Действие на групата на Галоа

14. Група на разлагане и поле на разлагане

Нека $R \subset T$ са дедекиндови пръстени, такива че T е крайнопороден R-модул. Нека $\mathfrak{p}$ е прост идеал на R и нека $\mathfrak{P}$ е прост идеал на T, който лежи над $\mathfrak{p}$. Полето от остатъци $T/\mathfrak{P}$ (съотв. $R/\mathfrak{p}$) ще бъде означавано с $\overline{T}$ (съотв. $\overline{R}$). За всеки елемент $\alpha \in T$ (съотв. $\beta \in R$), ще означаваме с $\overline{\alpha}$ (съотв. $\overline{\beta}$) елементът $\alpha + \mathfrak{P} \in T/\mathfrak{P}$ (съотв. $\beta + \mathfrak{p} \in R/\mathfrak{p}$). За всеки полином $f = \sum_{i=0}^{n} a_i X^{n-i}$ с коефициенти в пръстена R, ще означаваме с $\overline{f}$ полинома $\sum_{i=0}^{n} \overline{a_i} X^{n-i} \in \overline{R}[X]$. Полиномът $\overline{f} \in \overline{R}[X]$ се нарича *редукция на* полинома $f \in R[X]$ по модул $\mathfrak{p}$. Непосредствено се проверява, че изображението $R[X] \to \overline{R}[X]$, зададено с $f \mapsto \overline{f}$, е епиморфизъм на пръстени.
Да напомним, че полето L е *нормално* разширение на полето K, когато всеки неразложим полином с коефициенти в K, който има корен в L, се разлага на линейни множители в пръстена от полиноми $L[X]$.

Твърдение 14.1. *Нека простият идеал $\mathfrak{P}$ на T лежи над простия идеал $\mathfrak{p}$ на R. Ако полето от частни L на T е нормално разширение на полето от частни K на R, то полето от остатъци $\overline{T}$ е нормално разширение на полето от остатъци $\overline{R}$.*

Доказателство. Нека полиномът $g \in \overline{R}[X]$ е неразложим над $\overline{R}$ и нека g има корен $\overline{\alpha} \in \overline{T}$, където $\alpha \in T$. Ще покажем, че g се разлага на линейни множители в пръстена от полиноми $\overline{T}[X]$.
Да означим с f минималния полином на α над полето K и да забележим, че $f \in R[X]$, защото α е цял над R. Освен това g дели $\overline{f}$, защото $\overline{f}(\overline{\alpha}) = \overline{f(\alpha)} = \overline{0}$. Тъй като полето L е нормално разширение на полето K, полиномът f се разлага на линейни множители в пръстена от полиноми $L[X]$:

$$f = \prod_{i=1}^{n} (X - \alpha_i), \quad \alpha_i \in L,\ i = 1, \ldots, n.$$

Сега всички елементи $\alpha_i \in L$, $i = 1, \ldots, n$, са цели над пръстена R, откъдето следва, че те са също така цели над пръстена T. Но T е цялозатворен пръстен, поради което $\alpha_i \in T$ за всички $i = 1, \ldots, n$. След редукция на полинома f по модул $\mathfrak{P}$ получаваме

$$\overline{f} = \prod_{i=1}^{n} (X - \overline{\alpha_i}), \quad \overline{\alpha_i} \in \overline{T},\ i = 1, \ldots, n,$$

и тъй като g дели $\overline{f}$, то g също се разлага на линейни множители в пръстена от полиноми $\overline{T}[X]$. □

Отсега нататък ще предполагаме, че полето L е *нормално сепарабелно* разширение на полето K и ще означаваме групата на Галоа на L над K с $G_{L|K}$. Ясно е, че пръстенът T е инвариантен спрямо действието на $G_{L|K}$, т.е. $\sigma(T) = T$

за всеки автоморфизъм $\sigma \in G_{L|K}$. Също така е ясно, че ако I е идеал на T и $\sigma \in G_{L|K}$, то $\sigma(I)$ е идеал на T и изображението

$$\overline{\sigma} : T/I \to T/\sigma(I), \quad \overline{\sigma}(\alpha + I) = \sigma(\alpha) + \sigma(I),\ \alpha \in T,$$

