Факториални дедекиндови пръстени. Разширения на дедекиндови пръстени

12. Факториални дедекиндови пръстени

Лема 12.1. *Нека R е факториален пръстен и нека p е елемент на R. Тогава*

$$p \text{ е неразложим елемент на } R \;\Leftrightarrow\; (p) \text{ е прост идеал на } R.$$

Доказателство. ($\Rightarrow$): Ако $a, b \notin (p)$, то p не дели a и p не дели b, откъдето получаваме, че p не дели ab. Следователно $ab \notin (p)$.

($\Leftarrow$): Нека $p = ab$. Тъй като идеалът (p) е прост, то или $a \in (p)$ или $b \in (p)$. Ако $a \in (p)$, то $b \in R^*$; ako $b \in (p)$, то $a \in R^*$. □

Твърдение 12.2. *Всеки факториален дедекиндов пръстен R е област на главни идеали.*

Доказателство. Да покажем, че всеки прост идеал $\mathfrak{p} \neq \{0\}$ на R е главен идеал. Нека $x \in \mathfrak{p} \setminus \{0\}$. Тогава съществуват неразложими елементи $p_i \in R$, $i = 1, \ldots, r$, такива че $x = \prod_{i=1}^{r} p_i$. Тъй като идеалът $\mathfrak{p}$ е прост, то някой от елементите p_i принадлежи на $\mathfrak{p}$, т.е. $(p_i) \subset \mathfrak{p}$ за някой индекс $0 \leq i \leq r$. Сега (p_i) е прост идеал на R според Лема 12.1 и тъй като R е дедекиндов пръстен, то (p_i) е максимален идеал на R. Следователно $\mathfrak{p} = (p_i)$, т.е. $\mathfrak{p}$ е главен идеал. Тъй всеки идеал на R се представя като произведение на прости идеали, то всеки идеал на R е главен. □

Пример 12.3. Нека $F = \mathbb{Q}(\sqrt{-5})$ и нека D е пръстенът на целите алгебрични числа във F. От Упражнение 8.12 знаем, че

$$D = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

Пръстенът D е дедекиндов, но не е факториален, защото

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

и целите алгебрични числа $2, 3, 1 + \sqrt{-5}$ и $1 - \sqrt{-5}$ са неразложими елементи на пръстена D. За да докажем последното твърдение, да забележим, че ако $\alpha = a + b\sqrt{-5} \in D$, то $N_{\mathbb{Q}}^{F}(\alpha) = a^2 + 5b^2$. Ясно е, че $N_{\mathbb{Q}}^{F}(\alpha) \neq 2, 3$ за всяко цяло алгебрично число $\alpha \in D$. Да предположим, че $2 = \alpha_1\alpha_2$, където $\alpha_1, \alpha_2 \in D$. Тогава $N_{\mathbb{Q}}^{F}(\alpha_1)N_{\mathbb{Q}}^{F}(\alpha_2) = 4$, откъдето получаваме, че или $N_{\mathbb{Q}}^{F}(\alpha_1) = 1$ или $N_{\mathbb{Q}}^{F}(\alpha_2) = 1$, т.е. или $\alpha_1 \in D^*$ или $\alpha_2 \in D^*$. Следователно 2 е неразложим елемент на пръстена D. По същия начин проверяваме, че $3, 1 + \sqrt{-5}$ и $1 - \sqrt{-5}$ са неразложими елементи на пръстена D.

Задача 12.4. Нека F и D са както в Пример 12.3 и нека $\mathfrak{p}_1$, $\mathfrak{p}_2$ и $\mathfrak{p}_3$ са следните идеали на D:

$$\mathfrak{p}_1 = (2, 1 + \sqrt{-5}),\ \mathfrak{p}_2 = (3, 1 + \sqrt{-5}),\ \mathfrak{p}_3 = (3, 1 - \sqrt{-5}).$$

Да се докаже, че $\mathfrak{p}_1$, $\mathfrak{p}_2$ и $\mathfrak{p}_3$ са прости идеали на D, такива че

$$\mathfrak{p}_1^2 = (2),\ \mathfrak{p}_2\mathfrak{p}_3 = (3),\ \mathfrak{p}_1\mathfrak{p}_2 = (1 + \sqrt{-5}),\ \mathfrak{p}_1\mathfrak{p}_3 = (1 - \sqrt{-5}).$$

Ние ще използуваме следващата добре известна лема, за да докажем, че всеки дедекиндов пръстен с краен брой максимален прости идеали е факториален.

