Дедекиндови пръстени

9. Пръстени на дискретно нормиране

Дефиниция 9.1. Изображението v от полето K в множеството $\mathbb{Z}\cup\{\infty\}$ се нарича дискретно нормиране на полето K, когато v удовлеторява следните условия:

(i) $v(xy) = v(x) + v(y)$, $x, y \in K$;

(ii) $v(x + y) \geq \min\{v(x), v(y)\}$, $x, y \in K$;

(iii) $v(x) = \infty \Leftrightarrow x = 0$.

Задача 9.1. Да се докаже, че $v(x + y) = \min\{v(x), v(y)\}$, когато $v(x) \neq v(y)$.

Дискретно нормиране $v : K \to \mathbb{Z} \cup \{\infty\}$, такова че $v(K^*) = 0$, се нарича *тривиално дискретно нормиране*. Ясно е, че за всяко поле K съществува единствено тривиално дискретно нормиране на K.
От условия (i) и (ii) на Дефиниция 9.1 следва, че множеството

$$R_v = \{x \in R : v(x) \geq 0\}$$

е подпръстен на K. Пръстенът R_v се нарича *пръстен на нормиране асоцииран с дискретното нормиране* v.

Твърдение 9.2. *Нека R_v е пръстен на нормиране, който е асоцииран с нетривиално дискретно нормиране v на полето K. Тогава*

(i) $R_v^* = \{x \in K : v(x) = 0\}$;

(ii) R_v е локален пръстен с максимален идеал $\mathfrak{m}_v = \{x \in K : v(x) > 0\}$;

(iii) всеки идеал I в R_v е главен;

(iv) ако елементът $t \in R_v$ поражда идеала $\mathfrak{m}$, то хомоморфизмът на абелеви групи

$$R_v^* \times \mathbb{Z} \to K^*, \quad R_v^* \times \mathbb{Z} \ni (u, q) \mapsto ut^q \in K^*, \tag{9.1}$$

е изоморфизъм;

(v) всеки идеал $I \neq \{0\}$ в R_v е степен на идеала $\mathfrak{m}_v$;

(vi) пръстенът R_v е цялозатворен.

Доказателство. Ясно е, че ако $x, y \in R_v$, то x дели y тогава и само тогава, когато $v(x) \leq v(y)$.

(i) Тъй като $v|_{K^*}$ е хомоморфизъм от K^* в $\mathbb{Z}$, то $v(x^{-1}) = -v(x)$ за всеки $x \in K^*$. Остава да забележим, че $R_v^* = \{x \in K^* : v(x) \geq 0, v(x^{-1}) \geq 0\}$.

(ii) От условия (i) и (ii) на Дефиниция 9.1 следва, че $\mathfrak{m}_v$ е идеал в R_v. Тъй като $R_v = \mathfrak{m}_v \cup R_v^*$, то идеалът $\mathfrak{m}_v$ е максимален.

(iii) Нека $m_I \in \mathbb{Z} \cup \{\infty\}$ е минимален елемент на множеството $v(I)$ и нека t_I е елемент на I, такъв че $v(t_I) = m_I$. Тогава $I = (t_I)$. Наистина, ако $x \in I$, то $v(t_I) \leq v(x)$, откъдето следва, че t_I дели x.

(iv) Тъй като $v(K^*)$ е подгрупа на $\mathbb{Z}$, то $v(K^*) = m\mathbb{Z}$ за някое естествено число m. Ясно е, че $v(t) = m$. Нека $x \in K^*$, $v(x) = qm$ и $u = t^{-q}x$. Тогава $u \in R_v^*$ и $x = ut^q$, откъдето следва, че хомомоморфизмът (9.1) е сюрективен. Ако $ut^q = 1$

за някой $u \in R^*$ и някое цяло число q, то $-mq = v(t^{-q}) = v(u) = 0$, откъдето $q = 0$ и $u = 1$. Следователно хомомоморфизмът (9.1) е инжективен.

(v) Нека елементът $t \in R_v$ поражда идеала $\mathfrak{m}_v$. Според (iii) съществува елемент $0 \neq x \in R_v$, такъв че $I = (x)$. Според (iv) съществуват елемент $u \in R_v^*$ и цяло число $q \geq 0$, такива че $x = ut^q$. Следователно $I = (ut^q) = (t^q) = (t)^q = \mathfrak{m}_v^q$.

(vi) Нека $x \in K^*$ и нека $a_1, \ldots, a_n$ са елементи на R_v^*, такива че

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

Тогава $1 + a_1 x^{-1} + \cdots + a_n x^{-n} = 0$ и $v(a_1 x^{-1} + \cdots + a_n x^{-n}) = v(-1) = 0$. Следователно $0 \geq \min\{v(a_1 x^{-1}), \ldots, v(a_n x^{-n})\} \geq \min\{v(x^{-1}), \ldots, v(x^{-n})\}$, откъдето получаваме, че $v(x) \geq 0$, т.е. $x \in R_v$. □

Дефиниция 9.2. Нека локалният пръстен R е област с поле от частни K. Ще казваме, че R е *пръстен на дискретно нормиране*, когато съществува нетривиално дискретно нормиране v на полето K, такова че

$$R = R_v = \{x \in K : v(x) \geq 0\}.$$

Забележка 9.3. Лесно се вижда, че ако v_1 и v_2 са дискретни нормирания на полето K, такива че $R_{v_1} = R_{v_2}$, то $v_2 = rv_1$, където r е положително рационално число.

