Universidade Federal de Sergipe
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL - PROFMAT

Divisibilidade em Domínios de Integridade

Por

Márcio Monte Alegre Sousa

Mestrado Profissional em Matemática - São Cristóvão - SE

Abril de 2013

Universidade Federal de Sergipe
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL - PROFMAT

Márcio Monte Alegre Sousa

Divisibilidade em Domínios de Integridade

Trabalho apresentado ao Departamento de Matemática da Universidade Federal de Sergipe como requisito final para a obtenção do título de Mestre em Matemática pelo PROFMAT

Orientador: Prof. Dr. Danilo Felizardo Barboza

São Cristóvão - Sergipe
Abril de 2013

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Sousa, Márcio Monte Alegre
S725d Divisibilidade em domínios de integridade / Márcio Monte Alegre Sousa; orientador Danilo Felizardo Barboza. – São Cristóvão, 2013.
26 f.

Dissertação (Mestrado Profissional em Matemática em Rede Nacional – Profmat) – Universidade Federal de Sergipe, 2013.

1. Álgebra. 2. Anéis (Álgebra). 3. Algoritmos. I. Barboza, Danilo Felizardo, orient. II. Título

CDU 512.55

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe ,como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Divisibilidade em Domínios de Integridade

por

Márcio Monte Alegre Souza

Aprovada pela Banca Examinadora:

Prof. Dr. Danilo Felizardo Barbosa - UFS
Orientador

Prof. Dr. Claudio Tadeu Cristino - UFRPE
Primeiro Examinador

Prof. Dr. Zaqueu Alves Ramos - UFS
Segundo Examinador

São Cristóvão, 11 de abril de 2013

Cidade Universitária "Prof. José Aloísio de Campos" – Av. Marechal Rondon, s/no - Jardim Rosa Elze – Campus de São Critóvão. Tel. (00 55 79) 2105-6986 – Fax (0 xx 55 79) 2105-6566
CEP: 49100-000 - São Cristóvão – Sergipe - Brasil – E-mail: promat_ufs@yahoo.com.br

Sumário

Agradecimentos

À Deus;
À minha família, em especial, minha mãe Maria José ao meu pai Laércio (in memorian), meus irmãos;
Aos meus colegas Profmatianos;
À minha companheira Maria Eloísa;
Aos meus professores do PROFMAT;
À CAPES
E a todos que participaram de forma direta e indireta para a conclusão deste trabalho.

Resumo

Este trabalho tem como objetivo estudar a divisibilidade em domínios de integridade para tanto, ele foi estruturado da seguinte forma: inicialmente faz-se uma abordagem básica que servirá como pré-requisito para o seu desenvolvimento, em seguida, faremos um estudo sobre os domínios euclidianos e o domínio dos inteiros de Gauss, culminando com a aplicação dos resultados obtidos na caracterização dos ideais primos do anel dos inteiros de Gauss.

Palavras Chaves: Anéis, Subanéis, Ideais, Domínio euclidiano, Inteiros de Gauss.

Abstract

This paper is aimed to study the divisibility in integrality domain. So, it was structured that way: at first it is done a basic approach which will be a pre domain for its development, right after it will be done a study about Euclidean domain and Gaussian integer domains culminating in the enforcement of the results gotten in the characterization of prime ideals Gaussian's integers ring.

Key Words: Rings, Subrings, Ideals, Euclidean domain, Gaussian integers.

Introdução

O termo álgebra moderna significa a área da matemática que se ocupa em estudar as estruturas algébricas. A grosso modo, as estruturas algébricas mais simples são constituidas por um conjunto não vazio e operações binárias, nele definidos, sujeitas a certos axiomas.

Entre as diversas estruturas algébrica figura a de anel. Ela é definida por um conjunto não vazio A e operações $+ : A \times A \to A$, $\cdot : A \times A \to A$ satisfazendo as condições listadas na Definição 1.1. Esta estrutura é de fundamental importância para a matemática contemporânea. Uma das razões é que ela é abstração de sistemas clássicos como: Matrizes, Inteiros e Polinômios (objetos estes que fazem parte do discurso de todas as áreas da matemática).

Nosso interesse nesse trabalho é estudar uma aspecto particular dos anéis, a saber: *a divisibilidade*. Para fazê-lo dividiremos o texto em quatro capítulos.

No primeiro capítulo desenvolvemos as noções e resultados preliminares.

No capítulo 2 estudamos a divisibilidade no contexto dos domínios euclidianos. Como veremos, esses são anéis que generalizam a noção de divisão euclidiana existente no anel de inteiros tal como conhecemos desde o ensino básico. Entre os resultados provados nessa parte, aparece a caracterização dos ideais em um domínio euclidiano.

No capítulo 3 fazemos uma abordagem sobre o domínio dos inteiro de Gauss, enfatizando sobretudo o fato de que este é um domínio euclidiano, e consequentemente Noetheriano e de fatoração única.

Finalmente no último capítulo aplicamos os resultados obtidos nos capítulos anteriores para caracterizar os ideais primos do anel dos inteiros de Gauss.

Capítulo 1

Domínio de integridade

1.1 Anel e Subanel

Definição 1.1 Seja A um conjunto não vazio onde estejam definidas duas operações, as quais chamaremos de adição e multiplicação em A e denotaremos por $+$ e $\cdot$.
Assim,

$$\begin{array}{rcccc} + & : A \times A & \to & A \\ & (a,b) & \mapsto & a+b \end{array} \qquad \begin{array}{rcccc} \cdot & : A \times A & \to & A \\ & (a,b) & \mapsto & a \cdot b \end{array}$$

Chamamos $(A, +, \cdot)$ um **anel** se as seguintes propriedades são verificadas quaisquer que sejam $a, b, c \in A$.