Лема 12.5. *Нека $I, P_1, \ldots, P_r$ са идеали на пръстена R. Ако $P_3, \ldots, P_r$ са прости идеали и $I \not\subset P_i$, $i = 1, \ldots, r$, то $I \not\subset \cup_{i=1}^{r} P_i$.*

Доказателство. Ще използуваме принципа на математическата индукция.
Нека $r = 2$. Да изберем $x \in I \setminus P_1$ и $y \in I \setminus P_2$. Тогава поне един от елементите $x, y, x + y$ не принадлежи на $P_1 \cup P_2$. Наистина, ако $x \in P_2$ и $y \in P_1$, то $x + y \notin P_1 \cup P_2$.
Нека $r > 2$. Можем да предполагаме, че между идеалите P_i, $i = 1, \ldots, r$, няма включвания. Да изберем елемент $x \in I \setminus \cup_{i=1}^{r-1} P_i$ - това е възможно според индукционната хипотеза. Тъй като идеалът P_r е прост, то $IP_1 \ldots P_{r-1} \not\subset P_r$. Нека $y \in IP_1 \ldots P_{r-1} \setminus P_r$. Сега или x или $x + y$ не принадлежи на $\cup_{i=1}^{r} P_i$. Наистина, ако $x \in P_r$, то $x + y \notin \cup_{i=1}^{r-1} P_i$ и $x + y \notin P_r$. □

Дефиниция. Пръстен с краен брой максимални идеали се нарича полулокален.

Теорема 12.6. *Всеки полулокален дедекиндов пръстен R е област на главни идеали.*

Доказателство. Нека $\mathfrak{p}_i$, $i = 1, \ldots, n$, са всички различни максимални идеали на полулокалния дедекиндов пръстен R. Тъй като всеки идеал на R се представя като произведение на прости идеали, то е достатъчно да докажем, че всеки от идеалите $\mathfrak{p}_i$, $i = 1, \ldots, n$, е главен. Да забележим, че $\mathfrak{p}_i \not\subset \mathfrak{p}_i^2$ и $\mathfrak{p}_i \not\subset \mathfrak{p}_j$, когато $j \neq i$. От Лема 12.5 следва, че съществува елемент $x_i \in \mathfrak{p}_i$, такъв че $x_i \notin \mathfrak{p}_i^2$ и $x_i \notin \mathfrak{p}_j$, $j \neq i$. Тогава $(x_i) = \mathfrak{p}_i$, $i = 1, \ldots, n$. □

Задача 12.7. Да се докаже, че всеки идеал I на един дедекиндов пръстен R може да се породи от най-много два елемента.

13. Разширения на дедекиндови пръстени

Нека $R \subset T$ са дедекиндови пръстени, такива че T е крайнопороден R-модул. Тогава полето от частни L на T е крайно разширение на полето от частни K на R. Наистина, нека $S = R \setminus \{0\}$. Тогава областта T_S е крайномерно векторно пространство над полето $K = R_S$. Следователно T_S е поле и от включванията $T \subset T_S \subset L$ следва, че $T_S = L$.
Нека $\mathfrak{P}$ е прост идеал на T и нека $\mathfrak{p} = \mathfrak{P} \cap R$. Според Твърдение 6.9, ако идеалът $\mathfrak{P}$ е максимален в T, то идеалът $\mathfrak{p}$ е максимален в R. От тук следва, че ако $\mathfrak{P} \neq 0$, то $\mathfrak{p} \neq 0$. От сега нататък ще разглеждаме само такива прости идеали на R и T, които са различни от нулевия идеал.

Дефиниция 13.1. Нека $\mathfrak{p}$ е прост идеал на R. Ако $\mathfrak{P}$ е прост идеал на T, такъв че $\mathfrak{p} = \mathfrak{P} \cap R$, то ще казваме, че $\mathfrak{P}$ *лежи над* $\mathfrak{p}$ и ще пишем $\mathfrak{P}|\mathfrak{p}$.

Забележка 13.1. Ясно е, че простият идеал $\mathfrak{P}$ на T лежи над простия идеал $\mathfrak{p}$ на R тогава и само тогава, когато $\mathfrak{p} \subset \mathfrak{P}$.