В някои от следващите доказателства ще използуваме така наречения *принцип на ньотеровата индукция*. Нека R е пръстен и нека $\mathcal{A}$ е множество от идеали на R. В $\mathcal{A}$ въвеждаме наредба по следния начин:

$$I_1 < I_2 \quad \Leftrightarrow \quad I_1 \text{ се съдържа строго в } I_2.$$

Казваме, че $I \in \mathcal{A}$ е *максимален елемент* на $\mathcal{A}$, когато от $I \leq J$, $J \in \mathcal{A}$, следва, че $I = J$.

Твърдение 9.4 (Принцип на ньотеровата индуция). *Нека $\mathcal{A}$ е множество от идеали на ньотеров пръстен R и нека $\mathbb{P}$ е пропозиция, удовлетворяваща следните две условия:*

(i) $\mathbb{P}$ е вярна за всички максимални елементи на $\mathcal{A}$;

(ii) Ако $I \in \mathcal{A}$ не е максимален елемент на $\mathcal{A}$ и $\mathbb{P}$ е вярна за всички елементи J на $\mathcal{A}$, такива че $I < J$, то $\mathbb{P}$ е вярна за елемента I.

Тогава $\mathbb{P}$ е вярна за всички елементи на $\mathcal{A}$.

Доказателство. Нека $\mathcal{B} = \{I \in \mathcal{A} : \mathcal{P}$ не е вярна за $I\}$. Ако множеството $\mathcal{B}$ не е празно, то от ньотеровостта на R следва, че в $\mathcal{B}$ съществува максимален елемент I. От условие (i) следва, че I не е максимален елемент на $\mathcal{A}$. Тъй като I е максимален елемент на $\mathcal{B}$, то $\mathbb{P}$ е вярна за всички $J \in \mathcal{A}$, такива че $I < J$. Сега от условие (ii) следва, че $\mathbb{P}$ е вярна за I. Полученото противоречие показва, че $\mathcal{B} = \emptyset$ и $\mathbb{P}$ е вярна за всички $I \in \mathcal{A}$. □

Твърдение 9.5. *Нека R е локален пръстен, който не е поле. Тогава следните условия са еквивалентни:*

(i) R е пръстен на дискретно нормиране;

(ii) R е област на главни идеали;

(iii) R е ньотерова област и максималният идеал $\mathfrak{m}$ на R е главен.

Доказателство. (i) $\Rightarrow$ (ii). Следва от Твърдение 9.2 (iii).

(ii) $\Rightarrow$ (iii). От дефинициите на област на главни идеали и ньотеров пръстен следва, че всяка област на главни идеали е ньотеров пръстен.

(iii) $\Rightarrow$ (i). Нека $\mathfrak{m} = (t)$, $t \in R \setminus \{0\}$. По-долу ще докажем, че хомоморфизмът на абелеви групи $\theta : R^* \times \mathbb{Z} \to K^*$, определен с формулата

$$\theta(u, q) = ut^q, \quad u \in R^*, \ q \in \mathbb{Z},$$

е изоморфизъм. Нека $p_2 : R^* \times \mathbb{Z} \to \mathbb{Z}$ е проекцията $p_2(u, q) = q$, $u \in R^*$, $q \in \mathbb{Z}$. Да означим с v_0 хомоморфизма на абелеви групи $p_2 \circ \theta^{-1} : K^* \to \mathbb{Z}$:

$$v_0 \ : \ K^* \xrightarrow{\theta^{-1}} R^* \times \mathbb{Z} \xrightarrow{p_2} \mathbb{Z}.$$

Нека изображението $v : K \to \mathbb{Z} \cup \{\infty\}$ е дефинирано по следния начин

$$v(x) = \begin{cases} v_0(x) & \text{когато } x \in K^*; \\ \infty & \text{когато } x = 0. \end{cases} \tag{9.2}$$

Тогава v е дискретно нормиране на полето K, такова че $R = R_v$.
Да докажем горните твърдения.

