s^{n-1} , получаваме

$$s^{-1} = -(a_1 + \dots + a_n s^{n-1}), \quad a_1, \dots, a_n \in S,$$

откъдето следва, че $s^{-1} \in S$. \square

ПРИМЕР 6.4. Пръстенът $\mathbb{Q}[X]/(X^2)$ е цяло разширение на \mathbb{Q} , което не е поле.

ЗАБЕЛЕЖКА 6.5. От Твърдение 6.3 следва, че пръстените от цели алгебрични числа не са полета. Наистина, всеки пръстен от цели алгебрични числа R е цяло разширение на пръстена на целите числа \mathbb{Z} . Тъй като \mathbb{Z} не е поле, то и R не е поле.

Следващата лема е едно просто, но полезно наблюдение.

ЛЕМА 6.6. Нека пръстенът R е цяло разширение на пръстена S и нека $\varphi : R \rightarrow \overline{R}$ е сюрективен хомоморфизъм на пръстени. Да означим с \overline{S} подпръстена $\varphi(S) \subset \overline{R}$. Тогава пръстенът \overline{R} е цяло разширение на пръстена \overline{S} .

ДОКАЗАТЕЛСТВО. Нека $\overline{\alpha} \in \overline{R}$ и нека α е елемент на R , такъв че $\overline{\alpha} = \varphi(\alpha)$. Съществува моничен полином $f = X^n + a_1X^{n-1} + \dots + a_n \in S[X]$, такъв че $f(\alpha) = 0$. Нека $\overline{f} = X^n + \varphi(a_1)X^{n-1} + \dots + \varphi(a_n) \in \overline{S}[X]$. Да проверим, че $\overline{f}(\overline{\alpha}) = 0$:

$$\begin{aligned}\overline{f}(\overline{\alpha}) &= \overline{\alpha}^n + \varphi(a_1)\overline{\alpha}^{n-1} + \dots + \varphi(a_n) \\ &= \varphi(\alpha)^n + \varphi(a_1)\varphi(\alpha)^{n-1} + \dots + \varphi(a_n) \\ &= \varphi(\alpha^n + a_1\alpha^{n-1} + \dots + a_n) = \varphi(f(\alpha)) = 0.\end{aligned}$$

Следователно всеки елемент $\overline{\alpha} \in \overline{R}$ е цял над \overline{S} . \square

Нека пръстенът R е цяло разширение на пръстена S , I е идеал в R и $J = I \cap A$. Да означим с $i : R \rightarrow R/I$ естественият хомоморфизъм от R във факторпръстена R/I . Според теоремата за хомоморфизмите на пръстени, пръстенът $i(S)$ е естествено изоморфен на факторпръстена S/J . Използвайки този изоморфизъм, ние ще отъждествяваме S/J с $i(S)$, и ще разглеждаме факторпръстена S/J като подпръстен на факторпръстена R/I .

ЛЕМА 6.7. Нека пръстенът R е цяло разширение на пръстена S , I е идеал в R и $J = I \cap A$. Тогава фактор-пръстенът R/I е цяло разширение на фактор-пръстена S/J .

ДОКАЗАТЕЛСТВО. Твърдението следва от Лема 6.6, защото $i : R \rightarrow R/I$ е сюрективен хомоморфизъм на пръстени. \square

ЗАБЕЛЕЖКА 6.8. Не е трудно да се види, че Лема 6.6 и Лема 6.7 са еквивалентни.

ТВЪРДЕНИЕ 6.9. Ако пръстенът R е цяло разширение на пръстена S и \mathfrak{P} е прост идеал в R , то \mathfrak{P} е максимален идеал в R тогава и само тогава, когато $\mathfrak{p} = \mathfrak{P} \cap S$ е максимален идеал в S .

ДОКАЗАТЕЛСТВО. От Лема 6.7 следва, че R/\mathfrak{P} е цяло разширение на S/\mathfrak{p} . Следователно R/\mathfrak{P} е поле тогава и само тогава, когато S/\mathfrak{p} е поле (Твърдение 6.3). \square

ТВЪРДЕНИЕ 6.10. Нека областта R е цяло разширение на областта S и нека I е идеал в R . Ако $I \neq \{0\}$, то $I \cap S \neq \{0\}$.