Да забележим, че ако $\mathfrak{P}|\mathfrak{p}$, то от теоремата за хомоморфизмите следва, че полето $T/\mathfrak{P}$ е разширение на полето $R/\mathfrak{p}$:

$$\begin{tikzcd} R \arrow[r, hook] \arrow[d] & T \arrow[d] \\ R/\mathfrak{p} \arrow[r, hook] & T/\mathfrak{P} \end{tikzcd}$$

Нещо повече, полето $T/\mathfrak{P}$ е *крайно* разширение на полето $R/\mathfrak{p}$, защото пръстенът T е крайнопороден R-модул.

Дефиниция 13.2. Нека $\mathfrak{P}|\mathfrak{p}$. Тогава степента $[T/\mathfrak{P} : R/\mathfrak{p}]$ се нарича *степен на разклонение на* $\mathfrak{P}$ *над* $\mathfrak{p}$ и се означава с $f(\mathfrak{P}|\mathfrak{p})$ (или $f(\mathfrak{P})$).

Ако $\mathfrak{P}|\mathfrak{p}$, то $\mathfrak{p}$ се съдържа в максималния идеал $\mathfrak{P}T_{\mathfrak{P}}$ на локализацията $T_{\mathfrak{P}}$:

$$\begin{array}{ccccc}
\mathfrak{p} & \hookrightarrow & \mathfrak{P} & \hookrightarrow & \mathfrak{P}T_{\mathfrak{P}} \\
\downarrow & & \downarrow & & \downarrow \\
R & \hookrightarrow & T & \hookrightarrow & T_{\mathfrak{P}}
\end{array}$$

Тъй като $T_{\mathfrak{P}}$ е пръстен на дискретно нормиране, то съществува естествено число e, такова че

$$\mathfrak{p}T_{\mathfrak{P}} = (\mathfrak{P}T_{\mathfrak{P}})^e.$$

Дефиниция 13.3. Нека $\mathfrak{P}|\mathfrak{p}$ и нека $\mathfrak{p}T_{\mathfrak{P}} = (\mathfrak{P}T_{\mathfrak{P}})^e$, $e \in \mathbb{N}$. Тогава естественото число e се нарича *индекс на разклонение на* $\mathfrak{P}$ *над* $\mathfrak{p}$ и се означава с $e(\mathfrak{P}|\mathfrak{p})$ (или $e(\mathfrak{P})$).

Теорема 13.2. *Нека* $\mathfrak{p}$ *е прост идеал на* R. *Тогава*

$$\sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P})f(\mathfrak{P}) = [L : K].$$

От Теорема 13.2 следва, че:

(i) за всеки прост идеал $\mathfrak{p}$ на R съществува поне *един* прост идеал $\mathfrak{P}$ на T, който лежи над $\mathfrak{p}$ (това означава, че $\mathfrak{p}T \neq T$);

(ii) за всеки прост идеал $\mathfrak{p}$ на R съществуват само *краен* брой прости идеали $\mathfrak{P}$ на T, който лежат над $\mathfrak{p}$.

Следващата лема описва простите идеали на T, които лежат над даден прост идеал $\mathfrak{p}$ на R.

Лема 13.3. *Нека* $\mathfrak{p}$ *е прост идеал на* R *и нека*

$$\mathfrak{p}T = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}, \quad e_i > 0,\ i = 1, \ldots, r,$$

е разлагането на идеала $\mathfrak{p}T$ *на прости идеали в пръстена* T. *Тогава*

(i) идеалите $\mathfrak{P}_i$, $i = 1, \ldots, r$, *изчерпват простите идеали на* T, *които лежат над* $\mathfrak{p}$*;*

(ii) $e(\mathfrak{P}_i) = e_i$, $i = 1, \ldots, r$.

Доказателство. (i) Тъй като всеки от идеалите $\mathfrak{P}_i$, $i = 1, \ldots, r$, съдържа $\mathfrak{p}$, то всеки от тях лежи над $\mathfrak{p}$. Обратно, ако $\mathfrak{P}$ е прост идеал на T, който лежи над $\mathfrak{p}$, то

$$\mathfrak{P} \supset \mathfrak{p}T = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i},$$

откъдето следва, че $\mathfrak{P}$ съвпада с някой от идеалите $\mathfrak{P}_i$, $i = 1, \ldots, r$.