A1. Para todo $a, b, c \in A$, $(a + b) + c = a + (b + c)$ (associatividade da adição);

A2. Existe $0 \in A$ tal que $a + 0 = 0 + a = a$ (existência do elemento neutro com respeito à adição);

A3. Para todo $x \in A$ existe um único $y \in A$, denotado por $y = -x$, tal que $x + y = y + x = 0$ (existência do inverso aditivo);

A4. Para todo $a, b \in A$, $a + b = b + a$ (comutatividade da adição);

A5. Para todo $a, b, c \in A$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associatividade da multiplicação);

A6. Para todo $a, b, c \in A$, $a \cdot (b+c) = a \cdot b + a \cdot c$; $(a+b) \cdot c = a \cdot c + b \cdot c$ (distributividade à esquerda e à direita).

Um anel $(A, +, \cdot)$ que satisfaz a propriedade:

A7. Existe $1 \in A - \{0\}$, tal que $x \cdot 1 = 1 \cdot x = x$, qualquer que seja $x \in A$.

é chamado um **anel com unidade**.

Se um anel $(A, +, \cdot)$ satisfaz a propriedade:

A8. Para todo $x, y \in A,\ x \cdot y = y \cdot x$;

dizemos que $(A, +.)$ é um **anel comutativo**.

Se um anel $(A, +, \cdot)$ satisfaz a propriedade:

A9. Dados $x, y \in A,\ x \cdot y = 0 \Rightarrow x = 0$ ou $y = 0$;

dizemos que $(A, +, \cdot)$ é um **anel sem divisores de zero**.

Observação 1.1 Para efeito de simplificação da notação seguiremos o hábito comum de omitir o símbolo da multiplicação. Assim, em vez de $x \cdot y$ escreveremos simplesmente xy.

Finalmente temos a noção principal desse trabalho

Definição 1.2 Se $(D, +, \cdot)$ é um anel comutativo, com unidade e sem divisores de zero, dizemos que $(D, +, \cdot)$ é um **domínio de integridade**.

Exemplo 1.1 Os seguintes anéis são exemplos de domínios de integridade: $\mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C}$.

Se um anel comutativo com elemento unidade $(A, +, \cdot)$ e satisfaz a propriedade:

A10. Para cada $x \in A - \{0\}$ existe $y \in A$ tal que $xy = yx = 1$;

dizemos que $(A, +, \cdot)$ é um **corpo**.

Exemplo 1.2 Dos domínios listados no Exemplo 1.1 temos que $\mathbb{Q},\ \mathbb{R},\ \mathbb{C}$ são corpos.

Todo corpo A é um domínio de integridade. De fato, dados $x, y \in A$ suponhamos que $xy = 0$. Se $y \neq 0$, pela propriedade (A10), existe $y' \in A$ tal que

$$yy' = y'y = 1.$$

Logo, $x = xyy' = 0y' = 0$ e portanto A é um domínio de integridade.

Obviamente, a recíproca dessa afirmação não é verdadeira. O exemplo mais básico é o dos inteiros $\mathbb{Z}$. Contudo, se adicionarmos a hipótese de finitude sobre o domínio temos a seguinte proposição:

Proposição 1.1 *Seja D um domínio finito. Então D é corpo.*

Prova. Seja $x \in D - \{0\}$. A função

$$\begin{array}{rccc} \varphi & : D - \{0\} & \to & D - \{0\} \\ & a & \mapsto & ax \end{array}$$

Esta φ é injetora. De fato,

$$a \cdot x = a' \cdot x \Rightarrow (a - a')x = 0 \Rightarrow a = a'.$$

Logo, φ é também sobrejetora, já que $D - \{0\}$ é finito. Portanto, existe $y \in D - \{0\}$ tal que $\varphi(y) = 1$, ou seja, $yx = 1$. □

Definição 1.3 Sejam $(A, +, \cdot)$ um anel e B um subconjunto de A. Dizemos que B é um **subanel** de A se as seguintes condições são satisfeitas:

(i) $0 \in B$;

(ii) Se $x, y \in B$ então $x - y \in B$;

(iii) Se $x, y \in B$ então $xy \in B$.

Como B é um subconjunto não vazio de A, segue que B herda as propriedades associativa, comutativa e distributiva, logo B é um anel.

Exemplo 1.3 Se A é um anel, então $\{0\}$ e A são subanéis de A.

Exemplo 1.4 $\mathbb{Z}[\sqrt{p}] := \{a + b\sqrt{p}; \quad a, b \in \mathbb{Z}\}$ é um subanel de $\mathbb{R}$ para qualquer primo p.

Obviamente, $\mathbb{Z}[\sqrt{p}] \subset \mathbb{R}$. Por outro lado, também temos:
(i) $0 = 0 + 0\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$.
(ii) Dados $x = a + b\sqrt{p}$ e $y = c + d\sqrt{p}$ temos:

$$x - y = a + b\sqrt{p} - (c + d\sqrt{p}) = (a - c) + (b - d)\sqrt{p} \in \mathbb{Z}[\sqrt{p}].$$

(iii) Dados $x = a + b\sqrt{p}$ e $y = c + d\sqrt{p}$ temos:

$$x \cdot y = (a + b\sqrt{p}) \cdot (c + d\sqrt{p}) = ac + ad\sqrt{p} + bc\sqrt{p} + bdp = (ac + bdp) + (ad + bc)\sqrt{p} \in \mathbb{Z}[\sqrt{p}].$$

Portanto, $\mathbb{Z}[\sqrt{p}]$ é um subanel de $\mathbb{R}$.

1.2 Ideais

A definição de ideal foi introduzida no final do século XIX por Kummer e Dedekind a fim de estudar certas questões em teoria dos números. Essa noção tornou-se um objetivo central na teoria dos anéis.

