

Teoria Algébrica dos números

Aula 9: Fatoração Única de Ideais

Ramon M. Nunes

UFC

26 de março de 2020

Resumo da Aula

1 Aula Passada

- Enunciado do Teorema
- Recapitulando: Prova da Existência

2 Aula de Hoje

- Unicidade
- Teorema Chinês dos Restos
- Ideais fracionários
- Exercícios propostos

Aula Passada

Na aula passada estávamos provando o teorema da fatoração única de ideais para domínios de Dedekind, cuja definição, relembramos aqui.

Definição

Um *domínio de Dedekind* é um domínio integral $\mathcal{O}$ satisfazendo as seguintes propriedades:

- $\mathcal{O}$ é noetheriano,
- $\mathcal{O}$ é integralmente fechado ,
- Todo ideal primo de $\mathcal{O}$ é maximal.

O teorema

Precisamente estávamos provando o seguinte resultado:

Teorema (Fatoração única de ideais)

Seja $\mathcal{O}$ um domínio de Dedekind. Todo ideal $\mathfrak{a}$ de $\mathcal{O}$, $\mathfrak{a} \neq (0), (1)$ admite uma fatoração

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r,$$

onde $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ são ideais primos e esta fatoração é única, a menos da ordem.

Existência

Para provar a existência, nós procedemos por absurdo.

Caso existisse pelo menos um ideal que não possuisse fatoração em primos, o lema de Zorn nos garantiria que existe um ideal $\mathfrak{a}$ que é maximal com esta propriedade (não possuir fatoração).

Além disso, $\mathfrak{a} \subseteq \mathfrak{p}$ para algum ideal primo $\mathfrak{p}$.

Segue então de um dos lemas da aula passada que $\mathfrak{a}\mathfrak{p}^{-1}$ é um ideal estritamente maior que $\mathfrak{a}$, onde

$$\mathfrak{p}^{-1} := \{\alpha \in K; \alpha\mathfrak{p} \subseteq \mathcal{O}\}.$$

Existência (cont.)

Além disso, pela maximalidade de $\mathfrak{a}$, temos que $\mathfrak{a}\mathfrak{p}^{-1}$ possui uma fatoração.

Em seguida, utilizando que todo ideal primo é maximal, mostramos que $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.

E assim, a igualdade $\mathfrak{a} = (\mathfrak{a}\mathfrak{p}^{-1})\mathfrak{p}$ gera uma contradição, o que conclui a prova da existência.

Aula de Hoje

Unicidade

Segue da definição de ideal primo que se $\mathfrak{p}$ é um ideal primo e $\mathfrak{a}$ e $\mathfrak{b}$ são ideais de $\mathcal{O}$ então:

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p} \text{ ou } \mathfrak{b} \subseteq \mathfrak{p}$$

Prova: Basta supor por absurdo que existe um elemento $\alpha \in \mathfrak{a} \setminus \mathfrak{p}$ e ver que para todo elemento $\beta \in \mathfrak{b}$, tem-se $\alpha\beta \in \mathfrak{p}$ e, portanto, $\beta \in \mathfrak{p}$.

Lembre que se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais de $\mathcal{O}$, então dizemos que $\mathfrak{a} \mid \mathfrak{b}$ exatamente quando $\mathfrak{b} \subseteq \mathfrak{a}$. Com isso em mente e iterando o fato acima, concluímos que

$$\mathfrak{p} \mid \mathfrak{a}_1 \dots \mathfrak{a}_r \Rightarrow \mathfrak{p} \mid \mathfrak{a}_i \text{ para algum } i \leq r.$$

Unicidade (parte 2)

Suponha agora que $\mathfrak{a}$ é um ideal de $\mathcal{O}$ admitindo duas fatorações em ideais primos

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s, \quad (1)$$

onde todos os $\mathfrak{p}_i$'s e todos os $\mathfrak{q}_j$'s são primos. Em particular temos que

$$\mathfrak{p}_1 \mid \mathfrak{q}_1 \dots \mathfrak{q}_s.$$

Pelo que acabamos de ver, isso implica que $\mathfrak{p}_1 \supseteq \mathfrak{q}_j$ para algum $j \leq s$. Como $\mathfrak{q}_j$ é um ideal primo e $\mathcal{O}$ é de Dedekind, trata-se de um ideal maximal. Portanto, concluímos que $\mathfrak{p}_1 = \mathfrak{q}_j$.

Unicidade (parte 3)

Supondo S.P.G. que $j = 1$ e multiplicando os dois lados de (1) por p^{-1} , deduzimos:

$$p_1^{-1} p_1 \dots p_r = q_1^{-1} q_1 \dots q_s \Leftrightarrow p_2 \dots p_r = q_2 \dots q_s,$$

Utilizamos aqui os seguintes fatos mencionados na aula passada:

1. $pp^{-1} = \mathcal{O}$, 2. A multiplicação de ideais é *associativa*

Repetindo o processo com p_2 , depois com p_3 e assim sucessivamente, concluimos que $r = s$ e a menos de uma re-ordenação dos q_j , temos $p_i = q_i$ para $i = 1, 2, \dots, r$. O que conclui a prova da unicidade no teorema.