е изоморфизъм на пръстени. От тук следва, че ако $\mathfrak{P}$ е прост идеал на T, то $\sigma(\mathfrak{P})$ също е прост идеал на T. Да забележим, че ако простият идеал $\mathfrak{P}$ се намира над простия идеал $\mathfrak{p}$ на R, то простият идеал $\sigma(\mathfrak{P})$ също се намира над $\mathfrak{p}$. Следователно групата на Галоа $G_{L|K}$ действува на множеството от всички прости идеали на T, които се намират над даден прост идеал $\mathfrak{p}$ на R. По нататък ще видим, че това действие е транзитивно.

Лема 14.2. *Да предположим, че $\sigma\mathfrak{P} = \mathfrak{P}$ за всеки $\sigma \in G_{L|K}$. Тогава хомоморфизмът на групи $G_{L|K} \to G_{\overline{T}|\overline{R}}$, зададен с*

$$G_{L|K} \ni \sigma \longmapsto \overline{\sigma} \in G_{\overline{T}|\overline{R}},$$

е епиморфизъм.

Доказателство. За нашите цели е достатъчно да докажем Лема 14.2, когато полето $\overline{T}$ е сепарабелно разширение на полето $\overline{R}$. (Доказателството в общия случай е аналогично.)
Нека $\gamma \in \overline{T}$ е примитивен елемент на полето $\overline{T}$ над полето $\overline{R}$ и нека $\gamma_i \in \overline{T}$, $i = 1, \ldots, k$, са всички спрегнати елементи на γ над полето $\overline{R}$, т.е. γ_i, $i = 1, \ldots, k$, са всички корени на минималния полином $g \in \overline{R}[X]$ на γ над $\overline{R}$. Тогава $\tau(\gamma) \in \{\gamma_1, \ldots, \gamma_k\}$ за всеки $\tau \in G_{\overline{T}|\overline{R}}$. Освен това, ако $\tau_1(\gamma) = \tau_2(\gamma)$ за някои $\tau_1, \tau_2 \in G_{\overline{T}|\overline{R}}$, то $\tau_1 = \tau_2$, защото γ поражда $\overline{T}$ над $\overline{R}$.
Да изберем елемент $\alpha \in T$, такъв че $\overline{\alpha} = \gamma$, и да означим с $f \in R[X]$ минималния полином на α над K. Тогава f се разлага на линейни множители в $T[X]$,

$$f = \prod_{j=1}^{l} (X - \alpha_j)\ , \quad \alpha_j \in T,\ j = 1, \ldots, k,$$

и $\overline{f}$ се разлага на линейни множители в $\overline{T}[X]$,

$$\overline{f} = \prod_{j=1}^{l} (X - \overline{\alpha_j})\ , \quad \overline{\alpha_j} \in \overline{T},\ j = 1, \ldots, k.$$

Тъй като $\overline{f}(\gamma) = \overline{f}(\overline{\alpha}) = \overline{f(\alpha)} = \overline{0}$, то полиномът g дели полинома $\overline{f}$, откъдето следва, че $\{\gamma_1, \ldots, \gamma_k\} \subset \{\overline{\alpha_1}, \ldots, \overline{\alpha_l}\}$.
Нека τ е произволен автоморфизъм от групата на Галоа $G_{\overline{T}|\overline{R}}$. Тогава съществува корен α_j, $1 \leq j \leq l$, на f, такъв че $\tau(\gamma) = \overline{\alpha_j}$. Тъй като α и α_j са спрегнати над K, съществува автоморфизъм $\sigma \in G_{L|K}$, такъв че $\sigma(\alpha) = \alpha_j$. Сега $\overline{\sigma}(\gamma) = \overline{\sigma}(\overline{\alpha}) = \overline{\sigma(\alpha)} = \overline{\alpha_j} = \tau(\gamma)$, откъдето следва, че $\overline{\sigma} = \tau$. □

Дефиниция 14.1. Нека $\mathfrak{P}$ е прост идеал на T. Тогава групата

$$G_{\mathfrak{P}} = \{\sigma \in G_{L|K} : \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

се нарича *група на разлагане* на простия идеал $\mathfrak{P}$.

