Irredutibilidade Polinomial E Algoritmos Em

Corpos Finitos

Leandro Miranda Zatesko
Bacharelando em Ciência Da Computação

Dr. Jair Donadelli Jr.
Orientador

UFPR 2008

Leandro Miranda Zatesko

Irredutibilidade Polinomial E Algoritmos Em

Corpos Finitos

Monografia de revisão bibliográfica apresentada na Universidade Federal do Paraná, sob a orientação do Prof. Dr. Jair Donadelli Jr., do Departamento de Informática da mesma universidade, para a obtenção do título de bacharel em Ciência da Computação.

Curitiba, dezembro de 2008.

Folha de aprovação

Monografia de revisão bibliográfica sob o título *"Irredutibilidade Polinomial E Algoritmos Em Corpos Finitos"*, apresentada por Leandro Miranda Zatesko e aprovada em 9 de dezembro de 2008, em Curitiba, Estado do Paraná, pela banca examinadora constituída pelos professores:

Dr. Jair Donadelli Jr. (DInf–UFPR)

Dr. Renato Carmo (DInf–UFPR)

Dr. Edson Ribeiro Alvares (DMat–UFPR)

Resumo

No desenvolvimento da Matemática Moderna, várias estruturas algébricas foram propostas com o objetivo de organizar logicamente e axiomatizar a Álgebra. Dentre essas estruturas, uma que tem recebido atenção especial dos matemáticos nas últimas décadas é o caso finito da estrutura chamada de "corpo". Basicamente, um corpo é um sistema matemático em que valem a adição, a subtração, a multiplicação e a divisão para todos os elementos (com exceção da divisão por zero). Corpos são um caso particular de anéis. Embora polinômios possam ser construídos sobre anéis quaisquer, o interesse no estudo dos corpos finitos vem associado ao interesse no estudo de polinômios sobre corpos finitos. Polinômios sobre corpos finitos têm aplicações diversas na Matemática, na Engenharia e na Tecnologia. Em particular, o estudo da irredutibilidade polinomial sobre corpos finitos é muito importante. O presente trabalho, portanto, apresenta um algoritmo, proposto por Michael O. Rabin, para testar a irredutibilidade de um polinômio de grau n sobre um corpo finito com p elementos, analisa o algoritmo, cujo tempo de execução é dado por

$$T(n) = O\big((n \log n (\log \log n) \log p)^2\big),$$

e ainda fornece um esboço da fundamentação teórica por trás dos conceitos empregados, deixando uma orientação bibliográfica e uma motivação para pesquisas futuras.

Abstract

While Modern Math was being developed, many algebric structures were proposed with the objective of organizing logically and axiomatizing the Algebra. Among these structures, one which has been received special attention from the mathematicians in last decades is the finite case of the structure called “field”. Basically, a field is a mathematic system in which are available the addition, the subtraction, the multiplication and the division for all the elements (excepting division by zero). Fields are a particular case of rings. Although polynomials can be constructed over any rings, the interest in the study of finite fields comes associated to the interest in the study of polynomials over finite fields. Polynomials over finite fields have many applications in Math, Engineering and Technology. Particularly, the study of polynomial irreducibility over finite fields is very important. The present work, therefore, presents an algorithm, proposed by Michael O. Rabin, for testing the irreducibility of a polynomial of degree n over a finite field with p elements, analyzes the algorithm, whose execution time is given by

$$T(n) = O\big((n \log n (\log \log n) \log p)^2\big),$$

and also shows a sketch of the theoretical foundations in the background of the used concepts, leaving a bibliographic orientation and a motivation for future researches.

Sumário

1 Introdução **1**

2 Esboço dos fundamentos teóricos **5**
2.1 Polinômios 5
2.2 Anéis de polinômios 7
2.3 Divisibilidade e irredutibilidade polinomial 11

3 O algoritmo **17**

4 Conclusão **19**

A Fundamentos algébricos **21**
A.1 Conceitos preliminares 21
A.1.1 Partições 21
A.1.2 Relações 21
A.1.3 Divisibilidade no conjunto dos números inteiros 22
A.1.4 Funções 26
A.1.5 Operações 27
A.2 Grupos e subgrupos 28
A.2.1 Grupos 28
A.2.2 Grupos abelianos 32
A.2.3 Subgrupos 32
A.2.4 Classes laterais 34
A.2.5 Grupos finitos 36
A.2.6 Grupos cíclicos 37
A.2.7 Subgrupos normais e grupos quocientes 41
A.3 Anéis e estruturas afins 43
A.3.1 Anéis 43
A.3.2 Subanéis 44
A.3.3 Anéis comutativos 45
A.3.4 Anéis com unidade 45
A.3.5 Domínios de integridade 46
A.3.6 Corpos 48
A.3.7 Corpos finitos 48
A.3.8 Subcorpos 49
A.3.9 Ideais 50
A.3.10 Anéis quocientes 52
A.4 Espaços vetoriais 55
A.4.1 Conceituação 55

A.5 Espaços vetoriais gerados por subcorpos 57

Lista de Símbolos

$d(f)$ — grau do polinômio f p. 6
a_k — $a(k)$, sendo a uma função com suporte finito p. 6
$f \equiv g$ — identidade entre os polinômios f e g p. 6
$\underline{0}(x)$ — polinômio $\underline{0}(x) = \underline{0}$ p. 6
$\underline{1}(x)$ — polinômio $\underline{1}(x) = \underline{1}$ p. 6
$\mathrm{id}(x)$ — polinômio identidade: $\mathrm{id}(x) = x$ p. 6
$\rho(f)$ — conjunto das raízes do polinômio f p. 7
$-f(x)$ — polinômio $(-f)(x) = -\big(f(x)\big)$ p. 7
$R[x]$ — conjunto de todos os polinômios sobre R p. 7
$f_1 \backslash f_2$ — divisibilidade do polinômio f_1 pelo polinômio f_2 p. 11
$K(M)$ — o menor subcorpo que contém ambos K e M p. 13
$T(n)$ — tempo de execução de um algoritmo com tamanho da entrada n p. 18
2^A — conjunto potência (ou conjunto das partes) de A p. 21
$a \sim b$ — relação $\sim$ entre a e b p. 21
$a \nsim b$ — negação da relação $\sim$ entre a e b p. 21
$[a]_\sim$ — classe de equivalência de a por $\sim$ p. 22
$^A\!/_\sim$ — conjunto quociente de A por $\sim$ p. 22
$d \backslash z$ — divisibilidade do inteiro d pelo inteiro z p. 23
$a \equiv b \pmod m$ — congruência entre a e b módulo m p. 25
$[z]_m$ — classe de equivalência de z pela relação de congruência módulo m p. 25
$f\colon A \to B$ — função de A em B p. 26
$f(a)$ — imagem de a por f p. 26
$f(S)$ — conjunto das imagens dos elementos de S por f p. 26
$f^{-1}(b)$ — imagem inversa de b por f p. 26
$f^{-1}(S)$ — conjunto das imagens inversas dos elementos de S por f p. 26
A^B — conjunto das funções de B em A p. 26
$A \simeq B$ — correspondência biunívoca entre A e B p. 26
$a * b$ — imagem de (a, b) por $*$ p. 27
$*_S$ — restrição de $*$ a S p. 27
$\overline{a}$ — elemento simétrico de a p. 28
$\bigsqcup_{j=m}^{n} a_j$ — $a_m * a_{m+1} * \cdots * a_n$ p. 31
$H \subseteq (G, *)$ — propriedade de subgrupo de H em relação a $(G, *)$ p. 32
$a \sim b \pmod H$ — relação de congruência à direita entre a e b módulo H p. 34
$a \backsim b \pmod H$ — relação de congruência à esquerda entre a e b módulo H p. 34
$a * H$ — classe lateral à direita de a módulo H p. 34
$H * a$ — classe lateral à esquerda de a módulo H p. 34
$[G : H]$ — cardinalidade do conjunto quociente de G por $\sim$ ou $\backsim$ módulo H p. 36
a^{*n} — n-ésima iteração de $*$ sobre a p. 37
$\langle a \rangle$ — subgrupo gerado por a p. 40

$^{G}/_{N}$ — grupo quociente de G por N p. 41
$N_1 * N_2$ — multiplicação dos subgrupos normais N_1 e N_2 p. 41
$\underline{0}$ — elemento neutro de uma operação denotada por $+$ p. 43
$-r$ — simétrico de r em relação a uma operação denotada por $+$ p. 43
ab — $a \cdot b$ p. 43
$a - b$ — $a + (-b)$ p. 43
nr — n-ésimo múltiplo de r p. 44
$L \subseteq (R, +, \cdot)$ — propriedade de subanel de L em relação a $(R, +, \cdot)$ p. 44
$\underline{1}$ — elemento neutro de uma operação denotada por $\cdot$ p. 45
r — elemento simétrico de r em relação a uma operação denotada por $\cdot$ p. 46
r^n — n-ésima potência de r p. 46
$K \subseteq (F, +, \cdot)$ — propriedade de subcorpo de K em relação a $(F, +, \cdot)$ p. 49
$\langle S \rangle$ — ideal gerado por S p. 51
$\langle s \rangle$ — ideal gerado por $\{s\}$ p. 51
$^{R}/_{J}$ — anel de classes de resíduos de R por J p. 53
$\mathbb{F}_p$ — corpo de Galois de ordem p p. 54
$\mathbf{0}$ — elemento neutro de uma operação denotada por $+$ p. 56
$-\boldsymbol{u}$ — simétrico de $\boldsymbol{u}$ em relação a uma operação denotada por $+$ p. 56
$a\boldsymbol{u}$ — $a \cdot \boldsymbol{u}$ p. 56
$\boldsymbol{u} - \boldsymbol{v}$ — $\boldsymbol{u} + (-\boldsymbol{v})$ p. 56
$\dim(V, +, \cdot)$ — dimensão do espaço vetorial $(V, +, \cdot)$ p. 56
$[F : K]$ — dimensão do espaço vetorial de F sobre K p. 57
$\mathbb{F}_q$ — corpo de Galois de ordem $q = p^m$ p. 58

Capítulo 1

Introdução

Embora muitas das disciplinas da Matemática terem sido axiomatizadas e organizadas logicamente há muitos séculos, e isso pode se verificar quando tomamos como exemplo a Geometria, cuja primeira axiomatização foi proposta em cerca de 300 a.C. por Euclides em sua obra "Elementos", a Álgebra só foi receber tal devido tratamento bastante tarde, já que os primeiros esforços nesse sentido datam no mínimo do século XIX, um século bastante importante na história da Matemática Moderna. Se o leitor se lembrar, foi justamente nesse século que Georg Cantor propôs a Teoria (Ingênua) dos Conjuntos.

Porém, os conjuntos de Cantor não constituíram a única formulação teórica importante do século. Em seu estudo sobre a resolução de equações por radicais, grande febre da época, o matemático francês Évariste Galois (1811–1832) propôs em 1830, pela primeira vez na história, o conceito de "grupo" com esse nome. Vale ressaltar que isso não significa que o conceito de "grupo" não tivesse aparecido intuitivamente antes, por exemplo, na obra de Joseph-Louis Lagrange (1736–1813). No entanto, foi Galois quem lhe deu a devida organização lógica e axiomatização, que utilizamos até hoje.

Assim como os grupos, outras estruturas algébricas aparecerem em meados do século XIX. O conceito de "corpo", por exemplo, já aparecia intuitivamente nas obras do norueguês Niels Henrik Abel (1802–1829) e Galois e foi apresentado explicitamente pelos "corpos de grau finito" do alemão R. Dedekind (1831–1916) em seu estudo sobre os "números algébricos". A definição de "anel", por sua vez, embora tenha sido formalizada apenas em 1914 pelo alemão A. Fraenkel (1891–1965), já aparecia, inclusive com esse nome, nas obras de D. Hilbert (1852–1943).

Dentro da história da Álgebra Moderna, os corpos finitos, mais especificamente os corpos de Galois, são em teoria tão "velhos" quanto a Teoria de Corpos propriamente dita. Entretanto, foi apenas nas últimas décadas, com a emergência da Matemática Discreta como uma disciplina que recebesse grande atenção dos matemáticos, que os corpos finitos vieram ser estudados com mais profundidade e interesse. Nesse ínterim, a Teoria de Corpos Finitos acabou produzindo importantíssimas aplicações tanto na Matemática quanto na Engenharia e na Tecnologia. Algumas das aplicações encontram-se principalmente na Combinatória, na Teoria de Codificação, na Criptologia, na Criptografia, no estudo de circuitos com retroalimentação, na geração de seqüências pseudo-aleatórias, na Teoria dos Números e na manipulação de símbolos algébricos.

Se conceitos como “grupos”, “corpos” e “anéis” são relativamente novos (ao menos explicitamente), o mesmo não ocorre com os polinômios. Pode-se dizer que o conceito de “polinômio” seja, ao menos intuitivamente, tão antigo quanto a própria Álgebra e que remonte suas origens às obras clássicas gregas, das quais advieram as três disciplinas “Geometria”, “Aritmética” e “Álgebra”. Contudo, foi apenas no século XVI, com a criação do “Cálculo Literal” por François Viète (1540–1603), que a linguagem das fórmulas revolucionou a Matemática, tornando-se possível generalizar expressões. Todavia, foi pouco tempo depois, na obra de René Descartes (1596–1650), que as expressões matemáticas ganharam a forma que utilizamos até hoje. Foi Descartes que introduziu a convenção de se denotar variáveis por x, y e z e constantes ou parâmetros por a, b e c. Também foi ele quem criou a notação exponencial para indicar potências e quem pela primeira vez, muito provavelmente, usou o princípio da identidade de polinômios. O mais curioso, no entanto, é que a principal preocupação intelectual de Descartes não era a Matemática, mas a Filosofia. Muitos hoje acreditam que foi justamente por isso que Descartes publicou apenas um trabalho matemático: sua obra entitulada “*Géometrie*”, listada atualmente como uma das obras mais importantes de toda a história da Matemática. Com tudo isso, podemos sem medo afirmar que o século XVII foi um dos mais importantes para a história da Teoria de Polinômios, mas não podemos negligenciar o fato de que conceitos algébricos mais sutis, como o de irredutibilidade polinomial, só receberam atenção juntamente com as transformações pelas quais a Matemática passou no século XIX.

No presente trabalho, pretendemos introduz o leitor aos conceitos elementares relacionados à irredutibilidade polinomial em corpos finitos e ainda apresentar um algoritmo utilizado para testar se um polinômio sobre um corpo finito é ou não irredutível. O algoritmo que mostraremos foi proposto por Michael O. Rabin em 1978[4], com custo inferior aos custos dos algoritmos publicados anteriormente. Para podermos, portanto, abordar os conceitos e o algoritmo, exporemos também um pouco da fundamentação teórica necessária para as demonstrações utilizadas.

Assim, no capítulo 2 nos dedicaremos principalmente a construir um esboço de alguns conceitos da Teoria de Polinômios, incluindo a irredutibilidade polinomial em corpos finitos. É muito importante destacar que o esboço se atém especialmente a muito daquilo que vai ser utilizado posteriormente e que não contempla nem mesmo os resultados mais interessantes ou de maior impacto, por fugiram do escopo da pesquisa. O mesmo vale para as demonstrações. Como alguns teoremas exigem conceitos mais avançados que os que nós pretendemos abordar, dada a realidade deste texto, dedicar-nos-mos a fundamentar os conceitos mais elementares e não nos preocuparemos tanto em explanar exaustivamente todos os passos presentes nas entrelinhas das demonstrações mais avançadas. Recomendamos fortemente a consulta às referências bibliográficas expostas para que o leitor possa contemplar melhor esses conceitos fundamentais sobre polinômios e corpos finitos e facilmente perceber que o que foi exposto aqui se trata de uma pequeníssima porção de um universo fascinante.

No capítulo 3, por sua vez, nos aplicaremos finalmente a exibir o algoritmo. Discorreremos também um pouco, ainda que não muito formalmente, sobre o custo do algoritmo e daremos nossas conclusões a respeito.

Dado o contexto de nossa revisão bibliográfica, fornecemos também um breve

apêndice sobre Álgebra Moderna, abordando alguns dos conceitos e algumas das demonstrações utilizadas. Para o leitor mais interessado no assunto, indicamos também referências bibliográficas para o tema.

Para facilitar a leitura, disponibilizamos os seguintes recursos:

1. uma lista de símbolos, contendo as principais notações adotadas no texto;
2. uma numeração única para definições, notações, nomenclaturas e observações, referenciadas pelo número do capítulo em que se encontram;
3. uma numeração única para teoremas, propriedades, lemas e corolários, também referenciados pelo número do capítulo em que se encontram;
4. um índice remissivo contemplando os principais conceitos utilizados nos capítulos e apêndices;
5. notas de margem que ajudam na localização dos conceitos do índice remissivo.

Por fim, ressaltamos que, embora o objetivo do presente trabalho não seja fornecer uma base teórica completa sobre o assuto de irredutibilidade polinomial em corpos finitos, acreditamos que ele possa servir como uma apresentação do tema para alunos de graduação e uma orientação bibliográfica para pesquisas futuras. O algoritmo apresentado ainda vem acompanhado de sugestões de implementação que podem ser experimentadas por qualquer leitor com noções básicas de programação, e as demonstrações mais complicadas podem ser melhor acompanhadas no material indicado nas referências.

Capítulo 2

Esboço dos fundamentos teóricos

Com o objetivo de fundamentar teoricamente o algoritmo exibido no capítulo 3, esboçamos no presente capítulo a conceituação elementar da Teoria de Polinômios (seção 2.1) e da Teoria de Anéis de Polinômios (seção 2.2) e, por último, esboçamos os conceitos de divisibilidade e irredutibilidade polinomial, chegando ao teorema 2.12, de cuja aplicação extrairemos nosso algoritmo.

Como já mencionado na introdução do documento, daremos uma ênfase especial aos conceitos e às demonstrações que poderão nos ser úteis posteriormente e não contemplaremos nem mesmo os resultados mais interessantes ou de maior impacto relacionados ao assunto. Além do mais, deixaremos de abordar explicitamente muitos conceitos e demonstrações que eram estritamente relacionados ao nosso texto, optando por não carregar demais o trabalho. Novamente sugerimos a consulta à bibliografia para que o leitor acompanhe melhor esses conceitos e essas demonstrações.

2.1 Polinômios

Atualmente, a Matemática Moderna define o conceito de polinômio graças ao conceito de "função com suporte finito", elaborado especificamente para a axiomatização da Teoria de Polinômios. O leitor notará também que toda a abordagem sobre polinômios que construiremos será, pelo menos em primeira instância, bastante genérica, diferente daquela da Matemática Clássica. Na realidade, todo o presente capítulo caberia muito bem no apêndice sobre fundamentação algébrica, o qual preferimos destinar a conceitos mais elementares ainda, como as estruturas algébricas tradicionais da Álgebra Moderna.

Definição 2.1. Sendo $(G, *)$ um grupo qualquer, dizemos que uma função qualquer a de contradomínio G possui suporte finito em $(G, *)$ se e somente se o conjunto $a^{-1}(G \setminus \{e\})$ é finito, sendo e o elemento neutro do grupo.

suporte finito de uma função

Observação 2.2. Sendo $(R, +, \cdot)$ um anel qualquer e a uma função com suporte finito em $(R, +)$, note-se que a soma $\sum_{k \in \mathbb{N}} a(k)$ é bem definida, já que é finito seu número de termos diferentes de $\underline{0}$, e que ou $a^{-1}(R \setminus \{\underline{0}\})$ é vazio ou possui um máximo.

Entendido o conceito de função com suporte finito, podemos nos arriscar a uma definição de "polinômio".

polinômio

indeterminada de um polinômio

DEFINIÇÃO 2.3. Sendo $(R, +, \cdot)$ um anel qualquer e $a\colon \mathbb{N} \to R$ uma função com suporte finito em $(R, +)$, chamamos de polinômio sobre $(R, +, \cdot)$ com indeterminada x a expressão

$$f(x) = \sum_{k\in\mathbb{N}} a(k)x^k$$

para qualquer $x \in R$. Ademais, se o conjunto $a^{-1}(R \setminus \{0\}$, além de finito, também não for vazio, chamaremos de grau de f o número natural

grau de um polinômio

$$d(f) = \max\left(a^{-1}(R \setminus \{\underline{0}\})\right).$$

Se, entretanto, $a^{-1}(R \setminus \{zero\}$ for vazio, convencionamos que $d(f) = +\infty$.

OBSERVAÇÃO 2.4. Note-se que f pode ser escrito na forma

$$f(x) = \sum_{k=0}^{d(f)} a_k x^k, \tag{2.1}$$

forma padrão de um polinômio

denotando-se $a(k)$ por a_k. Assim, dizemos que a equação 2.1 é a forma padrão de f. Ademais, note-se também que não apenas uma função com suporte finito determina um e só um polinômio, mas também que um polinômio determina uma e só uma função com suporte finito, motivo pelo qual nos permitimos a nos referir a um polinômio sem necessariamente explicitar sua função com suporte finito.

termo constante de um polinômio

termo dominante de um polinômio

NOMENCLATURA 2.5. Sendo $f(x)$ um polinômio sobre um anel $(R, +, \cdot)$ e sendo a sua função com suporte finito, chamamos a_0 de termo constante de $f(x)$. Se $f(x)$ possui grau finito então também chamamos $a_{d(f)}$ de termo dominante de $f(x)$.

polinômio constante

NOMENCLATURA 2.6. Um polinômio é dito constante se e só se seu grau é 0.

A nomenclatura 2.7, que apresentamos a seguir, trata de um dos princípios mais importantes e elementares da Teoria de Polinômios pura: o princípio da identidade de polinômios, apresentado por Descartes no século XVII. O leitor mais atento deve perceber que não há confusão entre os conceitos de identidade e de igualdade de polinômios. Como um polinômio é uma expressão, dois polinômios $f(x)$ e $g(x)$ sobre um anel são iguais se $f(r)$ e $g(r)$ são iguais para todo elemento r do anel. Isso não significa necessariamente que as expressões que formam f e g sejam equivalentes. Na verdade, um resultado muito conhecido dentro da Teoria de Polinômios é que polinômios sobre um domínio de integridade — e, portanto, sobre um corpo — são idênticos se e somente se são iguais.

princípio da identidade de polinômios

polinômios idênticos

NOMENCLATURA 2.7 (Princípio da identidade de polinômios)**.** Dizemos que dois polinômios f e g sobre um anel $(R, +, \cdot)$ são idênticos, e escrevemos $f \equiv g$, se e só se $a_k = b_k$ para todo $k \in \mathbb{N}$, sendo a a função com suporte finito do polinômio f e b a função com suporte finito do polinômio g.

NOTAÇÃO 2.8. Sendo $(R, +, \cdot)$ um anel, usamos $\underline{0}(x)$, $\underline{1}(x)$ e $\mathrm{id}(x)$ para denotar respectivamente os polinômios:

$$\underline{0}(x) = \underline{0};$$
$$\underline{1}(x) = \underline{1};$$
$$\mathrm{id}(x) = x.$$

polinômio identidade

Costumamos também chamar $\mathrm{id}(x)$ de polinômio identidade.