Algumas consequências

Agrupando as diferentes aparições de ideais primos na fatoração de um ideal $\mathfrak{a}$, podemos escrever

$$\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_r^{\nu_r}, \quad (\nu_i > 0).$$

No futuro, quando escrevermos uma equação assim, estaremos assumindo tácitamente que os $\mathfrak{p}_i$ são primos 2-a-2 distintos.

Além disso, por motivos de tradição (e simplicidade), escrevemos

$$a = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_r^{\nu_r} \text{ no lugar de } (a) = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_r^{\nu_r}, \\ (\mathfrak{a}, \mathfrak{b}) = 1 \text{ no lugar de } (a) = (\mathfrak{a}, \mathfrak{b}) = \mathcal{O}.$$

Teorema Chinês dos Restos

Relembre o teorema chinês dos restos da teoria dos anéis:

Teorema (TCR)

Seja R um anel (comutativo) e $I_1, \dots, I_n$ ideais de R tais que $I_i + I_j = R$ para quaisquer $i \neq j$. Então, seja $I = I_1 \cap \dots \cap I_n = I_1 \dots I_n$. Então, o homomorfismo natural

$$R/I \rightarrow R/I_1 \times \dots \times R/I_n$$

é um isomorfismo.

Estamos particularmente interessados em aplicações do TCR aos domínios de Dedekind $\mathcal{O}$.

Ideais fracionários

Durante a prova da fatoração única de ideais, introduzimos o conjunto

$$\mathfrak{p}^{-1} = \{x \in K; x\mathfrak{p} \subseteq \mathcal{O}\},$$

e mostramos que $\mathfrak{p}^{-1} \supsetneq \mathcal{O}$. De modo que $\mathfrak{p}^{-1}$ não é um ideal. Vale porém que

$$\begin{aligned} x, y \in \mathfrak{p}^{-1} &\Rightarrow x + y \in \mathfrak{p}^{-1}, \\ \lambda \in \mathcal{O}, x \in \mathfrak{p}^{-1} &\Rightarrow \lambda x \in \mathfrak{p}^{-1}. \end{aligned}$$

Ou seja, $\mathfrak{p}^{-1}$ é um $\mathcal{O}$ -módulo. Definiremos a seguir uma classe de

$\mathcal{O}$ -módulos, incluindo $\mathfrak{p}^{-1}$ que está para os ideais de $\mathcal{O}$ assim como os elementos do corpo de frações de um anel estão para os elementos deste anel.

Ideais fracionários (parte 2)

Chegamos então à seguinte definição.

Definição

Um *ideal fracionário* de K é um $\mathcal{O}$ -submódulo finitamente gerado e não-nulo de K .

A seguir, um exemplo:

Exemplo

Todo $\alpha \in K^\times$ define um ideal fracionário definido por

$$(\alpha) := \alpha\mathcal{O}.$$

Por analogia com o caso clássico, esses são chamados de *ideais fracionários principais*. Note que os ideais fracionários principais formam um grupo, que denotaremos por P_K

Ideais fracionários (parte 3)

Lembre que como estamos supondo que $\mathcal{O}$ é domínio de Dedekind, temos que $\mathcal{O}$ é noetheriano. Vale portanto o seguinte resultado:

Proposição

$\mathfrak{a} \subseteq K$ é um ideal fracionário se, e somente se existe $c \in \mathcal{O}$, $c \neq 0$ tal que $c\mathfrak{a}$ é um ideal de $\mathcal{O}$.

Prova: Primeiramente, seja $c\mathfrak{a}$ um ideal do anel noetheriano $\mathcal{O}$. Então $c\mathfrak{a}$ é finitamente gerado. Seja $\{\alpha_1, \dots, \alpha_n\}$ Um conjunto gerador de $c\mathfrak{a}$. Segue que $\{\alpha_1 c^{-1}, \dots, \alpha_n c^{-1}\}$ é um conjunto gerador do $\mathcal{O}$ -módulo $\mathfrak{a}$. Por outro lado, seja $\{\beta_1, \dots, \beta_m\}$ um conjunto gerado do $\mathcal{O}$ -módulo $\mathfrak{a}$. escrevendo cada β_i como uma fração de $e \in \mathcal{O}$ e tomando c como o produto dos denominadores, vemos que $c\beta_i \in \mathcal{O}$ para todo i . De modo que $c\mathfrak{a}$ é um $\mathcal{O}$ -módulo gerado por elementos de $\mathcal{O}$. Isto é, um ideal.

Ideais fracionários (parte 4)

Nós definimos o produto de ideais fracionários da mesma forma que o produto de ideais de $\mathcal{O}$. Quando for necessário, para evitar confusão, nos referiremos aos ideais de $\mathcal{O}$ como *ideais inteiros*.

