# Tópicos Avançados em Ciência da Computação I: Introdução à Teoria de Códigos para Criptografia Pós-quântica

Daniel Panario
School of Mathematics and Statistics
Carleton University

IC - Unicamp, Sala 351 do IC-3
das 13:30 as 18:30 em 16-17 de janeiro de 2020,
das 13:30 as 17:30 em 20-24 de janeiro de 2020



# Introdução aos Corpos Finitos: Parte I

Daniel Panario
School of Mathematics and Statistics
Carleton University

16-17 de janeiro de 2020

## Conteúdo da aula

- Porque corpos finitos? Breve introdução às aplicações dos corpos finitos, à teoria de códigos e à criptografia.
- Estruturas algébricas. Definições de grupo, anel e corpo; propriedades e exemplos. Característica de um corpo. Extensões e espaços vetoriais.
- Polinômios: divisibilidade, máximo divisor comum, algoritmo estendido de Euclides, fatoração única de polinômios, representação polinomial.
- Corpos finitos: característica prima, corpo de decomposição. Existência e unicidade de corpos finitos, propriedades; subcorpos de um corpo finito. Elementos primitivos e normais. Funções traço e norma.

Texto: Tópicos de Corpos Finitos com Aplicações em Criptografia e Teoria de Códigos, Ariane M. Masuda e Daniel Panario. Publicações Matemáticas do IMPA, 26 Colóquio Brasileiro de Matemática, 2007.



## Porque corpos finitos?

A pesquisa em corpos finitos une várias áreas de matemática:

Álgebra: extensões de corpos e teoria de Galois.

Matemática discreta: representações dos elementos de corpos finitos, algoritmos em corpos finitos, usos dos corpos finitos em construções de objetos combinatórios.

Teoria de números: contar elementos e polinômios sobre corpos finitos com propriedades especiais.

Muitos projetos que usam corpos finitos podem ser aplicados quase imediatamente em problemas no "mundo real". Corpos finitos são usados amplamente em áreas como:

Teoria de códigos; Criptografia; Comunicações e Engenharia Elétrica; Ciência da Computação.

## Porque corpos finitos?

A pesquisa em corpos finitos une várias áreas de matemática:

Álgebra: extensões de corpos e teoria de Galois.

Matemática discreta: representações dos elementos de corpos finitos, algoritmos em corpos finitos, usos dos corpos finitos em construções de objetos combinatórios.

Teoria de números: contar elementos e polinômios sobre corpos finitos com propriedades especiais.

Muitos projetos que usam corpos finitos podem ser aplicados quase imediatamente em problemas no "mundo real". Corpos finitos são usados amplamente em áreas como:

Teoria de códigos; Criptografia; Comunicações e Engenharia Elétrica; Ciência da Computação.



## Aplicações dos corpos finitos

Corpos finitos são aplicados em inúmeras (infinitas?) áreas. É impossível dar uma lista completa de problemas onde os corpos finitos estão sendo usados.

Damos uma lista longa e incompleta de áreas de pesquisa onde os corpos finitos são aplicados com alguns exemplos.

A principal fonte de aplicações são a criptografia e a teoria de códigos. Discutimos essas aplicações a seguir.

# Aplicações em criptografia

- Sistemas criptográficos:
  - Método de Diffie-Hellman para compartilhar uma chave;
  - Método de assinatura digital de ElGamal;
  - RSA (e polinômios de permutação sobre corpos finitos);
  - Sistemas criptográficos baseados em curvas elípticas e hyperelípticas;
  - Sistema criptográfico de Chor-Rivest;
  - Sistema criptográfico Powerline;
  - Sistema criptográfico de McEliece (códigos de Goppa); etc.

- Criptografia Pós-Quântica:
  - Baseada em códigos;
  - Baseada em polinômios multivariados;
  - Baseada em hash (poucos corpos finitos);
  - Baseada em reticulados (poucos corpos finitos);
  - Baseada em isogenias (algo de corpos finitos);



# Aplicações em criptografia

- Segurança:
  - o problema do logaritmo discreto;
  - método do cálculo de índices e suas variántes: algoritmos de Waterloo e de Coppersmith.

- Cifras de fluxo:
  - WG (Welch-Gong);
  - RC4; etc.

- Cifras de bloco:
  - AES (Advanced Encryption Standard): Rijndael;
  - RC6 (polinômios de permutação sobre anéis de inteiros).