Ясно е, че изображението $G_{\mathfrak{P}} \to G_{\overline{T}|\overline{R}}$, зададено с $G_{\mathfrak{P}} \ni \sigma \mapsto \overline{\sigma} \in G_{\overline{T}|\overline{R}}$, е хомоморфизъм на групи. Както обаче подсказва Лема 14.2, вярно е повече.

Теорема 14.3. *Хомоморфизмът на групи $G_{\mathfrak{P}} \to G_{\overline{T}|\overline{R}}$, зададен с*

$$G_{\mathfrak{P}} \ni \sigma \longmapsto \overline{\sigma} \in G_{\overline{T}|\overline{R}},$$

е епиморфизъм.

С помоща на следващите няколко леми ще сведем Теорема 14.3 до Лема 14.2. Нека първо установим, че групата на Галоа $G_{L|K}$ действува транзитивно на множеството от всички прости идеали на T, които се намират над даден прост идеал $\mathfrak{p}$ на R.

Лема 14.4. *Нека $\mathfrak{P}_1$ и $\mathfrak{P}_2$ са два прости идеала на T, които се намират над простия идеал $\mathfrak{p}$ на R. Тогава съществува автоморфизъм $\sigma \in G_{L|K}$, такъв че $\sigma\mathfrak{P}_1 = \mathfrak{P}_2$.*

Доказателство. Да предположим, че $\sigma\mathfrak{P}_1 \neq \mathfrak{P}_2$ за всеки $\sigma \in G_{L|K}$. Тогава $\mathfrak{P}_2 \not\subset \sigma\mathfrak{P}_1$, $\sigma \in G_{L|K}$, и според Лема 12.5 съществува елемент $\alpha \in R$, такъв че

$$\alpha \in \mathfrak{P}_2, \qquad \alpha \notin \sigma\mathfrak{P}_1,\ \sigma \in G_{L|K}. \tag{14.1}$$

От формулата за $N_K^L(\alpha)$ получаваме

$$N_K^L(\alpha) = \alpha \prod_{\sigma \in G_{L|K},\ \sigma \neq \mathrm{id}} \sigma(\alpha) \in \mathfrak{P}_2 \cap R = \mathfrak{p}.$$

Следователно $N_K^L(\alpha) \in \mathfrak{P}_1$ и тъй като $\mathfrak{P}_1$ е прост идеал на T, то $\sigma(\alpha) \in \mathfrak{P}_1$ за някой $\sigma \in G_{L|K}$. Тогава $\alpha \in \sigma^{-1}\mathfrak{P}_1$, което противоречи на (14.1). Полученото противоречие показва, че $\sigma\mathfrak{P}_1 = \mathfrak{P}_2$ за някой $\sigma \in G_{L|K}$. □

Забележка 14.5. Ясно е, че $G_{\sigma(\mathfrak{P})} = \sigma G_{\mathfrak{P}} \sigma^{-1}$ за всеки $\sigma \in G_{L|K}$. От Лема 14.4 следва, че ако простите идеали $\mathfrak{P}_1$ и $\mathfrak{P}_2$ лежат над един и същи прост идеал $\mathfrak{p}$ на R, то техните групите на разлагане са спрегнати в $G_{L|K}$.

