Група на класовете от дивизори. Степен на разклонение и индекс на разклонение

10. Група на класовете от дивизори на числово поле

Нека E е крайно разширение на полето на рационалните числа $\mathbb{Q}$ и нека A е пръстенът на целите алгебрични числа в E.

Дефиниция 10.1 (Еквивалентни идеали). Идеалите $I, J \in \mathrm{Div}(A)$ се наричат *еквивалентни*, когато $J = xI$ за някое $0 \neq x \in E$.

Когато идеалите I и J са еквивалентни, ще пишем $I \sim J$ и ще казваме, че I и J принадлежат на един и същи *клас от дивизори*. От горната дефиниция следва, че $I \sim J$ тогава и само тогава, когато JI^{-1} е дробен главен идеал.
Да означим с H подгрупата на $\mathrm{Div}(A)$, която се състои от всички главни дробни идеали. Ясно е, че изображението $E^* \to H$, зададено с $E^* \ni x \longmapsto (x) \in H$ е изоморфизъм на мултипликативната група на полето E^* и групата H. Този изоморфизъм ни позволява да отъждествяваме групите E^* и H и отсега нататък ние ще пишем E^* вместо H. Да забележим, че идеалите I и J са еквивалентни точно когато техните образи във факторгрупата $\mathrm{Div}(A)/E^*$ съвпадат.

Дефиниция 10.2 (Група на класовете от дивизори). Факторгрупата

$$\mathrm{Cl}(A) = \mathrm{Div}(A)/E^*$$

се нарича *група на класовете от дивизори* на пръстена A.

Ако пръстенът A е област на главни идеали, то всеки дробен идеал на A е главен, защото всеки дробен идеал $I \in \mathrm{Div}(A)$ има представяне $I = a^{-1}J$, където $a \in A$ и $J \subseteq A$. Следователно $\mathrm{Cl}(A) = \{1\}$, когато A е област на главни идеали. Обратно, ако групата $\mathrm{Cl}(A)$ е тривиална, то всеки идеал I в A е главен, т. е. A е област на главни идеали.
Ще покажем, че групата $\mathrm{Cl}(A)$ е крайна. За тази цел ще използваме следната лема, която е обобщение на теоремата за деление с частно и остатък в пръстена на целите числа:

Лема 10.1. *Съществува положително цяло число M (което зависи само от полето E), притежаващо следното свойство: за всеки две цели алгебрични числа $\alpha, \beta \in A$, $\beta \neq 0$, съществуват цяло число t, $1 \leq t \leq M$, и цяло алгебрично число $\omega \in A$, такива че $|\mathrm{N}(t\alpha - \omega\beta)| < |\mathrm{N}(\beta)|$.*

Доказателство. От мултипликативността на нормата следва, че неравенството $|\mathrm{N}(t\alpha - \omega\beta)| < |\mathrm{N}(\beta)|$ е еквивалентно на неравенството

$$|\mathrm{N}(t\,\frac{\alpha}{\beta} - \omega)| = |\mathrm{N}\left(\frac{t\alpha - \omega\beta}{\beta}\right)| = \frac{|\mathrm{N}(t\alpha - \omega\beta)|}{|\mathrm{N}(\beta)|} < 1.$$

Нека $\gamma = \alpha/\beta \in E$. Достатъчно е да докажем, че съществува цяло число $M > 0$, такова че за всяко $\gamma \in E$ е в сила $|\mathrm{N}(t\gamma - \omega)| < 1$ за някое $1 \leq t \leq M$ и някое $\omega \in A$.

Нека $x_1, \ldots, x_n \in A$ е базис на A над $\mathbb{Z}$ и нека $\sigma_1, \ldots, \sigma_n : E \to \mathbb{C}$ са всички влагания на полето E в полето на комплексните числа. Тогава всяко $\gamma \in E$ има единствено представяне $\gamma = \sum_{i=1}^{n} \gamma_i x_i$ и ние можем да оценим $|\mathrm{N}(\gamma)|$ както следва:

$$|\mathrm{N}(\gamma)| = |\prod_{j=1}^{n} \sigma_j(\gamma)| = |\prod_{j=1}^{n} \sigma_j \left(\sum_{i=1}^{n} \gamma_i x_i \right)| = |\prod_{j=1}^{n} \left(\sum_{i=1}^{n} \sigma_j(\gamma_i)\sigma(x_i) \right)|$$
$$\leq \prod_{j=1}^{n} \left(\sum_{i=1}^{n} |\sigma_j(\gamma_i)||\sigma(x_i)| \right) \leq C(\max_i |\gamma_i|)^n,$$

където $C = \prod_{j=1}^{n} \left(\sum_{i=1}^{n} |\sigma_j(x_i)| \right)$. Да изберем естествено число m, за което е в сила неравенството $m^n > C$ и нека $M = m^n$.