Definição 1.4 Um subanel I de um anel A será chamado de **ideal** de A se possuir a seguinte propriedade: se $a \in A$ e $b \in I$, então $a \cdot b \in I$ e $b \cdot a \in I$.

Claramente, $\{0\}$ e A são ideais de A (ditos **ideais triviais** de A). Os ideais não triviais de A são também chamados ideais próprios de A.

Observação 1.2 Se A é um anel com unidade e $1 \in I$, onde I é um ideal de A, então $I = A$. Isso acontece pois: $I \subset A$ e $\forall \ \ a \in A, \ \ a \cdot 1 \in I$, já que $1 \in I$; logo, $A \subset I$.

Exemplo 1.5 Se I e J são ideais de A, então $I + J := \{i + j; \ \ i \in I \ \ e \ \ j \in J\}$ é um ideal.

Exemplo 1.6 Seja S um subconjunto de um anel comutativo A. Definamos

$$(S) := \{a_1 \cdot s_1 + \ldots + a_n \cdot s_n \mid a_i \in A; s_i \in S; n \in \mathbb{N}\}.$$

Este é um ideal de A chamado ideal **gerado** por S.

Quando $S = \{a\}$ então escrevemos (a) em vez de (S). Nesse caso dizemos que (a) é um **ideal principal**.

Definição 1.5 Anéis onde todo ideal é principal chama-se **anel de ideais principais** ou **anel principal**.

Exemplo 1.7 Obviamente todo corpo é um anel de ideais principais pois, seus únicos ideais são os triviais (gerados por 0 e 1).

Exemplo 1.8 O domínio $\mathbb{Z}$ dos inteiros é um domínio de ideais principais. Para verificar essa afirmação seja I um ideal qualquer de $\mathbb{Z}$. Se $I = \{0\}$, então $I = (0)$. Suponhamos então que $I \neq \{0\}$. Considere $n = \min\{x \in I; x > 0\}$. Claramente $I \supseteq (n)$. Reciprocamente, seja $h \in I$. Pelo algoritmo de Euclides, temos

$$h = qn + r$$

com $0 \leq r < n$. Como h e $n \in I$, o inteiro $r = h - qn \in I$. Pela minimalidade de n devemos ter $r = 0$ e portanto $h = qn$, ou seja, $h \in (n)$. Logo, $I = (n)$.

Observação 1.3 No capítulo 2 daremos outros exemplos de domínios de ideais principais, entre eles, o anel de polinômios $K[x]$, onde K é corpo.

1.3 Divisibilidade em domínios de integridade

Definição 1.6 Seja D um domínio de integridade. Seja $a \in D$, dizemos que um elemento $b \in D$ é um **divisor** (ou **fator**) de a (em D) se existe $c \in D$ tal que $a = bc$; dizemos também que b divide a, ou que a é múltiplo de b, denotamos por $b \mid a$.

Definição 1.7 Um elemento $a \in D$ é **invertível** em D se existe $b \in D$ tal que $ab = 1$. Denotaremos por $U(D)$ o conjunto dos elementos invertíveis de D.

É fácil mostrar que:

1) $1 \in U(D)$;

2) Se $a, b \in U(D)$, então $ab \in U(D)$;

3) Como $U(D) \subset D$, então a multiplicação em $U(D)$ é associativa.;

4) $a \in U(D) \Rightarrow a^{-1} \in U(D)$.

Definição 1.8 Dois elementos $a, b \in D$ são **associados** em D se existe um $u \in D$, u invertível em D, tal que $a = ub$.

Definição 1.9 Um elemento $a \in D \setminus \{0\}$ é **irredutível** em D se as duas condições seguintes são satisfeitas:

(i) a não é invertível em D;

(ii) a não possui fatoração não-trivial em D, isto é, se $a = bc$, com $b,\ c \in D$ então b ou c é invertível em D.

Note que os únicos divisores de um elemento irredutível a são os elementos associados de a em D e os elementos invertíveis de D.

Definição 1.10 Um elemento $a \in D \setminus \{0\}$ não invertível é dito **primo** se $a \mid bc$, então $a \mid b$ ou $a \mid c$, com $b, c \in D$.

Exemplo 1.9 O número 2 é irredutível em $\mathbb{Z}$, pois os seus únicos divisores são ± 1 e ± 2, isto é, $2 = 1 \cdot 2$ ou $2 = -1 \cdot (-2)$ onde $1,\ -1$ são invertíveis em $\mathbb{Z}$.

Exemplo 1.10 O número 4 não é irredutível em $\mathbb{Z}$ pois $2 \mid 4$ e 2 não é invertível nem associado de 4 em $\mathbb{Z}$.

A relação entre elementos primos e irredutíveis é dada nas três proposições a seguir:

Proposição 1.2 *Num domínio de integridade todo elemento primo é irredutível.*

Prova. Seja p um elemento primo de um domínio D e suponha que para algum $a \in D$ tenhamos $a \mid p$. Queremos provar que a é invertível ou que a é um associado de p. Com efeito, se $a \mid p$, então $p = a \cdot b$, para algum $b \in D$. Logo $p \mid a \cdot b$ e como p é primo, temos que $p \mid a$ ou $p \mid b$. Suponhamos inicialmente que $p \mid a$. Como por hipótese $a \mid p$ então a é um associado de p. Em seguida suponhamos que $p \mid b$. Da igualdade $p = a \cdot b$, e como $p \mid b$ então, $b = pt$ para algum $t \in D \Rightarrow p = apt \Rightarrow at = 1 \Rightarrow a$ é invertível. □

Corolário 1 *Sejam $p, p_1, ..., p_n$ elementos primos de um domínio de integridade. Se $p \mid p_1...p_n$, então p é associado de p_i para algum $i = 1, ..., n$.*

Prova. Se $p \mid p_1...p_n$, então pela definição de elemento primo, juntamente com um argumento simples de indução, segue-se que $p \mid p_i$ para algum $i = 1, ..., n$. Agora, como p_i é primo, pela proposição acima ele é irredutível e como $p \mid p_i$ e p não é invertível (por ser primo), segue-se que p é associado de p_i. □

Observação 1.4 Nem sempre a recíproca da Proposição 1.2 é verdadeira. Os primeiros exemplos em que esse fenômeo ocorre são anéis da forma $\mathbb{Z}[\zeta] = \{f(\zeta) \mid f \in \mathbb{Z}[X]\}$ onde ζ é uma raiz n-ésima de -1, com valores de n adequados. Entretanto, o resultado é válido com hipóteses adicionais como podemos ver na proposição abaixo.