## Aplicações na teoria de códigos

- Aplicações clássicas:
  - Códigos BCH;
  - Códigos Reed-Solomon;
  - Códigos que corrigem "burst" erros;
  - Códigos de convolução;
  - Códigos baseados em curvas algébricas; etc.
- Aplicações recentes:
  - Códigos LDPC (low density parity check);
  - Códigos turbo.



## Aplicações em engenharia

- LFSR (feedback shift register sequences);
- geradores de números pseudo-aleatórios;
- radar e sonar (seqüências sobre corpos finitos, funções APN);
- processamento de sinais digitais: transformadas (de Fourier discreta, de Hadamard); teoria espectral, etc.

Para mais informação ver o livro de Golomb e Gong (2005).

## Aplicações em matemática

- Geometria finita: geometria afim e projetiva; construções de planos projectivos com um número finito de pontos e linhas.
- Planejamentos combinatórios: BIBD (balance incomplete block designs), quadrados latinos e MOLS (mutually orthogonal latin squares), etc.
- Há também aplicações recentes em bioinformática e sistemas dinâmicos sobre corpos finitos.

Para mais informação ver (propaganda sem vergonha...):

Handbook of Finite Fields
by Gary Mullen and Daniel Panario

published by CRC in 2013.



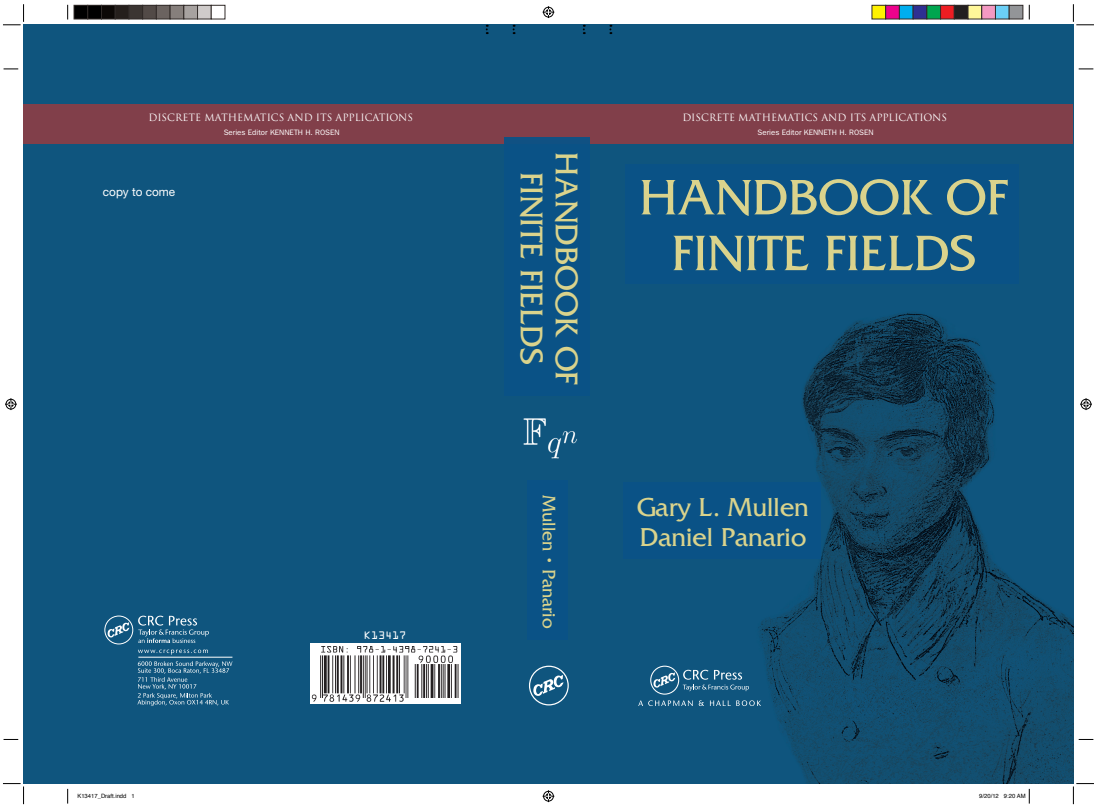
## Aplicações em matemática

- Geometria finita: geometria afim e projetiva; construções de planos projectivos com um número finito de pontos e linhas.
- Planejamentos combinatórios: BIBD (balance incomplete block designs), quadrados latinos e MOLS (mutually orthogonal latin squares), etc.
- Há também aplicações recentes em bioinformática e sistemas dinâmicos sobre corpos finitos.