Твърдение 14.6. *Нека $\mathfrak{P}_1$ и $\mathfrak{P}_2$ са прости идеали на T, които се намират над простия идеал $\mathfrak{p}$ на R. Тогава $e(\mathfrak{P}_1) = e(\mathfrak{P}_2)$ и $f(\mathfrak{P}_1) = f(\mathfrak{P}_2)$.*

Доказателство. Нека $\sigma \in G_{L|K}$ е такъв, че $\sigma\mathfrak{P}_1 = \mathfrak{P}_2$ и нека

$$\mathfrak{p}T = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \dots \mathfrak{P}_r^{e_r}. \tag{14.2}$$

Прилагайки автоморфизма σ към (14.2) получаваме

$$\mathfrak{p}T = \sigma(\mathfrak{p}T) = \sigma(\mathfrak{P}_1)^{e_1}\sigma(\mathfrak{P}_2)^{e_2} \dots \sigma(\mathfrak{P})_r^{e_r} = \mathfrak{P}_2^{e_1}\sigma(\mathfrak{P}_2)^{e_2} \dots \sigma(\mathfrak{P})_r^{e_r}. \tag{14.3}$$

Сега от (14.2), (14.3) и единствеността на разлагането на прости идеали в пръстена T получаваме

$$e(\mathfrak{P}_2) = e_2 = e_1 = e(\mathfrak{P}_1).$$

Освен това, от изоморфизма $T/\mathfrak{P}_1 \cong T/\sigma(\mathfrak{P}_1) = T/\mathfrak{P}_2$ следва, че

$$f(\mathfrak{P}_1) = [T/\mathfrak{P}_1 : R/\mathfrak{p}] = [T/\mathfrak{P}_2 : R/\mathfrak{p}] = f(\mathfrak{P}_2). \qquad \square$$

Твърдение 14.6 показва, че когато полето L е нормално разширение на полето K, степените на разклонение и индексите на разклонение на всички прости идеали на T, които лежат над даден прост идеал $\mathfrak{p}$ на R, са едни и същи. Следователно

$$\mathfrak{p}T = (\mathfrak{P}_1 \dots \mathfrak{P}_r)^e, \text{ където } e = e(\mathfrak{P}_1) = \dots = e(\mathfrak{P}_r),$$

и $efr = [L : K]$, където $f = f(\mathfrak{P}_1) = \dots = f(\mathfrak{P}_r)$. Освен това,

$$r = |G_{L|K} : G_{\mathfrak{P}}| = |G_{L|K}|/|G_{\mathfrak{P}}|,$$

защото действието на $G_{L|K}$ върху множеството $\{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$ е транзитивно. Тъй като $|G_{L|K}| = [L : K]$, ние получаваме, че

$$|G_{\mathfrak{P}}| = ef. \tag{14.4}$$

Дефиниция 14.2. Нека $\mathfrak{P}$ е прост идеал на T. Тогава полето

$$L^d = \{x \in L : \sigma(x) = x \text{ за всеки } \sigma \in G_{\mathfrak{P}}\}$$

се нарича *поле на разлагане* на простия идеал $\mathfrak{P}$.

Забележка 14.7. От основната теорема на теорията на Галоа знаем, че

$$G_{L|L^d} = G_{\mathfrak{P}}. \tag{14.5}$$

Да означим с T^d пръстенът $T \cap L^d$. Следващата лема показва, че T^d е дедекиндов пръстен с поле от частни L^d.

Лема 14.8. *Нека E е подполе на L, което съдържа полето K. Тогава пръстенът $T_E = E \cap T$ е дедекиндов пръстен с поле от частни E.*

Доказателство. Нека S е мултипликативно затвореното множество $R \setminus \{0\}$. Тъй като $T_S = L$, то всеки елемент $x \in L$ има представяне $x = t/s$, където $t \in T$, $s \in S$. Ако освен това $x \in E$, то $t = sx \in E$, откъдето $t \in T \cap E = T_E$. Следователно всеки елемент $x \in E$ има представяне $x = t/s$, където $t \in T_E$, $s \in S$. От съществуването на такова представяне следва, че полето на частни на T_E е E.