Хомоморфизмът θ е изоморфизъм.
Първо ще установим, че хомоморфизмът θ е сюрективен. Тъй като всеки елемент на K^* е частно на два елемента на $R \setminus \{0\}$, то е достатъчно да докажем, че всеки елемент $x \in R \setminus \{0\}$ има представяне

$$x = ut^q, \quad \text{където } u \in R^*, \ q \geq 0. \tag{9.3}$$

Ние ще докажем, че за всеки главен идеал (x), $x \in R \setminus \{0\}$, съществува цяло число $q \geq 0$, такова че $(x) = (t^q)$. За тази цел ще използваме ньотерова индукция. Да разгледаме множеството $\mathcal{A}$ от всички ненулеви главни идеали на пръстена R:

$$\mathcal{A} = \{ \, (x) \ : \ x \in R \setminus \{0\} \, \}.$$

Единственият максимален елемент на $\mathcal{A}$ е целият пръстен $R = (t^0)$. Да предположим, че $(x) \in \mathcal{A}$, $(x) \neq R$ и всеки главен идеал (y), който съдържа строго идеала (x), се поражда от t^q за някое цяло число $q \geq 0$. Тъй като $(x) \neq R$, то $x \in \mathfrak{m}$, откъдето $x = yt$ за някой $y \in R$. Да забележим, че идеалът (y) съдържа строго идеала (x), защото $t \notin R^*$. Следователно $(y) = (t^q)$ за някое цяло число $q \geq 0$, откъдето получаваме $(x) = (t)(y) = (t^{q+1})$. Сега от принципа на ньотеровата индукция следва, че за всеки $x \in R \setminus \{0\}$ съществува цяло число $q \geq 0$, такова че $(x) = (t^q)$. Тъй като от $(x) = (t^q)$ следва, че $x = ut^q$ за някой $u \in R^*$, то съществуването на представяне (9.3) е доказано.
Сега да установим, че хомоморфизмът θ е инжективен, т.е. $\ker \theta = \{(1, 0)\}$. Нека $\theta(u, q) = ut^q = 1$, където $u \in R^*$ и $q \in \mathbb{Z}$. Тогава $t^{|q|} \in R^* = R \setminus \mathfrak{m}$. Тъй като $t^q \in \mathfrak{m}$, когато $q > 0$, то $q = 0$ и $u = 1$. Следователно хомоморфизмът θ е инжективен, откъдето следва, че θ е изоморфизъм.

Множеството $R_v = \{x \in K : v(x) \geq 0\}$ съвпада с пръстена R.
Да забележим, че $t^q \notin R$, когато $q < 0$. Наистина, ако $t^q \in R$ за някое $q < 0$, то $t^{-q} \in \mathfrak{m}$ ще се окаже обратим елемент в R. Тъй като θ е изоморфизъм, то всеки елемент $x \in K^*$ се представя като $x = ut^q$, където $q = v(x)$ и $u \in R^*$. Ако $v(x) \geq 0$, то $x \in R$. Обратно, ако $x = ut^q \in R$, то $t^q \in R$, откъдето $v(x) = q \geq 0$.

Изображението $v : K \to \mathbb{Z} \cup \{\infty\}$ е дискретно нормиране на полето K.
Да проверим условия (i), (ii) и (iii) на Дефиниция 9.1:

(i) Ако $x = 0$ или $y = 0$, то $v(xy) = \infty$ и $v(x) + v(y) = \infty$. Ако $x, y \in K^*$, то $v(xy) = v(x) + v(y)$, защото $v|_{K^*} = v_0$ и v_0 е хомоморфизъм на абелеви групи.

(ii) Ако $x = 0$ (съответно $y = 0$), то $v(x + y) = v(y) = \min\{\infty, v(y)\}$ (съответно $v(x + y) = v(x) = \min\{v(x), \infty\}$).

Ако $x, y \in K^*$, то $x = ut^q$ и $y = u't^{q'}$, където $u, u' \in R^*$ и $q, q' \in \mathbb{Z}$. Тогава $v(x) = q$, $v(y) = q'$, и без ограничение на общността можем да предполагаме, че $q \leq q'$. Сега

$$x + y = ut^q + u't^{q'} = t^q(u + u't^{q'-q}).$$

Тъй като $u + u't^{q'-q} \in R$, то $v(u + u't^{q'-q}) \geq 0$, откъдето получаваме

$$v(x + y) = v(t^q) + v(u + u't^{q'-q}) \geq v(t^q) = v(x) = \min\{v(x), v(y)\}.$$

(iii) От дефиниция (9.2) е ясно, че $v(x) = \infty \Leftrightarrow x = 0$. □

От Твърдение 9.2 знаем, че всеки пръстен на дискретно нормиране е цялозатворен ньотеров локален пръстен, в който всички прости идеали са нулевият идеал и максималният идеал. Следващата важна теорема показва, че всеки пръстен притежаващ тези свойства е пръстен на дискретно нормиране.

Теорема 9.6. *Нека R е локална област, в която всички прости идеали са нулевият идеал $\{0\}$ и максималният идеал $\mathfrak{m}$. Тогава следните условия са еквивалентни:*

(i) R е пръстен на дискретно нормиране;

(ii) R е цялозатворен ньотеров пръстен.