PROPRIEDADE 2.1. *Sendo f um polinômio sobre um anel $(R,+,\cdot)$, se $f(x) \neq \underline{0}(x)$ então $a_{d(f)} \neq \underline{0}$.*

DEMONSTRAÇÃO. É imediato que se $f(x) \equiv \underline{0}(x)$ então $f(x) = \underline{0}(x)$, já que, da notação 2.8 e do teorema 2.7, para todo $r \in R$,

$$f(r) = \underline{0}.$$

Portanto, se $f(x) \neq \underline{0}(x)$ então $f(x) \not\equiv \underline{0}(x)$ e, assim, $a^{-1}(R \setminus \{\underline{0}\}) \neq \emptyset$ e, conseqüentemente, pela definição de grau, como $d(f) = \max\big(a^{-1}(R \setminus \{\underline{0}\})\big)$, $a_{d(f)} \neq \underline{0}$. ♦

Não podemos esquecer que uma das principais causas das transformações profundas pelas quais a Álgebra passou no século XIX devem-se sobretudo ao problema de encontrar raízes de uma equação. Se observarmos atentamente, perceberemos que as equações estudadas na época eram na realidade polinômios sobre o anel — mais especificamente corpo — dos números reais. Assim, apresentamos a seguir o conceito genérico atualmente aceito como o de raiz de um polinômio.

DEFINIÇÃO 2.9. Sendo f um polinômio sobre um anel $(R,+,\cdot)$, dizemos que um elemento u de R é raiz de f se e só se $f(u) = \underline{0}$. Se, porém, todos os elementos de R são raízes de f então dizemos que f é identicamente nulo, já que é igual ao polinômio $\underline{0}(x)$.

raiz de um polinômio

polinômio identicamente nulo

NOTAÇÃO 2.10. Sendo f um polinômio sobre um anel $(R,+,\cdot)$, $\rho(f)$ denota o conjunto das raízes de f.

NOTAÇÃO 2.11. Sendo f um polinômio sobre um anel $(R,+,\cdot)$, usamos $-f(x)$ para denotar o polinômio

$$(-f)(x) = -\big(f(x)\big).$$

2.2 Anéis de polinômios

Em 1824, N. H. Abel provou que não há fórmula geral por radicais para resolver equações de grau no mínimo 5. Entretanto, todos sabiam que alguns casos particulares dessas equações eram resolúveis por radicais. O que, então, caracterizava essas equações especiais? Foi respondendo a essa pergunta que Galois delineou pela primeira vez o conceito de grupo, associando a cada equação um grupo de permutações das raízes da equação e mostrando que a resolubilidade por radicais dependia de uma propriedade de que esses grupos poderiam ou não gozar.

Assim, podemos observar a relação estreita entre os polinômios e as estruturas algébricas modernas já no século XIX. Não demorou muito para que os polinômios fossem formalizados sobre anéis — como já abordamos na seção 2.1 — e menos tempo ainda se passou para que surgisse o conceito de anéis de polinômios, que abordaremos a seguir.

TEOREMA 2.2. *Sendo $(R,+,\cdot)$ um anel qualquer, $R[x]$ o conjunto de todos os polinômios sobre R e as operações de adição e multiplicação de polinômios definidas como*

$$(f+g)(x) = f(x) + g(x) \qquad \text{e}$$
$$(fg)(x) = f(x)g(x),$$

$(R[x],+,\cdot)$ é um anel, o anel de polinômios sobre o anel $(R,+,\cdot)$.

anel de polinômios

DEMONSTRAÇÃO. Tomemos f_1, f_2 e f_3 polinômios de $R[x]$ cujas formas padrões sejam:

$$\begin{aligned} f_1(x) &= \sum_{k=0}^{d(f_1)} a_k x^k; \\ f_2(x) &= \sum_{k=0}^{d(f_2)} b_k x^k; \\ f_3(x) &= \sum_{k=0}^{d(f_3)} c_k x^k. \end{aligned} \tag{2.2}$$

De (2.2), a associatividade e a comutatividade da adição de polinômios seguem da própria associatividade e comutatividade da adição de elementos de R. Verifica-se também a existência de um polinômio que sirva de elemento neutro para a adição de polinômios na medida em que $f_1(x)+\underline{0}(x) = f_1(x)$. Ademais, o polinômio $(-f_1)(x)$ serve de simétrico de $f_1(x)$ em relação a $\underline{0}(x)$. Assim, concluímos que $(R[x],+)$ se trata um grupo abeliano.

Como a associatividade da multiplicação de polinômios segue da própria associatividade da multiplicação de elementos de R, resta-nos apenas mostrar a distributividade da multiplicação de polinômios sobre a adição de polinômios. Para tanto, notemos, de (2.2), que

$$\begin{aligned} f_1(x)\big(f_2(x)+f_3(x)\big) &= \sum_{k=0}^{d(f_1)} a_k x^k \left(\sum_{k=0}^{d(f_2)} b_k x^k + \sum_{k=0}^{d(f_3)} c_k x^k \right) \\ &= \left(\sum_{k=0}^{d(f_1)} a_k x^k \right)\left(\sum_{k=0}^{d(f_2)} b_k x^k \right) + \left(\sum_{k=0}^{d(f_1)} a_k x^k \right)\left(\sum_{k=0}^{d(f_3)} c_k x^k \right) \\ &= \big(f_1(x)+f_2(x)\big)+f_3(x), \end{aligned}$$

como queríamos mostrar. ♦

As propriedades 2.3, 2.4 e 2.7 relacionam as propriedades dos anéis dos polinômios com as propriedades dos anéis sobre os quais aqueles polinômios são formados. O leitor mais atento perceberá que não há uma propriedade que defina como corpo o anel de polinômios sobre corpos. O motivo é que tal propriedade não existe. Deixamos como um interessante exercício a demonstração de que um anel de polinômios sobre corpos não é necessariamente um corpo.

PROPRIEDADE 2.3. *Sendo $(R,+,\cdot)$ um anel, $(R,+,\cdot)$ é comutativo se e somente se $(R[x],+,\cdot)$ é comutativo.*

DEMONSTRAÇÃO. Admitamos inicialmente que $(R,+,\cdot)$ seja um anel comutativo. Como, do teorema 2.2, $(R,+,\cdot)$ é um anel, falta-nos apenas mostrar a comutatividade da multiplicação de polinômios, que segue imediatamente da comutatividade da multiplicação de elementos de R, já que $(R,+,\cdot)$ se trata de um anel comutativo.

Por outro lado, suponhamos agora que $(R[x],+,\cdot)$ é que se trata de um anel comutativo. Já sabemos, por hipótese, que $(R,+,\cdot)$ é um anel. Assim, falta-nos, desta vez, apenas mostrar a comutatividade da multiplicação de elementos de R. Tomemos, então, a e b em R e tomemos também os polinômios constantes

$$f_a(x) = a \qquad \text{e} \qquad f_b(x) = b.$$

Como $(R[x],,+,\cdot)$ é comutativo, $f_a \cdot f_b = f_b \cdot f_a$ e, portanto, $a \cdot b = b \cdot a$, e concluimos a demonstração. ♦

PROPRIEDADE 2.4. *Sendo $(R,+,\cdot)$ um anel, $(R,+,\cdot)$ possui unidade se e somente se $(R[x],+,\cdot)$ possui unidade.*

DEMONSTRAÇÃO. Supondo que $(R,+,\cdot)$ possui unidade, é imediato verificar que $(R[x],+,\cdot)$, que é um anel por causa do teorema 2.2, também possui unidade, já que, como $\underline{1}$ é a unidade de $(R,+,\cdot)$,

$$\begin{aligned}\underline{1}(x)\cdot f(x) &= \underline{1}\left(\sum_{k=0}^{d(f)} a_k x^k\right)\\ &= \sum_{k=0}^{d(f)} 1\cdot a_k \cdot x^k\\ &= \sum_{k=0}^{d(f)} a_k x^k\\ &= f(x),\end{aligned}$$

para todo $f \in R[x]$.

Por outro lado, suponhamos que $(R[x],+,\cdot)$ possua uma unidade

$$u(x) = \sum_{k=0}^{d(u)} y_k x^k.$$

Logo, para todo $a \in R$, sendo $f_a(x)$ o polinômio constante definido por $f_a(x) = a$, observa-se que $(f_a \cdot u)(x) = f_a(x)$ e que $(u \cdot f_a)(x) = f_a(x)$, já que u é unidade do anel $(R[x],+,\cdot)$. Em particular, temos, para algum $x_0 \in R$, que $(f_a \cdot u)(x_0) = f_a(x_0)$, $(u \cdot f_a)(x_0) = f_a(x_0)$ e, portanto, que

$$a\left(\sum_{k=0}^{d(u)} y_k {x_0}^k\right) = a$$

e que

$$\left(\sum_{k=0}^{d(u)} y_k {x_0}^k\right) a = a.$$

Logo, como $\sum_{k=0}^{d(u)} y_k {x_0}^k \in R$, encontramos uma unidade para o anel $(R,+,\cdot)$, já que $\sum_{k=0}^{d(u)} y_k {x_0}^k$ vale como elemento neutro da multiplicação para qualquer elemento a de R. ♦

LEMA 2.5. *Sendo f_1, f_2 e f_3 polinômios sobre um anel $(R,+,\cdot)$, se $f_1 \equiv f_2 + f_3$ e se $f_2 \not\equiv \underline{0}$ então*

$$d(f_2) \leqslant d(f_1).$$

DEMONSTRAÇÃO. Suponhamos que $d(f_2) > d(f_1)$. Sendo a e b as funções com suporte finito de, respectivamente, f_1 e f_2, como

$$f_2(x) \equiv a_{d(f_2)} x^{d(f_2)} + \sum_{k=0}^{d(f_2)-1} a_k x^k,$$

e, portanto,

$$f_1(x) \equiv a_{d(f_2)}x^{d(f_2)} + \sum_{k=0}^{d(f_2)-1} a_k x^k + f_3(x),$$

e como, da propriedade 2.1, já que $f_2 \not\equiv \underline{0}$, $d(f_2) \in b^{-1}(R \setminus \{\underline{0}\})$, $d(f_2) \in a^{-1}(R \setminus \{\underline{0}\})$, uma vez que $b^{-1}(R \setminus \{\underline{0}\}) \subseteq a^{-1}(R \setminus \{\underline{0}\})$. Assim, porque

$$d(f_1) = \max\big(a^{-1}(R \setminus \{\underline{0}\})\big),$$

e porque $d(f_2) > d(f_1)$, temos que

$$d(f_2) > \max\big(a^{-1}(R \setminus \{\underline{0}\})\big),$$

o que é um absurdo, já que $d(f_2) \in a^{-1}(R \setminus \{\underline{0}\}$. ♦

LEMA 2.6. *Sendo f e g polinômios sobre um domínio de integridade $(R, +, \cdot)$,*

$$d(fg) = d(f) + d(g).$$

DEMONSTRAÇÃO. Se $f(x) \equiv \underline{0}(x)$ ou $g(x) \equiv \underline{0}(x)$, a desigualdade se verifica trivialmente na medida em que $d(f)+d(g) = +\infty$. Assumamos, portanto, que $f(x) \not\equiv \underline{0}(x)$ e que $g(x) \not\equiv \underline{0}(x)$. Sabemos, sendo a e b as funções com suporte finito de, respectivamente, f e g, que

$$f(x) \equiv a_{d(f)}x^{d(f)} + f_1(x) \qquad \text{e que} \qquad g(x) \equiv b_{d(g)}x^{d(g)} + g_1(x),$$

para algum polinômio f_1 e algum polinômio g_1 sobre $(R, +, \cdot)$. Assim,

$$f(x)g(x) \equiv a_{d(f)}b_{d(g)}x^{d(f)+d(g)} + a_{d(f)}x^{d(f)}g_1(x) + b_{d(g)}x^{d(g)}f_1(x). \tag{2.3}$$

Como $f(x) \neq \underline{0}(x)$ e $g(x) \neq \underline{0}(x)$, temos, da propriedade 2.1, que $a_{d(f)} \neq \underline{0}$ e $b_{d(g)} \neq \underline{0}$. Como $(R, +, \cdot)$ é um domínio de integridade, $a_{d(f)}b_{d(g)} \neq \underline{0}$ e, portanto, do lema 2.5,

$$d\big(a_{d(f)}b_{d(g)}x^{d(f)+d(g)}\big) = d(f) + d(g) \leqslant d\big(f(x)g(x)\big).$$

Resta-nos ainda provar que $d(fg) \leqslant d(f) + d(g)$. Suponhamos que $d(fg) > d(f) + d(g)$ e tomemos c a função de suporte finito do polinômio fg, α a função com suporte finito de f_1 e β a função com suporte finito de g_1. Tomemos também os conjuntos:

$$A = \begin{cases} \big\{d(g) + \ell \colon \ell \in \alpha^{-1}(R \setminus \{\underline{0}\})\big\}, & \text{se } p_1(x) \not\equiv \underline{0}(x); \\ \emptyset & \text{caso contrário;} \end{cases}$$

$$B = \begin{cases} \big\{d(f) + \ell \colon \ell \in \beta^{-1}(R \setminus \{\underline{0}\})\big\}, & \text{se } q_1(x) \not\equiv \underline{0}(x); \\ \emptyset & \text{caso contrário;} \end{cases}$$

Como (2.3) se trata de uma identidade polinomial, então

$$c^{-1}(R \setminus \{\underline{0}\}) = \{d(f) + d(g)\} \cup A \cup B.$$

Contudo, $d(fg) \notin \{d(f) + d(g)\}$, pois, por hipótese, $d(fg) > d(f) + d(g)$. Também $d(fg) \notin A$, pois, se A não é vazio então $\max A = d(g) + d(f_1)$ e, portanto, $\max A \leqslant d(g) + d(f)$, uma vez que, do lema 2.5, já que $f_1 \not\equiv \underline{0}$ ($A \neq \emptyset$), $d(f_1) \leqslant d(g)$. E, finalmente, $d(fg) \notin B$, pois, se B não é vazio então $\max B = d(f)+d(g_1)$ e, portanto, $\max B \leqslant d(f) + d(g)$, uma vez que, do lema 2.5, já que $g_1 \not\equiv \underline{0}$ ($B \neq \emptyset$), $d(g_1) \leqslant d(g)$. Assim, $d(fg) \notin c^{-1}(R \setminus \{\underline{0}\})$, o que é um absurdo, já que c é a função de suporte finito de pq. Conseqüentemente, $d(fg) \leqslant d(f) + d(g)$. ♦

PROPRIEDADE 2.7. *Sendo $(R,+,\cdot)$ um anel, $(R,+,\cdot)$ é um domínio de integridade se e só se $(R[x],+,\cdot)$ é um domínio de integridade.*

DEMONSTRAÇÃO. Suponhamos inicialmente que $(R,+,\cdot)$ seja um domínio de integridade. Das propriedades 2.3 e 2.4, como $(R,+,\cdot)$ é um anel comutativo com unidade, verifica-se também que $(R[x],+,\cdot)$ é um anel comutativo com unidade. Para mostrarmos que vale a lei do anulamento do produto, sendo f e g polinômios de $R[x]$, utilizaremos a forma contrapositiva. Suponhamos que $f(x) \neq \underline{0}(x)$ e que $g(x) \neq \underline{0}(x)$. Do lema 2.6, como $(R,+,\cdot)$ é um domínio de integridade, $d(fg) = d(f) + d(g)$. Como $d(f)$ e $d(g)$ são números naturais finitos, $d(fg)$ também é um número natural finito. Portanto, $(fg)(x) \neq \underline{0}(x)$, como queríamos mostrar.

Admitamos agora que $(R[x],+,\cdot)$ é que se trata de um domínio de integridade. Por hipótese, $(R,+,\cdot)$ é um anel e, das propriedades 2.3 e 2.4, é comutativo e possui unidade. Por fim, para mostrarmos que vale a lei do anulamento do produto, também utilizaremos a forma contrapositiva. Notemos que, para a e b em $R \setminus \{\underline{0}\}$, vale, já que $(R[x],+,\cdot)$ se trata de um domínio de integridade, que $(f_a \cdot f_b)(x) \neq \underline{0}(x)$, sendo f_a e f_b os polinômios constantes $f_a(x) = a$ e $f_b(x) = b$. Portanto, $ab \neq \underline{0}$, como queríamos mostrar. ♦

2.3 Divisibilidade e irredutibilidade polinomial

Por último, apresentamos os conceitos aos quais pretendíamos chegar. O leitor notará a relação direta entre o conceito de irredutibilidade polinomial e o conceito de divisibilidade polinomial, motivo pelo qual decidimos apresentar ambas as definições numa mesma seção. Vale lembrar que é justamente pertinente a esses assuntos que a maioria dos resultados mais interessantes conhecidos são deixados de lado, dada a imensidão do que já se conhece.

DEFINIÇÃO 2.12. Dizemos que um polinômio f_1 de um anel de polinômios $(R[x],+,\cdot)$ divide um outro polinômio f_2 do mesmo anel, e escrevemos $f_1 \backslash f_2$, se e só se existe polinômio $g \in R[x]$ tal que $f_2 = f_1 g$.

NOMENCLATURA 2.13. Quando $f_1 \backslash f_2$, sendo f_1 e f_2 polinômios de um anel de polinômios $(R[x],+,\cdot)$, dizemos que:

(i) f_2 é <u>divisível</u> por f_1; — divisibilidade polinomial

(ii) f_2 é <u>múltiplo</u> de f_1; — múltiplo de um polinômio

(iii) f_1 é <u>divisor</u> de f_2; — divisor de um polinômio

(iv) g é um <u>quociente da divisão</u> de f_2 por f_1, sendo g um polinômio tal que $f_2 = f_1 g$. — quociente de uma divisão polinomial

O leitor deve ter notado a semelhança da nomenclatura 2.13 com aquela utilizada para divisibilidade de números inteiros, que, a saber, é apresentada na nomenclatura A.13. Não poderia ser de outro modo, já que as construções teóricas são bastante similares. Assim, embora não demonstraremos o resultado apresentado na observação 2.14, não é de se assustar que ele valha e que sua demonstração seja muito parecida com aquela utilizada para mostrar a validade do algoritmo da divisão para números inteiros. O leitor ainda notará que abandonaremos os polinômios sobre anéis quaisquer e nos ateremos em especial aos

anéis sobre corpos. Isso se faz necessário para a construção do embasamento teórico que se segue.

algoritmo da divisão para polinômios

OBSERVAÇÃO 2.14 (Algoritmo da divisão para polinômios)**.** Se $g(x) \neq \underline{0}(x)$ é um polinômio de $F[x]$, sendo $(F, +, \cdot)$ um corpo, então para todo $f \in F[x]$ existem dois polinômios q e r em $F[x]$ tais que

$$f = qg + r \qquad \text{e} \qquad d(r) < d(g).$$

O teorema 2.8, que apresentamos a seguir, é um dos mais elementares da Teoria de Polinômios. Perceber-se-á que boa parte do que for explanado neste texto a partir daqui será relacionado ao resultado do teorema.

TEOREMA 2.8. *Sendo f um polinômio sobre um corpo $(F, +, \cdot)$, um elemento $\alpha \in F$ é uma raiz de f se e só se $(x - \alpha)$ divide $f(x)$.*

DEMONSTRAÇÃO. Suponhamos inicialmente que α seja raiz de F. Como $x - \alpha$ não é $\underline{0}$ para todo $x \in F$, temos, da observação 2.14, que $f(x)$ pode ser escrito como:

$$f(x) = q(x)(x - \alpha) + r(x),$$

sendo $r(x)$ um polinômio de grau menor que o grau de $x - \alpha$, portanto, 0. Assim,

$$f(x) = q(x)(x - \alpha) + \beta,$$

para algum $\beta \in F$. Dessarte, temos que

$$f(\alpha) = q(\alpha)(\alpha - \alpha) + \beta = q(\alpha)(\underline{0}) + \beta = \beta$$

e, conseqüentemente, que

$$f(x) = q(x)(x - \alpha) + f(\alpha).$$

Mas, como $f(\alpha) = \underline{0}$, já que α é uma raiz de f,

$$f(x) = q(x)(x - \alpha).$$

Logo, concluímos que $x - \alpha$ divide $f(x)$.

Por outro lado, admitamos agora que $x - \alpha$ divide $f(x)$. Assim, $f(x)$ pode ser escrito como:

$$f(x) = (x - \alpha)q(x).$$

Portanto,

$$f(\alpha) = (\alpha - \alpha)q(x) = (\underline{0})q(x) = \underline{0},$$

como queríamos demonstrar. ♦

A seguir, chegamos na definição que contribui para o título do presente trabalho. O conceito de irredutibilidade polinomial sobre corpos, como se nota, se trata na verdade de um conceito bastante simples, mas muito poderoso. Futuramente comentaremos um pouco da importância de se testar a irredutibilidade de polinômios sobre corpos finitos e de se encontrarem polinômios irredutíveis sobre corpos finitos.

polinômio irredutível

polinômio primo

DEFINIÇÃO 2.15. Seja $(F, +, \cdot)$ um corpo. Dizemos que um polinômio $p \in F[x]$ é irredutível sobre $F[x]$ (ou irredutível em $F[x]$, ou primo em $F[x]$) quando e só quando $d(p) > 0$ e, para quaisquer p_1 e p_2 em $F[x]$, $p = p_1 p_2$ implicar sempre que ou p_1 ou p_2 seja um polinômio constante.

NOTAÇÃO 2.16. Sendo K um subcorpo de um corpo $(F,+,\cdot)$ e M qualquer subconjunto de F, usamos $K(M)$ para denotar o conjunto

$$K(M) = \bigcap_{L\subseteq(F,+,\cdot)K\cup M\subseteq L} L.$$

PROPRIEDADE 2.9. *Sendo K um subcorpo de um corpo $(F,+,\cdot)$ e M qualquer subconjunto de F, $K(M)$ é um subcorpo de $(F,+,\cdot)$.*

DEMONSTRAÇÃO. Sabemos que $\underline{0} \in K(M)$, já que, do teorema A.56, $\underline{0}$ pertence a qualquer subcorpo L de $(F,+,\cdot)$. Tomemos agora x e y elementos de $K(M)$. Assim, x e y são elementos de qualquer subcorpo L de $(F,+,\cdot)$ tal que $K\cup M\subseteq L$. Suponhamos, então, que $x-y\notin K(M)$. Logo, existe um subcorpo L_0 de $(F,+,\cdot)$ tal que $K\cup M\subseteq L_0$ e tal que $x-y\notin L_0$, o que, também por causa do teorema teosubcorpo, é um absurdo, já que L_0 é um subcorpo e já que x e y são elementos de L_0.

Vamos agora mostrar que se $x\in K(M)$ e $y\in K(M)\setminus\{\underline{0}\}$ então $xy^{-1}\in K(M)$. Se $K(M)\setminus\{\underline{0}\}=\emptyset$ então a condicional se verifica trivialmente. Portanto, assumamos que $K(M)\setminus\{\underline{0}\}\neq\emptyset$ e tomemos $x\in K(M)$ e $y\in K(M)\setminus\{\underline{0}\}$. Dessarte, x e y são elementos de qualquer subcorpo L de $(F,+,\cdot)$ tal que $K\cup M\subseteq L$. Se, contudo, supuséssemos que $xy^{-1}\notin K(M)$, teríamos a existência de um subcorpo L_0 de $(F,+,\cdot)$ tal que $K\cup M\subseteq L$ e tal que $xy^{-1}\notin L_0$, o que seria um absurdo, dado que, por L_0 ser um subcorpo e por x e y pertencerem a L_0, L_0 deveria conter xy^{-1} por causa do teorema A.56.