(ii) Тъй като $\mathfrak{P}_j T_{\mathfrak{P}_i} = T_{\mathfrak{P}_i}$, когато $j \neq i$, то

$$\mathfrak{p}T_{\mathfrak{P}_i} = (\mathfrak{p}T)T_{\mathfrak{P}_i} = (\prod_{j=1}^{r} \mathfrak{P}_j^{e_j})T_{\mathfrak{P}_i} = \prod_{j=1}^{r} (\mathfrak{P}_j T_{\mathfrak{P}_i})^{e_j} = (\mathfrak{P}_i T_{\mathfrak{P}_i})^{e_i},$$

което показва, че $e(\mathfrak{P}_i) = e_i$, $i = 1, \ldots, r$. □

Първо ще докажем Теорема 13.2, когато R е пръстен на дискретно нормиране.

Лема 13.4. *Нека R е пръстен на дискретно нормиране с максимален идеал $\mathfrak{m}$ и нека*

$$\mathfrak{m}T = \prod_{i=1}^{r} \mathfrak{M}_i^{e_i}, \quad e_i > 0, \ i = 1, \dots, r,$$

където $\mathfrak{M}_i$, $i = 1, \dots, r$, са всички различни максимални идеали на T. Нека $f_i = f(\mathfrak{M}_i)$, $i = 1, \dots, r$. Тогава

(i) T е свободен R-модул от ранг $[L : K]$;

(ii) $T/\mathfrak{m}T \cong T/\mathfrak{M}_1^{e_1} \times \dots \times T/\mathfrak{M}_r^{e_r}$;

(iii) $\dim_{R/\mathfrak{m}} T/\mathfrak{M}_i^{e_i} = e_i f_i$, $i = 1, \dots, r$;

(iv) $\sum_{i=1}^{r} e_i f_i = [L : K]$.

Доказателство. (i) Тъй като R е пръстен на главни идеали и T е крайнопороден R-модул без торзия, то T е свободен R-модул. Нека $t_1, \dots, t_n$ е базис на T като R-модул и нека $S = R \setminus \{0\}$. Тогава лесно се проверява, че $t_1, \dots, t_n \in T$ е също така базис на локализацията T_S като R_S-модул. Но $R_S = K$ и както отбелязахме, локализацията T_S съвпада с L. Следователно $n = [L : K]$.

(ii) Тъй като идеалите $\mathfrak{M}_i$, $i = 1, \dots, r$, са максимални, то те са взаимно прости, т.е. $\mathfrak{M}_i + \mathfrak{M}_j = T$ за $i \neq j$. Тогава идеалите $\mathfrak{M}_i^{e_i}$, $i = 1, \dots, r$, са също взаимно прости и според китайската теорема за остатъците

$$T/\mathfrak{M}_1^{e_1} \times \dots \times T/\mathfrak{M}_r^{e_r} \cong T/(\mathfrak{M}_1^{e_1} \dots \mathfrak{M}_r^{e_r}) = T/\mathfrak{m}T.$$

(iii) Нека проверим, че

$$\dim_{R/\mathfrak{m}} T/\mathfrak{M}_i^{e_i} = \sum_{j=0}^{e_i - 1} \dim_{R/\mathfrak{m}} \mathfrak{M}_i^j/\mathfrak{M}_i^{j+1}, \quad i = 1, \dots, r. \tag{13.1}$$

От изоморфизма на линейни пространства

$$\mathfrak{M}_i^j/\mathfrak{M}_i^{j+1} \cong (\mathfrak{M}_i^j/\mathfrak{M}^{e_i})/(\mathfrak{M}_i^{j+1}/\mathfrak{M}^{e_i}), \quad j = 0, \dots, e_i - 1,$$

получаваме

$$\dim_{R/\mathfrak{m}} \mathfrak{M}_i^j/\mathfrak{M}_i^{j+1} = \dim_{R/\mathfrak{m}} \mathfrak{M}_i^j/\mathfrak{M}^{e_i} - \dim_{R/\mathfrak{m}} \mathfrak{M}_i^{j+1}/\mathfrak{M}^{e_i}, \ j = 0, \dots, e_i - 1.$$