За $\gamma \in E$, $\gamma = \sum_{i=1}^{n} \gamma_i x_i$, нека $\gamma_i = a_i + b_i$, където $a_i \in \mathbb{Z}$ и $0 \leq b_i < 1$. Да положим $[\gamma] = \sum_{i=1}^{n} a_i x_i$ и $\{\gamma\} = \sum_{i=1}^{n} b_i x_i$. Тогава $\gamma = [\gamma] + \{\gamma\}$, където $[\gamma] \in A$ и координатите на $\{\gamma\}$ са в интервала $[0, 1)$.

Нека изображението $\varphi : E \to \mathbb{R}^n$ е определено с $\varphi \left(\sum_{i=1}^{n} \gamma_i x_i \right) = (\gamma_1, \gamma_2, \ldots, \gamma_n)$. За всяко $\gamma \in E$ точката $\varphi(\{\gamma\})$ лежи в единичния куб. Да разбием единичния куб на подкубове със страна $1/m$ и да разгледаме всички точки $\varphi(\{k\gamma\})$ за $1 \leq k \leq m^n + 1$. Тъй като броят на точките е по-голям от броя на подкубовете, поне две от тях се намират в един и същи подкуб; нека това са точките, които съответстват на $h\gamma$ и $l\gamma$ $(h > l)$. Тогава $h\gamma = [h\gamma] + \{h\gamma\}$, $l\gamma = [l\gamma] + \{l\gamma\}$ и

$$t\gamma = (h-l)\gamma = \underbrace{([h\gamma] - [l\gamma])}_{\omega} + \underbrace{(\{h\gamma\} - \{l\gamma\})}_{\delta} = \omega + \delta,$$

където $1 \leq t = h - l \leq m^n = M$, $\omega \in A$ и абсолютната стойност на координатите на δ е по-малка или равна на $1/m$.

Сега от горната оценка следва, че $|\mathrm{N}(\delta)| \leq C(\max_i |\delta_i|)^n \leq C(1/m)^n < 1$, което завършва доказателството на лемата. □

Теорема 10.2. *Групата* $\mathrm{Cl}(A)$ *на класовете от дивизори е крайна.*

Доказателство. Да забележим първо, че всеки дробен идеал K на A е еквивалентен на някой идеал $I \subseteq A$ — наистина за всеки дробен идеал K на A съществува цяло алгебрично число $a \in A$, такова че $I = aK \subseteq A$ и според определението на еквивалентни идеали е в сила $K \sim I$. Нека M е естественото число, определено в Лема 10.1. Ще покажем, че всеки идеал $(0) \neq I \subseteq A$ е еквивалентен на идеал J в A, такъв че $(M!) \subseteq J \subseteq A$. Тъй като само краен брой идеали J в A удовлетворяват последното условие (виж Лема 8.1), групата $\mathrm{Cl}(A)$ е крайна.

Нека $(0) \neq I \subseteq A$ е идеал в A и нека $0 \neq \beta \in I$ е елемент на I с минимална абсолютна стойност на нормата, т. е. $|\mathrm{N}(\alpha)| \geq |\mathrm{N}(\beta)|$ за всеки $0 \neq \alpha \in I$. Нека $\alpha \in I$ — тогава съществуват естествено число t, $1 \leq t \leq M$, и цели алгебрични числа $\omega, \delta \in A$, такива че $t\alpha = \omega\beta + \delta$ и $\mathrm{N}(\delta) < \mathrm{N}(\beta)$. Тъй като $\delta = t\alpha - \omega\beta \in I$, то $\delta = 0$. Следователно за всеки елемент $\alpha \in I$ съществува естествено число t, $1 \leq t \leq M$, такова че $t\alpha \in (\beta)$, откъдето $(M!)I \subseteq (\beta)$. Да забележим, че $(M!)(\beta) \subseteq (M!)I$, защото $\beta \in I$. Сега от $(M!)(\beta) \subseteq (M!)I \subseteq (\beta)$ следва, че $(M!) \subseteq (\beta)^{-1}(M!)I \subseteq A$. Нека J е идеалът $(\beta)^{-1}(M!)I$ — тогава J изпълнява условията $J \sim I$ и $(M!) \subseteq J \subseteq A$. □

Следствие 10.3. *Нека h_A е редът на групата* $\mathrm{Cl}(A)$. *За всеки идеал* $I \in \mathrm{Div}(A)$ *идеалът* I^{h_A} *е главен.*

Доказателство. Ако G е крайна група от ред k, то $g^k = e$ за всеки $g \in G$. Следователно $(IE^*)^{h_A} = I^{h_A}E^* = E^*$ за всеки $I \in \mathrm{Div}(A)$, т. е. I^{h_A} е главен идеал. □