В доказателството на Теорема 9.6 ще използваме понятието асоцииран прост идеал. Да припомним, че ако $\mathfrak{a}$ и $\mathfrak{b}$ са идеали на пръстена R, то тяхното частно $\mathfrak{a} : \mathfrak{b}$ се дефинира по следния начин:

$$\mathfrak{a} : \mathfrak{b} = \{x \in R : x\mathfrak{b} \subset \mathfrak{a}\}.$$

От дефиницията на $\mathfrak{a} : \mathfrak{b}$ следва, че $\mathfrak{a} \subset \mathfrak{a} : \mathfrak{b}$. Лесно се проверява, че е $\mathfrak{a} : \mathfrak{b}$ идеал на R, такъв че $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subset \mathfrak{a}$. Нещо повече, ако $\mathfrak{c}$ е идеал на R, такъв че $\mathfrak{c}\mathfrak{b} \subset \mathfrak{a}$, то $\mathfrak{c} \subset \mathfrak{a} : \mathfrak{b}$.

Дефиниция. Нека $I \neq R$ е идеал в пръстена R. Простият идеал $\mathfrak{p} \subset R$ се нарича *асоцииран прост идеал на I*, когато съществува $x \in R$, $x \notin I$, такъв че

$$\mathfrak{p} = (I) : (x) = \{y \in R : xy \in I\}.$$

Ясно е, че ако $\mathfrak{p}$ е асоцииран прост идеал на I, то $\mathfrak{p} \supset I$. Множеството на асоциираните прости идеали на идеала I в пръстена R се означава с $\operatorname{Ass}_R I$. Множеството $\operatorname{Ass}_R \{0\}$ се означава с $\operatorname{Ass} R$.

Задача 9.7. Нека $I \neq R$ е идеал на пръстена R и нека $\mathfrak{p}$ е прост идеал на R, който съдържа идеала I. Да се докаже, че

$$\mathfrak{p} \in \operatorname{Ass}_R I \;\Leftrightarrow\; \mathfrak{p}/I \in \operatorname{Ass} R/I.$$

Лема 9.8. *Нека $I \neq R$ е идеал на пръстена R. Тогава всеки максимален елемент в множеството от идеали*

$$\mathcal{A} = \{\, I : (x) \;:\; x \notin I \,\}$$

е асоцииран прост идеал на I.

Доказателство. Нека $\mathfrak{p} = I : (x)$, $x \notin I$, е максимален елемент в $\mathcal{A}$. Ако $\mathfrak{p}$ не е прост идеал, то съществуват елементи $s, t \in R$, такива че $s, t \notin \mathfrak{p}$, а $st \in \mathfrak{p}$. Следователно $sx \notin I$ и $stx \in I$. Нека $\mathfrak{a} = I : (sx) \in \mathcal{A}$. Тогава $\mathfrak{p} \subset \mathfrak{a}$, защото ako $yx \in I$, то $y(sx) \in I$. Освен това $t \in \mathfrak{a}$, защото $t(sx) \in I$. Тъй като $t \notin \mathfrak{p}$, то $\mathfrak{p} \neq \mathfrak{a}$. Това обаче противоречи на максималността на $\mathfrak{p}$ в $\mathcal{A}$. Следователно $\mathfrak{p}$ е прост идеал. □

Твърдение 9.9. *Ако R е ньотеров пръстен, то $\operatorname{Ass}_R I \neq \emptyset$ за всеки идеал $I \neq R$.*

Доказателство. Твърдението следва от Лема 9.8, тъй като всяко непразно множество от идеали на ньотеров пръстен съдържа максимален елемент. □

Задача 9.10. Нека R е ньотеров пръстен. Да се докаже, че множеството на всички делители на нулата в R съвпада с $\cup_{\mathfrak{p}\in \operatorname{Ass} R}\mathfrak{p}$.

Следващата лема ще бъде използувана в доказателството на Теорема 9.6.

Лема 9.11. *Нека R е област с поле от частни K. Ако елементът $x \in K$ е цял над R, то съществува $s \in R \setminus \{0\}$, такъв че $sx^n \in R$ за всяко $n \in \mathbb{N}$. Обратното също е вярно, когато пръстенът R е ньотеров: ако за елемента $x \in K$ съществува $s \in R \setminus \{0\}$, такъв че $s^n x \in R$ за всяко $n \in \mathbb{N}$, то x е цял над R.*

Доказателство. Ако $x \in K$ е цял над R, то пръстенът $R[x]$ е крайнопороден R-модул. Нека елементите $x_i = y_i/s_i$, $y_i \in R$, $s_i \in R\setminus\{0\}$, $i = 1, \dots, n$, пораждат $R[x]$ над R. Да положим $s = \prod_{i=1}^{n} s_i$. Тогава $s \neq 0$ и $sR[x] \subset R$, откъдето следва, че $sx^n \in R$ за всяко $n \in \mathbb{N}$.
Обратно, нека R е ньотеров пръстен и нека елементите $s \in R \setminus \{0\}$ и $x \in K$ са такива, че $sx^n \in R$ за всяко $n \in \mathbb{N}$. Тогава $sR[x] \subset R$ е идеал на R, откъдето следва, че $sR[x]$ е крайнопороден R-модул. Освен това, изображението $g : R[x] \to sR[x]$, определено с формулата $g(y) = sy$, $y \in R[x]$, е изоморфизъм на R-модули, защото $s \neq 0$. Следователно $R[x]$ е крайнопороден R-модул и елементът x е цял над R. □