Следователно

$$\begin{aligned}
\sum_{j=0}^{e_i-1} \dim_{R/\mathfrak{m}} \mathfrak{M}_i^j/\mathfrak{M}_i^{j+1} &= \sum_{j=0}^{e_i-1} (\dim_{R/\mathfrak{m}} \mathfrak{M}_i^j/\mathfrak{M}^{e_i} - \dim_{R/\mathfrak{m}} \mathfrak{M}_i^{j+1}/\mathfrak{M}^{e_i}) \\
&= \sum_{j=0}^{e_i-1} \dim_{R/\mathfrak{m}} \mathfrak{M}_i^j/\mathfrak{M}^{e_i} - \sum_{j=1}^{e_i} \dim_{R/\mathfrak{m}} \mathfrak{M}_i^j/\mathfrak{M}^{e_i} \\
&= \dim_{R/\mathfrak{m}} T/\mathfrak{M}^{e_i} - \dim_{R/\mathfrak{m}} \mathfrak{M}_i^{e_i}/\mathfrak{M}^{e_i} \\
&= \dim_{R/\mathfrak{m}} T/\mathfrak{M}^{e_i}.
\end{aligned}$$

Да забележим, че всеки от идеалите $\mathfrak{M}_i^j$, $j \geq 0$ е главен, защото пръстенът T е полулокален (виж Теорема 12.6). Следователно всеки идеал $\mathfrak{M}_i^j$, $j \geq 0$, е изоморфен на T като T-модул откъдето следва, че всеки фактор-модул $\mathfrak{M}_i^j/\mathfrak{M}_i^{j+1}$, $j \geq 0$, е изоморфен на $T/\mathfrak{M}_i$ като линейно пространство над $T/\mathfrak{M}_i$. Но тогава всеки фактор-модул $\mathfrak{M}_i^j/\mathfrak{M}_i^{j+1}$, $j \geq 0$, е изоморфен на $T/\mathfrak{M}_i$ като линейно пространство над $R/\mathfrak{m}$. Следователно

$$\dim_{R/\mathfrak{m}} \mathfrak{M}_i^j/\mathfrak{M}_i^{j+1} = \dim_{R/\mathfrak{m}} T/\mathfrak{M}_i = f_i, \quad j \geq 0.$$

Окончателно от (13.1) получаваме, че $\dim_{R/\mathfrak{m}} T/\mathfrak{M}_i^{e_i} = \sum_{j=0}^{e_i-1} f_i = e_i f_i$.

(iv) Тъй като T е свободен R-модул от ранг $[L:K]$, то $T/\mathfrak{m}T$ е линейно пространство над $R/\mathfrak{m}$ с размерност $[L:K]$. От (ii) и (iii) получаваме

$$[L:K] = \dim_{R/\mathfrak{m}} T/\mathfrak{m}T = \sum_{i=1}^{r} \dim_{R/\mathfrak{m}} T/\mathfrak{M}_i^{e_i} = \sum_{i=1}^{r} e_i f_i. \qquad \square$$

Лема 13.5. *Нека P е прост идеал на пръстена A и нека S е мултипликативно затворено подмножество на A, такова че $S \cap P = \emptyset$. Да означим пръстена A_S с $\widetilde{A}$ и идеала PA_S с $\widetilde{P}$. Тогава*

(i) $\widetilde{A} \subset A_P$, $PA_P \cap \widetilde{A} = \widetilde{P}$ и $\widetilde{A}_{\widetilde{P}} = A_P$;

(ii) ако P е максимален идеал на A, то естественото влагане $A/P \xrightarrow{i} \widetilde{A}/\widetilde{P}$ е изоморфизъм на полета.

Доказателство. (i) Включването $\widetilde{A} \subset A_P$ следва от включването $S \subset A \setminus P$.

$$\begin{tikzcd}
P \arrow[r, hook] \arrow[d, hook] & \widetilde{P} \arrow[r, hook] \arrow[d, hook] & PA_P \arrow[d, hook] \\
A \arrow[r, hook] & \widetilde{A} \arrow[r, hook] & A_P
\end{tikzcd}$$

Ако $x \in PA_P \cap \widetilde{A}$, то $x = p/t = a/s$, където $p \in P$, $t \notin P$, $a \in A$, $s \in S$. Тогава $ta = sp \in P$ и тъй като $t \notin P$, то $a \in P$. Следователно $x = a/s \in PA_S = \widetilde{P}$. Сега от $PA_P \cap \widetilde{A} = \widetilde{P}$ следва, че $\widetilde{A}_{\widetilde{P}} \subset A_P$. Освен това, тъй като $A \cap \widetilde{P} = P$, всеки елемент на $A \setminus P$ е обратим в $\widetilde{A}_{\widetilde{P}}$. Следователно $\widetilde{A}_{\widetilde{P}} = A_P$.