Proposição 1.3 *Num domínio principal um elemento é irredutível se, e somente se, é primo.*

Prova. Seja p um elemento não nulo e não invertível de um domínio principal D. Se p é primo, então p é irredutível pela Proposição 1.1.

Agora, suponhamos a irredutível tal que $a|bc$. Considere o ideal $I = (a) + (b)$.

Como D é um domínio principal, então $I = (d)$ para algum $d \in D$. Mas $a \in I = (d)$, o que nos fornece $a = dr$ para algum $r \in D$.

Da hipótese de a ser irredutível segue que d ou r é invertível.

Se d é invertível, então $I = (d) = D$. Daí, $1 \in (a) + (b)$, ou seja, $1 = ax_0 + by_0$. Logo,

$$c = acx_0 + bcy_0, \tag{1.1}$$

ou seja, $a|c$ já que as duas parcelas do segundo membro de (1.1) são divisíveis por a.

Por outro lado, se r é invertível, então da relação $a = dr$ vem $d = r^{-1}a$. Como $b \in I = (d)$, existe $\ell \in D$ tal que $b = \ell d = \ell \cdot r^{-1} \cdot a$. Logo, $a|b$. □

Lema 1.1 *Num domínio de ideais principais D, toda cadeia ascendente de ideais*

$$I_1 \subset I_2 \subset ... \subset I_n \subset ...$$

é estacionária; isto é, existe um índice m tal que

$$I_m = I_{m+1} = ...$$

Prova. Verifica-se facilmente que $\bigcup_{j\geq 1} I_j$ é um ideal de D, pois $I_1 \subset I_2 \subset ...$. Como D é um domínio principal, existe $a \in D$ tal que $\bigcup_{j\geq 1} I_j = (a)$. Segue daí que $a \in \bigcup_{j\geq 1} I_j$ e, portanto, $a \in I_m$ para algum m . Logo, $a \in I_n$ para todo $n \geq m$ e, consequentemente, $(a) \subset I_n$ para todo $n \geq m$. Como para todo n, temos que $I_n \subset \bigcup_{j\geq 1} I_j = (a)$, segue-se que $I_n = (a)$ para todo $n \geq m$. □

A propriedade sobre cadeias de ideais que aparece no enunciado do lema acima é chamada **condição de cadeia ascendente**. Costumamos abreviar esta terminologia por c.c.a.

Domínios onde se verifica a c.c.a chamam-se **Noetherianos**. Pelo lema acima e o Exemplo 1.8 segue que $\mathbb{Z}$ é um domínio Noetheriano. Além disso, em $\mathbb{Z}$ um elemento é primo se, e somente, ele é irredutível. Isso é o que nos ensina a seguinte proposição.

Proposição 1.4 *Todo elemento não nulo e não invertível de um domínio principal possui pelo menos um divisor irredutível.*

Prova. Sejam D um domínio principal e a um elemento de D não nulo e não invertível. Se a é irredutível, nada temos a provar. Suponha agora que a seja redutível, isto é $a = a_1b_1$ onde a_1 e b_1 não são invertíveis e não associados. Portanto,

$$(a) \subsetneq (a_1) \subsetneq D,$$

onde $(a) \neq (a_1)$ pois a e a_1 não são associados e $(a_1) \neq D$ pois a_1 é não invertível.

Se a_1 é irredutível, o resultado fica estabelecido. Se a_1 é redutível, então $a_1 = a_2b_2$ onde a_2, b_2 não são invertíveis nem associados. Portanto

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq D.$$

E assim sucessivamente, obtendo uma cadeia estritamente crescente de ideais

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq ... \subsetneq (a_n) \subsetneq ...,$$

Como D é um DIP, tal cadeia é estacionária, isto é, $\exists r$ tal que $(a) \subsetneq (a_1) \subsetneq ... \subsetneq (a_r) \Rightarrow a_r$ é irredutível. □

Definição 1.11 Um domínio de integridade D é chamado **domínio de fatoração única** (DFU), se todo elemento $a \in D$ não nulo e não invertível se fatora como produto de um número finito de elementos irredutíveis. Além disso, tal fatoração é única a menos da ordem dos fatores e de elementos associados, isto é, se $p_1, ..., p_n, \quad q_1, ...q_m$ são elementos irredutíveis de A e se

$$p_1 \cdots p_n = q_1 \cdots q_m,$$

então $n = m$ e após o reordenação de $q_1, ..., q_n$, se necessário, temos que p_i e q_i são associados para todo $i = 1, ..., n$.