Finalmente, por causa do teorema A.56, temos que $K(M)$ é um subcorpo de $(F,+,\cdot)$. ♦

O conceito que apresentamos a seguir, de "corpos de decomposição", é de fato bastante relacionado com o conceito de "corpos de extensão", que não abordamos — o que não significa que não utilizamos — com mais detalhes no presente trabalho. Em linhas gerais, um se K é um subcorpo de um corpo $(F,+,\cdot)$, dizemos que $(F,+,\cdot)$ é um corpo de extensão de K. O conceito pode ser facilmente entendido quando pensamos no corpo dos números complexos como um corpo de extensão do corpo dos números reais. Na verdade, a principal motivação para o estudo de corpos de extensão está justamente no estudo de raízes de polinômios sobre corpos. Sabemos que nem todas as raízes de polinômios sobre o corpo dos reais pertencem a $\mathbb{R}$, mas é muito conhecido que todas elas pertencem a $\mathbb{C}$. Uma argumentação, que não será devidamente abordada no presente trabalho, mostra um resultado parecido para corpos finitos. Em particular, todas as raízes de um polinômio de grau n sobre $\mathbb{F}_p$ estão no corpo de extensão $\mathbb{F}_{p^n}$.

corpo de extensão

DEFINIÇÃO 2.17. Seja K um subcorpo de um corpo $(F,+,\cdot)$. Dizemos que um polinômio $p\in K[x]$ de grau positivo finito decompõe [1] $(F,+,\cdot)$ se e somente se existe um subconjunto finito $A=\{\alpha_j : j\in[|A|]\}$ de F tal que

decomposição de um corpo por um polinômio

$$p(x) = a_0\prod_{j=1}^{|A|}(x-\alpha_j),$$

sendo a_0 o termo constante de $p(x)$. Ademais, dizemos que $(F,+,\cdot)$ é um corpo de decomposição polinomial [2] de p sobre K se e só se p decompõe $(F,+,\cdot)$ e $F=K(A)$.

corpo de decomposição polinomial

[1] Em inglês, *splits*.
[2] Em inglês, *splitting field*.

LEMA 2.10. *Sendi q uma potência de um primo, sendo $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m e sendo n um número natural, $f(x)$ divide $x^{q^n} - x$ se e somente se m divide n.*

DEMONSTRAÇÃO. Suponhamos inicialmente que $f(x)$ divida $x^{q^n} - x$ e tomemos α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Como α é raiz de $f(x)$, temos do teorema 2.8 que $x-\alpha$ divide $f(x)$ e, portanto, que $x-\alpha$ divide x^{q^n}. Assim, novamente do teorema 2.8, α é uma raiz de x^{q^n} e, conseqüentemente, $\alpha = \alpha^{q^n}$. Logo, do teorema A.54, $\alpha \in \mathbb{F}_{q^n}$, e, mais que isso, $\mathbb{F}_q(\{\alpha\})$ é um subcorpo de $\mathbb{F}_{q^n}$. Entretanto, como $[\mathbb{F}_q(\{\alpha\}) : \mathbb{F}_q] = m$ e $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, temos, do teorema A.68, que m divide n.

Assumamos agora que m divida n. Da propriedade A.70, $(\mathbb{F}_{q^m}, +, \cdot)$ é um subcorpo de $(\mathbb{F}_{q^n}, +, \cdot)$. Tomemos agora uma raiz α de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Logo, $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, e, conseqüentemente, $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Finalmente, como $\alpha \in \mathbb{F}_{q^n}$, $\alpha^{q^n} = \alpha$ (teorema A.54), o que nos leva a concluir que α é uma raiz também de $x^{q^n} - x$. Dessarte, $f(x)$ divide $x^{q^n} - x$, como queríamos mostrar. ♦

TEOREMA 2.11. *Sendo f um polinômio irredutível de grau m em $\mathbb{F}_q[x]$, f possui uma raiz α em $\mathbb{F}_{q^m}$. Ademais, são também raízes de f todos os elementos do conjunto*

$$\left\{\alpha^{q^j} \in \mathbb{F}_{q^m} : j \in [0..(m-1)]\right\}.$$

DEMONSTRAÇÃO. Notemos primeiramente que, tomando uma raiz α de f no corpo de decomposição de f sobre $\mathbb{F}_q$, temos que $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e, portanto, que $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Em particular, $\alpha \in \mathbb{F}_{q^m}$. Ademais, se tivermos $\beta \in \mathbb{F}_{q^m}$ uma raiz de f, teremos que, sendo a uma função com suporte finito para f,

$$\begin{aligned}
f(\beta^q) &= \sum_{j=0}^{m} a_j \beta^{qj} \\
&= \sum_{j=0}^{m} a_j^q \beta^{qj} \qquad \text{(teorema A.54)} \\
&= \left(\sum_{j=0}^{m} a_j \beta^j\right)^q \qquad \text{(observação A.71)} \\
&= f(\beta)^q \\
&= \underline{0}.
\end{aligned}$$

Assim, provamos que sempre que $\beta \in \mathbb{F}_{q^m}$, β^q é uma raiz de f e, conseqüentemente, $\beta^q \in \mathbb{F}_{q^m}$. Como havíamos mostrado que $\alpha \in \mathbb{F}_{q^m}$, podemos, então, concluir que todos os elementos do conjunto

$$\left\{\alpha^{q^j} \in \mathbb{F}_{q^m} : j \in [0..(m-1)]\right\}$$

são raízes de f, como queríamos mostrar. ♦

Por fim, apresentamos o teorema que será a base para a construção do algoritmo que estudaremos no capítulo 3.

TEOREMA 2.12. *Sendo n um natural não nulo, p um primo positivo,*

$$L = \{\ell_j : 1 \leqslant j \leqslant n\}$$

o conjunto de todos os divisores primos de n, $k = |L|$ *e*

$$m_j = \frac{n}{\ell_j}, \quad \forall j \in [k],$$

um polinômio $g \in \mathbb{Z}_p[x]$ *de grau* n *é irredutível em* $\mathbb{Z}_p[x]$ *se e só se:*

(2.12.i) $g(x) \backslash \left(x^{p^n} - x\right)$*;*

(2.12.ii) para todo $j \in [k]$*, o polinômio constante* $\underline{1}(x)$ *é o único polinômio que divide ambos* $g(x)$ *e* $x^{p^{m_j}} - x$*.*

PROVA. Assumamos inicialmente que $g(x)$ seja irredutível em $\mathbb{Z}_p[x]$. Do teorema 2.11, temos que toda raiz α de $g(x)$ pertence a $\mathbb{F}_{p^n}$. Como $\mathbb{F}_{p^n}$ é um corpo finito com p^n elementos, temos, do teorema A.54, que

$$\alpha^{p^n} = \alpha,$$

o que caracteriza α como raiz do polinômio $x^{p^n} - x$ e nos traz, do teorema 2.8, que

$$(x - \alpha) \backslash \left(x^{p^n} - x\right).$$

Logo,

$$g(x) \backslash \left(x^{p^n} - x\right)$$

e provamos (i). Ademais, temos que, para qualquer natural m menor que n, $g(x)$ não tem raízes em $\mathbb{F}_{p^m}$. Portanto, para toda raiz α de $g(x)$ e todo natural m menor que n, sabemos, também do teorema 2.8, que

$$(x - \alpha) \not\backslash \left(x^{p^m} - x\right).$$

Como para todo divisor $d(x)$ de $g(x)$ diferente do polinômio constante $\underline{1}(x)$ existe um subconjunto Γ do conjunto das raízes de $g(x)$ tal que

$$\prod_{\gamma \in \Gamma} (x - \gamma) = d(x),$$

temos que nenhum divisor de $g(x)$ diferente do polinômio constante $\underline{1}(x)$ divide $x^{p^m} - x$, sendo m um natural menor que n. Assim, em particular, temos que nenhum divisor de $g(x)$ diferente do polinômio constante $\underline{1}(x)$ divide $x^{p_j^m} - x$, para todo $j \in [k]$, e provamos (ii).

Inversamente, assumamos agora (i) e (ii). Como

$$(x - \alpha) \backslash \left(x^{p^n} - x\right),$$

qualquer que seja α raiz de $g(x)$, todas as raízes de $g(x)$ estão em $\mathbb{F}_{p^n}$. Queremos demonstrar que g é irredutível. Suponhamos, entretanto, que g seja redutível e tomemos g_1 um divisor irredutível não constante de g. Sendo m o grau de g_1, com $m < n$, sabemos, do teorema 2.11, que todas as raízes de $g_1(x)$ pertencem a $\mathbb{F}_{p^m}$, que é gerado sobre $\mathbb{Z}_p$ por qualquer uma dessas raízes, conforme o mesmo teorema 2.11. Já que g_1 é um divisor de g, temos que $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ e que $m \backslash n$. Como $m < n$, é trivial que $m \backslash m_t$ para algum $t \in [k]$. Assim, analogamente, todas as raízes de g_1 estão em $\mathbb{F}_{p^{m_t}}$. Portanto, $g_1(x)$, que não é o polinômio constante $\underline{1}(x)$, divide ambos $g(x)$ e $x^{p^{m_t}} - x$, o que contraria (ii). Conseqüentemente, $g(x)$ é irredutível. ♦

Capítulo 3

O algoritmo

O teorema 2.12, com o qual encerramos o capítulo 2, nos fornece por ser bicondicional um eficiente algoritmo para testar a irredutibilidade de um polinômio $g(x) \in \mathbb{F}_q[x]$ de grau n. Em linhas gerais, o que o algoritmo faz é tentar verificar (i) e (ii). Vejamos:

IRREDUTÍVEL$\big(g(x)\big)$

Entrada: um polinômio $g \in \mathbb{F}_q[x]$ de grau n.
Saída: *"verdadeiro"* ou *"falso"*.

1. Calcule $f_1(x) \leftarrow x^{p^n}$ módulo $g(x)$.
2. Calcule $f_2(x) \leftarrow f_1(x) - x$ módulo $g(x)$.
3. Se $f_2 \neq \underline{0}$ então devolva *"falso"*.
4. Para cada $j \in [k]$:
5. Calcule $f_{1_j}(x) \leftarrow x^{p^{m_j}}$ módulo $g(x)$.
6. Calcule $f_{2_j}(x) \leftarrow f_{1_j}(x) - x$ módulo $g(x)$.
7. Para cada raiz α de g:
8. Calcule $f_{3_{j_\alpha}}(x) \leftarrow (x - \alpha) f_{2_j}(x)$ módulo $g(x)$.
9. Se $f_{3_{j_\alpha}} \neq \underline{0}$ então devolva *"falso"*.

É imediato que as linhas 1–3 testam (i). Ademais, notemos que, para todo $j \in [k]$, o polinômio constante $\underline{1}(x)$ é o único polinômio que divide ambos $g(x)$ e $x^{p^{m_j}} - x$ se e somente se $(x - \alpha)(x^{p^{m_j}} - x)$ módulo $g(x)$, qualquer que seja α raiz de $g(x)$ não é divisor de $g(x)$. Esse resultado pode ser facilmente demonstrado e garante que as linhas 4–9 testam (ii).

Um resultado bastante conhecido nos assegura que x^{p^n} módulo $g(x)$ pode ser calculado com no máximo $2 \log p^n$ multiplicações polinomiais módulo $g(x)$. Além disso, como computamos módulo $g(x)$, nunca precisamos tratar de polinômios de grau maior que $2n$ durante o processo.

Em 1977, o alemão Schonhage[5] mostrou que a multiplicação de dois po-

linômios de grau n sobre corpos finitos pode ser feita em $O(n \log n \log\log n)$ operações do corpo. Por outro lado, sabemos, como mostrado em [1], que encontrar o resto da divisão de uma multiplicação de polinômios de grau no máximo n por um polinômio de grau no máximo n pode ser feito também em $O(n \log n \log\log n)$ operações do corpo. Assim, a linha 1 pode ser executada com

$$O\big(2 \log p^n (n \log n \log\log n + n \log n \log\log n)\big) = O\big(n^2 (\log n \log\log n) \log p\big) \qquad (3.1)$$

operações de $\mathbb{F}_p$. Como as linhas 2–3 podem ser executadas em tempo constante, a estimativa 3.1 vale para todo o conjunto de linhas 1–3.

Também por causa dos mesmos resultados mostrados por [1], podemos concluir que a linha 8 pode ser executada com

$$O(n \log n \log\log n) + O(n \log n \log\log n) = O(n \log n \log\log n)$$

operações de $\mathbb{F}_p$, estimativa que vale na realidade para todo o conjunto de linhas 8–9. Dessarte, como $g(x)$ possui no máximo n raízes, as linhas 7–9 podem ser executadas com $O(n^2 \log n \log\log n)$ operações em $\mathbb{F}_p$. Utilizando a mesma argumentação que usamos para as linhas 1–3, e lembrando que $O(m^j) = O(n)$ para todo $j \in [k]$, concluímos que as linhas 5–6 também podem ser executadas com $O\big(n^2 (\log n \log\log n) \log p\big)$ operações em $\mathbb{F}_p$. Finalmente, como $k \leqslant \log n$, temos que as linhas 4–9 podem ser executadas com

$$O\big(\log n (n^2 (\log n \log\log n) \log p + n^2 \log n \log\log n)\big) = O\big((n \log n)^2 (\log\log n) \log p\big),$$

e, portanto, todo o algoritmo pode ser executado com

$$O\big(n^2 (\log n \log\log n) \log p\big) + O\big((n \log n)^2 (\log\log n) \log p\big) = O\big((n \log n)^2 (\log\log n) \log p\big)$$

operações sobre $\mathbb{F}_p$. Uma vez que cada operação sobre $\mathbb{F}_p$, na medida em que representamos elementos de $\mathbb{F}_p$ por $O(\log p)$ *bits*, pode ser feita em $O(\log p \log\log p)$ operações elementares, chegamos à seguinte estimativa para o tempo do algoritmo:

$$\begin{aligned} T(n) &= O\big((n \log n)^2 (\log\log n) \log p\big) O(\log p \log\log p) \\ &= O\big((n \log n (\log\log n) \log p)^2\big). \end{aligned}$$

Capítulo 4

Conclusão

O conceito de irredutibilidade polinomial sobre corpos finitos vem sido estudado profundamente nas últimas décadas, de cujos estudos derivaram aplicações diversas, como aplicações na Combinatória, na Teoria de Codificação, na Criptologia, na Criptografia, no estudo de circuitos com retroalimentação, na geração de seqüências pseudo-aleatórias, na Teoria dos Números e na manipulação de símbolos algébricos. No presente trabalho, após havermos construído um esboço teórico que fundamentou nossa abordagem, apresentamos um algoritmo para testar a irredutibilidade de um polinômio sobre um corpo finito, elaborado por M. Rabin[4]. Ademais, ainda analisamos o custo computacional desse algoritmo e concluímos que se trata de um algoritmo bastante eficiente. Para testar se um polinômio de grau n sobre um corpo finito com p elementos é irredutível, mostramos que o tempo do algoritmo é dado por:

$$T(n) = O\big((n \log n (\log \log n) \log p)^2\big).$$

Além disso, ainda fornecemos o algoritmo num formato bastante passível de implementação e indicamos uma bibliografia que contivesse sugestões de implementações eficientes para as operações utilizadas.

Apêndice A

Fundamentos algébricos

A.1 Conceitos preliminares

A.1.1 Partições

Definição A.1. Sendo A um conjunto qualquer, o conjunto potência, ou conjunto das partes, de A, denotado por 2^A, é o conjunto de todos os subconjuntos de A.

conjunto potência

conjunto das partes

Definição A.2. Sendo A um conjunto e $\mathscr{F}$ um subconjunto de 2^A, dizemos que $\mathscr{F}$ é uma partição de A se e só se:

partição

(i) nenhum elemento de $\mathscr{F}$ é vazio;

(ii) dois elementos de $\mathscr{F}$ ou são iguais ou são disjuntos;

(iii) a união de todos os elementos de $\mathscr{F}$ é o próprio conjunto A.

A.1.2 Relações

Definição A.3. Sendo A e B conjuntos quaisquer, uma relação $\sim$ entre A e B é qualquer subconjunto de $A \times B$. Mais especificamente, se $A = B$, diz-se que $\sim$ é uma relação sobre A, ou uma relação em A.

relação

Notação A.4. Sendo $\sim$ uma relação entre um conjunto A e um conjunto B, escrevemos, para todo $a \in A$ e todo $b \in B$, $a \sim b$ sempre que $(a, b) \in \sim$ e $a \nsim b$ sempre que $(a, b) \notin \sim$.

Nomenclatura A.5. Dizemos que uma relação $\sim$ sobre um conjunto A é reflexiva quando e só quando se $a \sim a$ para todo elemento a e A.

relação reflexiva

Nomenclatura A.6. Dizemos que uma relação $\sim$ sobre um conjunto A é simétrica quando e só quando, para todo a e todo b elementos de A, vale que se $a \sim b$ então $b \sim a$.

relação simétrica

Nomenclatura A.7. Dizemos que uma relação $\sim$ sobre um conjunto A é transitiva quando e só quando, para quaisquer a, b e c elementos de A, vale que se $a \sim b$ e $b \sim c$ então $a \sim c$.

relação transitiva

Nomenclatura A.8. Dizemos que uma relação $\sim$ sobre um conjunto A é anti-simétrica quando e só quando, para todo a e todo b elementos de A, vale que se $a \sim b$ e $b \sim a$ então $a = b$.

relação anti-simétrica

relação de equivalência

NOMENCLATURA A.9. Dizemos que uma relação $\sim$ sobre um conjunto não vazio A é uma relação de equivalência sobre A se e só se $\sim$ é reflexiva, simétrica e transitiva.

classe de equivalência

DEFINIÇÃO A.10. Sendo $\sim$ uma relação de equivalência sobre um conjunto não vazio A e a um elemento de A, a classe de equivalência de a por $\sim$ é o conjunto

$$[a]_\sim = \{b \in A : b \sim a\}$$

conjunto quociente

DEFINIÇÃO A.11. O conjunto quociente de um conjunto não vazio A por uma relação $\sim$ sobre A, denotado por ${}^{A}\!/_{\sim}$ é o conjunto

$$A/_\sim = \{[a]_\sim : a \in A\}$$

TEOREMA A.1. *O conjunto quociente de um conjunto não vazio A por uma relação $\sim$ sobre A é uma partição de A.*

DEMONSTRAÇÃO. Como A não é vazio, seja y qualquer um de seus elementos. É imediato que $[y]_\sim$ não seja vazio, já que pelo menos $y \in [y]_\sim$, uma vez que $\sim$ se trata de uma relação reflexiva.

Agora, sejam a e b elementos de A. Sabemos que se $[a]_\sim = [b]_\sim$ então $[a]_\sim$ e $[b]_\sim$ não são disjuntos, pois nem $[a]_\sim$ nem $[b]_\sim$ é vazio. Para mostrarmos que se $[a]_\sim \neq [b]_\sim$ então $[a]_\sim$ e $[b]_\sim$ são disjuntos, utilizaremos a forma contrapositiva. Suponhamos que $[a]_\sim$ e $[b]_\sim$ não sejam conjuntos disjuntos e tomemos x um elemento qualquer de $[a]_\sim \cap [b]_\sim$. Assim, $x \sim a$; portanto, $a \sim x$, e, como $x \sim b$, $a \sim b$ e $b \sim a$. Logo, vale que, para todo $\alpha \in [a]_\sim$, $\alpha \sim b$, já que $\alpha \sim a$ e $a \sim b$, e, conseqüentemente, que $\alpha \in [b]_\sim$, o que nos leva a concluir que $[a]_\sim \subseteq [b]_\sim$. Por outro lado, vale também que, para todo $\beta \in [b]_\sim$, $\beta \sim a$, já que $\beta \sim b$ e $b \sim a$, e, conseqüentemente, que $\beta \in [a]_\sim$, o que nos leva a concluir que $[b]_\sim \subseteq [a]_\sim$. Por fim, mostramos o que queríamos: que $[a]_\sim = [b]_\sim$.

Resta-nos ainda concluir que

$$\bigcup_{a \in A} [a]_\sim = A.$$

Da definição de classe de equivalência segue naturalmente que $[a]_\sim \subseteq A$ para todo $a \in A$, e, portanto,

$$\bigcup_{a \in A} [a]_\sim \subseteq A.$$

Tomemos agora $x \in A$. Como $\sim$ é reflexiva, é imediato que $x \in [x]$, e, dessarte, que $x \in \bigcup_{a \in A} [a]_\sim$. Finalmente, demonstramos que

$$A \subseteq \bigcup_{a \in A} [a]_\sim$$

e encerramos nossa prova. ♦

A.1.3 Divisibilidade no conjunto dos números inteiros

O conceito de divisibilidade no conjunto dos números inteiros está no núcleo da Teoria dos Números. A partir dele serão desenvolvidos os principais e mais interessantes conceitos e resultados da teoria que hoje possui aplicações inclusive para Criptografia e segurança de sistemas.

DEFINIÇÃO A.12. Dizemos que um número inteiro d divide um número inteiro z, e escrevemos $d\backslash z$, se e só se existe um número inteiro k tal que $z = dk$.

NOMENCLATURA A.13. Quando $d\backslash z$, sendo d e z inteiros, dizemos que:

(i) z é divisível por d; — divisibilidade

(ii) z é múltiplo de d; — múltiplo de um número inteiro

(iii) d é divisor de z; — divisor de um número inteiro

(iv) k é o quociente da divisão de z por d, sendo k um inteiro tal que $z = dk$. — quociente de uma divisão

PROPRIEDADE A.2. *Qualquer número inteiro divide* 0.

DEMONSTRAÇÃO. Sendo d um inteiro qualquer, é verdade que $0 = d \cdot 0$. Portanto, $d\backslash 0$, tendo 0 como quociente. ♦

PROPRIEDADE A.3. 0 *divide somente o próprio* 0.

DEMONSTRAÇÃO. É imediato que $0\backslash 0$, uma vez que $0 = 0k$ não importando o inteiro k. Temos então apenas de mostrar que se $0\backslash z$ então $z = 0$, qualquer que seja o inteiro z. Ora, se $0\backslash z$ então existe um inteiro k tal que $z = 0k$ e, portanto, $z = 0$, como queríamos mostrar. ♦

PROPRIEDADE A.4. *Sendo* d *e* z *inteiros, se* $d\backslash z$ *então* $|d| \leqslant |z|$.

DEMONSTRAÇÃO. Suponhamos que $d\backslash z$ e tomemos um inteiro k tal que $z = dk$. Assim, verifica-se que $|z| = |d||k|$ e, conseqüentemente, que $|z| \geqslant |d|$. ♦

PROPRIEDADE A.5. *Apenas os inteiros* 1 *e* -1 *dividem o número* 1.