Para mais informação ver (propaganda sem vergonha...):

Handbook of Finite Fields
by Gary Mullen and Daniel Panario

published by CRC in 2013.






# História dos corpos finitos

A teoria de corpos finitos desenvolveu-se amplamente no século XIX, porém a sua origem data dos séculos XVII e XVIII. Os primeiros pesquisadores a considerar corpos finitos foram:

Pierre de Fermat, Leonhard Euler, Joseph-Louis Lagrange, Adrien-Marie Legendre e Carl Friedrich Gauss.

Na época, os únicos corpos finitos conhecidos eram os corpos contendo um número primo de elementos.

A aparição em 1830 do artigo Sur la théorie des nombres de Évariste Galois (1811-1832), foi fundamental para o surgimento de várias questões quanto à estrutura de corpos finitos em geral.

Em 1857, Richard Dedekind caracterizou corpos finitos com $p^n$ elementos, onde $p$ é primo, em termos de anéis quocientes de polinômios. Anos mais tarde, em 1893, Eliakim H. Moore mostrou que qualquer corpo finito contém $p^n$ elementos.

Dedekind também introduziu a fórmula de inversão de Möbius em corpos finitos para estudar o número de polinômios irredutíveis de certo grau.

O livro de Leonard Dickson, publicado em 1901, já tinha os resultados mais importantes sobre a estrutura de corpos finitos.
A seguir, apresentamos uma pequena lista com alguns desses resultados.



1. O número de elementos num corpo finito é uma potência da característica prima do corpo.
2. Se $p$ é primo e $n$ é um inteiro positivo, então existe um único corpo finito com $p^n$ elementos, a menos de isomorfismos.
3. O grupo multiplicativo dos elementos não nulos de um corpo finito é cíclico.
4. Seja $F$ um corpo com $p^n$ elementos. O número de elementos num subcorpo de $F$ é da forma $p^d$, onde $d$ é um divisor de $n$. Reciprocamente, se $d$ divide $n$, então existe um subcorpo de $F$ com $p^d$ elementos.
5. Todo elemento $a$ num corpo finito com $q$ elementos satisfaz $a^q = a$.

No século XX, o uso de corpos finitos foi extremamente difundido, em parte devido à aparição dos computadores.

# Grupos

**Definição**

*Um grupo $(G, *)$ é um conjunto $G$ munido de uma operação binária $*$ onde*

(a) *para todo $a, b \in G$, $a * b \in G$;*

(b) *para todo $a, b, c \in G$, $a * (b * c) = (a * b) * c$;*

(c) *existe um elemento $e \in G$ tal que $a * e = e * a = a$ para todo $a \in G$;*

(d) *para todo $a \in G$, existe um elemento $b \in G$ tal que $a * b = b * a = e$.*

*O grupo $G$ é Abeliano se $G$ é um grupo e*

(e) *para todo $a, b \in G$, $a * b = b * a$.*

Exemplos: $(\mathbb{Z}, +)$, e $(\mathbb{Q} \setminus \{0\}, \cdot)$.



# Grupos

**Definição**

*Um grupo $(G, *)$ é um conjunto $G$ munido de uma operação binária $*$ onde*

(a) *para todo $a, b \in G$, $a * b \in G$;*

(b) *para todo $a, b, c \in G$, $a * (b * c) = (a * b) * c$;*

(c) *existe um elemento $e \in G$ tal que $a * e = e * a = a$ para todo $a \in G$;*

(d) *para todo $a \in G$, existe um elemento $b \in G$ tal que $a * b = b * a = e$.*

*O grupo $G$ é Abeliano se $G$ é um grupo e*

(e) *para todo $a, b \in G$, $a * b = b * a$.*

Exemplos: $(\mathbb{Z}, +)$, e $(\mathbb{Q} \setminus \{0\}, \cdot)$.

