Група на дивизорите

8. Прости идеали в пръстен на алгебрични числа

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

Лема 8.1. *Факторпръстенът A/I е краен за всеки идеал $I \neq (0)$ в A.*

Доказателство. Според Твърдение 2.5 идеалът I съдържа цяло число $m \neq 0$. Тъй като пръстенът A/I е факторпръстен на $A/(m)$, то е достатъчно да докажем, че факторпръстенът $A/(m)$ е краен за всяко цяло число $m \neq 0$. За тази цел да забележим, че от изоморфизма на абелеви групи $A \cong \mathbb{Z}^n$ следва, че абелевата група $A/(m)$ е изоморфна на $(\mathbb{Z}/m\mathbb{Z})^n$, откъдето $|A/(m)| = |m|^n$. □

Твърдение 8.2. *Всеки прост идеал $P \neq (0)$ в A е максимален.*

Доказателство. От Лема 8.1 знаем, че пръстенът A/P е крайна област, а всяка крайна област е поле. □

Нека $I \neq (0)$ е идеал в A. Тогава всеки идеал във факторпръстена A/I е от вида J/I, където J е идеал в A, който съдържа идеала I. Освен това, ако $P \supseteq I$ е идеал в A, то P/I е прост идеал в A/I точно когато P е прост идеал в A. Тъй като факторпръстенът A/I е краен, то той съдържа само краен брой прости идеали, откъдето следва, че I се съдържа само в краен брой прости идеали на пръстена A. Да забележим, че всеки прост идеал P/I в пръстена A/I е максимален (и минимален!) идеал в A/I, защото P е максимален идеал в A според Твърдение 8.2.
Да напомним, че ако K и L са идеали в пръстена A, множеството

$$(K : L)_A = \{x \in A : xL \subseteq K\}$$

е идеал в A, който се нарича *частно на идеалите K и L в пръстена A*. От определението на идеала $(K : L)_A$ следва, че $(K : L)_A L \subseteq K$. Ясно е, че ако J е идеал в R, такъв че $JL \subset K$, то $J \subseteq (K : L)_A$. Когато идеалът $L = (y)$ главен, ще използваме означението $(K : y)_A$ за частното на идеалите K и (y), а когато $K = (x)$ също е главен идеал, ще пишем $(x : y)_A$.

Лема 8.3. *Нека B е ньотеров пръстен с краен брой прости идеали, всеки от които е едновременно минимален и максимален прост идеал в B. Тогава за всеки прост идеал Q в B съществува елемент $y \in B$ такъв, че $Q = (0 : y)_B$.*

Доказателство. Нека $Q = Q_1, \ldots, Q_r$ са всички *различни* прости идеали в B и нека $\mathfrak{N} = Q_1 \cap \cdots \cap Q_r$ е нилрадикалът на B. Тъй като B е ньотеров пръстен, идеалът $\mathfrak{N}$ е нилпотентен, откъдето следва, че съществува естествено число N, такова че $Q_1^N \cdots Q_r^N = (Q_1 \cdots Q_r)^N = (0)$.
Да предположим, че $Q_2^N \cdots Q_r^N = (0)$. Тогава $Q_1 \supseteq (0) = Q_2^N \cdots Q_r^N$ и тъй като Q_1 е прост идеал, то Q_1 съдържа някой идеал Q_j, $j = 2, \ldots, r$. Тъй като всички идеали Q_j, $j = 2, \ldots, r$, са максимални, то $Q_1 = Q_j$, което е в противоречие с $Q_1 \neq Q_j$, $j = 2, \ldots, r$. Следователно $Q_2^N \cdots Q_r^N \neq (0)$.

Нека $0 \neq z \in Q_2^N \cdots Q_r^N$; тогава $zQ^N = (0)$. Нека l е най-малкото естествено число, такова че $zQ^l = (0)$ и нека $0 \neq y \in zQ^{l-1}$. Тогава $yQ = (0)$ и $(0 : y)_B = Q$, защото $y \neq 0$ и Q е максимален идеал в B. □

Твърдение 8.4. *Нека $I \neq (0)$ е идеал в A и нека $P \supseteq I$ е прост идеал в A. Тогава $P = (I : y)_A$ за някой $y \in A$.*

Доказателство. Нека Q е идеалът P/I в пръстена A/I. Според Лема 8.3 съществува елемент $\overline{y} \in A/I$, такъв че $Q = (0 : \overline{y})_B$. Нека $y \in A$ е такъв, че $\overline{y} = y + I$. Тогава лесно се проверява, че $P = (I : y)_A$. □

Следствие 8.5. *Всеки прост идеал $P \neq (0)$ в A е частно на два главни идеала.*

Доказателство. Нека $0 \neq x \in P$ и нека $I = (x)$. Според Твърдение 8.4 е в сила $P = (I : y)_A$ за някое $y \in A$, т. е. $P = (x : y)_A$. □

9. Дробни идеали на A

Дефиниция 9.1 (Дробен идеал). Нека $I \neq (0)$ е A-подмодул на полето E. Ще казваме, че I е *дробен идеал на A*, когато съществува число $0 \neq a \in A$, такова че $aI \subseteq A$.