DEMONSTRAÇÃO. Seja x um inteiro que divida 1. Da propriedade A.4, $|x| \leqslant 1$; portanto, $x \in \{0, 1, -1\}$. Como, da propriedade A.3, $0 \not\backslash 1$, e como $1\backslash 1$ e $-1\backslash 1$, temos que apenas 1 e -1 dividem 1. ♦

PROPRIEDADE A.6. $z\backslash z$ *para todo* $z \in \mathbb{Z}$.

DEMONSTRAÇÃO. Seja z um inteiro. Como $z = z \cdot 1$, é verdade que $z\backslash z$. ♦

PROPRIEDADE A.7. *Sendo* d *e* z *inteiros, se* $d\backslash z$ *então* $d\backslash -z$.

DEMONSTRAÇÃO. Se $d\backslash z$ então existe um k inteiro tal que $z = dk$ e, portanto, $-z = -dk = d(-k)$. Como $-k$ é inteiro, $d\backslash -z$. ♦

PROPRIEDADE A.8. *Sendo* a, b *e* c *inteiros, se* $a\backslash b$ *e* $b\backslash c$ *então* $a\backslash c$.

DEMONSTRAÇÃO. Suponhamos que $a\backslash b$ e que $b\backslash c$. Assim, existem k_1 e k_2 inteiros tais que $b = ak_1$ e $c = bk_2$. Portanto,

$$c = bk_2 = (ak_1)k_2 = a(k_1k_2),$$

e, como (k_1k_2) é um número inteiro, $a\backslash c$. ♦

PROPRIEDADE A.9. *Sendo* a, b, c *e* d *inteiros, se* $a\backslash b$ *e* $c\backslash d$ *então* $ac\backslash bd$.

DEMONSTRAÇÃO. Suponhamos que $a\backslash b$ e que $c\backslash d$. Assim, existem k_1 e k_2 inteiros tais que $b = ak_1$ e $d = ck_2$. Portanto,

$$bd = (ak_1)(ck_2) = (ac)(k_1k_2),$$

e, como (k_1k_2) é um número inteiro, $ac\backslash bd$. ♦

PROPRIEDADE A.10. *Se um inteiro d divide um inteiro z então d divide qualquer múltiplo de z.*

DEMONSTRAÇÃO. Sejam d e z inteiros tais que $d\backslash z$. Seja m um inteiro qualquer. Queremos mostrar que $d\backslash mz$. Sendo k um inteiro tal que $z = dk$, temos que $mz = m(dk)$ e, assim, que $mz = d(mk)$. Como mk é um inteiro, concluímos que $d\backslash mz$. ♦

PROPRIEDADE A.11. *Sendo a, b e c inteiros, se $a\backslash b$ e $a\backslash c$ então*

$$a\backslash(mb + nc),$$

quaisquer que sejam m e n números inteiros.

DEMONSTRAÇÃO. Suponhamos que $a\backslash b$ e que $a\backslash c$. Assim, existem k_1 e k_2 inteiros tais que $b = ak_1$ e $c = ak_2$. Portanto, sendo m e n inteiros quaisquer,

$$\begin{aligned} mb + nc &= m(ak_1) + n(ak_2) \\ &= a(mk_1) + a(nk_2) \\ &= a(mk_1 + nk_2). \end{aligned}$$

Assim, já que $(mk_1 + nk_2)$ é um número inteiro, concluímos que $a\backslash(mb + nc)$. ♦

PROPRIEDADE A.12. *Um inteiro d divide um inteiro z se e somente se d divide $|z|$.*

DEMONSTRAÇÃO. Se $d\backslash z$ então existe um inteiro k tal que $z = dk$ e, portanto, como

$$|z| = |dk| = |d||k| = sd|k| = d(s|k|),$$

$d\backslash|z|$, já que $(s|k|)$ é inteiro, sendo

$$s = \begin{cases} 1, & \text{se } d \geqslant 0; \\ -1, & \text{caso contrário.} \end{cases}$$

Por outro lado, se $d\backslash|z|$ então existe um inteiro k tal que $|z| = dk$ e, portanto, como $z = s|z|$, temos que

$$z = s|z| = sdk = d(sk),$$

sendo

$$s = \begin{cases} 1, & \text{se } z \geqslant 0, \\ -1, & \text{caso contrário.} \end{cases}$$

Por fim, como (sk) é um inteiro, temos que $d\backslash z$ e concluímos a demonstração. ♦

PROPRIEDADE A.13. *Se um número primo p divide ab, sendo a e b inteiros, então $p\backslash a$ ou $p\backslash b$.*

DEMONSTRAÇÃO. Suponhamos que $p \backslash ab$ mas que $p \not\backslash a$ e que $p \not\backslash b$. Assim, p não é um dos primos da fatoração de a nem tampouco algum dos primos da fatoração de b, o que contraria o teorema fundamental da Aritmética, já que a fatoração de ab é única e composta pelos primos de a e de b. ♦

A seguir, apresentamos a definição da principal relação de equivalência em Teoria dos Números.

DEFINIÇÃO A.14. Dizemos que um inteiro a é cônguruo a um inteiro b módulo um inteiro m, e escrevemos congruência

$$a \equiv b \pmod{m}$$

se e só se $m \backslash (a - b)$.

TEOREMA A.14. *Sendo m um inteiro não nulo, a relação de congruência é uma relação de equivalência sobre $\mathbb{Z}$.*

DEMONSTRAÇÃO. É imediato que, para todo $z \in \mathbb{Z}$,

$$z \equiv z \pmod{m},$$

já que $m \backslash (z - z)$, conforme a propriedade A.2.

Sejam a e b inteiros. Se

$$a \equiv b \pmod{m}$$

então $m \backslash (a - b)$ e, portanto, da propriedade A.7, $m \backslash (b - a)$, e, conseqüentemente,

$$b \equiv a \pmod{m}.$$

Resta-nos ainda mostrar a transitividade da congruência. Para tanto, tomemos a, b e c inteiros tais que

$$\begin{aligned} a &\equiv b \pmod{m} \quad \text{e} \\ b &\equiv c \pmod{m}. \end{aligned}$$

Como $m \backslash (a - b)$ e $m \backslash (b - c)$, temos, da propriedade A.11, que

$$m \backslash \big((a - b) + (b - c)\big)$$

e, dessarte, que

$$m \backslash (a - c)$$

e, assim, que

$$a \equiv c \pmod{m},$$

como queríamos mostrar. ♦

NOTAÇÃO A.15. Sendo m um inteiro não nulo, escrevemos $\mathbb{Z}_m$ para denotar o conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo m. Além disso, sendo z um inteiro, utilizamos $[z]_m$ para denotar a classe de equivalência de z por essa mesma relação.

A.1.4 Funções

Um caso particular de relações são as chamadas "funções", um dos conceitos mais antigos — ao menos intuitivamente — e de maiores aplicações na Engenharia e Tecnologia. É do estudo das funções que surgiu o Cálculo Diferencial e Integral, considerada uma das disciplinas mais importantes da Matemática Contínua Aplicada.

função
aplicação

DEFINIÇÃO A.16. Sendo f uma relação entre um conjunto qualquer A e um conjunto qualquer B, dizemos que f é uma função, ou aplicação, de A em B e escrevemos $f\colon A \to B$ se e somente se para todo elemento a de A existir um e apenas um elemento b de B tal que afb.

domínio de uma função

NOMENCLATURA A.17. Sendo f uma função de um conjunto A num conjunto B, dizemos que A é o domínio de f e que B, o contradomínio de f.

contradomínio de uma função
imagem

NOMENCLATURA A.18. Sendo f uma função de um conjunto A num conjunto B e sendo a um elemento de A, a imagem de a por f, denotado por $f(a)$, é o único elemento b de B tal que afb.

NOTAÇÃO A.19. Sendo f uma função de um conjunto A num conjunto B e sendo S um subconjunto de A, usamos $f(S)$ para denotar o conjunto

$$f(S) = \{f(s)\colon s \in S\}\,.$$

imagem inversa

DEFINIÇÃO A.20. Sendo f uma função de um conjunto A num conjunto não vazio B e sendo b um elemento de B, a imagem inversa de b por f, denotada por $f^{-1}(b)$, é o conjunto

$$f^{-1}(b) = \{a \in A\colon f(a) = b\}\,.$$

NOTAÇÃO A.21. Sendo f uma função de um conjunto A num conjunto B e sendo S um subconjunto de B, usamos $f^{-1}(S)$ para denotar o conjunto

$$f^{-1}(S) = \left\{f^{-1}(s)\colon s \in S\right\}.$$

NOTAÇÃO A.22. Sendo A e B conjuntos, utilizamos A^B para denotar o conjunto de todas as funções de B em A.

função injetiva
função injetora

NOMENCLATURA A.23. Dizemos que uma função f de um conjunto A num conjunto B é injetiva, ou injetora, ou ainda uma injeção, quando e só quando vale que se x e y são elementos distintos de A então $f(x) \neq f(y)$.

injeção
função sobrejetiva
função sojetora

NOMENCLATURA A.24. Dizemos que uma função f de um conjunto A num conjunto B é sobrejetiva, ou sobrejetora, ou ainda uma sobrejeção, quando e só quando $f(A) = B$.

sobrejeção
função bijetiva
função bijetora

NOMENCLATURA A.25. Dizemos que uma função f de um conjunto A num conjunto B é bijetiva, ou bijetora, ou ainda uma bijeção, quando e só quando f for ao mesmo tempo injetiva e sobrejetiva.

bijeção
correspondência biunívoca entre dois conjuntos

NOMENCLATURA A.26. Dizemos que dois conjuntos A e B correspondem-se biunivocamente, e escrevemos $A \simeq B$, se e só se existe uma bijeção de A em B.

A.1.5 Operações

Um caso particular de funções, as operações sobre conjuntos, embora também se tratem de conceitos bastante antigos intuitivamente, constituem um dos pilares das estruturas algébricas da Matemática Moderna, como poderemos observar adiante.

DEFINIÇÃO A.27. Sendo A um conjunto qualquer, uma operação sobre A é qualquer função $*$ cujo domínio seja $A \times A$ e o contradomínio, A. — operação

NOMENCLATURA A.28. Sendo $*$ uma operação sobre um conjunto A, dizemos que A é munido da operação $*$. — conjunto munido de uma operação

NOTAÇÃO A.29. Sendo A um conjunto munido de uma operação $*$ e sendo a e b elementos de A, denotamos $*(a, b)$ por $a * b$.

NOMENCLATURA A.30. Dizemos que uma operação $*$ sobre um conjunto A é associativa se e só se, para quaisquer a, b e c elementos de A, — associatividade

$$a * (b * c) = (a * b) * c.$$

NOMENCLATURA A.31. Dizemos que uma operação $*$ sobre um conjunto A é comutativa se e só se, para quaisquer a e b elementos de A, — comutatividade

$$a * b = b * a.$$

NOMENCLATURA A.32. Dizemos que uma operação $\triangle$ sobre um conjunto A é distributiva em relação a uma outra operação $*$ sobre A se e só se, para quaisquer a, b e c elementos de A, — distributividade

$$a\triangle(b * c) = (a\triangle b) * (a\triangle c) \qquad \text{e}$$
$$(a * b)\triangle c = (a\triangle c) * (b\triangle c).$$

NOMENCLATURA A.33. Sendo A um conjunto munido de uma operação $*$ e S um subconjunto de A, dizemos que S é fechado para a operação $*$ se e só se $r * s$ pertence a S para quaisquer elementos r e s de S. — conjunto fechado para uma operação

DEFINIÇÃO A.34. Sendo A um conjunto munido de uma operação $*$ e S um subconjunto de A fechado para $*$, a restrição da operação $*$ a S é a operação $*_S \colon S \times S \to S$ definida por: — restrição de uma operação

$$r *_S s = r * s.$$

NOMENCLATURA A.35. Dizemos que um elemento e é um elemento neutro para uma operação $*$ sobre um conjunto A se e só se vale que — elemento neutro

$$a * e = e * a = a,$$

para todo elemento a de A.

Uma vez que definimos o conceito de "elemento neutro", estamos em condições de definir o conceito de "elemento simétrico". Vale ressaltar que são justamente esses conceitos, mais o da associatividade, que formaram o conceito de "grupo", exibido logo a seguir.

O leitor deve ainda notar que, embora a nomenclatura A.37 exija que, para um elemento a de A ser simetrizável, a precise possuir simétrico em relação a todo elemento neutro, podemos tranqüilamente definir o mesmo conceito em relação a um elemento neutro específico.

elemento simétrico

NOMENCLATURA A.36. Sendo um conjunto não vazio A munido de uma operação $*$ para a qual um elemento e de A é um elemento neutro e sendo a e $\overline{a}$ elementos de A, dizemos que $\overline{a}$ é o elemento simétrico de a em relação a e se e só se

$$a * \overline{a} = \overline{a} * a = e.$$

elemento simetrizável

NOMENCLATURA A.37. Dizemos que um elemento a de um conjunto não vazio A munido de uma operação $*$ é simetrizável em relação a $*$ se e só se existir um elemento simétrico de a em relação a qualquer elemento neutro para $*$.

elemento regular para uma operação

NOMENCLATURA A.38. Sendo um conjunto não vazio A munido de uma operação $*$, dizemos que um elemento a de A é regular para a operação $*$ se, para quaisquer que sejam x e y elementos de A, valem as seguintes condicionais:

(i) se $a * x = a * y$ então $x = y$;

(ii) se $x * a = y * a$ então $x = y$.

A.2 Grupos e subgrupos

A.2.1 Grupos

grupo

DEFINIÇÃO A.39. Sendo G um conjunto qualquer e $*$ uma operação sobre G, dizemos que $(G, *)$ é um grupo se e somente se:

(i) a operação $*$ é associativa;

(ii) existe algum elemento neutro em G para a operação $*$;

(iii) todo elemento de G é simetrizável.

OBSERVAÇÃO A.40. Se $(G, *)$ é um grupo então G não é vazio, já que precisa haver em G pelo menos um elemento neutro para $*$.

PROPRIEDADE A.15. *A existência de elemento neutro em um grupo $(G, *)$ é única.*

DEMONSTRAÇÃO. Sejam e e f elementos neutros de um grupo $(G, *)$. Queremos, então, demonstrar que $e = f$. Como e é um elemento de G e f é um elemento neutro, temos que

$$e = e * f = f * e.$$

Mas, como f é um elemento de G e e é um elemento neutro, temos também que

$$f * e = f.$$

Portanto, $e = f$, como queríamos demonstrar. ♦

PROPRIEDADE A.16. *A existência de simétrico de um elemento de G em relação ao elemento neutro de um grupo $(G, *)$ é única.*

DEMONSTRAÇÃO. Seja e o elemento neutro de um grupo $(G, *)$ e seja a um elemento qualquer de G. Sejam $\overline{a}_1$ e $\overline{a}_2$ simétricos de a em relação a e. Queremos, então, mostrar que $\overline{a}_1 = \overline{a}_2$. Sabemos que

$$\overline{a}_1 = \overline{a}_1 * e \tag{A.1}$$

e, já que $\overline{a}_2$ é simétrico de a, que

$$e = a * \overline{a}_2. \tag{A.2}$$

Substituindo (A.2) em (A.1), temos que

$$\overline{a}_1 = \overline{a}_1 * (a * \overline{a}_2)$$

e, portanto, dos axiomas da definição de grupo, que

$$\begin{aligned} \overline{a}_1 &= (\overline{a}_1 * a) * \overline{a}_2 \\ &= e * \overline{a}_2 \\ &= \overline{a}_2, \end{aligned}$$

como queríamos demonstrar. ♦

PROPRIEDADE A.17. *O simétrico do elemento neutro e de um grupo é próprio elemento e.*

DEMONSTRAÇÃO. Seja $\overline{e}$ o simétrico do elemento neutro e de um grupo $(G, *)$. Queremos mostrar que $\overline{e} = e$. Sabemos, por e ser elemento neutro, que

$$\overline{e} = \overline{e} * e.$$

Por outro lado, por $\overline{e}$ ser o simétrico de e, temos que

$$\overline{e} * e = e$$

e, portanto, que

$$\overline{e} = e,$$

como queríamos demonstrar. ♦

PROPRIEDADE A.18. *Sendo a um elemento de um grupo $(G, *)$,*

$$\overline{\overline{a}} = a.$$

DEMONSTRAÇÃO. Sabemos que

$$\overline{\overline{a}} = \overline{\overline{a}} * e$$

e, como $e = \overline{a} * a$, que

$$\overline{\overline{a}} = \overline{\overline{a}} * \big(\overline{a} * a\big).$$

Portanto, dos axiomas da definição de grupo, temos que

$$\begin{aligned} \overline{\overline{a}} &= \big(\overline{\overline{a}} * \overline{a}\big) * a \\ &= e * a \\ &= a, \end{aligned}$$

como queríamos demonstrar. ♦

PROPRIEDADE A.19. *Sendo $(G, *)$ um grupo e a e b elementos de G,*

$$\overline{a * b} = \overline{b} * \overline{a}.$$

DEMONSTRAÇÃO. Vamos mostrar que:

$$(a * b) * (\overline{b} * \overline{a}) = e; \tag{A.3}$$
$$(\overline{b} * \overline{a}) * (a * b) = e. \tag{A.4}$$

Dos axiomas da definição de grupo, temos que

$$\begin{aligned}(a * b) * (\overline{b} * \overline{a}) &= \big((a * b) * \overline{b}\big) * \overline{a} \\ &= \big(a * (b * \overline{b})\big) * \overline{a} \\ &= (a * e) * \overline{a} \\ &= a * \overline{a} \\ &= e\end{aligned}$$

e, portanto, mostramos (A.3). Analogamente,

$$\begin{aligned}(\overline{b} * \overline{a}) * (a * b) &= \big((\overline{b} * \overline{a}) * a\big) * b \\ &= \big(\overline{b} * (\overline{a} * a)\big) * b \\ &= (\overline{b} * e) * b \\ &= \overline{b} * b \\ &= e,\end{aligned}$$

e, portanto, mostramos (A.4) e concluímos a demonstração. ⧫

PROPRIEDADE A.20. *Em um grupo $(G, *)$, todo elemento de G é regular para a operação $*$.*

DEMONSTRAÇÃO. Sejam a, x e y elementos de G. Queremos mostrar que:

(A.20.i) se $a * x = a * y$ então $x = y$;

(A.20.ii) se $x * a = y * a$ então $x = y$.

Suponhamos primeiramente que $a * x = a * y$. Assim, temos que

$$\overline{a} * (a * x) = \overline{a} * (a * y)$$

e, portanto, que

$$(\overline{a} * a) * x = (\overline{a} * a) * y$$

e, conseqüentemente, que

$$x = y.$$

Agora valha que $x * a = y * a$. Dessarte,

$$(x * a) * \overline{a} = (y * a) * \overline{a};$$

logo,

$$x * (a * \overline{a}) = y * (a * \overline{a})$$

e, por fim,

$$x = y,$$

o que encerra a demonstração. ⧫

PROPRIEDADE A.21. *Em um grupo $(G, *)$, sendo a e b elementos de G, a equação*

$$a * x = b \tag{A.5}$$

tem conjunto solução unitário, constituído do elemento $(\overline{a} * b)$, assim como a equação

$$x * a = b, \tag{A.6}$$

cuja única solução é $(b * \overline{a})$.

DEMONSTRAÇÃO. Vamos mostrar que:

(A.21.i) a solução da equação A.5 é única;

(A.21.ii) $(\overline{a} * b)$ é solução da equação A.5;

(A.21.iii) a solução da equação A.6 é única;

(A.21.iv) $(b * \overline{a})$ é solução da equação A.6.

Sejam x_1 e x_2 soluções da equação A.5. Assim, $a * x_1 = a * x_2$ e, portanto, da propriedade A.20, $x_1 = x_2$.

Dos axiomas da definição de grupo, é verdade que

$$a * (\overline{a} * b) = (a * \overline{a}) * b = e * b = b.$$

Portanto, $(\overline{a} * b)$ é solução da equação A.5.

Sejam x_1 e x_2 soluções da equação A.6. Dessarte, $x_1 * a = x_2 * a$ e, conseqüentemente, da propriedade A.20, $x_1 = x_2$.

Dos axiomas da definição de grupo, é verdade que

$$(b * \overline{a}) * a = b * (a * \overline{a}) = b * e = b.$$

Logo, $(b * \overline{a})$ é solução da equação A.6. ♦

NOTAÇÃO A.41. Sendo e o elemento neutro de um grupo $(G, *)$, m e n números inteiros e a uma injeção de $[m..n]$ em G, denotando-se $a(j)$ por a_j,

$$\bigsqcup_{j=m}^{n} a_j = \begin{cases} e, & \text{se } m > n; \\ a_m * \left(\bigsqcup_{j=m+1}^{n} a_j \right), & \text{se } m \leqslant n. \end{cases}$$

TEOREMA A.22. *Sendo e o elemento neutro de um grupo $(G, *)$, m e n números inteiros e a uma injeção de $[m..n]$ em G, denotando-se $a(j)$ por a_j,*

$$\overline{\bigsqcup_{j=m}^{n} a_j} = \bigsqcup_{j=m}^{n} \overline{a_{n-j+m}}.$$

DEMONSTRAÇÃO. Se $m > n$, a igualdade se mostra trivialmente na medida em que tanto

$$\overline{\bigsqcup_{j=m}^{n} a_j} = e$$

quanto

$$\bigsqcup_{j=m}^{n} \overline{a_{n-j+m}} = e.$$

Suponhamos, então, que $m \leqslant n$. Se $m - n = 0$, temos que

$$\begin{aligned}
\overline{\bigsqcup_{j=m}^{n} a_j} &= \overline{a_m * \left(\bigsqcup_{j=m+1}^{n} a_j \right)} \\
&= \overline{a_m * e} \\
&= \overline{a_m} \\
&= \overline{a_m} * \overline{e} \\
&= \overline{a_m} * \left(\bigsqcup_{j=m+1}^{n} \overline{a_{n-j+(m+1)}} \right) \\
&= \bigsqcup_{j=m}^{n} \overline{a_{n-j+m}}.
\end{aligned}$$

Seja k um número natural. Por indução em $m - n$, suponhamos que, para dois números inteiros r e s, sempre que $r - s \in [0..k]$ valha que

$$\overline{\bigsqcup_{j=r}^{s} a_j} = \bigsqcup_{j=r}^{s} \overline{a_{s-j+r}}.$$

Queremos afinal mostrar que se $m - n = k + 1$ então

$$\overline{\bigsqcup_{j=m}^{n} a_j} = \bigsqcup_{j=m}^{n} \overline{a_{n-j+m}}.$$

Da notação A.41 e da propriedade A.19,

$$\overline{\bigsqcup_{j=m}^{n} a_j} = \overline{a_m * \left(\bigsqcup_{j=m+1}^{n} a_j \right)} = \overline{\left(\bigsqcup_{j=m+1}^{n} a_j \right)} * \overline{a_m},$$

e, da hipótese da indução, como $n - (m + 1) \in [0..k]$,

$$\overline{\bigsqcup_{j=m}^{n} a_j} = \left(\bigsqcup_{j=m+1}^{n} \overline{a_{n-j+(m+1)}} \right) * \overline{a_m} = \bigsqcup_{j=m}^{n} \overline{a_{n-j+m}},$$

como queríamos demonstrar. ♦

A.2.2 Grupos abelianos

grupo abeliano
grupo comutativo

DEFINIÇÃO A.42. Dizemos que um grupo $(G, *)$ é abeliano (ou comutativo) se e somente se a operação $*$ é comutativa.