Teorema 1 *Todo domínio de ideais principais é um domínio de fatoração única.*

Prova. Seja D um domínio principal e a um elemento não nulo e não invertível de D. Pela proposição 1.3, o elemento a tem pelo menos um divisor irredutível p_1, logo existe $a_1 \neq 0$ tal que

$$a = a_1 p_1$$

Se a_1 não é invertível, então ele possui um divisor irredutível p_2, logo

$$a = a_2 p_2 p_1$$

Assim, sucessivamente, determinando uma sequência de pares de elementos (a_i, p_i) com os p_i irredutíveis e tais que $a_i = a_{i+1} p_{i+1}$. Mostraremos que este procedimento tem que parar após um número finito de passos, isto é, para algum n temos que a_n é invertível. Com efeito, se nenhum dos elementos $a_1, ..., a_n, ...$ fosse invertível, teríamos para todo i que $a_{i+1} \mid a_i$ e a_i não é associado de a_{i+1}, logo teríamos a seguinte cadeia infinita

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq ... \subsetneq (a_n) \subsetneq ...,$$

Tal sequência é estacionária, pois D é um DIP, ou seja, $(a) \subset (a_1) \subset ... \subset (a_n)$ para algum n. Portanto, para algum n temos que a_n é invertível. Fazendo $a_n = u$, temos que

$$a = p_1 ... p_{n-1}(u p_n)$$

com $p_1, ..., p_{n-1}, up_n$ irredutíveis (portanto, pela proposição 1.2, também primos).
Unicidade: Suponhamos que $a \neq 0$ e não invertível tal que $a = p_1 ... p_r$ e $a = q_1 ... q_s$ onde os $p_i^{'s}$ e os $q_j^{'s}$ são irredutíveis. Assim, $p_1 ... p_r = q_1 ... q_s$. Se $r \neq s$, então $r > s$ ou $r < s$. Suponhamos $r < s$. Ora, $p_1 \mid q_1 ... q_s$ portanto, $p_1 \mid q_j$ para algum j, que podemos , sem perda de generalidade, supor que $p_1 \mid q_1$, ou seja, $q_1 = p_1 u_1$ onde u_1 é invertível, pois q_1 é irredutível. Daí $p_1 = u_1^{-1} q_1$. De $p_1 ... p_r = q_1 ... q_s$, vem

$$u_1^{-1} q_1 p_2 ... p_r = q_1 q_2 ... q_s$$

ou seja,

$$u_1^{-1} p_2 ... p_r = q_2 ... q_s$$

Repetindo o processo e observando que $r < s$ temos:

$$u_1^{-1}u_2^{-1}...u_r^{-1} = q_{r+1}...q_s$$

$u_1^{-1}u_2^{-1}...u_r^{-1} = u$ é invertível. Logo, $q_{r+1}...q_s = u \Rightarrow (q_{r+1}...q_s)u^{-1} = 1 \Rightarrow q_{r+1}$ é invertível o que é um absurdo. Logo, $r = s$. Assim, $a = p_1...p_r = q_1...q_r$ e resta apenas verificar que os fatores irredutíveis são associados. □

Observação 1.5 A recíproca desse teorema não é verdadeira. Por exemplo, podemos mostrar que $\mathbb{Z}[X]$ é um domńio fatorial mas não é um domínio de ideais principais.

Corolário 2 *Os anéis $\mathbb{Z}$ e $K[X]$, com K corpo, são domínios de fatoração única.*

Demonstração: $\mathbb{Z}$ é um DIP, portanto $\mathbb{Z}$ é um DFU. $K[X]$ é um DIP, portanto $K[X]$ é um DFU.

Todo corpo, por ter todos os seus elementos não nulos invertíveis, é um DFU.

Vê-se facilmente que se a é primo, então todo associado de a é primo.

Exemplo 1.11 O número 2 é primo em $\mathbb{Z}$. De fato, se $2 \mid b \cdot c$, então b ou c tem que ser par (pois o produto de dois números ímpares é ímpar).

Exemplo 1.12 O número 3 é primo em $\mathbb{Z}$. De fato, suponha que $3 \mid b \cdot c$. e que $3 \nmid b$. Assim, $\text{mdc}(3, b) = 1 \Rightarrow 1 = 3r + bs$ para algum $r, s \in \mathbb{Z}$. Multiplicando os dois membros da igualdade acima por c temos:

$$c = 3cr + bcs \Rightarrow 3 \mid c$$

Exemplo 1.13 O número 4 não é primo em $\mathbb{Z}$ pois $4 \mid 2 \cdot 6$ e no entanto, temos $4 \nmid 2$ e $4 \nmid 6$.

Corolário 3 *Em $\mathbb{Z}$ um elemento é primo se, e somente se, ele é irredutível.*

Demonstração: Isso decorre do fato de que num domínio de integridade, todo elemento primo é irredutível e de que num domínio principal, todo elemento primo é irredutível e $\mathbb{Z}$ ser um domínio principal.

Capítulo 2

Domínios euclidianos

Essencialmente o algorítmo de Euclides diz que em $\mathbb{Z}$ podemos fazer a divisão de um elemento a por um elemento $b \neq 0$ obtendo um resto "pequeno", ou mais precisamente, um resto cujo valor absoluto é menor do que o valor absoluto de b. É essa idéia que vamos generalizar. Para isso, precisamos então de um conjunto com duas operações $(+, \cdot)$ e uma maneira de "medir" se um elemento do conjunto é menor do que um outro. Um domínio euclidiano será um domínio no qual existe um algorítmo similar ao algorítmo de Euclides.