За да докажем, че T_E е дедекиндов пръстен ще проверим, че T_E е цялозатворен ньотеров пръстен, в който всеки прост идеал $P \neq \{0\}$ е максимален. Цялозатвореността на T_E следва тривиално от цялозатвореността на T. Тъй като T е крайнопороден модул над ньотеровия пръстен R, то T_E е също крайнопороден над R, откъдето следва, че T_E е ньотеров пръстен. Ако $P \neq \{0\}$ е прост идеал на T_E, то $P \cap R \neq \{0\}$ според Твърдение 6.10. Тогава $P \cap R$ е максимален идеал на R, откъдето следва, че P е също максимален идеал на T_E (виж Твърдение 6.9). □

Да означим с $\mathfrak{Q}$ простия идеал $\mathfrak{P} \cap T^d$ на T^d. Ясно е, че $\mathfrak{P}$ лежи над $\mathfrak{Q}$ и $\mathfrak{Q}$ лежи над $\mathfrak{p}$.

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

Според Лема 14.4 групата на Галоа $G_{L|L^d}$ действува транзитивно на множеството на простите идеали на T, които се намират над $\mathfrak{Q}$. Но $G_{L|L^d} = G_{\mathfrak{P}}$ според (14.5), поради което $\sigma(\mathfrak{P}) = \mathfrak{P}$ за всеки автоморфизъм $\sigma \in G_{L|L^d}$. Следователно $\mathfrak{P}$ е *единственият* прост идеал на T, който лежи над простия идеал $\mathfrak{Q}$ на T^d.

Задача 14.9. Нека $E \supset K$ е подполе на L, такова че $\mathfrak{P}$ е единственият прост идеал на T, който лежи над простия идеал $\mathfrak{P} \cap T_E$ на T_E. Да се докаже, че $E \supset L^d$.

Лема 14.10. *Естественото влагане на полета $R/\mathfrak{p} \to T^d/\mathfrak{Q}$ е изоморфизъм.*

$$\begin{array}{ccccc} R & \hookrightarrow & T^d & \hookrightarrow & T \\ \downarrow & & \downarrow & & \downarrow \\ R/\mathfrak{p} & = & T^d/\mathfrak{Q} & \hookrightarrow & T/\mathfrak{P} \end{array}$$

Доказателство. Ще докажем Лема 14.10, като за всеки елемент $x \in T^d$ посочим елемент $y \in R$, такъв че $y \equiv x \mod \mathfrak{Q}$.
Нека $\overline{K} \supset K$ е алгебричното затваряне на полето K и нека $\tau_1, \ldots, \tau_s : L^d \to \overline{K}$ са всички различни влагания на полето L^d в полето $\overline{K}$, такива че $\tau_i|_K = \mathrm{id}_K$, $i = 1, \ldots, s$. Всяко от влаганията τ_i, $i = 1, \ldots, s$, може да се продължи до

автоморфизъм $\sigma_i \in G_{L|K}$, $i = 1, \ldots, s$, такъв че $\sigma_i|L^d = \tau_i$, $i = 1, \ldots, s$. Без ограничение на общността можем да предполагаме, че $\sigma_1 = \mathrm{id}_L$. Тогава $\sigma_i \notin G_{\mathfrak{P}}$, $i = 2, \ldots, s$, защото $\sigma|_{L^d} = \mathrm{id}_{L^d}$ за всеки $\sigma \in G_{\mathfrak{P}}$. Нека $\mathfrak{Q}_i = \sigma_i^{-1}(\mathfrak{P}) \cap T^d$, $i = 1, \ldots, s$. Тогава $\mathfrak{Q}_i \neq \mathfrak{Q}$, когато $i \neq 1$, защото $\mathfrak{P}$ е единственият прост идеал на T, който лежи над простия идеал $\mathfrak{Q}$ на T^d.
Нека $x \in T^d$. Според китайската теорема за остатъците съществува елемент $z \in T^d$, такъв че

$$z \equiv x \mod \mathfrak{Q}, \qquad z \equiv 1 \mod \mathfrak{Q}_i,\ i = 2, \ldots, s.$$