Очевидно всеки ненулев идеал на A е дробен идеал на A. Да забележим, че всеки дробен идеал на A е крайнопороден A-модул, защото A е ньотеров пръстен. Обратно, ако $I \neq (0)$ е крайнопороден A-подмодул на E, то лесно се вижда, че I е дробен идеал на A.
Ако I е дробен идеал на A и $a \in A$, то $aI \subseteq I$. Както показва следващата важна лема, обратното твърдение също е вярно.

Лема 9.1. *Ако I е дробен идеал на A и $aI \subseteq I$ за някое $a \in E$, то $a \in A$.*

Доказателство. Нека числата $x_1, x_2, \ldots, x_m \in I$ пораждат I като A-модул. Тогава

$$\begin{array}{l} ax_1 = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m \\ ax_2 = a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ ax_m = a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mm}x_m \end{array} , \qquad a_{ij} \in A,\ 1 \leq i, j \leq m.$$

откъдето следва, че векторът $(x_1, x_2, \ldots, x_m) \neq 0$ е собствен вектор, със собствена стойност a, на матрицата $(a_{ij}) \in M_m(A)$. Тогава a е корен на характеристичния полином на матрицата (a_{ij}), откъдето следва, че a е цяло алгебрично число, т. е. $a \in A$. □

Непосредствено се проверява, че ако I и J са дробни идеали на A, множествата

$$IJ = \{x_1y_1 + \cdots + x_my_m : x_1, \ldots x_m \in I, y_1, \ldots, y_m \in J\},$$
$$(I : J)_E = \{x \in E : xJ \subseteq I\},$$

са отново дробни идеали на A, които се наричат съответно *произведение на I и J* и *частно на I и J в E*. Според Лема 9.1 за всеки дробен идеал I на A е в сила равенството $(I : I)_E = (1)$.

Дефиниция 9.2 (Обратим дробен идеал). Дробният идеал I на A се нарича *обратим*, когато съществува дробен идеал J на A, такъв че $IJ = (1)$.

Ако I и J са дробни идеали, такива че $IJ = (1)$, то $J \subseteq (A : I)_E$. Тогава $(1) = IJ \subseteq I(A : I) \subseteq (1)$, откъдето $I(A : I)_E = (1)$ и $J = (A : I)_E$. Следователно дробният идеал I е обратим точно когато $I(A : I)_E = (1)$. Ако I е обратим дробен идеал, то ще означаваме идеала $(A : I)_E$ с I^{-1}. За всяко $0 \neq x \in E$ главният идеал $(x) = \{ax : a \in A\}$ е обратим, като $(x)^{-1} = (x^{-1})$.

Лема 9.2. *Всеки прост идеал $P \neq (0)$ в A е обратим.*

Доказателство. Тъй като $P \subseteq P(A:P)_E \subseteq A$ и тъй като P е максимален идеал в A, то е достатъчно да докажем, че $P(A:P)_E \neq P$.
Нека $x, y \in A$ са такива, че $P = (x:y)_A = \{a \in A : ay \in (x)\}$ (виж Лема 8.5). Тогава $yP \subseteq (x)$, откъдето $x^{-1}yP \subseteq A$, т. е. $x^{-1}y \in (A:P)_E$.
Да предположим, че $x^{-1}yP \subseteq P$. Тогава $x^{-1}y \in A$ според Лема 9.1, откъдето $y \in (x)$ и $P = (x:y)_A = (1)$. Полученото противоречие показва, че $x^{-1}yP \neq P$. Тъй като $x^{-1}y \in (A:P)_E$, то $P(A:P)_E \neq P$, което влече $P(A:P)_E = A$. □

Да отбележим, че ако $P \neq (0)$ е прост идеал в A, то от равенството $PP^{-1} = (1)$ следва строгото включване $P^{-1} \supset A$.