Definição 2.1 Um domínio euclidiano $(D, +, \cdot, \varphi)$ é um domínio de integridade $(D, +, \cdot)$ com uma função

$$\varphi : D - \{0\} \to \mathbb{N} = \{0, 1, 2, \ldots\}.$$

que satisfaz as seguintes propriedades:

i) $\forall a, b \in D, b \neq 0$, existem $t, r \in D$ tais que

$$a = b \cdot t + r, \quad \text{com} \quad \begin{cases} \varphi(r) & < & \varphi(b) \\ \text{ou } r & = & 0 \end{cases}$$

ii) $\varphi(a) \leq \varphi(ab)$, $\forall a, b \in D - \{0\}$

Observação 2.1 a) Dados dois elementos $\alpha \neq 0$ e $\beta \neq 0$ de um domínio euclidiano $(D, +, \cdot, \varphi)$, nós os comparamos via a função φ , em $\mathbb{N}$ com a ordem usual. É claro que poderíamos fazer isso com uma função $\varphi : D \backslash \{0\} \to \mathbb{S}$, onde $\mathbb{S}$ seria um conjunto totalmente ordenado qualquer no lugar de $\mathbb{N}$; dessa forma, também teríamos uma noção de divisão com resto nesses domínios. Além disso, se supusermos a condição mais forte que S seja bem ordenado, isto é, que todo subconjunto não vazio de S tem um menor elemento ($\mathbb{N}$ com a ordem usual é bem ordenado), então todas as propriedades que vamos provar para os domínios euclidianos seriam também satisfeitas.

Por isso, vários autores dão uma definição de anel euclidiano usando uma função $\varphi : \mathbb{D} \setminus \{0\} \to \mathbb{S}$ com $\mathbb{S}$ subconjunto bem ordenado qualquer no lugar de $\mathbb{N}$ com a ordem usual.

b) Na definição de domínio euclidiano exigimos que a função φ satisfizesse a condição pouco natural $\varphi(a) \leq \varphi(ab) \forall \ \ a, b \in \mathbb{D} \setminus \{0\}$. Essa exigência é puramente técnica; ela vai permitir simplificar as provas dos teoremas a seguir.

Exemplo 2.1 $\mathbb{Z}$ é um domínio euclidiano
Demonstração: Seja $\varphi : \mathbb{Z} \setminus \{0\} \to \mathbb{N} = \{0, 1, 2, ...\}$ definida por $\varphi(x) = |x|$.

1) Sabemos que $a, b \in \mathbb{Z} \setminus \{0\}$ do algorítmo da divisão, temos que existe um $q \in \mathbb{Z}$ e um único $r \in \mathbb{Z}$ tais que $a = bq + r$, onde $0 \leq r < |b|$, ou seja, $a = bq + r$ onde $r = 0$ ou $\varphi(r) = |r| = r < |b|$.

2) $\forall \ \ a, \ \ b \ \in \mathbb{Z} \setminus \{0\}, \ \ \varphi(a) = |a| > 0$ e $\varphi(b) = |b| > 0$, ou seja, $\varphi(a) \geq 1$ e $\varphi(b) \geq 1$. Mas, de $1 \leq |b|$ vem $|a| \leq |a||b|$, ou seja $\varphi(a) \leq \varphi(ab)$

Proposição 2.1 *Se K é um corpo então $K[x]$ é um domínio euclidiano.*

Prova. Seja $\varphi : K[x] \setminus \{0\} \to \mathbb{N}$, definida por $\varphi(f(x)) =$ grau de $f(x)$.

1) Dados $f(x), \ \ g(x) \ \ \in K[x] \setminus \{0\}$ sabemos que existe um único $q(x) \in K[x]$ e um único $r(x) \in K[x]$ tais que $f(x) = g(x)q(x) + r(x)$, onde $r(x) = 0$ ou grau de $r(x) <$ grau de $g(x)$, ou seja, $r(x) = 0$ ou $\varphi(r(x)) < \varphi(g(x))$

2) $\forall \ \ f(x), g(x) \in K[x] \setminus \{0\}$, sabemos que $\varphi(f(x)g(x)) =$ grau de $(f(x)g(x)) =$ grau de $f(x)$ + grau de $g(x)$, pois $K[x]$ é um domínio de integridade. Assim, $\varphi(f(x)g(x)) = \varphi(f(x)) + \varphi(g(x)) \Rightarrow \varphi(f(x)) \leq \varphi(f(x)g(x))$.

□

Teorema 2 *Todo domínio euclidiano é um domínio de ideais principais.*

Prova. Sejam $(D, +, \cdot, \varphi)$ um domínio euclidiano e I um ideal em D. Se $I = (0)$ então I é principal. Se $I \neq (0)$, então existe $\ x \in I - \{0\}$. Seja $S = \{\varphi(x) \mid x \in I - \{0\}\}$. Se $0 \in S$, então 0 é o elemento mínimo de S, pois $\varphi(x) \geq 0, \ \ \forall \ \ x \in D \setminus \{0\}$. Se $0 \notin S$, então S é um subconjunto não vazio de $\mathbb{N} \setminus \{0\}$ e pelo princípio da boa ordem S tem um elemento mínimo. Seja portanto $\varphi(a)$ o elemento mínimo de S, e considere $J = (a)$. Temos $J \subset I$, pois $a \in I$.

Mostraremos que I é principal. De fato, se $b \in I$, então do fato de D ser um domínio euclidiano, resulta $b = aq + r$ onde $r = 0$ ou $\varphi(r) < \varphi(a)$. Mas, $r = b - aq \in I$ e da minimalidade de $\varphi(a)$, resulta $r = 0$. Assim, $b = aq$ o que implica $I \subset J$.

Do exposto, $I = J = (a)$. □

Observação 2.2 A recíproca desse teorema não é verdadeira. O domínio

$$D := \left\{ z_1 \frac{1}{2} + z_2 \frac{\sqrt{-19}}{2} \mid z_1, z_2 \in \mathbb{Z}, \text{ de mesma paridade} \right\}$$

é um domínio de ideais principais mas não é euclidiano.

Corolário 4 *$\mathbb{Z}$ e $K[x]$ são domínios principais. Em particular, eles são Noetherianos.*

Demonstração: $\mathbb{Z}$ e $K[x]$ são domínios euclidianos $\Rightarrow \mathbb{Z}$ *e* $K[x]$ são domínios principais $\Rightarrow \mathbb{Z}$ *e* $K[x]$ são Noetherianos.