(ii) Нека $\varphi : A \to A/P$ и $\widetilde{\varphi} : \widetilde{A} \to \widetilde{A}/\widetilde{P}$ са естествените хомоморфизми на факторизация.

$$\begin{tikzcd}
A \arrow[r, hook] \arrow[d, "\varphi"'] & \widetilde{A} \arrow[d, "\widetilde{\varphi}"] \arrow[dl, "\varphi_S"] \\
A/P \arrow[r, hook, "i"] & \widetilde{A}/\widetilde{P}
\end{tikzcd}$$

Нека хомоморфизмът $\varphi_S : \widetilde{A} \to A/P$ е определен с формулата

$$\varphi_S(a/s) = \varphi(a)\varphi(s)^{-1}, \quad a \in A,\ s \in S.$$

Тъй като $\widetilde{\varphi} = i \circ \varphi_S$, влагането i е сюрективно. $\square$

Лема 13.6. *Нека $\mathfrak{p}$ е прост идеал на R и нека $\mathfrak{P}$ е прост идеал на T, който лежи над $\mathfrak{p}$. Да означим с $\widetilde{R}$ (съотв. $\widetilde{T}$) пръстена $R_{\mathfrak{p}}$ (съотв. $T_{\mathfrak{p}}$) и с $\widetilde{\mathfrak{p}}$ (съотв. $\widetilde{\mathfrak{P}}$) идеала $\mathfrak{p}\widetilde{R}$ (съотв. $\mathfrak{P}\widetilde{T}$). Тогава*

(i) $\widetilde{\mathfrak{P}}$ лежи над $\widetilde{\mathfrak{p}}$;

(ii) $e(\widetilde{\mathfrak{P}}|\widetilde{\mathfrak{p}}) = e(\mathfrak{P}|\mathfrak{p})$;

(iii) $f(\widetilde{\mathfrak{P}}|\widetilde{\mathfrak{p}}) = f(\mathfrak{P}|\mathfrak{p})$.

Доказателство. (i) Тъй като $\widetilde{\mathfrak{P}} \supset \widetilde{\mathfrak{p}}$, то $\widetilde{\mathfrak{P}}|\widetilde{\mathfrak{p}}$.

(ii) Според Лемма 13.5 (i) локализацията $\widetilde{T}_{\widetilde{\mathfrak{P}}}$ съвпада с локализацията $T_{\mathfrak{P}}$. Освен това, от включванията $R \subset \widetilde{R} \subset T_{\mathfrak{P}}$ следва, че

$$\widetilde{\mathfrak{p}}\widetilde{T}_{\widetilde{\mathfrak{P}}} = \widetilde{\mathfrak{p}}T_{\mathfrak{P}} = (\mathfrak{p}\widetilde{R})T_{\mathfrak{P}} = \mathfrak{p}T_{\mathfrak{P}}.$$

Следователно $e(\widetilde{\mathfrak{P}}|\widetilde{\mathfrak{p}}) = e(\mathfrak{P}|\mathfrak{p})$.

(iii) Според Лемма 13.5 (ii) влаганията $R/\mathfrak{p} \to \widetilde{R}/\widetilde{\mathfrak{p}}$ и $T/\mathfrak{P} \to \widetilde{T}/\widetilde{\mathfrak{P}}$ са изоморфизми. Следователно

$$f(\widetilde{\mathfrak{P}}|\widetilde{\mathfrak{p}}) = [\widetilde{T}/\widetilde{\mathfrak{P}} : \widetilde{R}/\widetilde{\mathfrak{p}}] = [T/\mathfrak{P} : R/\mathfrak{p}] = f(\mathfrak{P}|\mathfrak{p}). \qquad \square$$

Сега можем да сведем Теорема 13.2 до Лема 13.4.