ДОКАЗАТЕЛСТВО. Нека $0 \neq \alpha \in I$. Тогава съществуват $s_i \in S$, $i = 1, \dots, n$, такива че $\alpha^n + \sum_{i=1}^n s_i \alpha^{n-i} = 0$. Тъй като R е област, то можем да предполагаме, че $s_n \neq 0$. Нека $\beta = \alpha^{n-1} + \sum_{i=1}^{n-1} s_i \alpha^{n-i} \in R$. Тогава $\beta\alpha = -s_n \neq 0$. Освен това $\beta\alpha \in I \cap S$, откъдето следва, че $I \cap S \neq \{0\}$. \square

ПРИМЕР 6.11. Нека $R = \mathbb{Q}[X]/(X^2)$, $x = X + (X^2) \in R$ и I е главният идеал породен от x в R . Тогава R е цяло разширение на \mathbb{Q} , $I \neq \{0\}$, но $I \cap \mathbb{Q} = \{0\}$.

ТВЪРДЕНИЕ 6.12. Нека R е пръстен от алгебрични числа и \mathfrak{P} е прост идеал в R . Ако $\mathfrak{P} \neq \{0\}$, то \mathfrak{P} е максимален идеал в R .

ДОКАЗАТЕЛСТВО. Нека $\mathfrak{p} = \mathbb{Z} \cap \mathfrak{P}$. Тъй като $\mathfrak{P} \neq \{0\}$, то от Твърдение 6.10 следва, че $\mathfrak{p} \neq \{0\}$. Следователно \mathfrak{p} е максимален идеал в \mathbb{Z} . Сега от Твърдение 6.9 следва, че \mathfrak{P} е максимален идеал в R . \square

Нека R е област. Ще означаваме с R^* множеството на обратимите елементи в R :

$$R^* = \{x \in R : xy = 1 \text{ за някой } y \in R\}.$$

От определението е ясно, че R^* е група относно умножението в R . Един елемент $0 \neq a \in R$ се нарича *разложим*, когато съществуват елементи $b, c \in R \setminus R^*$, такива че $a = bc$. Един елемент $0 \neq p \in R \setminus R^*$ се нарича *неразложим*, когато той не е разложим. Елементите $a, b \in R$ се наричат *асоциирани*, когато a дели b и b дели a . Два елемента $a, b \in R$ са асоциирани тогава и само тогава, когато $a = bu$, за някой $u \in R^*$. Ако p е неразложим елемент в R и $q \in R$ е делител на p , то или $q \in R^*$ или q е асоцииран с p .

ДЕФИНИЦИЯ. Казваме, че областта R е *факториален* пръстен, когато са изпълнени следните условия:

(i) Всеки елемент $0 \neq a \in R$ има представяне

$$a = u \prod_{i=1}^r p_i,$$

където $u \in R^*$, а $p_i \in R$, $i = 1, \dots, r$, са неразложими елементи в R ;

(ii) ако

$$a = u \prod_{i=1}^r p_i = v \prod_{j=1}^s q_j$$

са две такива представяния, то $r = s$ и след подходяща пермутация на множителите елементът p_i е асоцииран с елемента q_i , $i = 1, \dots, r$.

ТВЪРДЕНИЕ 1. Ако R е факториален пръстен и p е неразложим елемент в R , то главният идеал (p) е прост.

ДОКАЗАТЕЛСТВО. Трябва да докажем, че ако a и b са елементи на R , такива че p дели произведението ab , то p дели някой от множителите a и b . Нека елементът $c \in R$ е такъв че $pc = ab$. Да разложим a, b и c на неразложими елементи:

$$a = u \prod_{i=1}^r p_i, \quad b = u' \prod_{j=1}^{r'} p'_j, \quad c = u'' \prod_{k=1}^{r''} p''_k.$$

Тогава

$$u'' p \prod_{k=1}^{r''} p''_k = uu' \prod_{i=1}^r p_i \prod_{j=1}^{r'} p'_j. \quad (0.2)$$

От тъждество (0.2) следва, че p е асоцииран с някой от неразложимите елементи в множеството $\{p_i\}_{i=1}^r \cup \{p'_j\}_{j=1}^{r'}$. Следователно p дели някой от множителите a и b . \square

Библиография

- [1] У. Рудин, Реален и комплексен анализ, "Наука и Изкуство", София 1984.