11. Степен на разклонение и индекс на разклонение

Да напомним, че ако идеалът I в пръстена A е различен от нулевия идеал, то идеалът $I \cap \mathbb{Z}$ в пръстена на целите числа $\mathbb{Z}$ също е различен от нулевия идеал (Твърдение 2.5). Ако $P \neq (0)$ е прост идеал в пръстена A, то $P \cap \mathbb{Z} \neq (0)$ е прост идеал в пръстена на целите числа $\mathbb{Z}$, т. е. $P \cap \mathbb{Z} = (p)$ за някое просто число p. Тогава ограничението на хомоморфизма на факторизация $A \to A/P$ върху пръстена $\mathbb{Z}$ индуцира влагане на полето $\mathbb{Z}_p = \mathbb{Z}/(p) \hookrightarrow A/P$; тъй като A е крайнопороден модул над $\mathbb{Z}$, полето A/P е крайно разширение на полето $\mathbb{Z}_p$.

Дефиниция 11.1 (Степен на разклонение). Степента $[A/P : \mathbb{Z}_p]$ на полето A/P над полето $\mathbb{Z}_p$ се нарича *степен на разклонение* на простия идеал P и се означава с f_P.

Да отбележим, че полето A/P съдържа p^{f_p} елемента, $|A/P| = p^{f_p}$.
Според Теорема 9.4 идеалът pA в пръстена A се разлага на произведение на прости идеали. Тъй като $pA \subseteq P$, простият идеал P присъства в разлагането на pA: $pA = P^e P_2^{e_2} \cdots P_r^{e_r}$, където $P_2, \ldots, P_r$ са прости идеали в A и $e > 0$.

Дефиниция 11.2 (Индекс на разклонение). Степента e, с която простият идеал P участва в разлагането $pA = P^e P_2^{e_2} \cdots P_r^{e_r}$, се нарича *индекс на разклонение* на P и се означава с e_P.

Пример 11.1. Нека A $= \mathbb{Z}[i]$ е пръстенът на целите гаусови числа.

(а) От $2 = i(1-i)^2$ следва, че $2A = P^2$, където $P = (1-i)$. Тъй като $A/(1-i) \cong \mathbb{Z}_2$, то $f_P = 1$ и $e_P = 2$.
(б) Нека p е просто число, $p \equiv 3 \mod 4$. Тогава $P = pA$ е прост идеал в A, като $A/P \cong \mathbb{Z}_p[x]/(x^2+1)$ е поле с p^2 елемента. Следователно $f_P = 2$ и $e_P = 1$.
(в) Нека p е просто число, $p \equiv 1 \mod 4$. Тогава $p = a^2+b^2 = (a-bi)(a+bi)$, където a и b са цели числа. Нека $P_1 = (a-bi)$ и $P_2 = (a+bi)$ — тогава $A/P_1 \cong \mathbb{Z}[x]/(a-bx) \cong \mathbb{Z}_p$, $A/P_2 \cong \mathbb{Z}[x]/(a+bx) \cong \mathbb{Z}_p$ и $pA = P_1P_2$. Следователно $f_{P_1} = f_{P_2} = 1$ и $e_{P_1} = e_{P_2} = 1$.

Нека p е просто цяло число и нека $pA = P_1^{e_1}P_2^{e_2}\cdots P_r^{e_r}$, $e_i > 0$, $i = 1, \ldots, r$, е разлагането на pA на два по два различни прости идеали в пръстена A. Да забележим, че всеки прост идеал P в A, такъв че $P \cap \mathbb{Z} = (p)$ съвпада с някой от идеалите $P_1, P_2, \ldots, P_r$. Наистина, от $P \cap \mathbb{Z} = (p)$ следва, че $p \in P$, откъдето $P \supseteq pA = P_1^{e_1}P_2^{e_2}\cdots P_r^{e_r}$. Тъй като P е прост идеал, то P съдържа някой от идеалите $P_1, P_2, \ldots, P_r$: $P \supseteq P_i$ за някое $1 \leq i \leq r$, а тъй като P_i е максимален идеал, то P съвпада с P_i.
Степените на разклонение и индексите на разклонение на простите идеали $P_1, P_2, \ldots, P_r$, които участват в разлагането на идеала pA, са свързани със следната важна зависимост:

Теорема 11.2. $\sum_{i=1}^{r} e_{P_i} f_{P_i} = [E : \mathbb{Q}]$.