Доказателство на Теорема 9.6.
(i) $\Rightarrow$ (ii). Следва непосредствено от Твърдение 9.2.
(ii) $\Rightarrow$ (i). Достатъчно е докажем, че максималният идеал $\mathfrak{m}$ е главен (виж Твърдение 9.5). Нека $x \in \mathfrak{m} \setminus \{0\}$. Тъй като $\mathfrak{m}$ е единственият прост идеал, който съдържа идеала (x), то $\mathfrak{m}$ е асоцииран прост идеал на (x). Следователно съществува елемент $y \in R$, $y \notin (x)$, такъв че $y\mathfrak{m} \subset (x)$. Нека $z = x^{-1}y \in K$. Тогава $z \notin R$, защото $y \notin (x)$. Освен това $z\mathfrak{m} \subset R$, защото $y\mathfrak{m} \subset (x)$. Тъй като $z\mathfrak{m}$ е идеал в R, то или $z\mathfrak{m} \subset \mathfrak{m}$ или $z\mathfrak{m} = R$. Да предположим, че $z\mathfrak{m} \subset \mathfrak{m}$. Тогава $z^n\mathfrak{m} \subset \mathfrak{m}$, за всяко $n \in \mathbb{N}$. В частност, $xz^n \in R$ за всяко $n \in \mathbb{N}$. Сега от Лема 9.11 получаваме, че z е цял над R. Това обаче противоречи на цялозатвореността на R, защото $z \notin R$. Следователно $z\mathfrak{m} = R$ и идеалът $\mathfrak{m} = z^{-1}R$ е главен. □

10. Дробни идеали и обратими идеали на област

Дефиниция 10.1. Нека R е област с поле от частни K. Казваме, че R-подмодулът $I \subset K$, $I \neq \{0\}$, е *дробен идеал на* R, когато съществува $s \in K^*$, такъв че $sI \subset R$.

Ясно е, че всеки крайнопороден R-подмодул на K е дробен идеал на R. Ако пръстенът R е ньотеров, то всеки дробен идеал на R е крайнопороден. Наистина R-модулите I и sI са изоморфни за всеки $s \in K^*$, откъдето следва, че I е крайнопороден R-модул тогава и само тогава, когато sI е крайнопороден R-модул. Дробният идеал I на R се нарича *главен*, когато I се поражда като R-модул от един елемент $x \in K^*$: $I = (x) = \{rx : r \in R\}$.
Произведението IJ и частното $I : J$ на дробните идеали I и J се определят както за обикновени идеали:

$$IJ = \{x_1y_1 + \cdots + x_ny_n : x_i \in I,\ y_i \in J,\ n \in \mathbb{N}\},$$
$$I : J = \{x \in K : xJ \subset I\}.$$

Непосредствено се проверява, че IJ и $I : J$ са също дробни идеали на R.

Ако S е мултипликативно затворено подмножество на R, то лесно се вижда, че множеството

$$I_S = IR_S = \{\, x/s : x \in I,\ s \in S \,\}$$

е дробен идеал на R_S. Ако $\mathfrak{p}$ е прост идеал на R и $S = R \setminus \mathfrak{p}$, то ние ще означаваме I_S с $I_{\mathfrak{p}}$.

Лема 10.1. *Нека I и J са дробни идеали, а S е мултипликативно затворено подмножество на R. Тогава*

(i) $(IJ)_S = I_S J_S$;

(ii) ако дробният идеал J е крайнопороден, то $(I : J)_S = I_S : J_S$.

Доказателство. (i) Наистина $(IJ)_S = R_S(IJ) = (R_S I)(R_S J) = I_S J_S$.

(ii) Ясно е, че $(I : J)_S \subset I_S : J_S$. Ще докажем обратното включване. Нека $x_1, \ldots, x_m \in J$ пораждат идеала J. Тогава $z \in I : J \;\Leftrightarrow\; zx_i \in I,\ i = 1, \ldots, m$. Ако $x \in I_S : J_S$, то $xx_i = y_i/s_i$, където $y_i \in I$, $s_i \in S$, $i = 1, \ldots, m$. Да положим $s = \prod_{i=1}^m s_i \in S$. Сега $(sx)x_i \in I$, $i = 1, \ldots, m$, откъдето получаваме $sx \in I : J$. Следователно $x \in (I : J)_S$. □

От дефинициите следва, че $I(R : I) \subset R$ за всеки дробен идеал I на R. Тъй като $R : (x) = (x^{-1})$, за всеки $x \in K^*$, то $I(R : I) = R$ за всеки главен дробен идеал I на R.