Сега ще установим, че $N_K^{L^d}(z) \equiv x \mod \mathfrak{Q}$. Тъй като $N_K^{L^d}(z) \in R$, това ще завърши доказателството на Лема 14.10. От $\sigma_i(\mathfrak{Q}_i) \subset \mathfrak{P}$, $i = 1, \ldots, s$, получаваме сравненията

$$z \equiv x \mod \mathfrak{P}, \qquad \sigma_i(z) \equiv 1 \mod \mathfrak{P},\ i = 2, \ldots, s.$$

От последните сравнения следва, че

$$N_K^{L^d}(z) = \prod_{i=1}^{s} \tau_i(z) = \prod_{i=1}^{s} \sigma_i(z) = z \prod_{i=2}^{s} \sigma_i(z) \equiv x \mod \mathfrak{P}.$$

Тъй като $N_K^{L^d}(z), x \in T^d$, то $N_K^{L^d}(z) \equiv x \mod \mathfrak{Q}$. □

Доказателство на Теорема 14.3.
Според Лема 14.2 хомоморфизмът $G_{\mathfrak{P}} = G_{L|L^d} \to G_{\overline{T}|T^d/\mathfrak{Q}}$, зададен с

$$G_{\mathfrak{P}} \ni \sigma \longmapsto \overline{\sigma} \in G_{\overline{T}|T^d/\mathfrak{Q}},$$

е епиморфизъм. Според Лема 14.10 групата $G_{\overline{T}|T^d/\mathfrak{Q}}$ съвпада с групата $G_{\overline{T}/\overline{R}}$. □

15. Група на инерция и поле на инерция

Дефиниция 15.1. Ядрото на хомоморфизма $G_{\mathfrak{P}} \to G_{\overline{T}|\overline{R}}$, зададен с

$$G_{\mathfrak{P}} \ni \sigma \longmapsto \overline{\sigma} \in G_{\overline{T}|\overline{R}},$$

се нарича група на инерция на идеала $\mathfrak{P}$ и се означава с $T_{\mathfrak{P}}$.

Групата на инерция $T_{\mathfrak{P}}$ се състои от всички автоморфизми $\sigma \in G_{\mathfrak{P}}$, такива че

$$\sigma(\alpha) \equiv \alpha \mod \mathfrak{P} \qquad \text{за всеки } \alpha \in T.$$

Твърдение 15.1. *Нека $\mathfrak{P}$ е прост идеал на T, който лежи над простия идеал $\mathfrak{p}$ на R. Ако полето $\overline{T}$ е сепарабелно разширение на полето $\overline{R}$, то*

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

Доказателство. От Теорема 14.3 следва, че $|T_{\mathfrak{P}}| = |G_{\mathfrak{P}}|/|G_{\overline{T}|\overline{R}}|$. Ако разширението на полета $\overline{R} \subset \overline{T}$ е сепарабелно, то $|G_{\overline{T}|\overline{R}}| = [\overline{T} : \overline{R}] = f(\mathfrak{P})$. Тъй като $|G_{\mathfrak{P}}| = e(\mathfrak{P})f(\mathfrak{P})$, то $|T_{\mathfrak{P}}| = e(\mathfrak{P})$. □

Нека R е пръстен от алгебрични числа и нека $\mathfrak{p}$ е прост идеал на R. Тогава $\mathfrak{p} \cap \mathbb{Z}$ е прост идеал на $\mathbb{Z}$ и съществува просто число $p \in \mathbb{Z}$, такова че $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Тъй като $\overline{R}$ е крайно разширение на $\mathbb{Z}_p$, то $\overline{R}$ е крайно поле. Ако $T \supset R$ е пръстен от алгебрични числа и $\mathfrak{P}$ е прост идеал на T, който лежи над простия идеал $\mathfrak{p}$, то $\overline{R} \subset \overline{T}$ е разширение на крайни полета. Тъй като всяко разширение на крайни полета е сепарабелно, ние получаваме следното твърдение:

Твърдение 15.2. *Нека $R \subset T$ са пръстени от алгебрични числа, и нека $\mathfrak{P}$ е прост идеал на T, който се намира над простия идеал $\mathfrak{p}$ на R. Тогава*

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

Доказателство. Следва непосредствено от Твърдение 15.1. □