A.2.3 Subgrupos

subgrupo

DEFINIÇÃO A.43. De um grupo $(G, *)$ dizemos que um subconjunto não-vazio H de G é um subgrupo e escrevemos

$$H \subseteq (G, *)$$

se e somente se:

(i) H é fechado para a operação $*$;

(ii) $(H, *_H)$ também for é grupo.

TEOREMA A.23. *Sendo e o elemento neutro de um grupo $(G, *)$ e H um subconjunto não-vazio de G, H é um subgrupo de $(G, *)$ se e somente se $a * \overline{b} \in H$ para todo a e todo b elementos de H.*

DEMONSTRAÇÃO. Vamos mostrar que:

(A.23.i) se H é um subgrupo de $(G, *)$ então $a * \overline{b} \in H$ para todo a e todo b elementos de H;

(A.23.ii) se, para todo a e todo b elementos de H, $a * \overline{b} \in H$ então H é um subgrupo de $(G, *)$.

Suponhamos inicialmente que H seja um subgrupo de $(G, *)$ e indiquemos por e_H o elemento neutro de $(H, *_H)$. Como

$$e_H * e_H = e_H *_H e_H = e_H = e_H * e,$$

temos, da propriedade A.20, que

$$e_H = e.$$

Seja x um elemento qualquer de H e indiquemos por $\overline{x}_H$ o simétrico de x em $(H, *_H)$. Como

$$\overline{x}_H * x = \overline{x}_H *_H x = e_H = e = \overline{x} * x,$$

temos, novamente da propriedade A.20, que

$$\overline{x}_H = \overline{x}.$$

Por fim, tomemos a e b elementos de H. Como $(H, *_H)$ é um grupo, $a *_H \overline{b}_H \in H$. Entretanto, como mostramos, $\overline{b}_H = \overline{b}$. Logo, $a *_H \overline{b} = a * \overline{b} \in H$, e, assim, demonstramos (i).

Suponhamos agora que, para quaisquer a e b elementos de H, $a * \overline{b} \in H$ e demonstremos que H é um subgrupo de $(G, *)$. Uma vez que H não é vazio, tomemos um elemento x_0 de H. Assim, temos da hipótese que

$$x_0 * \overline{x_0} = e \in H.$$

Mais do que isso, temos utilizando novamente a hipótese também que, para todo $x \in H$,

$$e * \overline{x} = \overline{x} \in H.$$

Sejam a e b elementos de H. De acordo com o que acabamos de mostrar, $\overline{b}$ também pertence a H. Utilizando mais uma vez a hipótese, notificamo-nos de que

$$a * \overline{\overline{b}} = a * b \in H$$

e, portanto, de que $*$ é fechada para H. Como, valendo-nos de argumentos já utilizados nesta demonstração, $e = e_H \in H$, e $\overline{x} = \overline{x}_H \in H$ para todo $x \in H$, e como a associatividade da operação $*_H$ segue da associatividade de $*$ concluímos a demonstração de (ii). ♦

A.2.4 Classes laterais

NOTAÇÃO A.44. Sendo H um subgrupo de um grupo $(G, *)$ e a e b elementos quaisquer de G, escrevemos

$$a \sim b \pmod{H}$$

para denotar que $\overline{a} * b \in H$ e

$$a \backsim b \pmod{H}$$

para denotar que $a * \overline{b} \in H$.

TEOREMA A.24. *Sendo H um subgrupo de um grupo $(G, *)$, as relações definidas na notação A.44 são relações de equivalência.*

DEMONSTRAÇÃO. É imediato que, para qualquer elemento x de G,

$$x \sim x \pmod{H} \quad \text{e}$$
$$x \backsim x \pmod{H},$$

já que, do teorema A.23, $x * \overline{x} = e \in H$ e, por conseqüência, $e * \overline{(x * \overline{x})} = \overline{x} * x \in H$. Sejam x_1, x_2, y_1 e y_2 elementos de G e suponhamos que

$$x_1 \sim x_2 \pmod{H}, \quad \text{e}$$
$$y_1 \backsim y_2 \pmod{H}.$$

Como $\overline{x_1} * x_2 \in H$ e $y_1 * \overline{y_2} \in H$ e como H é um subgrupo, ambos $\overline{\overline{x_1} * x_2} = \overline{x_2} * x_1$ e $\overline{y_1 * \overline{y_2}} = y_2 * \overline{y_1}$ pertencem a H, e, portanto,

$$x_2 \sim x_1 \pmod{H}, \quad \text{e}$$
$$y_2 \backsim y_1 \pmod{H}.$$

Resta-nos ainda mostrar a transitividade dessas relações. Para tanto, tomemos a_1, a_2, a_3, b_1, b_2 e b_3 elementos de G e suponhamos que:

$$a_1 \sim a_2 \pmod{H};$$
$$a_2 \sim a_3 \pmod{H};$$
$$b_1 \backsim b_2 \pmod{H};$$
$$b_2 \backsim b_3 \pmod{H}.$$

Portanto, $\overline{a_1} * a_2$, $\overline{a_2} * a_3$, $b_1 * \overline{b_2}$ e $b_2 * \overline{b_3}$ são elementos de H e, como H é um subgrupo, também são elementos de H

$$(\overline{a_1} * a_2) * (\overline{a_2} * a_3) = a_1 * a_3, \quad \text{e}$$
$$(b_1 * \overline{b_2}) * (b_2 * \overline{b_3}) = b_1 * b_3.$$

Finalmente,

$$a_1 \sim a_3 \pmod{H}, \quad \text{e}$$
$$b_1 \backsim b_3 \pmod{H},$$

como queríamos mostrar. ♦

DEFINIÇÃO A.45. Sendo H um subgrupo de um grupo $(G, *)$ e a um elemento de G, a classe lateral à direita de a módulo H, denotada por $a * H$, é a classe de equivalência de a pela relação $\sim$ módulo H. Analogamente, a classe lateral à esquerda de a módulo H, denotada por $H * a$, é a classe de equivalência de a pela relação $\backsim$ módulo H.

classe lateral à direita

classe lateral à esquerda

PROPRIEDADE A.25. *Sendo H um subgrupo de um grupo $(G, *)$ e a um elemento de G,*

$$a * H = \{a * h \colon h \in H\}, \qquad \text{e}$$
$$H * a = \{h * a \colon h \in H\}.$$

DEMONSTRAÇÃO. Tomemos $x \in (a * H)$ e $y \in (H * a)$. Assim, da definição A.10, $\overline{x} * a = h_1$ e $y * \overline{a} = h_2$ pertencem a H. Portanto, $x = a * \overline{h_1}$, $y = h_2 * a$, e, conseqüentemente, $x \in \{a * h \colon h \in H\}$ e $y \in \{h * a \colon h \in H\}$, o que nos leva a concluir que

$$a * H \subseteq \{a * h \colon h \in H\} \qquad \text{e que}$$
$$H * a \subseteq \{h * a \colon h \in H\}.$$

Por outro lado, tomemos um elemento h de H. Sabemos que $(\overline{a * h}) * a = \overline{h}$ e, portanto, como H é um subgrupo, que

$$(a * h) \sim a \pmod{H}.$$

Da mesma forma, é verdade que $(h * a) * \overline{a} = h$ e, dessarte, que

$$(h * a) \backsim a \pmod{H}.$$

Logo, $(a * h) \in (a * H)$ e $(h * a) \in (H * a)$, e, finalmente,

$$\{a * h \colon h \in H\} \subseteq a * H, \qquad \text{e}$$
$$\{h * a \colon h \in H\} \subseteq H * a.$$

♦

COROLÁRIO A.26. *Sendo H um subgrupo de um grupo $(G, *)$ e a um elemento de G, $a * H \simeq H * a$.*

DEMONSTRAÇÃO. Seja $f \colon a * H \to H * a$ a função definida por

$$f(x) = h_x * a,$$

sendo h_x o elemento de H tal que $x = a * h_x$. Sejam x_1 e x_2 elementos distintos de $a * H$. Da propriedade A.20, $h_{x_1} \neq h_{x_2}$, sendo h_{x_1} o elemento de H tal que $x_1 = a * h_{x_1}$ e h_{x_2} o elemento de H tal que $x_2 = a * h_{x_2}$. Logo, também por causa da propriedade A.20, temos que $h_{x_1} * a \neq h_{x_2} * a$ e, conseqüentemente, que $f(x_1) \neq f(x_2)$, o que nos leva a concluir que f é injetiva.

Para mostrarmos que f é sobrejetiva, é suficiente que mostremos que $H * a \subseteq f(a * H)$. Para tanto, tomemos um elemento y de $H * a$, sendo h_y o elemento de H tal que $y = h_y * a$, e observemos que $f(a * h_y) = h_y * a$. Assim, $y \in f(a * H)$ e, dessarte, f também é sobrejetiva. ♦

COROLÁRIO A.27. *Sendo H um subgrupo de um grupo $(G, *)$ e a e b elemento quaisquer de G, $a * H \simeq b * H$.*

DEMONSTRAÇÃO. Seja $f \colon a * H \to b * H$ a função definida por

$$f(x) = b * h_x,$$

sendo h_x o elemento de H tal que $x = a * h_x$. Sejam x_1 e x_2 elementos distintos de $a * H$. Da propriedade A.20, $h_{x_1} \neq h_{x_2}$, sendo h_{x_1} o elemento de H tal que $x_1 = a * h_{x_1}$ e h_{x_2} o elemento de H tal que $x_2 = a * h_{x_2}$. Logo, também por

causa da propriedade A.20, temos que $b * h_{x_1} \neq b * h_{x_2}$ e, conseqüentemente, que $f(x_1) \neq f(x_2)$, o que nos leva a concluir que f é injetiva.

Para mostrarmos que f é sobrejetiva, é suficiente que mostremos que $b * H \subseteq f(a * H)$. Para tanto, tomemos um elemento y de $b * H$, sendo h_y o elemento de H tal que $y = b * h_y$, e observemos que $f(a * h_y) = b * h_y$. Assim, $y \in f(a * H)$ e, dessarte, f também é sobrejetiva. ⧫

A.2.5 Grupos finitos

grupo finito

ordem de um grupo finito

ordem de um subgrupo de um grupo finito

índice de um subgrupo num grupo

NOMENCLATURA A.46. Dizemos que um grupo $(G, *)$ é finito quando e só quando G é finito. Ademais, dizemos que $|G|$ é a ordem de $(G, *)$. Analogamente, se H é um subgrupo de $(G, *)$ então $|H|$ é a ordem de H.

DEFINIÇÃO A.47. Sendo H um subgrupo de um grupo finito $(G, *)$, chamamos de índice de H em G, e denotamos por $[G : H]$, a cardinalidade do conjunto quociente de G por qualquer uma das relações $\sim$ e $\backsim$ módulo H.

OBSERVAÇÃO A.48. Note-se que a arbitrariedade na escolha da relação módulo H tomada deve-se sobretudo ao corolário A.26.

teorema de Lagrange

TEOREMA A.28 (Teorema de Lagrange)**.** *Sendo $(G, *)$ um grupo finito, a ordem de qualquer subgrupo de $(G, *)$ divide a ordem de $(G, *)$.*

DEMONSTRAÇÃO. Seja H um subgrupo de $(G, *)$. Como G é finito, o conjunto Q quociente de G pela relação $\sim$ módulo H também é finito e, portanto, Q pode ser escrito como:

$$Q = \bigcup_{j=1}^{[G:H]} \{a_j * H\}.$$

Entretanto, do teorema A.1, Q é uma partição de G e, conseqüentemente,

$$G = \bigcup_{j=1}^{[G:H]} a_j * H.$$

Também por Q ser uma partição de G concluímos que se $k \neq \ell$, sendo ℓ e k elementos de $[[G : H]]$, então $a_k * H$ e $a_\ell * H$ são conjuntos disjuntos. Assim,

$$|G| = \sum_{j=1}^{[G:H]} |a_j * H|$$

e, do corolário A.27, como, para todo $j \in [[G : H]]$, $a_j * H \simeq e * H = H$,

$$|G| = \sum_{j=1}^{[G:H]} |H|.$$

Finalmente,

$$|G| = [G : H]\,|H|,$$

e, da definição A.12, como $[G : H]$ é um número inteiro, $|H| \setminus |G|$, como queríamos mostrar. ⧫

A.2.6 Grupos cíclicos

O conceito que apresentamos a seguir trata de um caso particular de grupo. Pelo princípio da indução, podemos somar 1 sucessivamente partindo de 0 e chegar em qualquer número natural. Entretanto, não é possível construir um processo semelhante para o grupo dos racionais, por exemplo. O motivo pelo qual isso ocorre é que os racionais não constituem o que é chamado de "grupo cíclico".

DEFINIÇÃO A.49. Seja $(G, *)$ um grupo de elemento neutro e, a um elemento qualquer de G e n um número natural. A n-ésima iteração de $*$ sobre a é o elemento de G definido por:

iteração de uma operação

$$a^{*n} = \begin{cases} \left(a^{*(n-1)}\right) * a, & \text{se } n > 0; \\ e, & \text{caso contrário.} \end{cases}$$

PROPRIEDADE A.29. *Sendo $(G, *)$ um grupo de elemento neutro e, a um elemento qualquer de G e n um número natural,*

$$a^{*n} = \begin{cases} a * \left(a^{*(n-1)}\right), & \textit{se } n > 0\textit{;} \\ e, & \textit{caso contrário.} \end{cases}$$

DEMONSTRAÇÃO. É imediato que $a^{*0} = e$. Por indução em n, suponhamos que, sendo k um natural, para todo $\ell \in [0..k]$ vale que

$$a^{*\ell} = \begin{cases} a * \left(a^{*(\ell-1)}\right), & \text{se } \ell > 0; \\ e, & \text{caso contrário.} \end{cases}$$

Como $k + 1 > 0$, queremos, então, mostrar que $a^{*(k+1)} = a * \left(a^{*((k+1)-1)}\right)$. Ora, da definição A.49,

$$a^{*(k+1)} = \left(a^{*((k+1)-1)}\right) * a.$$

Assim, uma vez que $(k + 1) - 1 = k \in [0..k]$, se $k = 0$ então $a^{*k} = e$ e, portanto,

$$\begin{aligned} a^{*(k+1)} &= e * a \\ &= a \\ &= a * e \\ &= a * \left(a^{*((k+1)-1)}\right), \end{aligned}$$

como queríamos mostrar. Se, entretanto, $k > 0$ então, da hipótese da indução e do axioma da associatividade,

$$\begin{aligned} a^{*(k+1)} &= \left(a * \left(a^{*(k-1)}\right)\right) * a \\ &= a * \left(\left(a^{*(k-1)}\right) * a\right), \end{aligned}$$

e, portanto, novamente da definição A.49,

$$a^{*(k+1)} = a * \left(a^{*((k-1)+1)}\right),$$

como queríamos mostrar. ♦

PROPRIEDADE A.30. *Sendo $(G, *)$ um grupo, a um elemento de G e n e m números naturais,*

$$a^{*m} * a^{*n} = a^{*(m+n)}.$$

DEMONSTRAÇÃO. É imediato que $a^{*m} * a^{*0} = a^{*(m+0)}$, já que $a^{*0} = e$, sendo e o elemento neutro do grupo. Seja k um número natural qualquer. Por indução em n, supondo que vale que $a^{*m} * a^{*\ell} = a^{*(m+\ell)}$ para todo $\ell \in [0..k]$, o que queremos é mostrar que $a^{*m} * a^{*(k+1)} = a^{*(m+(k+1))}$. Da definição A.49, como $k+1 > 0$,

$$a^{*m} * a^{*(k+1)} = a^{*m} * (a^{*k} * a) = (a^{*m} * a^{*k}) * a;$$

portanto, da hipótese da indução, como $k \in [0..k]$,

$$a^{*m} * a^{*(k+1)} = a^{*(m+k)} * a,$$

e, conseqüentemente, novamente da definição A.49,

$$a^{*m} * a^{*(k+1)} = a^{*((m+k)+1)} = a^{*(m+(k+1))},$$

como queríamos mostrar. ♦

PROPRIEDADE A.31. *Sendo $(G, *)$ um grupo, a um elemento de G e n e m números naturais,*

$$(a^{*m})^{*n} = a^{*(mn)}.$$

DEMONSTRAÇÃO. É imediato que $(a^{*m})^{*0} = a^{*(m\cdot 0)}$, já que $(a^{*m})^{*0} = \underline{1} = a^{*0}$. Seja k um número natural qualquer. Por indução em n, supondo que vale que $(a^{*m})^{*\ell} = a^{*(m\ell)}$ para todo $\ell \in [0..k]$, o que queremos é mostrar que $(a^{*m})^{*(k+1)} = a^{*(m(k+1))}$. Da definição de potência, como $k+1 > 0$,

$$(a^{*m})^{*(k+1)} = \left((a^{*m})^{*k}\right) * (a^{*m});$$

portanto, da hipótese da indução, como $k \in [0..k]$,

$$(a^{*m})^{*(k+1)} = a^{*(mk)} * a^{*m},$$

e, conseqüentemente, da proposição A.30,

$$(a^{*m})^{*(k+1)} = a^{*(mk+m)} = a^{*(m(k+1))},$$

como queríamos mostrar. ♦

PROPRIEDADE A.32. *Sendo $(G, *)$ um grupo, a e b elementos de G e n um número natural,*

$$(a * b)^{*n} = a^{*n} * b^{*n}.$$

DEMONSTRAÇÃO. Sabemos que, sendo e o elemento neutro de G, $(a*b)^{*0} = e = e*e = a^{*0} * b^{*0}$. Seja k um natural e suponhamos, por indução em n, que $(a*b)^{*\ell} = a^{*\ell} * b^{*\ell}$ para todo $\ell \in [0..k]$. Queremos então apenas mostrar que $(a*b)^{*(k+1)} = a^{*(k+1)} * b^{*(k+1)}$. Ora,

$$(a*b)^{*(k+1)} = (a*b)^{*k} * (a*b),$$

e, portanto, da hipótese de indução,

$$\begin{aligned}(a*b)^{*(k+1)} &= (a^{*k} * b^{*k}) * (a*b)\\ &= (a^{*k} * a) * (b^{*k} * b)\\ &= a^{*(k+1)} * b^{*(k+1)},\end{aligned}$$

como queríamos mostrar. ♦

PROPRIEDADE A.33. *Sendo $(G,*)$ um grupo, a um elemento de G e n um número natural,*

$$\overline{a^{*n}} = (\overline{a})^{*n}.$$

DEMONSTRAÇÃO. Sabemos que $\overline{a^{*0}} = \overline{e} = e = (\overline{a})^{*0}$, sendo e o elemento neutro de $(G,*)$. Suponhamos, então, por indução em n, que, sendo k um número natural, para todo ℓ
$in[0..k]$ vale que

$$\overline{a^{*\ell}} = (\overline{a})^{*\ell}.$$

Queremos, assim, por causa da nomenclatura A.36, apenas mostrar que:

(A.33.i) $\left(a^{*(k+1)}\right) * \left((\overline{a})^{*(k+1)}\right) = e$;

(A.33.ii) $\left((\overline{a})^{*(k+1)}\right) * \left(a^{*(k+1)}\right) = e$.

Sabemos, da definição A.49 e da propriedade A.29, e do axioma da associatividade, que

$$\begin{aligned}
\left(a^{*(k+1)}\right) * \left((\overline{a})^{*(k+1)}\right) &= \left(a * a^{*k}\right) * \left((\overline{a})^{*k} * \overline{a}\right) \\
&= a * \left(a^{*k} * (\overline{a})^{*k}\right) * \overline{a} \qquad \text{e que} \\
\left((\overline{a})^{*(k+1)}\right) * \left(a^{*(k+1)}\right) &= \left(\overline{a} * (\overline{a})^{*k}\right) * \left(a^{*k} * a\right) \\
&= \overline{a} * \left((\overline{a})^{*k} * a^{*k}\right) * a,
\end{aligned}$$

e, portanto, da hipótese da indução, que

$$\begin{aligned}
\left(a^{*(k+1)}\right) * \left((\overline{a})^{*(k+1)}\right) &= a * \left(a^{*k} * \overline{a^{*k}}\right) * \overline{a} \\
&= a * e * \overline{a} \\
&= e \qquad \text{e que} \\
\left((\overline{a})^{*(k+1)}\right) * \left(a^{*(k+1)}\right) &= \overline{a} * \left(\overline{a^{*k}} * a^{*k}\right) * a, \\
&= \overline{a} * e * a \\
&= e,
\end{aligned}$$

exatamente como queríamos mostrar. ♦

DEFINIÇÃO A.50. Dizemos que um grupo $(G,*)$ é <u>cíclico</u> se e somente se existe um a em G tal que, para todo $b \in G$, exista um $j \in \mathbb{N} \setminus \{0\}$ tal que $a^{*n} = b$. grupo cíclico

TEOREMA A.34. *Todo grupo cíclico é comutativo.*

DEMONSTRAÇÃO. Seja $(G,*)$ um grupo cíclico e seja a um elemento de G tal que, para todo $b \in G$, exista um $j \in \mathbb{N}$ tal que $a^{*n} = b$. Sejam x e y elementos de G e j_x e j_y números naturais tais que $a^{*j_x} = x$ e $a^{*j_y} = y$. Assim,

$$\begin{aligned}
x * y &= a^{*j_x} * a^{*j_y} \\
&= a^{*(j_x + j_y)} \\
&= a^{*(j_y + j_x)} \\
&= a^{*j_y} * a^{*j_x} \\
&= y * x,
\end{aligned}$$

como queríamos mostrar. ♦

LEMA A.35. *Sendo $(G,*)$ um grupo, a um elemento de G e n e m números naturais,*

$$a^{*n} * \overline{a^{*m}} = \begin{cases} e, & \text{se } n = m; \quad a^{*(n-m)}, \quad \text{se } n > m; a^{*(m-n)}, \quad \text{se } n < m. \end{cases}$$

DEMONSTRAÇÃO. Se $n = m$, a asserção se verifica imediatamente. Se $n > m$, porém, então, da propriedade A.30,

$$\begin{aligned} a^{*n} * \overline{a^{*m}} &= \left(a^{*(n-m)} * a^{*m}\right) * \overline{a^{*m}} \\ &= a^{*(n-m)} * \left(a^{*m} * \overline{a^{*m}}\right) \\ &= a^{*(n-m)} * e \\ &= a^{*(n-m)}. \end{aligned}$$