Дефиниция 10.2. Дробният идеал I на R се нарича *обратим*, когато

$$I(R : I) = R.$$

Ако дробният идеал I е обратим, то ние ще пишем I^{-1} вместо $R : I$. По-горе забелязахме, че всеки главен дробен идеал $I = (x)$ е обратим, като $I^{-1} = (x^{-1})$.

Задача 10.2. Нека R област и I е обратим дробен идеал на R. Да се докаже, че I е крайнопороден дробен идеал на R.

Твърдение 10.3. *Нека R е пръстен на дискретно нормиране с максимален идеал $\mathfrak{m}$. Тогава всеки дробен идеал на R е главен и множеството на дробните идеали на R е безкрайна циклична група, която се поражда от максималния идеал $\mathfrak{m}$.*

Доказателство. Нека $v : K \to \mathbb{Z} \cup \{\infty\}$ е дискретно нормиране на полето K, такова че $R_v = R$. Нека I е дробен идеал на R и нека s е елемент на K^*, такъв че $sI \subset R$. Тогава $v(sx) \geq 0$ за всеки $x \in I$, откъдето $v(x) \geq -v(s)$ за всеки $x \in I$. Следователно съществува елемент $x_I \in I$, такъв че $v(x_I) \leq v(x)$ за всеки $x \in I$. Да покажем, че $I = (x_I)$: ако $x \in I$, то $x = (xx_I^{-1})x_I$, където $xx_I^{-1} \in R$, защото $v(xx_I^{-1}) \geq 0$. Нека $t \in \mathfrak{m}$ поражда максималния идеал $\mathfrak{m}$. Тогава $x_I = ut^q$, където $u \in R^*$ и $q \in \mathbb{Z}$. Следователно $I = (x_I) = (ut^q) = \mathfrak{m}^q$. □

Задача 10.4. Нека R е локална област и I е обратим дробен идеал на R. Да се докаже, че I е главен дробен идеал.

Задача 10.5. Нека R е област и I е дробен идеал на R. Да се докаже, че следните условия са еквивалентни:

(i) I е обратим дробен идеал на R;

(ii) I е крайнопороден дробен идеал на R и I_P е обратим дробен идеал на R_P за всеки максимален идеал P на R.

11. Дедекиндови пръстени

Дефиниция 11.1. Пръстенът R се нарича *дедекиндов пръстен*, когато R удовлетворява следните условия:

(i) R е ньотеров пръстен;

(ii) R е цялозатворен пръстен;

(iii) всеки прост идеал $\mathfrak{p} \neq \{0\}$ на R е максимален.

Пример 11.1. Пръстенът на целите числа $\mathbb{Z}$ е дедекиндов пръстен.

Пример 11.2. Всяка област на главни идеали е дедекиндов пръстен.

Пример 11.3. Полиномиалният пръстен $\mathbb{Z}[X]$ е ньотеров и цялозатворен, но не е дедекиндов пръстен.

Пример 11.4. Нека D е пръстенът на целите алгебрични числа в едно крайно разширение F на полето на рационалните числа $\mathbb{Q}$. Тогава от Теорема 8.9, Твърдение 7.7 и Твърдение 6.12 следва, че D е дедекиндов пръстен.

Лема 11.5. *Нека $\mathfrak{p} \neq \{0\}$ е прост идеал на дедекиндовия пръстен R. Тогава локализацията $R_\mathfrak{p}$ е пръстен на дискретно нормиране.*

Доказателство. Ще използваме Теорема 9.6, за да докажем, че $R_\mathfrak{p}$ е пръстен на дискретно нормиране. Тъй като всеки прост идеал на $R_\mathfrak{p}$ е от вида $\mathfrak{q}R_\mathfrak{p}$, където $\mathfrak{q} \subset \mathfrak{p}$ е прост идеал на R, то всички прости идеали на $R_\mathfrak{p}$ са нулевият идеал $\{0\}$ и максималният идеал $\mathfrak{p}R_\mathfrak{p}$. Тъй като всеки идеал на $R_\mathfrak{p}$ е от вида $IR_\mathfrak{p}$, където I е идеал на R, то пръстенът $R_\mathfrak{p}$ е ньотеров. Тъй като пръстенът R е цялозатворен, то от Твърдение 7.4 следва, че пръстенът $R_\mathfrak{p}$ също е цялозатворен. Сега от Теорема 9.6 получаваме, че $R_\mathfrak{p}$ е пръстен на дискретно нормиране. $\square$

Теорема 11.6. *Ако R е дедекиндов пръстен, то всеки дробен идеал на R е обратим.*