Capítulo 3

O domínio $\mathbb{Z}[i]$

Definição 3.1 O conjunto $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z} \ \ e \ \ i^2 = -1\}$ é chamado conjunto dos **inteiros de Gauss**

Seja $\mathbb{Z}[i]$ munido das operações $+$ e $\cdot$ induzidas de $\mathbb{C}$. É de fácil verificação que $\mathbb{Z}[i]$ é um subdomínio de $\mathbb{C}$.

Seja $N : \mathbb{Z}[i] \to \mathbb{N}$ definida por $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$. N chama-se função norma e tem a seguinte propriedade

$$N(\alpha\beta) = N(\alpha)N(\beta), \forall \ \ \alpha, \beta \in \mathbb{Z}[i].$$

De fato, $N(\alpha\beta) = (\alpha\beta)(\overline{\alpha\beta}) = (\alpha\bar{\alpha})(\beta\bar{\beta}) = N(\alpha)N(\beta)$, onde $\bar{\alpha}$ e $\bar{\beta}$ são conjugados de α e β em $\mathbb{Z}[i]$.

Teorema 3 *Seja $\alpha \in \mathbb{Z}[i]$. As seguintes afirmações são equivalentes:*

(i) *α é invertível em $\mathbb{Z}[i]$.*

(ii) $N(\alpha) = 1$.

(iii) $\alpha \in \{-1, 1, -i, i\}$.

Demonstração: i) $\Rightarrow$ ii). α invertível $\Rightarrow \exists \beta \in \mathbb{Z}[i]$ tal que $\alpha\beta = 1 \Rightarrow N(\alpha\beta) = N(1) \Rightarrow N(\alpha)N(\beta) = 1$ com $N(\alpha), N(\beta) \in \mathbb{N} \Rightarrow N(\alpha) = N(\beta) = 1$.
ii) $\Rightarrow$ iii). Seja $\alpha = x + yi \in \mathbb{Z}[i]$ e $N(\alpha) = x^2 + y^2 = 1$

$$\begin{cases} x^2 = 0 \quad e \quad y^2 = 1 \\ \quad ou \\ x^2 = 1 \quad e \quad y^2 = 0 \end{cases}$$

$$\begin{cases} x = 0 \quad\ e \quad y = \pm 1 \\ \quad ou \\ x = \pm 1 \quad e \quad\ y = 0 \end{cases}$$

$$\begin{cases} \alpha = \pm i \\ ou \\ \alpha = \pm 1 \end{cases}$$

Logo $\alpha \in \{-1, 1, i, -i\}$.
iii) $\Rightarrow$ i) é trivial.

Teorema 4 *$\mathbb{Z}[i]$ é um domínio euclidiano*

Prova. Sejam $\alpha, \beta \in \mathbb{Z}[i]$, com $\beta \neq 0$. Mostremos que existem $\gamma, \rho \in \mathbb{Z}[i]$ tais que $\alpha = \beta\gamma + \rho$ com $\rho = 0$ ou $N(\rho) < N(\beta)$.

Devemos encontrar $\gamma \in \mathbb{Z}[i]$ tal que $N(\alpha - \beta\gamma) < N(\beta)$. Mas,

$$N(\alpha - \beta\gamma) = N\left(\beta \cdot \left(\frac{\alpha}{\beta} - \gamma\right)\right) = N(\beta)N\left(\frac{\alpha}{\beta} - \gamma\right) < N(\beta)$$

Portanto, devemos encontrar $\gamma \in \mathbb{Z}[i]$ tal que $N\left(\frac{\alpha}{\beta} - \gamma\right) < 1$. Como $\frac{\alpha}{\beta} \in \mathbb{C}$ então $\frac{\alpha}{\beta} = x + yi$ onde $x, y \in \mathbb{R}$.

Afirmação: $x, y \in \mathbb{Q}$.

Sejam $\alpha = a + bi$ e $\beta = c + di$ com $a, b, c, d \in \mathbb{Z}$.

$$\frac{\alpha}{\beta} = \alpha \cdot \frac{1}{\beta} = (a + bi)\frac{\bar{\beta}}{\beta\bar{\beta}} = (a + bi)\frac{c - di}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i = x + yi,$$

onde $x = \frac{ac + bd}{c^2 + d^2} \in \mathbb{Q}$ e $y = \frac{bc - ad}{c^2 + d^2} \in \mathbb{Q}$

Para concluir, considere o seguinte lema:

Lema 3.1 *Dado $c \in \mathbb{Q}$, existe um inteiro no intervalo $]c, c + 1]$.*

Demonstração: Sejam $a, b \in \mathbb{Z}$ com $b > 0$ e $c = \frac{a}{b} \in \mathbb{Q}$. Do algorítmo da divisão temos

$$a = bq + r$$

com $0 \leq r < b$. Assim,

$$\frac{a}{b} = q + \frac{r}{b}.$$

De $0 \leq r < b$ resulta,

$$0 \leq \frac{r}{b} < 1 \text{ e } c = \frac{a}{b} = q + \frac{r}{b}.$$

Desse modo,

$$\frac{a}{b} = q + \frac{r}{b} < q + 1 \Rightarrow \frac{a}{b} - 1 < q,$$

ou seja, $c < q + 1$. Observando que $c = q + \frac{r}{b}$ e $\frac{r}{b} \geq 0$, temos:

$$q \leq c \Rightarrow c < q+1 \leq c+1 \Rightarrow q+1 \in]c, c+1[\text{ e } q+1 \in \mathbb{Z}.$$

concluindo assim a prova do lema.

Voltando à demonstração do teorema, temos pelo lema que existem $r, s \in \mathbb{Z}$ tais que $|x-r| \leq \frac{1}{2}$ e $|y-s| \leq \frac{1}{2}$ (fazendo $c+1 = \frac{1}{2}$, ou seja, $c = -\frac{1}{2}$ no lema anterior).