Ще докажем Теорема 11.2 с помощта на китайската теорема за остатъците. Нека $I_1, I_2, \ldots, I_r$ са идеали в комутативен пръстен R и нека $I = I_1 \cap I_2 \cap \cdots \cap I_r$. Тогава хомоморфизмите на факторизация $R \to R/I_j$ индуцират хомоморфизъм

$R \to R/I_1 \times R/I_2 \times \cdots \times R/I_r$, $x \mapsto (x+I_1, x+I_2, \ldots, x+I_r)$ с ядро I и от теоремата за хомоморфизмите следва, че хомоморфизмът

$$R/I \longrightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_r,$$

определен с $x+I \mapsto (x+I_1, x+I_2, \ldots, x+I_r)$, е инективен.

Теорема (Китайска теорема за остатъците). *Нека $I_1, I_2, \ldots, I_r$ са два по два взаимно прости идеали в комутативен пръстен R (т. е. $I_j + I_k = R$ за $1 \le j \ne k \le r$). Тогава:*

(а) $I_1 \cap I_2 \cap \cdots \cap I_r = I_1 I_2 \cdots I_r$;

(б) *хомоморфизмът*

$$R/(I_1 I_2 \cdots I_r) \longrightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_r,$$

определен с $x + I_1 I_2 \cdots I_r \mapsto (x+I_1, x+I_2, \ldots, x+I_r)$, е изоморфизъм.

Да забележим, че различните прости идеали $P_1, P_2, \ldots, P_r$, които участват в разлагането $pA = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$, са два по два взаимно прости, защото са максимални. Техните степени $P_1^{e_1}, P_2^{e_2}, \ldots, P_r^{e_r}$, също са два по два взаимно прости идеали: да предположим, че $P_j^{e_j} + P_k^{e_k} \subset A$, за някои $j \ne k$. Тогава съществува максимален идеал M в A, такъв че $P_j^{e_j} + P_k^{e_k} \subseteq M$, т. е. $P_j^{e_j} \subseteq M$ и $P_k^{e_k} \subseteq M$. Следователно $P_j \subseteq M$ и $P_k \subseteq M$, защото M е прост идеал, откъдето $P_j = M$ и $P_k = M$, защото P_j и P_k са максимални идеали. Полученото противоречие показва, че идеалите $P_1^{e_1}, P_2^{e_2}, \ldots, P_r^{e_r}$ са два по два взаимно прости.
В доказателството на Теорема 11.2 ще използваме също следната лема:

Лема 11.3. *Нека $p > 0$ е просто цяло число и нека P е прост идеал в A, такъв че $P \cap \mathbb{Z} = (p)$. Тогава за всяко естествено число m пръстенът A/P^m съдържа $p^{m f_P}$ елемента.*

Доказателство. Първо ще покажем, че за всяко естествено число m абелевата група P^m/P^{m+1} съдържа p^{f_P} елемента. Нека $x \in P^m \setminus P^{m+1}$ и нека I е идеалът $(x) + P^{m+1}$. Тогава $P^{m+1} \subset I \subseteq P^m$, откъдето $P \subset P^{-m} I \subseteq A$. Следователно $P^{-m} I = A$, т. е. $P^m = I = (x) + P^{m+1}$. Да разгледаме хомоморфизма на абелеви групи $f : A \to P^m/P^{m+1}$, определен с $f(a) = ax + P^{m+1}$, $a \in A$. Образът на f е $I/P^{m+1} = P^m/P^{m+1}$, т. е. f е сюрективен, а тъй като $f \ne 0$ и $\ker f \supseteq P$, то $\ker f = P$. Следователно $P^m/P^{m+1} \cong A/P$, откъдето $|P^m/P^{m+1}| = p^{f_P}$.
Сега да разгледаме хомоморфизма на абелеви групи $g : A/P^{m+1} \to A/P^m$, определен с $g(a + P^{m+1}) = a + P^m$, $a \in A$. Ясно е, че g е сюрективен хомоморфизъм и $\ker g = P^m/P^{m+1}$. Тогава от теоремата на Лагранж следва, че

$$|A/P^{m+1}| = |P^m/P^{m+1}||A/P^m| = p^{f_P}|A/P^m|,$$

което завършва доказателството на лемата. □

Доказателство на Теорема 11.2: Според китайската теорема за остатъците е в сила изоморфизма:

$$A/pA \cong A/P_1^{e_{P_1}} \times A/P_2^{e_{P_2}} \times \cdots \times A/P_r^{e_{P_r}}.$$

От Лема 8.1 знаем, че $|A/pA| = p^n$, където $n = [E : \mathbb{Q}]$, а според Лема 11.3 е в сила $|A/P_j^{e_{P_j}}| = p^{e_{P_j} f_{P_j}}$, $j = 1, \ldots, r$. Следователно

$$p^n \;=\; p^{e_{P_1} f_{P_1}}\, p^{e_{P_2} f_{P_2}} \;\cdots\; p^{e_{P_r} f_{P_r}},$$

откъдето следва твърдението на теоремата. □