Лема 9.3. *Нека $(0) \neq I \subset A$ е идеал в A и нека $P \supset I$ е прост идеал в A. Тогава съществува собствен идеал $J \supset I$ в A, такъв че $I = PJ$.*

Доказателство. Нека $J = P^{-1}I$. Тогава $PJ = I$ и $I \subseteq J$, защото $1 \in P^{-1}$. Освен това от $I \subset P$, следва че $J = P^{-1}I \subset P^{-1}P = A$. Ако $I = J = P^{-1}I$, то $P^{-1} \subseteq (I:I)_E = A$ (виж Лема 9.1), което противоречи на строгото включване $P^{-1} \supset A$. Следователно $J \supset I$. □

Теорема 9.4. *Всеки идеал $(0) \neq I \subset A$ се представя по единствен начин (с точност до реда на множителите) като произведение на прости идеали.*

Доказателство. *Съществуване:*
Нека S е множеството от всички ненулеви собствени идеали в A, които не се представят като произведение на прости идеали. Да предположим, че $S \neq \emptyset$ — тогава S съдържа максимален елемент, защото A е ньотеров пръстен. Нека I е максимален елемент в множеството S. Тогава идеалът I не е прост и тъй като I е собствен идеал на A, то $I \subset P$ за някой прост идеал P в A. Сега според Лема 9.3 съществува собствен идеал $J \supset I$, такъв че $I = PJ$. Тъй като I е максимален елемент на S, идеалът J не принадлежи на множеството S, откъдето следва, че съществуват прости идеали $P_1, \ldots, P_k$ в A, такива че $J = P_1 \cdots P_k$. Тогава $I = PJ = PP_1 \cdots P_k$ се представя като произведение на прости идеали, което противоречи на определението на множеството S. Следователно $S = \emptyset$ и всеки ненулев собствен идеал в A се представя като произведение на прости идеали.
Единственост:
Нека $I = P_1 \cdots P_r = Q_1 \cdots Q_s$ са две представяния на идеала I като произведение на прости идеали. Тогава $P_1 \supseteq I = Q_1 \cdots Q_s$, откъдето следва, че простият идеал P_1 съдържа някой от идеалите $Q_1, \ldots, Q_s$. Тъй като идеалите $Q_1, \ldots, Q_s$ са максимални, то P_1 съвпада с някой от тях — след пермутация на $Q_1, \ldots, Q_s$ можем да предполагаме, че $P_1 = Q_1$. Умножавайки равенството $P_1 \cdots P_r = P_1 \cdots Q_s$ с P_1^{-1}, получаваме $P_2 \cdots P_r = Q_2 \cdots Q_s$, след което можем да приложим горното разсъждение за идеала P_2. По този начин установяваме, че $r = s$ и идеалите $Q_1, \ldots, Q_s$ са пермутация на идеалите $P_1, \ldots, P_r$. □

За всяко естествено число m и всеки прост идеал P нека $P^{-m} = (P^{-1})^m$ и нека $P^0 = (1)$. Тогава за всички цели числа m_1 и m_2 е в сила равенството $P^{m_1}P^{m_2} = P^{m_1+m_2}$.

Следствие 9.5. *Всеки дробен идеал I на A има единствено представяне*

$$I = P_1^{m_1} \cdots P_r^{m_r},$$

където $P_1, \ldots, P_r$ са прости идеали в A, а $m_1 \neq 0, \ldots, m_r \neq 0$ са цели числа.

Доказателство. Нека числото $a \in A$ е такова, че $aI \subset A$ и нека

$$(a) = P_1'^{k_1} \cdots P_r'^{k_r}, \qquad aI = P_1''^{k_1} \cdots P_s''^{k_s},$$

където $P'_1, \ldots, P'_r, P''_1, \ldots, P''_s$ са прости идеали в A, а $k_1, \ldots, k_r, l_1, \ldots, l_s$ са естествени числа. Тогава ${P'_1}^{k_1} \cdots {P'_r}^{k_r} I = {P''_1}^{k_1} \cdots {P''_s}^{k_s}$, откъдето следва, че $I = {P'_1}^{-k_1} \cdots {P'_r}^{-k_r} {P''_1}^{k_1} \cdots {P''_s}^{k_s}$. Следователно I се представя като произведение на степени на прости идеали. Единствеността на представянето следва от Теорема 9.4. □

Тъй като произведението на обратими дробни идеали е обратим дробен идеал, и тъй като всяка степен на прост идеал е обратим дробен идеал, то всеки дробен идеал на A е обратим. Нека $\mathrm{Div}(A)$ е множеството на всички дробни идеали на пръстена A. Тогава опреацията умножение на дробни идеали превръща $\mathrm{Div}(A)$ в абелева група, която се нарича *група на дивизорите на* A. Следствие 9.5 показва, че $\mathrm{Div}(A)$ е свободна абелева група:

Твърдение 9.6. *Групата от дивизорите* $\mathrm{Div}(A)$ *на* A *е свободна абелева група с базис всички прости идеали в* A.

Доказателство. Това е друга формулировка на Следствие 9.5.