Proposição

Os ideais fracionários de K formam um grupo abeliano, denotado por J_K . A identidade é o elemento $(1) = \mathcal{O}$ e um inverso de um ideal fracionário é definido por

$$\mathfrak{a}^{-1} := \{x \in K; x\mathfrak{a} \subseteq \mathcal{O}\}.$$

Prova no proximo quadro:

Ideais fracionários (parte 5)

Prova: A associatividade e comutatividade seguem da definição do produto de ideais fracionários. Além disso, se $\mathfrak{a}$ é um $\mathcal{O}$ -módulo,

$$\mathfrak{a} = 1\mathfrak{a} \subseteq \mathcal{O}\mathfrak{a} = \mathfrak{a}.$$

Dado $\mathfrak{p}$ um ideal primo, já vimos que $\mathfrak{p}\mathfrak{p}^{-1} = (1)$. Seja então $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ um ideal inteiro $\neq 0$ e tome $\mathfrak{b} := \mathfrak{p}_1^{-1} \dots \mathfrak{p}_r^{-1}$. Segue que $\mathfrak{b}\mathfrak{a} = (1)$. Em particular, $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Reciprocamente, se $x \in \mathfrak{a}^{-1}$, então $x \in x\mathfrak{a}\mathfrak{b} \subseteq \mathcal{O}\mathfrak{b} \subseteq \mathfrak{b}$. Logo, $\mathfrak{b} = \mathfrak{a}^{-1}$. Com isso, mostramos que $\mathfrak{a}\mathfrak{a}^{-1} = (1)$ para todo ideal inteiro $\neq 0$.

Para concluir, seja $\mathfrak{a}$ um ideal fracionário, e seja $c \in \mathcal{O}, c \neq 0$ tal que $c\mathfrak{a}$ seja um ideal de $\mathcal{O}$. Portanto, temos

$$\mathfrak{a}\mathfrak{a}^{-1} = (c\mathfrak{a})(c\mathfrak{a})^{-1} = (1).$$

Ideais fracionários (parte 6)

Como consequência das proposições acima, temos o seguinte resultado:

Corolário

Todo ideal fracionário $\mathfrak{a}$ de K admite uma representação única na forma

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}, \quad \nu_{\mathfrak{p}} \in \mathbb{Z},$$

onde $\nu_{\mathfrak{p}} = 0$ para quase todo¹ ideal primo $\mathfrak{p}$. Em outras palavras, J_K é o grupo livre gerado pelo conjunto dos ideais primos de $\mathcal{O}$.

A primeira proposição mostra que todo ideal fracionário se escreve na forma $\mathfrak{b}^{-1}\mathfrak{a}$ e segue da prova da segunda proposição que $\mathfrak{b}^{-1}$ é um produto de ideais fracionários da forma $\mathfrak{p}^{-1}$, onde $\mathfrak{p}$ é primo. A unicidade da representação segue da unicidade da fatoração para ideais inteiros

¹'quase todo' = 'todos, exceto uma quantidade finita'

Ideais fracionários (parte 7)

Para concluir nossas considerações sobre ideais fracionários, introduzimos agora grupo de classes Cl_K do corpo de frações de um domínio de Dedekind:

$$\text{Cl}_K := J_K / P_K,$$

onde J_K é o grupo dos ideais fracionários P_K é o subgrupo formados pelos ideais fracionários principais. Utilizando o grupo de classes e outros grupos associados a $\mathcal{O}$ e K , já indroduzidos previamente, formamos a seguinte sequência exata:

$$1 \rightarrow \mathcal{O}^\times \rightarrow K^\times \rightarrow J_K \rightarrow \text{Cl}_K \rightarrow 1,$$

onde o homomorfismo $K^\times \rightarrow J_K$ é dado por $\alpha \mapsto (\alpha)$ e os outros são dados por inclusões ou projeções naturais.

Ideais fracionários (parte 8)

Filosoficamente, o grupo de classes mede o quão longe o domínio $\mathcal{O}$ está de ser principal. De fato $\text{Cl}_K = 1$ significa que $\mathcal{O}$ é principal e quanto maior o grupo de classes, mais complexo será o grupo de ideais com relação aos grupo de ideais principais.

De uma maneira similar, o grupo $\mathcal{O}^\times$ mede o quanto perdemos ao trocar entre números e ideais.

Em um domínio de Dedekind qualquer, não há muito que se possa dizer sobre estes dois grupos: Cl_K e $\mathcal{O}^\times$. Contudo, nos caso em que $\mathcal{O} = \mathcal{O}_K$ é o anel de inteiros de um corpo de números, vamos mostrar importantes resultados de finitude sobre esses grupos. A saber:

Cl_K é finito e $\mathcal{O}^\times$ é um grupo livre finitamente gerado.

Exercícios Propostos

Para treinar, sugiro os seguintes exercícios do livro do Neukirch:

Seção 3: exercícios 1, 3, 9 e 10

Fim!