Доказателство. Да предположим, че дробният идеал I на R не е обратим. Тогава $I(R : I) \neq R$ е собствен идеал на R и съществува максимален идеал $\mathfrak{p}$, такъв че $I(R : I) \subset \mathfrak{p}$. След локализация спрямо $\mathfrak{p}$, идеалът $[I(R : I)]_\mathfrak{p}$ ще се съдържа в максималния идеал $\mathfrak{p}R_\mathfrak{p}$ на $R_\mathfrak{p}$. Обаче от Лема 10.1 следва, че

$$[I(R : I)]_\mathfrak{p} = I_\mathfrak{p}(R : I)_\mathfrak{p} = I_\mathfrak{p}(R_\mathfrak{p} : I_\mathfrak{p}) = R_\mathfrak{p},$$

защото $R_\mathfrak{p}$ е пръстен на дискретно нормиране и според Твърдение 10.3 всеки дробен идеал на $R_\mathfrak{p}$ е обратим. Полученото противоречие показва, че всеки дробен идеал I на R е обратим. $\square$

От Теорема 11.6 следва, че множеството на дробните идеали на един дедекиндов пръстен R е абелева група относно операцията умножение на дробни идеали. Ние ще означаваме тази група с $\operatorname{Div} R$ и ще я наричаме *група на дивизорите на пръстена R.*

Теорема 11.7. *Нека R е дедекиндов пръстен и нека $\mathcal{P} = \{\mathfrak{p}_i\}_{i \in I}$ е множеството на ненулевите прости идеали на R. Тогава $\operatorname{Div} R$ е свободна абелева група с базис $\mathcal{P}$.*

Доказателство. Ще разбием доказателството на няколко части.

Всеки идеал $I \neq \{0\}$ на R се представя като произведение на прости идеали. Отново ще използваме ньотерова индукция. Нека множеството $\mathcal{A}$ се състои от всички идеали $I \neq \{0\}$ на R. Единственият максимален елемент на $\mathcal{A}$ е целият пръстен R, който е произведение на празното множество от прости идеали. Да предположим, че $I \in \mathcal{A}$ е собствен идеал на R и всички идеали на R, които строго съдържат I, се представят като произведение на прости идеали. Тъй като $I \neq R$, то I се съдържа в максимален идеал $\mathfrak{p}$. Тогава $I \subset \mathfrak{p}^{-1}I \subset R$. Да покажем, че $I \neq \mathfrak{p}^{-1}I$. Ако $I = \mathfrak{p}^{-1}I$, то $\mathfrak{p}I = I$ и след локализация спрямо $\mathfrak{p}$ получаваме $(\mathfrak{p}R_{\mathfrak{p}})I_{\mathfrak{p}} = I_{\mathfrak{p}}$. Това е невъзможно, защото от Твърдение 10.3 знаем, че $\operatorname{Div} R_{\mathfrak{p}}$ е безкрайна циклична група. Следователно идеалът $\mathfrak{p}^{-1}I$ съдържа строго идеала I. Тогава $\mathfrak{p}^{-1}I$ се представя като произведение на прости идеали, откъдето следва, че I също се представя като произведение на прости идеали, защото $I = \mathfrak{p}(\mathfrak{p}^{-1}I)$. Сега от принципа на ньотеровата индукция следва, че всеки идеал $I \neq 0$ на R се представя като произведение на прости идеали.

Множеството $\mathcal{P}$ поражда групата $\operatorname{Div} R$.
Трябва да докажем, че за всеки дробен идеал I на R съществува представяне

$$I = \prod_{i \in I} \mathfrak{p}_i^{\alpha_i}, \quad \alpha_i \in \mathbb{Z},\ \alpha_i = 0 \text{ за почти всички } i \in I.$$

Нека $s \neq 0$ е елемент на R, такъв че $sI \subset R$. Тогава

$$(s) = \prod_{i \in I} \mathfrak{p}_i^{\beta_i}, \quad \beta_i \geq 0,\ \beta_i = 0 \text{ за почти всички } i \in I, \tag{11.1}$$

$$sI = \prod_{i \in I} \mathfrak{p}_i^{\gamma_i}, \quad \gamma_i \geq 0,\ \gamma_i = 0 \text{ за почти всички } i \in I. \tag{11.2}$$

Сега от (11.1), (11.2) и тъждеството $I = (s)^{-1}\, sI$ следва, че

$$I = \prod_{i \in I} \mathfrak{p}_i^{\gamma_i - \beta_i}, \quad \gamma_i - \beta_i \in \mathbb{Z},\ \gamma_i - \beta_i = 0 \text{ за почти всички } i \in I.$$

Множеството $\mathcal{P}$ е базис на групата $\operatorname{Div} R$.
Трябва да докажем, че ако

$$\prod_{i \in I} \mathfrak{p}_i^{\alpha_i} = R, \quad \alpha_i \in \mathbb{Z},\ \alpha_i = 0 \text{ за почти всички } i \in I, \tag{11.3}$$