Agora, escolhendo $\gamma = r + si$ e $\rho = \alpha - \beta\gamma$ temos:

$$\begin{aligned} N(\rho) &= N(\alpha - \beta\gamma) \\ &= N(\frac{\alpha}{\beta} - \gamma)N(\beta) \\ &= N(x + yi - (r + si))N(\beta) \\ &= N((x-r) + (y-s)i)N(\beta) \\ &= (|x-r|^2 + |y-s|^2)N(\beta) \\ &\leq (\frac{1}{4} + \frac{1}{4})N(\beta) \end{aligned}$$

logo,

$$N(\rho) \leq \frac{1}{2}N(\beta) \leq N(\beta).$$

Também, $N(\beta) \in \mathbb{N}$ e $N(\beta) \geq 1 \Rightarrow N(\alpha) \leq N(\alpha)N(\beta)$ pois $N(\alpha) \in \mathbb{N}$ ou seja $N(\alpha) \leq N(\alpha\beta)$. □

Corolário 5 *$\mathbb{Z}[i]$ é um domínio de ideais principais. Em particular, ele é Noetheriano e DFU.*

Capítulo 4

Aplicações

Neste capítulo estudaremos e determinaremos os primos em $\mathbb{Z}[i]$

1) Todo elemento primo em $\mathbb{Z}[i]$ divide algum primo de $\mathbb{Z}$
Demonstração: Seja $\pi \in \mathbb{Z}[i], \quad \pi - primo, \quad N(\pi) \in \mathbb{N} \setminus \{0\}$. $\mathbb{Z}$ é um DFU, então $N(\pi) = p_1^{r_1}...p_k^{r_k}$ onde os $p_i^{'s}$ são primos em $\mathbb{Z}$. Como $N(\pi) = \pi\bar{\pi}$, então $\pi\bar{\pi} = p_1^{r_1}...p_k^{r_k} \Rightarrow \pi \mid p_1^{r_1}...p_k^{r_k}$ e π é primo em $\mathbb{Z}[i] \Rightarrow \pi \mid p_i^{r_i}$ para algum $i = 1, ..., k \Rightarrow \pi \mid p_i$ para algum $i = 1, ..., r$.

2) Seja $\pi \in \mathbb{Z}[i]$. Se $N(\pi)$ é primo em $\mathbb{Z}$, então π é primo em $\mathbb{Z}[i]$.
Demonstração: Suponha que π não é primo em $\mathbb{Z}[i]$, isto é, $\pi = \pi_1\pi_2$ onde π_1 e π_2 não são invertíveis. Assim, $N(\pi_i) > 1, \quad i = 1, 2$ conforme teorema 3.
Mas, $N(\pi) \mid N(\pi_1)N(\pi_2) \Rightarrow N(\pi) \mid N(\pi_1)$ ou $N(\pi) \mid N(\pi_2)$ pois $N(\pi)$ é primo em $\mathbb{Z}$ e $N(\pi_i) > 1, \quad i = 1, 2$.
Se $N(\pi) \mid N(\pi_1)$, então $N(\pi_1) = N(\pi)q$, para algum $q \in \mathbb{Z} \Rightarrow N(\pi) = N(\pi)qN(\pi_2) \Rightarrow N(\pi_2)q = 1 \Rightarrow N(\pi_2) = q = 1$ o que é absurdo.

Exemplo 4.1 *$1 + i$ é primo em $\mathbb{Z}[i]$, pois $(1 + i)(1 - i) = 2$ que é inteiro primo.*

3) Se $p \in \mathbb{Z}$ é primo. As seguintes afirmações são equivalentes:

i) p é redutível em $\mathbb{Z}[i]$

ii) $p = \alpha \cdot \bar{\alpha}$ com α primo em $\mathbb{Z}[i]$

iii) p é soma de dois quadrados.

Demonstração: *i)⇒ ii). $p = \alpha\beta$ com α e β não invertíveis $p \in \mathbb{Z}$, $N(p) = p^2 = N(\alpha)N(\beta) \Rightarrow N(\alpha) = N(\beta) = p$ pois $N(\alpha), N(\beta) \in \mathbb{N} \Rightarrow N(\alpha) = p$ é primo em $\mathbb{Z} \Rightarrow \alpha$ é primo em $\mathbb{Z}[i]$*

De $p = \alpha\beta$ resulta $\beta = \dfrac{p}{\alpha} = \dfrac{p\bar{\alpha}}{\alpha\bar{\alpha}} = \dfrac{p\bar{\alpha}}{N(\alpha)} = \dfrac{p}{p}\bar{\alpha} = \bar{\alpha} \Rightarrow p = \alpha\bar{\alpha}$.

ii) ⇒ iii) é trivial

iii) ⇒ i)

Seja $p = a^2 + b^2 = (a + bi)(a - bi) \Rightarrow N(p) = N(a + bi)N(a - bi) \Rightarrow p^2 = N(a + bi)N(a - bi)$, $N(a + bi)$, $N(a - bi) \in \mathbb{N} \Rightarrow N(a + bi) =$

$= N(a - bi) = p \Rightarrow a + bi$ e $a - bi$ não são invertíveis, logo p é redutível em $\mathbb{Z}[i]$.

Referências Bibliográficas

[1] GARCIA, Arnaldo, *Elementos de álgebra*, IMPA, 2010.

[2] BROCHERO, Fábio, *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*, IMPA, 2011.

[3] HEFEZ, Abramo, *Curso de álgebra, volume 1*, IMPA, 2011.

[4] GONÇALVES, Adilson, *Introdução à álgebra*, IMPA, 1999.

[5] KLEINER, Israel, *A History of Abstract Algebra*, Birkhauser, 2007