Se $n < m$, por sua vez, então, da propriedade A.33,

$$a^{*n} * \overline{a^{*m}} = a^{*n} * (\overline{a})^{*m},$$

e, da propriedade A.30,

$$\begin{aligned} a^{*n} * \overline{a^{*m}} &= a^{*n} * \left((\overline{a})^{*n} * (\overline{a})^{*(m-n)}\right) \\ &= \left(a^{*n} * (\overline{a})^{*n}\right) * (\overline{a})^{*(m-n)}, \end{aligned}$$

e, novamente da propriedade A.33,

$$\begin{aligned} a^{*n} * \overline{a^{*m}} &= \left(a^{*n} * \overline{a^{*n}}\right) * \overline{a^{*(m-n)}} \\ &= e * \overline{a^{*(m-n)}} \\ &= \overline{a^{*(m-n)}}, \end{aligned}$$

como queríamos mostrar. ♦

LEMA A.36. *Sendo $(G,*)$ um grupo finito e a um elemento de G, existe um $t \in \mathbb{N} \setminus \{0\}$ tal que $a^{*t} = e$, sendo e o elemento neutro de $(G,*)$.*

DEMONSTRAÇÃO. Suponhamos que $a \neq e$, já que se $a = e$ então a afirmação se verifica trivialmente, e definamos, para todo $n \in \mathbb{N}$, os conjuntos:

$$A_n = \begin{cases} \emptyset, & \text{se } n = 0 \\ \{a^{*n}\} \cup A_{n-1}, & \text{caso contrário.} \end{cases}$$

É imediato que, para todo $n \in \mathbb{N}$, $A_n \subseteq G$, e, como G é finito, $|A_n| \leqslant |G|$. Suponhamos, então, que não exista inteiro positivo t tal que $a^{*t} = e$. Assim, não existe inteiro positivo s tal que $e \in A_s$. Portanto, para todo $n \in \mathbb{N}$, $a^{*n} \notin A_{n-1}$, pois se $a^{*n} \in A_{n-1}$ então haveria um inteiro positivo $j < n$ tal que $a^{*n} = a^{*j}$, e, dessarte, $a^{*(n-j)} = e$, e, como $n - j \leqslant n - 1$, e pertenceria a A_{n-1}. Logo, $|A_0| = 0$ e $|A_n| = |A_{n-1}| + 1$ para todo $n > 0$, e, por conseqüência, $|A_n| = n$ para todo $n \in \mathbb{N}$. Em particular, $\left|A_{|G|+1}\right| = |G| + 1$, o que é um absurdo. ♦

TEOREMA A.37. *Sendo $(G,*)$ um grupo finito e a um elemento de G, o conjunto*

$$\langle a \rangle = \left\{a^{*k} \colon k \in \mathbb{N} \setminus \{0\}\right\}$$

subgrupo gerado *é um subgrupo de $(G,*)$, chamado de subgrupo gerado por a.*

DEMONSTRAÇÃO. É claro que $\langle a\rangle \neq \emptyset$, pois ao menos $a^{*1} = a \in \langle a\rangle$. Sejam, portanto, j e k inteiros positivos. Sabemos, do lema A.35, que

$$a^{*j} * \overline{a^{astk}} = \begin{cases} e, & \text{se } j = k; \\ a^{*(j-k)}, & \text{se } j > k; \\ a^{*(k-j)}, & \text{se } k < j. \end{cases}$$

Logo, para mostrarmos que existe um $\ell \in \mathbb{N} \setminus \{0\}$ tal que $a^{*\ell} = a^{*j} * \overline{a^{astk}}$, e, dessarte, concluirmos que $a^{*j} * \overline{a^{astk}} \in \langle a\rangle$, basta que mostremos que existe um $t \in \mathbb{N} \setminus \{0\}$ tal que $a^{*t} = e$, o que é garantido pelo lema A.36. Assim, $a^{*j} * \overline{a^{astk}} \in \langle a\rangle$ e, conseqüentemente, do teorema A.23, $\langle a\rangle$ é um subgrupo de $(G, *)$, como queríamos mostrar. ♦

COROLÁRIO A.38. *Sendo $(G, *)$ um grupo finito e a um elemento de G, $(\langle a\rangle, *_{\langle a\rangle})$ é um grupo cíclico.*

DEMONSTRAÇÃO. Do teorema A.37, $(\langle a\rangle, *_{\langle a\rangle})$ é um grupo e, pela própria definição de $\langle a\rangle$, é cíclico. ♦

LEMA A.39. *Sendo $(G, *)$ um grupo finito e a um elemento de G, $|\langle a\rangle|$ é o menor inteiro positivo t tal que $a^{*t} = e$, sendo e o elemento neutro de $(G, *)$.*

DEMONSTRAÇÃO. Do lema A.36, temos a garantia da existência de um inteiro positivo t tal que $a^{*t} = e$. Vamos, então, mostrar primeiramente que $a^{*|\langle a\rangle|} = e$ e depois que se um inteiro positivo k é estritamente menor que $|\langle a\rangle|$ então $a^{*k} \neq e$.

Contrapositivamente, se $a^{*|\langle a\rangle|} \neq e$ então, como $e \in \langle a\rangle$, existe um inteiro positivo $j < |\langle a\rangle|$ tal que $a^{*j} = e$ e, portanto, para todo inteiro $\ell > j$, $a^{*\ell} = a^{*(\ell-j)}$, o que nos leva a concluir que $|\langle a\rangle| = j$, o que é um absurdo. Notemos ainda que esse mesmo argumento nos permite verificar que não pode existir um inteiro estritamente menor que $|\langle a\rangle|$ tal que $a^{*k} \neq e$, como queríamos mostrar. ♦

TEOREMA A.40. *Em qualquer grupo finito $(G, *)$ com elemento neutro e vale que*

$$a^{*|G|} = e$$

para todo $a \in G$.

DEMONSTRAÇÃO. Do teorema A.28 (teorema de Lagrange), $|\langle a\rangle| \setminus |G|$, já que, do teorema A.37, $\langle a\rangle$ é um subgrupo de $(G, *)$. Assim, sendo q um inteiro tal que $|G| = |\langle a\rangle|\, q$, temos, da propriedade A.31, que $a^{*|G|} = \left(a^{*|\langle a\rangle|}\right)^q$. Portanto, do lema A.39, $a^{*|G|} = e^q = e$, como queríamos mostrar. ♦

A.2.7 Subgrupos normais e grupos quocientes

NOMENCLATURA A.51. Dizemos que um subgrupo N de um grupo $(G, *)$ é um subgrupo normal de (G, ast) quando, e somente quando, para todo elemento x de G, subgrupo normal

$$x * N = N * x.$$

NOTAÇÃO A.52. Sendo N um subgrupo normal de $(G, *)$, utilizamos ${}^{G}\!/_{N}$ para denotar o conjunto quociente de G por qualquer uma das relações $\sim$ e $\backsim$ módulo N.

NOTAÇÃO A.53. Sendo N_1 e N_2 subgrupos quaisquer de um grupo $(G, *)$, utilizamos $N_1 * N_2$ para denotar o conjunto

$$N_1 = \{n * N_2 \colon n \in N_1\}.$$

OBSERVAÇÃO A.54. Notemos que, por causa da nomenclatura A.51, uma definição equivalente para a notação A.53 seria:

$$N_1 = \{N_1 * n \colon n \in N_2\}.$$

LEMA A.41. *A operação $*$, como convencionamos na notação A.53, é uma operação fechada sobre o conjunto quociente ${}^{G}\!/_{N}$.*

DEMONSTRAÇÃO. Mostraremos simplesmente que, sendo a e b elementos de G, $(a*N)*(b*N) = (a*b)*N$. Seja $x \in (a*N)*(b*N)$. Assim, da notação A.53, existe um elemento $a_1 \in (a*N)$ e um elemento $b_1 \in (b*N)$ tais que $x = a_1 * b_1$. Sabemos que $a_1 = a * n_a$ e $b_1 = b * n_b$ para algum n_a e algum n_b em N. Portanto,

$$x = (a * n_a)(b * n_b) = a * (n_a * b) * n_b.$$

Mas, como $(n_a * b) \in (N * b)$, e como $(N * b) = (b * N)$, há algum $n \in N$ tal que $n_a * b = b * n$. Dessarte,

$$x = a * (n_a * b) * n_b = a * (b * n) * n_b = (a * b) * (n * n_b),$$

e, já que $(n * n_b) \in N$, $x \in (a * b) * N$, o que nos traz que

$$(a * N) * (b * N) \subseteq (a * b) * N.$$

Mostraremos agora que $(a*b)*N \subseteq (a*N)*(b*N)$. Tomemos, para tanto, $x \in (a*b)*N$, o que garante a existência de um elemento n de N tal que $x = (a*b)*n$. Mas, sendo e o elemento neutro de $(G, *)$, temos que $x = (a * e) * (b * n)$, e, como $e \in N$, já que N é um subgrupo, podemos finalmente concluir que $x \in (a*N)*(b*N)$. ♦

TEOREMA A.42. *Sendo N um subgrupo normal de um grupo $(G, *)$, a operação $*$ e o conjunto quociente ${}^{G}\!/_{N}$ definem um grupo, chamado de grupo quociente de G por N.*

grupo quociente

DEMONSTRAÇÃO. Por causa do lema A.41, $*$ pode ser considerada uma operação sobre ${}^{G}\!/_{N}$. É fácil verificar que $*$ é associativa, já que, sendo a, b e c elementos de G,

$$\big((a * N) * (b * N)\big) * (c * N) \subseteq (a * N) * \big((b * N) * (c * N)\big) \quad \text{e}$$
$$(a * N) * \big((b * N) * (c * N)\big) \subseteq \big((a * N) * (b * N)\big) * (c * N),$$

uma vez que se $x \in \big((a * N) * (b * N)\big) * (c * N)$ então há n_a, n_b e n_c em N tais que

$$\begin{aligned} x &= \big((a * n_a) * (b * n_b)\big) * (c * n_c) \\ &= (a * n_a) * \big((b * n_b) * (c * n_c)\big), \end{aligned}$$

da mesma forma que se $x \in (a * N) * \big((b * N) * (c * N)\big)$ então há n_a, n_b e n_c em N tais que

$$\begin{aligned} x &= (a * n_a) * \big((b * n_b) * (c * n_c)\big) \\ &= \big((a * n_a) * (b * n_b)\big) * (c * n_c). \end{aligned}$$

Também a existência de um elemento neutro para $({}^{G}\!/_{N}, *)$ pode ser averiguada se notarmos que, do lema A.41, para todo $a \in G$,

$$(a * N) * (e * N) = (a * e) * N = a * N.$$

Por último, também por causa do lema A.41, é verdade que

$$(a * N) * (\overline{a} * N) = (a * \overline{a}) * N = e * N,$$

e, portanto, todo elemento de ${}^{G}\!/_{N}$ possui um simétrico em $({}^{G}\!/_{N}, *)$ em relação ao elemento neutro $(e * N)$. ♦

A.3 Anéis e estruturas afins

A.3.1 Anéis

DEFINIÇÃO A.55. Sendo um conjunto R munido de duas operações, $+$ e $\cdot$, dizemos que $(R, +, \cdot)$ é um anel se e só se: anel

(i) $(R, +)$ é um grupo abeliano;

(ii) $\cdot$ é uma operação associativa;

(iii) $\cdot$ é distributiva em relação a $+$.

NOTAÇÃO A.56. Em um anel cujas operações são, na ordem da definição, denotadas por $+$ e $\cdot$, sendo r qualquer elemento do anel, denotamos por

(i) $\underline{0}$ o elemento neutro de $+$ e

(ii) $-r$ o elemento simétrico de r em relação a $+$;

OBSERVAÇÃO A.57. Num anel $(R, +, \cdot)$, sempre assumimos a precedência de $\cdot$ sobre $+$. É também costume escrever simplesmente ab ao invés de $a \cdot b$, assim como $a - b$ ao invés de $a + (-b)$.

Além das propriedades de que um anel $(R, +, \cdot)$ goza por $(R, +)$ ser um grupo abeliano, outras demonstramos a seguir.

PROPRIEDADE A.43. *Sendo $(R, +, \cdot)$ um anel,*

$$r \cdot \underline{0} = \underline{0} \cdot r = \underline{0}.$$

DEMONSTRAÇÃO. Sabemos que

$$\begin{aligned} \underline{0} + \underline{0} \cdot r &= \underline{0} \cdot r \\ &= (\underline{0} + \underline{0})r \\ &= \underline{0} \cdot r + \underline{0} \cdot r, \end{aligned}$$

o que nos leva a concluir, por causa da propriedade A.20, que $\underline{0} = \underline{0} \cdot r$. Analogamente, a mesma propriedade, porque

$$\begin{aligned} \underline{0} + r \cdot \underline{0} &= r \cdot \underline{0} \\ &= r(\underline{0} + \underline{0}) \\ &= r \cdot \underline{0} + r \cdot \underline{0}, \end{aligned}$$

também nos leva a concluir que $\underline{0} = r \cdot \underline{0}$, e, assim, encerramos nossa demonstração. ♦

PROPRIEDADE A.44. *Sendo $(R, +, \cdot)$ e sendo a e b elementos de R,*

$$a(-b) = (-a)b = -(ab).$$

DEMONSTRAÇÃO. Sabemos, dos axiomas da definição de anel e da propriedade A.43, que

$$\begin{aligned} ab + \big(-(ab)\big) &= \underline{0} \\ &= a \cdot \underline{0} \\ &= a\big(b + (-b)\big) \\ &= ab + a(-b), \end{aligned}$$

o que nos leva a concluir, por causa da propriedade A.20, que $-(ab) = a(-b)$. Analogamente, a propriedade A.20, porque

$$\begin{aligned} ab + \big(-(ab)\big) &= \underline{0} \\ &= \underline{0} \cdot b \\ &= \big(a + (-a)\big)b \\ &= ab + (-a)b, \end{aligned}$$

também nos leva a concluir que $-(ab) = (-a)b$, e, assim, encerramos nossa demonstração. ♦

anel finito

NOMENCLATURA A.58. Dizemos que um anel $(R, +, \cdot)$ é finito quando e só quando R é finito.

múltiplo de um elemento de um anel

NOTAÇÃO A.59. Seja $(R, +, \cdot)$ um anel qualquer, seja r um elemento de R e seja n um número natural. O n-ésimo múltiplo de r no anel é o elemento definido por:

$$nr = \begin{cases} (n-1)r + r, & \text{se } n > 0; \\ \underline{0}, & \text{caso contrário.} \end{cases}$$

característica de um anel

DEFINIÇÃO A.60. Sendo $(R, +, \cdot)$ um anel qualquer, dizemos que um inteiro positivo n é a característica de $(R, +, \cdot)$ se e somente se

$$n = \min\{\ell \in \mathbb{N} \setminus \{0\} \colon \ell r = \underline{0} \text{ para todo } r \in R\}.$$

Se, entretanto, $\{\ell \in \mathbb{N} \setminus \{0\} \colon \ell r = \underline{0} \text{ para todo } r \in R\} = \emptyset$, dizemos que a característica do anel $(R, +, \cdot)$ é igual a 0.

A.3.2 Subanéis

subanel

DEFINIÇÃO A.61. De um anel $(R, +, \cdot)$ dizemos que um subconjunto não-vazio L de R é um subanel e escrevemos

$$L \subseteq (R, +, \cdot)$$

se e somente se:

(i) L é fechado para ambas as operações $+$ e $\cdot$;

(ii) $(L, +_H, \cdot_H)$ também é um anel.

TEOREMA A.45. *Sendo $(R, +, \cdot)$ um anel e L um subconjunto não vazio de R, L é um subanel de $(R, +, \cdot)$ se e só se $a - b$ e ab pertencerem a L para todo a e todo b elementos de L.*

DEMONSTRAÇÃO. Mostremos inicialmente que se L é um subanel de $(R, +, \cdot)$ então $a - b$ e ab pertencem a L, sendo a e b elementos de L. Para tanto, observemos que L é também um subgrupo de $(R, +)$, e, portanto, $a - b = a + (-b)$ é assim um elemento de L, do teorema A.23. Por sua vez, como L é fechado para a operação $\cdot$, $ab \in L$ de igual maneira.

Agora mostremos que se $a-b$ e ab pertencem a L para todo a e todo b elementos de L então L é um subanel de $(R, +, \cdot)$. Novamente do teorema A.23, sabemos que L é um subgrupo de $(R, +)$, já que $a-b \in L$, o que nos garante inclusive que $+_L$ se trata de uma operação fechada sobre R. Notemos que $\cdot_L$ também é fechada sobre

R, já que, da hipótese, $ab \in L$ para todo a e todo b elementos de L. Falta-nos, assim, mostrar que $(L, +_L, \cdot_L)$ satisfaz os axiomas de anel. No entanto, a comutatividade de $+_L$ é imediata, e, portanto, $(L, +_L)$ é um grupo abeliano, já que, como mencionamos, L é um subgrupo de $(R, +)$. Como a associatividade da operação $\cdot_L$ também é imediata, resta-nos assim apenas mostrar sua distributividade em relação a $+_L$, o que se verifica porque

$$a \cdot_L (b +_L c) = a(b + c) = ab + ac = a \cdot_L b +_L a \cdot_L c.$$

Assim, concluimos nossa demonstração. ♦

A.3.3 Anéis comutativos

DEFINIÇÃO A.62. Dizemos que um anel $(R, +, \cdot)$ é comutativo se e só se $\cdot$ satisfaz a propriedade da comutatividade.

anel comutativo

A.3.4 Anéis com unidade

DEFINIÇÃO A.63. Dizemos que um anel $(R, +, \cdot)$ é um anel com unidade se e somente se a operação $\cdot$ possui elemento neutro, chamado de unidade do anel.

anel com unidade

unidade de um anel

PROPRIEDADE A.46. *Um anel $(R, +, \cdot)$ pode possuir no máximo uma unidade.*

DEMONSTRAÇÃO. Sejam u_1 e u_2 unidades de um anel com unidade $(R, +, \cdot)$. Como u_1 é um elemento de R e u_2 é um elemento neutro para $\cdot$, temos que

$$u_1 = u_1 \cdot u_2 = u_2 \cdot u_1.$$

Como u_2 é um elemento de R e u_1 é um elemento neutro, temos que

$$u_2 \cdot u_1 = u_2.$$

Portanto, $u_1 = u_2$. ♦

PROPRIEDADE A.47. *Em um anel com unidade $(R, +, \cdot)$, cada elemento r de R só pode possuir no máximo um simétrico em relação a $\cdot$.*

DEMONSTRAÇÃO. Seja u a unidade de um anel com unidade $(R, +, \cdot)$ e seja s um elemento de R simetrizável em relação a $\cdot$, sendo s_1 e s_2 elementos simétricos de s. Como $s_1 = s_1 \cdot u$ e $u = s \cdot s_2$, temos que

$$\begin{aligned} s_1 &= s_1 \cdot (s \cdot s_2) \\ &= (s_1 \cdot s) \cdot s_2 \\ &= u \cdot s_2 \\ &= s_2, \end{aligned}$$

como queríamos demonstrar. ♦

NOTAÇÃO A.64. Em um anel com unidade cujas operações são, na ordem da definição, denotadas por $+$ e $\cdot$, sendo r um elemento simetrizável em relação a $\cdot$, denotamos por

(i) $\underline{1}$ o elemento neutro de $\cdot$ e

(ii) r^{-1} o elemento simétrico de r em relação a $\cdot$.

PROPRIEDADE A.48. *Sendo $(R,+,\cdot)$ um anel com unidade, sendo r e s elementos de R e sendo n e m números naturais,*

$$(nm)(rs) = (nr)(ms).$$

DEMONSTRAÇÃO. Sabemos que $(0m)(rs) = 0 = 0(ms) = (0r)(ms)$. Tomemos um natural k e, por indução em n, suponhamos que valha, para todo $\ell \in [0..k]$, que $(\ell m)(rs) = (\ell r)(ms)$. Queremos, então, somente mostrar que $((k+1)m)(rs) = ((k+1)r)(ms)$. Ora,

$$((k+1)m)(rs) = (km+m)(rs),$$

e, da propriedade A.30,

$$((k+1)m)(rs) = (km)(rs) + (1m)(rs),$$

e, da hipótese da indução, como 1 e k são elementos de $[0..k]$,

$$((k+1)m)(rs) = (kr)(ms) + r(ms)$$

e, da distributividade de $\cdot$ sobre $+$,

$$((k+1)m)(rs) = \big((kr)+r\big)(ms),$$

e, novamente da propriedade A.30,

$$((k+1)m)(rs) = \big((k+1)r\big)(ms),$$

como queríamos mostrar. ♦

potência

DEFINIÇÃO A.65. Seja $(R,+,\cdot)$ um anel com unidade, seja r um elemento de R e seja n um número natural. A n-ésima potência de r no anel é o elemento definido por:

$$r^n = \begin{cases} (r^{n-1})r, & \text{se } n > 0; \\ \underline{1}, & \text{caso contrário.} \end{cases}$$

OBSERVAÇÃO A.66. Sendo m um inteiro tal que $|m| > 1$ e definindo-se $+\colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ e $\cdot\colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ por

$$[a]_m + [b]_m = [a+b]_m \quad \text{e}$$
$$[a]_m[b]_m = [ab]_m,$$

é imediato verificar que $(\mathbb{Z}_m,+,\cdot)$ se trata de um anel com unidade, cuja unidade é $[1]_m$.

A.3.5 Domínios de integridade

anel de integridade

domínio de integridade

DEFINIÇÃO A.67. Dizemos que um anel comutativo com unidade $(R,+,\cdot)$ é um anel de integridade, ou domínio de integridade, se e somente se para quaisquer a e b elementos de R vale a lei do anulamento do produto: se $ab = \underline{0}$ então $a = \underline{0}$ ou $b = \underline{0}$.

lei do anulamento do produto

TEOREMA A.49. *Sendo m um inteiro tal que $|m| > 1$, $(\mathbb{Z}_m,+,\cdot)$ é um domínio de integridade se e só se m é um número primo.*

DEMONSTRAÇÃO. Suponhamos inicialmente que $(\mathbb{Z}_m, +, \cdot)$ seja um domínio de integridade e suponhamos que m não seja primo, mais especificamente, como $|m| > 1$, composto. Assim, existem a e b em $[1..(m-1)]$ tais que $|m| = ab$ e, conseqüentemente, da definição de $\cdot$ sobre $\mathbb{Z}_m$,

$$[a]_m[b]_m = [ab]_m = [|m|]_m = [0]_m,$$

contrariando a lei do anulamento do produto.

Falta-nos, portanto, somente mostrar que se m é primo então $(\mathbb{Z}_m, +, \cdot)$ é um domínio de integridade. Já sabemos que $(\mathbb{Z}_m, +, \cdot)$ se trata de um anel comutativo com unidade $[1]_m$, pois, para todo inteiro z, $[z]_m[1]_m = [z\dot{1}]_m = [z]_m$. Dessarte, resta-nos apenas mostrar que vale a lei do anulamento do produto. Sejam a e b inteiros e suponhamos, então, que $[a]_m[b]_m = [0]_m$. Queremos, assim, mostrar que $[a]_m = [0]_m$ ou $[b]_m = [0]_m$. Sabemos, como $[a]_m[b]_m = [ab]_m = [0]_m$, que $m \backslash ab$. Mas, da propriedade A.13, como m é primo, $m \backslash a$ ou $m \backslash b$. Finalmente, $[a]_m = [0]_m$ ou $[b]_m = [0]_m$. ♦

TEOREMA A.50. *Sendo $(R, +, \cdot)$ um anel comutativo com unidade, $(R, +, \cdot)$ é um domínio de integridade se e só se todo elemento de $R \setminus \{\underline{0}\}$ é regular para $\cdot$.*

DEMONSTRAÇÃO. Suponhamos que $(R, +, \cdot)$ seja um domínio de integridade. Sejam x e y elementos quaisquer de R e seja a um elemento de R diferente de $\underline{0}$. Suponhamos que $ax = ay$. Assim,

$$ax - ay = \underline{0},$$

e, portanto,

$$a(x - y) = \underline{0}.$$

Como $a \neq \underline{0}$ e $(R, +, \cdot)$ se trata de um domínio de integridade, temos então que $x - y = 0$ e, conseqüentemente, que $x = y$.