то $\alpha_i = 0$ за всеки индекс $i \in I$. За всеки индекс $i \in I$ нека $\psi_i : \operatorname{Div} R \to \operatorname{Div} R_{\mathfrak{p}_i}$ е изображението определено с формулата $\psi_i(I) = I_{\mathfrak{p}_i}$. Тогава от Лема 10.1 (i) следва, че за всеки индекс $i \in I$ изображението ψ_i е хомоморфизъм на групи. Да забележим, че ако $i \neq j$, то $\psi_i(\mathfrak{p}_j) = R_{\mathfrak{p}_i}$, защото $\mathfrak{p}_j \cap R \setminus \mathfrak{p}_i \neq \emptyset$. Прилагайки хомоморфизма ψ_i към (11.3) получаваме

$$(\mathfrak{p}_i R_{\mathfrak{p}_i})^{\alpha_i} = R_{\mathfrak{p}_i}, \quad i \in I.$$

Сега от Твърдение 10.3 следва, че $\alpha_i = 0$ за всеки индекс $i \in I$. $\square$

Допълнение: Локализация и прости идеали

Нека пръстенът T е разширение на пръстена R и нека I е идеал на R. Ще означаваме с IT минималния идеал на T, който съдържа идеала I. От определението следва, че

$$IT = \{ \sum_{i=1}^{k} t_i x_i \, : \, t_i \in T, \; x_i \in I, \; i = 1, \ldots, k, \; k \geq 1 \}$$

Ясно е, че $I \subset IT \cap R$. Освен това $(J \cap R)T \subset J$ за всеки идеал J на T. Следващата лема уточнява тези включвания, когато пръстенът T е локализация на пръстена R.

Лема. *Нека R е област и S е мултипликативно затворено подмножество на R. Тогава*

(i) $J = (J \cap R)R_S$ за всеки идеал J на R_S;

(ii) ако $\mathfrak{p}$ е прост идеал на R, такъв че $\mathfrak{p} \cap S = \emptyset$, то $\mathfrak{p}R_S$ е прост идеал на R_S и $\mathfrak{p} = \mathfrak{p}R_S \cap R$.

Доказателство. (i) Ако $x/s \in J$, то $x \in J \cap R$ и $x/s = (1/s)x$.

(ii) Ясно е, че

$$\mathfrak{p}R_S = \{ x/s \, : \, x \in \mathfrak{p}, \; s \in S \}.$$

Нека $\overline{R} = R/\mathfrak{p}$ и нека $i : R \to \overline{R}$ е естественият хомомоморфизъм от R във факторпръстена $\overline{R}$. Тогава $\overline{S} = i(S)$ е мултипликативно затворено подмножество на областта $\overline{R}$ ($0 \notin \overline{S}$, защото $\mathfrak{p} \cap S = \emptyset$). Да дефинираме хомоморфизъм на пръстени $i_S : R_S \to \overline{R}_{\overline{S}}$ с формулата

$$i_S(x/s) = i(x)/i(s), \qquad x \in R, \; s \in S.$$

Тогава $\operatorname{Ker} i_S = \mathfrak{p}R_S$, откъдето следва, че $\mathfrak{p}R_S$ е прост идеал на R_S, защото $\overline{R}_{\overline{S}}$ е област. Освен това $\mathfrak{p}R_S \cap R = \operatorname{Ker} \, i_S|_R = \mathfrak{p}$. $\square$

Твърдение. *Нека R е област и S е мултипликативно затворено подмножество на R. Да означим със $\operatorname{Spec} R$ (съотв. $\operatorname{Spec} R_S$) множеството на простите идеали на R (съотв. R_S). Тогава изображението*

$$\operatorname{Spec} R_S \ni \mathfrak{P} \longmapsto \mathfrak{P} \cap R \in \operatorname{Spec} R \tag{1}$$

задава биекция между $\operatorname{Spec} R_S$ и множеството на простите идеали на R, които не пресичат S.

Доказателство. Нека $\mathfrak{P}$ е прост идеал на R_S. Тогава $\mathfrak{P} \cap S = \emptyset$, защото всички елементи на S са обратими в R_S. Следователно идеалът $\mathfrak{p} = \mathfrak{P} \cap R \in \operatorname{Spec} R$ не пресича S. Тъй като $\mathfrak{P} = (\mathfrak{P} \cap R)R_S$, то (1) е инекция. Ако идеалът $\mathfrak{p} \in \operatorname{Spec} R$ не пресича S, то според горната лема $\mathfrak{p}R_S \in \operatorname{Spec} R_S$ и $\mathfrak{p} = \mathfrak{p}R_S \cap R$. $\square$

Следствие. *Нека $\mathfrak{p}$ е прост идеал на R. Тогава изображението*

$$\operatorname{Spec} R_{\mathfrak{p}} \ni \mathfrak{P} \longmapsto \mathfrak{P} \cap R \in \operatorname{Spec} R$$

задава биекция между $\operatorname{Spec} R_{\mathfrak{p}}$ и множеството на простите идеали на R, които се съдържат в $\mathfrak{p}$.

Доказателство. Следва от предишното твърдение, когато $S = R \setminus \mathfrak{p}$. $\square$