Доказателство на Теорема 13.2.
Да означим с $\widetilde{R}$ (съотв. $\widetilde{T}$) пръстена $R_{\mathfrak{p}}$ (съотв. $T_{\mathfrak{p}}$) и с $\widetilde{\mathfrak{p}}$ идеала $\mathfrak{p}\widetilde{R}$. Нека $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ са всички прости идеали на T, които лежат над $\mathfrak{p}$. Тогава

$$\widetilde{\mathfrak{P}}_1 = \mathfrak{P}_1\widetilde{T}, \ldots, \widetilde{\mathfrak{P}}_r = \mathfrak{P}_r\widetilde{T}$$

са всички максимални идеали на $\widetilde{T}$. Освен това $\widetilde{R}$ е пръстен на дискретно нормиране и $\widetilde{T}$ е крайнопороден $\widetilde{R}$-модул. Прилагайки Лема 13.6 и Лема 13.4 получаваме

$$\sum_{i=1}^{r} e(\mathfrak{P}_i|\mathfrak{p})f(\mathfrak{P}_i|\mathfrak{p}) = \sum_{i=1}^{r} e(\widetilde{\mathfrak{P}}_i|\widetilde{\mathfrak{p}})f(\widetilde{\mathfrak{P}}_i|\widetilde{\mathfrak{p}}) = [L : K]. \qquad \square$$

Пример 13.7. Нека $R = \mathbb{Z}$ и $T = \mathbb{Z}[i]$. Тогава $K = \mathbb{Q}$ и $L = \mathbb{Q}[i]$, като $[L : K] = 2$. Нека опишем простите идеали на $\mathbb{Z}[i]$, които лежат над даден прост идеал (p) на $\mathbb{Z}$.

Нека $p = 2$. Тъй като $2 = (1 + i)(1 - i)$ и $1 + i$, $1 - i$ са асоциирани елементи на $\mathbb{Z}[i]$, то $2\mathbb{Z}[i] = \mathfrak{P}^2$, където $\mathfrak{P} = (1 + i) = (1 - i)$. Тъй като $N_K^L(1 + i) = 2$ и тъй като 2 е просто число в $\mathbb{Z}$, то $1 + i$ е неразложим елемент на $\mathbb{Z}[i]$. Следователно $\mathfrak{P}$ е прост идеал в $\mathbb{Z}[i]$, защото $\mathbb{Z}[i]$ е пръстен на главни идеали. Ясно е, че $e(\mathfrak{P}) = 2$ и $f(\mathfrak{P}) = 1$.

Нека $p > 0$ е нечетно просто число, такова че $p \equiv 1 \mod 4$. От Пример 2.1 знаем, че съществуват цели числа a и b, такива че $p = a^2 + b^2 = (a + bi)(a - bi)$. Да забележим, че $a + bi$ и $a - bi$ не са асоциирани елементи на $\mathbb{Z}[i]$, защото $|a| \neq |b|$. Нека $\mathfrak{P}_1 = (a + bi)$ и $\mathfrak{P}_2 = (a - bi)$. Тогава $p\mathbb{Z}[i] = \mathfrak{P}_1\mathfrak{P}_2$ и $\mathfrak{P}_1 \neq \mathfrak{P}_2$. Тъй като $N_K^L(a + bi) = N_K^L(a + bi) = p$ и тъй като p е просто число в $\mathbb{Z}$, то $a+bi$ и $a-bi$ са неразложими елементи на $\mathbb{Z}[i]$. Следователно $\mathfrak{P}_1$ и $\mathfrak{P}_2$ са прости идеали на $\mathbb{Z}[i]$. Ясно е, че $e(\mathfrak{P}_1) = e(\mathfrak{P}_2) = 1$ и $f(\mathfrak{P}_1) = f(\mathfrak{P}_2) = 1$.

Нека $p > 0$ е нечетно просто число, такова че $p \equiv 3 \mod 4$. Тогава главният идеал $\mathfrak{P}$, който се поражда от p в $\mathbb{Z}[i]$ е прост. Наистина,

$$\frac{\mathbb{Z}[i]}{(p)} \cong \frac{\mathbb{Z}[X]}{(p, X^2 + 1)} \cong \frac{\mathbb{Z}_p[X]}{(X^2 + 1)}$$

и тъй като

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1,$$

полиномът $X^2 + 1$ е неразложим в $\mathbb{Z}_p[X]$, откъдето следва, че $\mathbb{Z}_p[X]/(X^2 + 1)$ е поле. Следователно $\mathfrak{P} = p\mathbb{Z}[i]$ е прост идеал на $\mathbb{Z}[i]$. Ясно е, че $e(\mathfrak{P}) = 1$ и $f(\mathfrak{P}) = 2$.