Agora, para completarmos a prova, suponhamos que todo elemento de $R \setminus \{\underline{0}\}$ seja regular para $\cdot$. Entretanto, suponhamos também que existam a e b elementos de R diferentes de $\underline{0}$ tais que $ab = \underline{0}$. Temos então que

$$ab = \underline{0} = a \cdot \underline{0};$$

mas, como a é regular para $\cdot$, concluímos que $b = \underline{0}$, o que é um absurdo. Assim, vale a lei do anulamento do produto. ♦

TEOREMA A.51. *Sendo $(R, +, \cdot)$ um anel (não necessariamente comutativo) com unidade no qual vale a lei do anulamento do produto, se $|R| > 1$ e se $(R, +, \cdot)$ tem característica positiva então a característica de $(R, +, \cdot)$ é um número primo.*

DEMONSTRAÇÃO. Seja n a característica de $(R, +, \cdot)$ Como $|R| > 1$, podemos tomar um $r \in R \setminus \{\underline{0}\}$ e, como $nr = \underline{0}$, concluir que $n \geqslant 2$. Suponhamos que n não seja um número primo. Então, como n é positivo no mínimo 2, existem k e m em $[2..(n-1)]$ tais que $n = km$. Assim,

$$n\underline{1} = (km)\underline{1} = (km)(\underline{1} \cdot \underline{1}),$$

e, da propriedade A.48,

$$n\underline{1} = (k \cdot \underline{1})(m \cdot \underline{1}) = \underline{0},$$

e, como vale a lei do anulamento do produto, $k \cdot \underline{1} = \underline{0}$ ou $m \cdot \underline{1} = \underline{0}$. Portanto, para todo $r \in R$, pelas propriedades A.48 e A.43,

$$kr = (k \cdot 1)(\underline{1} \cdot r) = (k \cdot \underline{1})r = \underline{0} \cdot r = \underline{0} \qquad \text{ou} \qquad mr = (m \cdot 1)(\underline{1} \cdot r) = (m \cdot \underline{1})r = \underline{0} \cdot r = \underline{0},$$

o que é um absurdo, já que n é o menor inteiro positivo ℓ tal que $\ell r = \underline{0}$. ♦

domínio de integridade finito

ordem de um domínio de integridade finito

NOMENCLATURA A.68. Dizemos que um domínio de integridade $(R, +, \cdot)$ é finito quando e só quando R é finito. Ademais, dizemos que $|R|$ é a ordem de $(R, +, \cdot)$.

A.3.6 Corpos

corpo

DEFINIÇÃO A.69. Sendo $(F, +, \cdot)$ um anel comutativo com unidade, $(F, +, \cdot)$ é um corpo [1] se e só se todo elemento de $F \setminus \{\underline{0}\}$ é simetrizável em relação e $\cdot$.

TEOREMA A.52. *Todo corpo é um domínio de integridade.*

DEMONSTRAÇÃO. Seja $(F, +, \cdot)$ um corpo. Tomemos a e b elementos quaisquer de F e suponhamos que $ab = \underline{0}$. Se, no entanto, supuséssemos que $a \neq \underline{0}$ e $b \neq \underline{0}$, teríamos, por causa da existência de a^{-1} e de b^{-1} garantida pela definição de corpo, que

$$\begin{aligned} \underline{0} &= a^{-1} \cdot \underline{0} \\ &= a^{-1}(ab) \\ &= (a^{-1}a)b \\ &= b, \end{aligned}$$

o que seria um absurdo. Assim, vale a lei do anulamento do produto, e, dessarte, concluimos que $(F, +, \cdot)$ também é um domínio de integridade. ♦

TEOREMA A.53. *Todo domínio de integridade finito é um corpo.*

DEMONSTRAÇÃO. Seja $(R, +, \cdot)$ um domínio de integridade finito. Como $R \setminus \{\underline{0}\} \neq \emptyset$, já que ao menos $\underline{1} \in R \setminus \{\underline{0}\}$, tomemos um elemento a de R diferente de $\underline{0}$. Vamos encontrar um elemento simétrico para a em relação a $\cdot$. Definamos a função $f_a \colon R \to R$ por:

$$f_a(r) = ar.$$

Sejam x e y elementos de R. Vamos mostrar que se $x \neq y$ então $f_a(x) \neq f_a(y)$ através da forma contrapositiva. Suponhamos que $f_a(x) = f_a(y)$. Portanto, $ax = ay$, e, assim, do teorema A.50, $x = y$. Mostrado que f_a se trata de uma injeção, notemos que se trata também de uma bijeção, já que possui domínio e contradomínio finitos e idênticos. Assim, $\underline{1} \in f_a(R)$, e, dessarte, existe um $r_1 \in R$ tal que $f_a(r_1) = \underline{1}$. Notemos, ademais, que

$$f_a(r_1) = ar_1 = \underline{1}.$$

Logo, r_1 é simétrico de a em relação a $\cdot$, como procurávamos. ♦

A.3.7 Corpos finitos

corpo finito

ordem de um corpo finito

NOMENCLATURA A.70. Dizemos que um corpo $(F, +, \cdot)$ é finito quando e só quando F é finito. Ademais, dizemos que $|F|$ é a ordem de $(F, +, \cdot)$.

[1] Em inglês, *field*.

TEOREMA A.54. *Sendo $(F,+,\cdot)$ um corpo finito, vale para todo a em F que*

$$a^{|F|} = a.$$

DEMONSTRAÇÃO. Seja a um elemento de F. Se $a = \underline{0}$ então a igualdade se verifica trivialmente. Se, por outro lado, $a \neq \underline{0}$ então $a \in F \setminus \{0\}$ e, como $(F \setminus \{0\}, \cdot)$ é um grupo finito, do teorema A.36, $a^{|F|-1} = \underline{1}$, e, portanto,

$$a^{|F|} = a \cdot a^{|F|-1} = a \cdot \underline{1} = a,$$

como queríamos mostrar. ♦

TEOREMA A.55. *Todo corpo finito possui característica prima.*

DEMONSTRAÇÃO. Seja $(F,+,\cdot)$ um corpo finito. Vamos primeiramente mostrar que a característica de $(F,+,\cdot)$ é positiva. Como $(F,+)$ é um grupo finito, então, do lema A.36, podemos tomar t o menor inteiro positivo tal que $t \cdot \underline{1} = \underline{0}$. Assim, para todo $r \in F$ vale, já que $(F \setminus \{\underline{0}\}, \cdot)$ é um grupo, por causa das propriedades A.32 e A.43,

$$tr = t(\underline{1} \cdot r) = (t \cdot \underline{1}) \cdot (tr) = \underline{0} \cdot (tr) = \underline{0}.$$

Para concluirmos que t se trata da característica de $(F,+,\cdot)$, basta mostrarmos que não existe um inteiro positivo $k < t$ tal que $kr = \underline{0}$ para todo $r \in F$. Supondo, no entanto, a existência desse k, temos que $k \cdot \underline{1} = \underline{0}$, o que contraria a escolha de t.

Mostrado que a característica de $(F,+,\cdot)$ é positiva, a demonstração se conclui por causa do teorema A.51 na medida em que $(F,+,\cdot)$ se trata de um anel com unidade e na medida em que, do teorema A.52, vale em $(F,+,\cdot)$ a lei do anulamento do produto. ♦

OBSERVAÇÃO A.71. Um resultado muito conhecido que não demonstraremos mas usaremos no presente trabalho é que se a e b são elementos de um corpo finito com característica p então

$$(a+b)^{p^n} = a^{p^n} + b^{p^n},$$

para todo natural n.

A.3.8 Subcorpos

DEFINIÇÃO A.72. Sendo $(F,+,\cdot)$ um corpo, dizemos que um subconjunto não vazio K de F é um subcorpo e escrevemos subcorpo

$$K \subseteq (F,+,\cdot)$$

se e somente se:

(i) K é fechado para ambas as operações $+$ e $\cdot$;

(ii) $(K,+_K,\cdot_K)$ também é um corpo.

TEOREMA A.56. *Sendo $(F,+,\cdot)$ um corpo, um subconjunto K de F é um subcorpo se e só se:*

(A.56.i) $\underline{0} \in K$ *e* $\underline{1} \in K$*;*

(A.56.ii) se $x \in K$ e $y \in K$ então $x - y \in K$;

(A.56.iii) se $x \in K$ e $y \in K \setminus \{\underline{0}\}$ então $xy^{-1} \in K$.

DEMONSTRAÇÃO. Suponhamos que K seja um subcorpo. Assim, como K é um subgrupo abeliano dos grupos abelianos $(F,+)$ e $(F \setminus \{\underline{0}\},\cdot)$, temos que $\underline{0} \in K$ e $\underline{1} \in K$. Sejam, então, x e y elementos de K. Novamente, como $K \subseteq (F,+)$, $x - y \in K$. Ainda, se $y \neq \underline{0}$, como $K \subseteq (F \setminus \{\underline{0}\},\cdot)$, $xy^{-1} \in K$.

Agora, suponhamos que:

(A.56.i) $\underline{0} \in K$ e $\underline{1} \in K$;

(A.56.ii) se $x \in K$ e $y \in K$ então $x - y \in K$;

(A.56.iii) se $x \in K$ e $y \in K \setminus \{\underline{0}\}$ então $xy^{-1} \in K$.

Dessarte, podemos concluir, pelo teorema A.23, que K se trata de um subgrupo abeliano tanto de $(F,+)$ quando de $(F,\cdot)$. Logo, K é um subcorpo de $(F,+,\cdot)$. ♦

NOMENCLATURA A.73. (i) Um subcorpo K de um corpo $(F,+,\cdot)$ é um subcorpo próprio de $(F,+,\cdot)$ se e só se $K \neq F$.

subcorpo próprio

corpo primo

(ii) Um corpo $(F,+,\cdot)$ é dito um corpo primo se e só se não possui subcorpos próprios.

subcorpo primo

(iii) Um subcorpo K de um corpo $(F,+,\cdot)$ é um subcorpo primo de $(F,+,\cdot)$ se e só se $(K,+_K,\cdot_K)$ é um corpo primo.

corpos isomorfos

DEFINIÇÃO A.74. Dizemos que dois corpos $(F_1,+_1,\cdot_1)$ e $(F_2,+_2,\cdot_2)$ são isomorfos e escrevemos $(F_1,+_1,\cdot_1) \simeq (F_2,+_2,\cdot_2)$ se e só se existe uma bijeção $f\colon F_1 \to F_2$ tal que, para todo a e todo b em F_1,

$$f(a +_1 b) = f(a) +_2 f(b), \qquad \text{e} \qquad f(a \cdot_1 b) = f(a) \cdot_2 f(b).$$

A.3.9 Ideais

DEFINIÇÃO A.75. Sendo $(R,+,\cdot)$ um anel, dizemos que um subconjunto J de R é um ideal sobre $(R,+,\cdot)$ se e somente se

ideal

(i) J é um subanel de $(R,+,\cdot)$ e

(ii) para qualquer $a \in J$ e qualquer $r \in R$, $ar \in J$ e $ra \in J$.

PROPRIEDADE A.57. *Sendo J um ideal sobre um anel $(R,+,\cdot)$ com unidade, se algum elemento simetrizável em relação a $\cdot$ pertence a J então $J = A$.*

DEMONSTRAÇÃO. Suponhamos que algum elemento simetrizável em relação a $\cdot$ pertença a J. Já sabemos que $J \subseteq R$, restando-nos apenas mostrar que $R \subseteq J$. Seja $r \in R$ e seja x, cuja existência é garantida pela hipótese, um elemento de J simetrizável em relação a $\cdot$. Sabemos que

$$r = r \cdot \underline{1} = r(u^{-1}u) = (ru^{-1})u.$$

Mas, da definição de ideal, como $(ru^{-1}) \in R$ e $u \in J$, $(ru^{-1})u \in J$, e, portanto, $r \in J$, como queríamos mostrar. ♦

NOTAÇÃO A.76. Sendo $(R,+,\cdot)$ um anel comutativo e S um subconjunto finito de R, utilizamos $\langle S\rangle$ para denotar o conjunto

$$\langle S\rangle = \left\{ \sum_{x\in S} xf(x) \;\middle|\; f \in R^S \right\}.$$

Quando S é um conjunto unitário, composto apenas por um elemento s, escrevemos $\langle s\rangle$ com o mesmo significado de $\langle S\rangle$.

OBSERVAÇÃO A.77. Note-se que, na particularidade da notação A.76 para conjuntos unitários,

$$\langle s\rangle = \{sr \mid r \in R\}.$$

TEOREMA A.58. *Sendo $(R,+,\cdot)$ um anel comutativo e S um subconjunto finito de R, $\langle S\rangle$ é um ideal sobre $(R,+,\cdot)$.*

DEMONSTRAÇÃO. Notemos primeiramente que $\langle S\rangle$ não é vazio, pois pelo menos

$$\underline{0} = \sum_{x\in S} x\cdot \underline{0}(x)$$

pertence a $\langle S\rangle$, sendo $\underline{0}\colon S \to R$ a função tal que $\underline{0}(x) = \underline{0}$ para todo $x \in S$.

Mostremos agora que $\langle S\rangle$ se trata de um subanel de $(R,+,\cdot)$. Sejam f_1 e f_2 elementos de A^S. Sabemos que

$$\sum_{x\in S} xf_1(x) - \sum_{x\in S} xf_2(x) = \sum_{x\in S} x\big(f_1(x) - f_2(x)\big),$$

e, como, para todo $x \in S$, $\big(f_1(x) - f_2(x)\big) \in R$, por R ser um anel, é um elemento de R^S a função $(f_1 - f_2)\colon S \to R$ definida por:

$$(f_1 - f_2)(x) = f_1(x) - f_2(x).$$

Dessarte,

$$\sum_{x\in S} xf_1(x) - \sum_{x\in S} xf_2(x) \in \langle S\rangle,$$

quaisquer que sejam f_1 e f_2 elementos de R^S. Como também é verdade que

$$\left(\sum_{x\in S} xf_1(x)\right)\left(\sum_{x\in S} xf_2(x)\right) = \sum_{x\in S} x\left(f_1(x)\left(\sum_{x\in S} xf_2(x)\right)\right) \in \langle S\rangle,$$

já que

$$f_1(x)\left(\sum_{x\in S} xf_2(x)\right) \in R$$

para todo $x \in S$, temos, do teorema A.45, que $\langle S\rangle$ é um subanel de $(R,+,\cdot)$.

Resta-nos ainda mostrar apenas que $xr \in \langle S\rangle$ para todo $x \in \langle S\rangle$ e $r \in R$, já que estamos trabalhando com um anel comutativo. Seja f uma função de S em R e seja r um elemento de R. Assim, verificamos que

$$\left(\sum_{x\in S} xf(x)\right)r = \sum_{x\in S} x\big(f(x)r\big) \in \langle S\rangle,$$

uma vez que $f(x)r \in R$ para todo $x \in S$. Conseqüentemente, $\langle S\rangle$ é um ideal sobre $(R,+,\cdot)$, como queríamos demonstrar. ♦

NOMENCLATURA A.78. Sendo $(R,+,\cdot)$ um anel comutativo e S um subconjunto finito de R, dizemos que $\langle S\rangle$ é o ideal gerado por S. Ainda, se $|S| = 1$ então dizemos que $\langle S\rangle$ é um ideal principal. Se todos os ideais sobre $(R,+,\cdot)$ são principais então dizemos que $(R,+,\cdot)$ é um anel principal.

ideal gerado

ideal principal

anel principal

A.3.10 Anéis quocientes

OBSERVAÇÃO A.79. Sendo J um ideal sobre um anel comutativo $(R,+,\cdot)$, J é um subgrupo normal de $(R,+)$, já que $(R,+)$ é abeliano e J, um subanel de $(R,+,\cdot)$. Portanto, $({}^{R}\!/_{J},+)$ se trata de um grupo quociente.

LEMA A.59. *Sendo J um ideal sobre um anel comutativo $(R,+,\cdot)$, a e b elementos quaisquer de R, a_1 e a_2 elementos quaisquer de $a+J$ e b_1 e b_2 elementos quaisquer de $b+J$,*

$$(a_1b_1)+J=(a_2b_2)+J$$

DEMONSTRAÇÃO. Como a_1 e a_2 pertencem a $a+J$, temos da definição A.45 que $-a_1+a\in J$, $-a_2+a\in J$ e, portanto, como J é um subgrupo de $(R,+)$,

$$-(-a_1+a)+(-a_2+a)=a_1-a_2\in J.$$

Analogamente, também temos que $b_1-b_2\in J$. Da definição A.75, como b_1 e a_2 também são elementos de R, percebemos que

$$b_1(a_1-a_2)\in J \quad \text{e} \quad a_2(b_1-b_2)\in J.$$

Conseqüentemente, como J é um ideal sobre $(R,+,\cdot)$,

$$b_1(a_1-a_2)+a_2(b_1-b_2)\in J,$$

e, assim,

$$a_1b_1-a_2b_1+a_2b_1-a_2b_2=a_1b_1-a_2b_2\in J.$$

Logo, como J é um subgrupo normal,

$$a_1b_1\sim a_2b_2 \pmod J.$$

Dessarte, se $x\in(a_1b_1)+J$ então

$$\begin{aligned} x &\sim a_1b_1 \pmod J \qquad \text{e, portanto,}\\ x &\sim a_2b_2 \pmod J, \end{aligned}$$

o que nos traz que $x\in(a_2b_2)+J$ e, por conseqüência, que

$$(a_1b_1)+J\subseteq(a_2b_2)+J.$$

Por outro lado, se $x\in(a_2b_2)+J$ então

$$\begin{aligned} x &\sim a_2b_2 \pmod J \qquad \text{e, portanto,}\\ x &\sim a_1b_1 \pmod J, \end{aligned}$$

o que nos traz que $x\in(a_1b_1)+J$ e, por conseqüência, que

$$(a_2b_2)+J\subseteq(a_1b_1)+J,$$

o que completa nossa demonstração. ♦

OBSERVAÇÃO A.80. O lema A.59 nos traz que $ab+J$ continua o mesmo conjunto não importando quais representantes sejam escolhidos das classes $a+J$ e $b+J$ para substituírem respectivamente a e b, o que garante que a operação introduzida pela notação A.81 seja bem definida.

NOTAÇÃO A.81. Sendo J um ideal sobre um anel comutativo $(R,+,\cdot)$, a e b elementos quaisquer de R, utilizamos $(a+J)(b+J)$ para denotar o conjunto

$$(a+J)(b+J) = (ab)+J.$$

OBSERVAÇÃO A.82. A operação $\cdot$, como convencionada na notação A.81, é uma operação fechada sobre o conjunto quociente ${}^{R}\!/_{J}$.

TEOREMA A.60. *Sendo J um ideal sobre um anel comutativo $(R,+,\cdot)$, as operações $+$ e $\cdot$, nessa ordem, e o conjunto quociente ${}^{R}\!/_{J}$ definem um anel, chamado de anel quociente (ou anel de classes de resíduos, ou anel de classes residuais) de R por J.*

anel quociente

anel de classes de resíduos

anel de classes residuais

DEMONSTRAÇÃO. Do teorema A.42, $({}^{R}\!/_{J},+)$ é o grupo quociente de R por J, possuindo $+$ sobre ${}^{R}\!/_{J}$ também a propriedade da comutatividade, já que

$$(x+J)+(y+J) = (x+y)+J = (y+x)+J = (y+J)+(x+J)$$

para todo x e todo y em R. Tomemos agora a, b e c elementos de R. É fácil também verificar que $\cdot$ sobre ${}^{R}\!/_{J}$ também goza da associatividade, pois

$$\begin{aligned}\big((a+J)(b+J)\big)(c+J) &= \big((ab)+J\big)(c+J)\\ &= \big((ab)c+J\big)\\ &= \big(a(bc)+J\big)\\ &= (a+J)\big((bc)+J\big)\\ &= (a+J)\big((b+J)(c+J)\big).\end{aligned}$$

Finalmente, notemos que vale também a distributividade de $\cdot$ sobre $+$:

$$\begin{aligned}(a+J)\big((b+J)+(c+J)\big) &= (a+J)\big((b+c)+J\big)\\ &= \big(a(b+c)+J\big)\\ &= \big((ab+ac)+J\big)\\ &= \big((ab)+J\big)+\big((ac)+J\big)\\ &= \big((a+J)(b+J)\big)+\big((a+J)(c+J)\big).\end{aligned}$$

Por tudo isso, concluimos que $({}^{R}\!/_{J},+,\cdot)$ se trata de um anel. ♦

OBSERVAÇÃO A.83. Note-se que o conjunto dos inteiros com as operações usuais de adição e multiplicação constituem um anel comutativo. Note-se ainda, da observação A.77 e da notação A.15, que

$$\langle p\rangle = \{pz\colon z\in\mathbb{Z}\} = [0]_p$$

e que

$$\begin{aligned}{}^{\mathbb{Z}}\!/_{\langle p\rangle} &= \bigcup_{z\in\mathbb{Z}} [z]_{\sim \text{ módulo } \langle p\rangle}\\ &= \bigcup_{z\in\mathbb{Z}} \{x\in\mathbb{Z}\colon x\sim z \pmod{\langle p\rangle}\}\\ &= \bigcup_{z\in\mathbb{Z}} \{x\in\mathbb{Z}\colon x\equiv z \pmod{p}\}\\ &= \bigcup_{j\in[0..(p-1)]} [j]_p\\ &= \mathbb{Z}_p\end{aligned}$$

TEOREMA A.61. *Sendo p um número primo, o anel quociente $(\mathbb{Z}/\langle p\rangle, +, \cdot)$ é um corpo.*

DEMONSTRAÇÃO. Do teorema A.49 e da observação A.83, sabemos que $(\mathbb{Z}/\langle p\rangle, +, \cdot)$ é um domínio de integridade. Como

$$\left|\mathbb{Z}/\langle p\rangle\right| = p,$$

$(\mathbb{Z}/\langle p\rangle, +, \cdot)$ se trata de um domínio de integridade finito e, portanto, do teorema A.53, de um corpo. ♦

COROLÁRIO A.62. *Para um número primo p, seja $\mathbb{F}_p$ o conjunto $[0..(p-1)]$ e seja $\phi\colon \mathbb{Z}/\langle p\rangle \to \mathbb{F}_p$ a bijeção definida por*

$$\phi\big([z]_p\big) = z.$$

Sejam também as operações $+$ e $\cdot$ sobre $\mathbb{F}_p$ definidas por:

$$z_1 + z_2 = \phi\big([z_1]_p + [z_2]_p\big);$$
$$z_1 \cdot z_2 = \phi\big([z_1]_p \cdot [z_2]_p\big).$$

Então, a estrutura formada por $\mathbb{F}_p$ e pelas operações definidas acima é um corpo finito, chamado de corpo de Galois de ordem p.

corpo de Galois

ordem de um corpo de Galois

DEMONSTRAÇÃO. A presente demonstração segue imediatamente do teorema A.61. ♦

PROPRIEDADE A.63. *Sendo p um primo positivo, todo corpo de Galois de ordem p possui característica p.*

DEMONSTRAÇÃO. Do teorema A.55, segue que $(\mathbb{F}_p, +, \cdot)$ possui característica prima q. Assim, $q \cdot 1 = 0$, e, portanto,

$$[q]_p = q \cdot [1]_p = [0]_p$$

no corpo $(\mathbb{Z}/\langle p\rangle, +, \cdot)$, e, conseqüentemente,

$$q \equiv 0 \pmod{p},$$

o que nos leva a concluir que $p \backslash q$. Mas, como q é primo e $|p| \neq 1$, $p = q$, como queríamos mostrar. ♦

LEMA A.64. *Se $(F, +, \cdot)$ é um corpo finito de característica q então o conjunto*

$$A = \{n(\underline{1})\colon n \in \mathbb{F}_q\}$$

é um subcorpo de $(F, +, \cdot)$.

DEMONSTRAÇÃO. É claro que $0(\underline{1}) = \underline{0}$ e $1(\underline{1}) = \underline{1}$ pertencem a A, já que $q \geqslant 2$. Temos, para todo $n \in \mathbb{F}_q$, que $(nq)(\underline{1}) = n(q(\underline{1})) = n(\underline{0}) = \underline{0}$. Assim, sendo $k \in \mathbb{F}_q$, é evidente que $-(k(\underline{1})) \in A$, já que $-(k(\underline{1})) = (q-k)(\underline{1})$. Assim, para todo natural ℓ, temos que $\ell(\underline{1}) - (k(\underline{1})) \in A$. Por último, admitamos que $k(\underline{1}) \neq \underline{0}$. Como $k \in \mathbb{F}_q \setminus \{0\}$ e $(\mathbb{F}_q, +, \cdot)$ é um corpo, então existe um $k^{-1} \in \mathbb{F}_q$. Assim, $(k^{-1})(\underline{1})$ é o inverso de $k(\underline{1})$ em relação à multiplicação sobre F e, portanto, para todo natural ℓ vale que $\ell(\underline{1})(k(\underline{1}))^{-1} \in A$, e, conseqüentemente, do teorema A.56, concluímos que A é um subcorpo de $(F, +, \cdot)$. ♦

TEOREMA A.65. *Se $(F,+,\cdot)$ é um corpo primo finito de característica p então $(F,+,\cdot) \simeq (\mathbb{F}_p,+,\cdot)$.*

DEMONSTRAÇÃO. Seja a função $f\colon \mathbb{F}_p \to F$ definida por:

$$f(k) = k(\underline{1}).$$

Vamos mostrar que:

(A.65.i) f é uma injeção;

(A.65.ii) f é uma sobrejeção;

(A.65.iii) f preserva a adição em $\mathbb{F}_p$;

(A.65.iv) f preserva a multiplicação em $\mathbb{F}_p$.

Mostraremos (i) da forma contrapositiva. Tomemos j e k elementos de $\mathbb{F}_p$ tais que $f(j) = f(k)$. Assim, $j(\underline{1}) = k(\underline{1})$, e, da propriedade A.20, como $(F,+)$ é um grupo, $j(\underline{1}) - k(\underline{1}) = \underline{0}$, e, da propriedade A.30, $(j-k)(\underline{1}) = \underline{0}$. Como p é a característica de $(F,+,\cdot)$, p é o menor inteiro positivo tal que $p(\underline{1}) = \underline{0}$. Dessarte, como $j-k < p$, $j-k = 0$ e, conseqüentemente, $j = k$, como queríamos mostrar.

Agora, supunhamos que f não seja sobrejetiva. Assim, existe um r em F para o qual não há um $j \in \mathbb{F}_p$ tal que $f(j) = r$. Assim, o conjunto $f(\mathbb{F}_p)$, do lemalemtcsg, é um subcorpo próprio de $(F,+,\cdot)$, o que é um absurdo, já que $(F,+,\cdot)$ é primo.

Por fim, é imediato verificar (iii) e (iv) e concluir a demonstração. ♦

A.4 Espaços vetoriais

A.4.1 Conceituação

DEFINIÇÃO A.84. Sendo V um conjunto qualquer, $(F,+,\cdot)$ um corpo qualquer e $+\colon V\times V \to V$ e $\cdot\colon F\times V \to V$ funções, dizemos que $(V,+,\cdot)$ é um <u>espaço vetorial</u> sobre $(F,+,\cdot)$ se e somente se: espaço vetorial

(i) $(V,+)$ é um grupo abeliano;

(ii) $\underline{1}\cdot\boldsymbol{u} = \boldsymbol{u}$ para todo $\boldsymbol{u} \in V$;

(iii) $a\cdot(b\cdot\boldsymbol{u}) = (a\cdot b)\cdot\boldsymbol{u}$ para todo $\boldsymbol{u}$ em V e todo a e todo b em F;

(iv) $a\cdot(\boldsymbol{u}+\boldsymbol{v}) = (a\cdot\boldsymbol{u}) + (a\cdot\boldsymbol{v})$ para todo $\boldsymbol{u}$ e todo $\boldsymbol{v}$ em V e todo a em F;

(v) $(a+b)\cdot\boldsymbol{u} = (a\cdot\boldsymbol{u}) + (b\cdot\boldsymbol{u})$ para todo $\boldsymbol{u}$ em V e todo a e todo b em F.

NOMENCLATURA A.85. Em um espaço vetorial $(V,+,\cdot)$ sobre um corpo $(F,+,\cdot)$, costumamos chamar:

(i) os elementos de V de <u>vetores</u>; vetor

(ii) os elementos de F de <u>escalares</u>; escalar

(iii) a operação $+$ de <u>adição de vetores</u>, ou <u>adição vetorial</u>; adição de vetores, adição vetorial

(iv) a operação $\cdot$ de <u>multiplicação por escalar</u>. multiplicação por escalar

A seguir introduzimos uma notação similar àquela que introduzimos para anéis.

NOTAÇÃO A.86. Em um espaço vetorial $(V,+,\cdot)$ sobre um corpo $(F,+,\cdot)$, sendo $\boldsymbol{u}$ qualquer elemento de V, denotamos por

vetor nulo

(i) $\mathbf{0}$ o elemento neutro de $+$, chamado de vetor nulo, e

(ii) $-\boldsymbol{u}$ o elemento simétrico de $\boldsymbol{u}$ em relação a $+$;

OBSERVAÇÃO A.87. Num espaço vetorial $(V,+,\cdot)$ sobre um corpo $(F,+,\cdot)$, podemos sempre assumir a precedência de $\cdot$ em relação a $+$. É também costume escrever simplesmente $a\boldsymbol{u}$ ao invés de $a\cdot\boldsymbol{u}$, assim como $\boldsymbol{u}-\boldsymbol{v}$ ao invés de $\boldsymbol{u}+(-\boldsymbol{v})$.

PROPRIEDADE A.66. *Num espaço vetorial $(V,+,\cdot)$ sobre um corpo $(F,+,\cdot)$, $\underline{0}\cdot\boldsymbol{u}=\mathbf{0}$ para todo $\boldsymbol{u}\in V$.*

DEMONSTRAÇÃO. Notemos que

$$\begin{aligned}\underline{0}\cdot\boldsymbol{u} &= (\underline{0}+\underline{0})\cdot\boldsymbol{u}\\ &= (\underline{0}\cdot\boldsymbol{u})+(\underline{0}\cdot\boldsymbol{u}),\end{aligned}$$

e, portanto, que $\underline{0}\cdot\boldsymbol{u}$ é elemento neutro para a operação $+$. Mas, como $(V,+)$ é um grupo, o elemento neutro de $+$ é único (propriedade A.15). Logo, $\underline{0}\cdot\boldsymbol{u}=\mathbf{0}$. ♦

DEFINIÇÃO A.88. Sendo $(V,+,\cdot)$ um espaço vetorial sobre um corpo $(F,+,\cdot)$, diz-se que um subconjunto S de V é linearmente dependente sobre $(V,+,\cdot)$ se e só se existe um subconjunto finito $U=\{\boldsymbol{u_k}\colon k\in[|U|]\}$ de S e uma função $f\colon U\to F\setminus\underline{0}$ tais que

conjunto linearmente dependente

$$\sum_{k=1}^{|U|} f(\boldsymbol{u_k})\boldsymbol{u_k}=\mathbf{0}.$$

conjunto linearmente independente

Caso contrário, diz-se que S é linearmente independente sobre $(V,+,\cdot)$..

DEFINIÇÃO A.89. Sendo $(V,+,\cdot)$ um espaço vetorial sobre um corpo $(F,+,\cdot)$, diz-se que um subconjunto S de V gera o espaço vetorial $(V,+,\cdot)$ se e só se, para todo $\boldsymbol{u}\in V$, existe uma função $f_u\colon S\to F$ tal que

espaço vetorial gerado por um subconjunto do conjunto de vetores

$$\boldsymbol{u}=\sum_{\boldsymbol{s}\in S} f_u(s)\boldsymbol{s}.$$

representação de um vetor por uma base

Nesse caso, dizemos que f_u é uma representação de $\boldsymbol{u}$ pela base S.

DEFINIÇÃO A.90. Sendo $(V,+,\cdot)$ um espaço vetorial sobre um corpo $(F,+,\cdot)$, diz-se que um subconjunto B de V é uma base de $(V,+,\cdot)$ se e só se B é um conjunto linearmente independente e gera $(V,+,\cdot)$.

base de um espaço vetorial

OBSERVAÇÃO A.91. Um resultado muito conhecido em Álgebra Linear, que não mostraremos no presente trabalho, é que quaisquer duas bases de um espaço vetorial correspondem-se biunivocamente, o que nos permite a nomenclatura A.92.

NOMENCLATURA A.92. Dizemos que um espaço vetorial $(V,+,\cdot)$ sobre um corpo $(F,+,\cdot)$ possui dimensão finita, ou que $(V,+,\cdot)$ é finito-dimensional, se as bases de $(V,+,\cdot)$ são conjuntos finitos, ocasião em que chamamos a cardinalidade de qualquer uma das bases de dimensão de $(V,+,\cdot)$, denotada por $\dim(V,+,\cdot)$. Se, por outro lado, as bases de $(V,+,\cdot)$ forem conjuntos infinitos, diremos que $(V,+,\cdot)$ possui dimensão infinita, ou que $(V,+,\cdot)$ é infinito-dimensional, e escreveremos $\dim(V,+,\cdot)=\infty$.

espaço vetorial de dimensão finita

espaço vetorial finito-dimensional

dimensão de um espaço vetorial

espaço vetorial de dimensão infinita

espaço vetorial infinito-dimensional

A.5 Espaços vetoriais gerados por subcorpos

Agora que apresentamos uma brevíssima conceituação acerca de espaços vetoriais, dedicaremo-nos a nossa aplicação do assunto: estudaremos os espaços vetoriais gerados por subcorpos, que nos permitirão o desenvolvimento de algumas argumentações importantes.

PROPRIEDADE A.67. *Sendo K um subcorpo de $(F,+,\cdot)$, $(F,+,\cdot)$ é um espaço vetorial sobre $(K,+_K,\cdot_K)$, dito o espaço vetorial gerado gerado por K, ou o espaço vetorial de F sobre K, sendo $\cdot\colon K\times F\to F$ a função definida, para todo $k\in K$ e todo $r\in F$, por:*

espaço vetorial gerado por um subcorpo

$$k\cdot \boldsymbol{r} = k\cdot \boldsymbol{r}.$$

DEMONSTRAÇÃO. É imediato que $(F,+)$ seja um grupo abeliano já que $(F,+,\cdot)$ se trata de um corpo. Também é verdade, para todo $\boldsymbol{r_1}$ e todo $\boldsymbol{r_2}$ em F, e para todo k_1 e todo k_2 em K, que:

(i) $\underline{1}\cdot \boldsymbol{r_1} = \underline{1}\cdot \boldsymbol{r_1} = \boldsymbol{r_1}$;

(ii) $k_1\cdot(k_2\cdot \boldsymbol{r_1}) = k_1\cdot(k_2\cdot \boldsymbol{r_1}) = (k_1\cdot k_2)\cdot \boldsymbol{r_1} = (k_1\cdot_K k_2)\cdot \boldsymbol{r_1}$;

(iii) $k_1\cdot(\boldsymbol{r_1}+\boldsymbol{r_2}) = k_1\cdot(\boldsymbol{r_1}+\boldsymbol{r_2}) = (k_1\cdot \boldsymbol{r_1})+(k_1\cdot \boldsymbol{r_2}) = (k_1\cdot \boldsymbol{r_1})+(k_1\cdot \boldsymbol{r_2})$.

(iv) $(k_1+_K k_2)\cdot \boldsymbol{r_1} = (k_1+k_2)\cdot \boldsymbol{r_1} = (k_1\cdot \boldsymbol{r_1})+(k_2\cdot \boldsymbol{r_1}) = (k_1\cdot \boldsymbol{r_1})+_K (k_2\cdot \boldsymbol{r_1})$.

Portanto, $(F,+,\cdot)$ é um espaço vetorial sobre $(K,+_K,\cdot_K)$. ♦

NOTAÇÃO A.93. Sendo K um subcorpo de um corpo finito $(F,+,\cdot)$, usamos $[F:K]$ para denotar a dimensão do espaço vetorial de F sobre K.

TEOREMA A.68. *Sendo L um subcorpo de um corpo finito $(M,+,\cdot)$ e K um subcorpo de $(L,+_L,\cdot_L)$,*

$$[M:K] = [M:L][L:M]$$

DEMONSTRAÇÃO. Como M é um corpo finito, sejam $A=\{\alpha_j\colon j\in[[M:L]]\}$ uma base para o espaço vetorial de M sobre L e $B=\{\beta_j\colon j\in[[L:K]]\}$ uma base para o espaço vetorial de L sobre K. Assim, para todo $\alpha\in M$ existe uma função γ de $[[M:L]]$ em L tal que

$$\alpha = \sum\nolimits_{j=1}^{[M:L]}\gamma_j\alpha_j,$$

denotando-se $\gamma(j)$ por γ_j. Como o contradomínio de γ é L e B é uma base para o espaço vetorial de L sobre K, existe, para cada $j\in[[M:L]]$, uma função r_j de $[[L:K]]$ em K tal que

$$\gamma_j = \sum\nolimits_{\ell=1}^{[L:K]} r_{(j,\ell)}\beta_\ell,$$

denotando-se $r_j(\ell)$ por $r_{(j,\ell)}$. Portanto,

$$\begin{aligned}\alpha &= \sum\nolimits_{j=1}^{[M:L]}\left(\sum\nolimits_{\ell=1}^{[L:K]} r_{(j,\ell)}\beta_\ell\right)\alpha_j\\ &= \sum\nolimits_{j=1}^{[M:L]}\sum\nolimits_{\ell=1}^{[L:K]} r_{(j,\ell)}\beta_\ell\alpha_j,\end{aligned}$$

Logo, Para mostrarmos que $[M:K]=[M:L][L:K]$, basta que mostremos que o conjunto $\{\beta_\ell\alpha_j\colon j\in[[M:L]]e\ell\in[[L:K]]\}$ é linearmente independente. Para tanto, tomemos, para cada $j\in[[M:L]]$ e cada $\ell\in[[L:K]]$, um $s_{(j,\ell)}$ tal que

$$\sum\nolimits_{j=1}^{[M:L]}\sum\nolimits_{\ell=1}^{[L:K]} s_{(j,\ell)}\beta_\ell\alpha_j = \underline{0}.$$

Dessarte,

$$\sum_{j=1}^{[M:L]}\left(\sum_{\ell=1}^{[L:K]} s_{(j,\ell)}\beta_\ell\right)\alpha_j = \underline{0},$$

e, como A é linearmente independente sobre o espaço vetorial de M sobre L,

$$\sum_{\ell=1}^{[L:K]} s_{(j,\ell)}\beta_\ell = \underline{0}$$

para todo $j \in [[M : L]]$ e, como B é linearmente independente sobre o espaço vetorial de L sobre K,

$$s_{(j,\ell)} = \underline{0}$$

para todo $j \in [[M : L]]$ e todo $\ell \in [[L : K]]$, como queríamos mostrar. ⧫

TEOREMA A.69. *Se $(F, +, \cdot)$ é um corpo finito, então $|F| = q^m$ para algum inteiro positivo m, sendo q a característica de $(F, +, \cdot)$.*

DEMONSTRAÇÃO. Vamos mostrar que existe um inteiro positivo m tal que $F \simeq \mathbb{F}_q^{[m]}$. Para tanto, tomemos um subcorpo primo K de $(F, +, \cdot)$. Sabemos, do teorema A.65, que $K \simeq \mathbb{F}_q$. Tomemos $m = [F : K]$ e uma base B para o espaço vetorial de F sobre K. Mostraremos, então, que $F \simeq K^B$. Para isso, basta que tomemos a bijeção $f\colon F \to K^B$ definida por:

$$f(r) = \alpha_r,$$

sendo $\alpha_r\colon B \to K$ a representação de r por B. ⧫

OBSERVAÇÃO A.94. Podemos estender a definição de corpo de Galois para potências de primos da seguinte maneira: sendo p um número primo, m um inteiro positivo e $q = p^m$, utilizamos $\mathbb{F}_q$ para denotarmos o conjunto $[0..(q-1)]$. É óbvio que $(\mathbb{F}_q, +, \cdot)$ também é um corpo, chamado de corpo de Galois de ordem q, sendo as operações $+$ e $\cdot$ módulo q.

corpo de Galois

ordem de um corpo de Galois

PROPRIEDADE A.70. *Se m é um divisor positivo de um inteiro positivo n e p é um primo positivo então $\mathbb{F}_{p^m}$ é um subcorpo de $(\mathbb{F}_{p^n}, +, \cdot)$.*

DEMONSTRAÇÃO. Como m divide n, $\mathbb{F}_{p^m}$ é evidentemente um subconjunto de $\mathbb{F}_{p^n}$. Da observação A.94, $(\mathbb{F}_{p^m}, +, \cdot)$ é um corpo. ⧫

Referências Bibliográficas

[1] A. V. Aho, J. E. Hopcroft, e J. D. Ullman.
The Design and Analysis of Algorithms.
Addison-Wesley, 1974.

[2] Hygino H. Domingues e Gelson Iezzi.
Álgebra Moderna.
Atual, São Paulo, quarta edição, 2003.

[3] R. Lidl e H. Niederreiter.
Introduction to Finite Fields and Their Applications.
Cambridge University Press, Cambridge, 1986.

[4] M. O. Rabin.
Probabilistic algorithms in finite fields.
9:273–280, 1980.

[5] A. Schonhage.
Schnelle Multiplikation von Polynomen uber Körpern der Charakteristic 2.
Acta Informatica, 1977.

Índice Remissivo

adição de vetores, 55
adição vetorial, 55
algoritmo da divisão para polinômios, 12
anel, 43
anel com unidade, 45
anel comutativo, 45
anel de classes de resíduos, 53
anel de classes residuais, 53
anel de integridade, 46
anel de polinômios, 7
anel finito, 44
anel principal, 51
anel quociente, 53
aplicação, 26
associatividade, 27

base de um espaço vetorial, 56
bijeção, 26

característica de um anel, 44
classe de equivalência, 22
classe lateral à direita, 34
classe lateral à esquerda, 34
comutatividade, 27
congruência, 25
conjunto das partes, 21
conjunto fechado para uma operação, 27
conjunto linearmente dependente, 56
conjunto linearmente independente, 56
conjunto munido de uma operação, 27
conjunto potência, 21
conjunto quociente, 22
contradomínio de uma função, 26
corpo, 48
corpo de decomposição polinomial, 13
corpo de extensão, 13
corpo de Galois, 54, 58
corpo finito, 48
corpo primo, 50
corpos isomorfos, 50
correspondência biunívoca entre dois conjuntos, 26

decomposição de um corpo por um polinômio, 13
dimensão de um espaço vetorial, 56
distributividade, 27
divisibilidade, 23
divisibilidade polinomial, 11
divisor de um número inteiro, 23
divisor de um polinômio, 11
domínio de integridade, 46
domínio de integridade finito, 48
domínio de uma função, 26

elemento neutro, 27
elemento regular para uma operação, 28
elemento simétrico, 28
elemento simetrizável, 28
escalar, 55
espaço vetorial, 55
espaço vetorial de dimensão finita, 56
espaço vetorial de dimensão infinita, 56
espaço vetorial finito-dimensional, 56
espaço vetorial gerado por um subconjunto do conjunto de vetores, 56
espaço vetorial gerado por um subcorpo, 57
espaço vetorial infinito-dimensional, 56

field, 48
forma padrão de um polinômio, 6
função, 26
função bijetiva, 26
função bijetora, 26
função injetiva, 26
função injetora, 26
função sobrejetiva, 26
função sojetora, 26

grau de um polinômio, 6
grupo, 28
grupo abeliano, 32
grupo cíclico, 39
grupo comutativo, 32
grupo finito, 36
grupo quociente, 42

ideal, 50
ideal gerado, 51
ideal principal, 51
imagem, 26
imagem inversa, 26
indeterminada de um polinômio, 6
índice de um subgrupo num grupo, 36
injeção, 26
iteração de uma operação, 37

lei do anulamento do produto, 46

multiplicação por escalar, 55
múltiplo de um elemento de um anel, 44
múltiplo de um número inteiro, 23
múltiplo de um polinômio, 11

operação, 27
ordem de um corpo de Galois, 54, 58
ordem de um corpo finito, 48
ordem de um domínio de integridade finito, 48
ordem de um grupo finito, 36
ordem de um subgrupo de um grupo finito, 36

partição, 21
polinômio, 6
polinômio constante, 6
polinômio identicamente nulo, 7
polinômio identidade, 6
polinômio irredutível, 12
polinômio primo, 12
polinômios idênticos, 6
potência, 46
princípio da identidade de polinômios, 6

quociente de uma divisão, 23
quociente de uma divisão polinomial, 11

raiz de um polinômio, 7
relação, 21
relação anti-simétrica, 21
relação de equivalência, 22
relação reflexiva, 21
relação simétrica, 21
relação transitiva, 21
representação de um vetor por uma base, 56
restrição de uma operação, 27

sobrejeção, 26
splitting field, 13
subanel, 44
subcorpo, 49
subcorpo primo, 50
subcorpo próprio, 50
subgrupo, 32
subgrupo gerado, 40
subgrupo normal, 41
suporte finito de uma função, 5

teorema de Lagrange, 36
termo constante de um polinômio, 6
termo dominante de um polinômio, 6

unidade de um anel, 45

vetor, 55
vetor nulo, 56