Daniel Panario | Introdução aos Corpos Finitos: Parte I | 16-17 de janeiro de 2020 | 15 / 77

# Grupos

**Definição**

*Um grupo $(G, *)$ é um conjunto $G$ munido de uma operação binária $*$ onde*

(a) *para todo $a, b \in G$, $a * b \in G$;*

(b) *para todo $a, b, c \in G$, $a * (b * c) = (a * b) * c$;*

(c) *existe um elemento $e \in G$ tal que $a * e = e * a = a$ para todo $a \in G$;*

(d) *para todo $a \in G$, existe um elemento $b \in G$ tal que $a * b = b * a = e$.*

*O grupo $G$ é Abeliano se $G$ é um grupo e*

(e) *para todo $a, b \in G$, $a * b = b * a$.*

Exemplos: $(\mathbb{Z}, +)$, e $(\mathbb{Q} \setminus \{0\}, \cdot)$.



# Anéis

**Definição**

*Um anel $(R, +, \cdot)$ é um conjunto $R$ munido de duas operações binárias $+$ e $\cdot$ onde*

(a) *$(R, +)$ é um grupo abeliano;*

(b) *$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo $a, b, c \in R$; e*

(c) *$a \cdot (b + c) = a \cdot b + a \cdot c$, $(b + c) \cdot a = b \cdot a + c \cdot a$ para todo $a, b, c \in R$.*

Exemplos: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n$ e $R[x]$, onde $R$ é um anel.

Se $R$ é um anel comutativo com identidade e se, para quaisquer $a, b \in R$ tais que $a \cdot b = 0$, tem-se que $a = 0$ ou $b = 0$, então $R$ é um domínio de integridade.

# Anéis

**Definição**

*Um anel $(R, +, \cdot)$ é um conjunto $R$ munido de duas operações binárias $+$ e $\cdot$ onde*

(a) *$(R, +)$ é um grupo abeliano;*

(b) *$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo $a, b, c \in R$; e*

(c) *$a \cdot (b + c) = a \cdot b + a \cdot c$, $(b + c) \cdot a = b \cdot a + c \cdot a$ para todo $a, b, c \in R$.*

Exemplos: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n$ e $R[x]$, onde $R$ é um anel.

Se $R$ é um anel comutativo com identidade e se, para quaisquer $a, b \in R$ tais que $a \cdot b = 0$, tem-se que $a = 0$ ou $b = 0$, então $R$ é um domínio de integridade.



# Corpos

**Definição**

*Um anel $(R, +, \cdot)$ é chamado um corpo se $(R^*, \cdot)$ é um grupo abeliano.*

Exemplos:

1. $\mathbb{Z}$ não é um corpo, mas $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos.
2. $\mathbb{Z}_n$ é um corpo se e somente se $n$ é primo.

Demonstração. Suponhamos que $\mathbb{Z}_n$ é um corpo com $n$ composto; digamos que $n = ab$ onde $1 < a, b < n$. Como $a \neq 0$, existe $\bar{a} \in \mathbb{Z}_n^*$ tal que $\bar{a}a = 1$. Assim,

$$b = 1 \cdot b = (\bar{a}a)b = \bar{a}(ab) = \bar{a}n = 0,$$

o que é uma contradição. Reciprocamente, seja $a \in \mathbb{Z}_n^*$ com $n$ primo. Então $\mathrm{mdc}(a, n) = 1$, isto é, existem inteiros $x$ e $y$ tais que $ax + ny = 1$. Logo $ax \equiv 1 \pmod{n}$. □

## Corpos

**Definição**

*Um anel $(R, +, \cdot)$ é chamado um corpo se $(R^*, \cdot)$ é um grupo abeliano.*

Exemplos:

1. $\mathbb{Z}$ não é um corpo, mas $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos.
2. $\mathbb{Z}_n$ é um corpo se e somente se $n$ é primo.

Demonstração. Suponhamos que $\mathbb{Z}_n$ é um corpo com $n$ composto; digamos que $n = ab$ onde $1 < a, b < n$. Como $a \neq 0$, existe $\bar{a} \in \mathbb{Z}_n^*$ tal que $\bar{a}a = 1$. Assim,

$$b = 1 \cdot b = (\bar{a}a)b = \bar{a}(ab) = \bar{a}n = 0,$$

o que é uma contradição. Reciprocamente, seja $a \in \mathbb{Z}_n^*$ com $n$ primo. Então $\mathrm{mdc}(a, n) = 1$, isto é, existem inteiros $x$ e $y$ tais que $ax + ny = 1$. Logo $ax \equiv 1 \pmod{n}$. □



## Corpos

**Definição**

*Um anel $(R, +, \cdot)$ é chamado um corpo se $(R^*, \cdot)$ é um grupo abeliano.*

Exemplos:

1. $\mathbb{Z}$ não é um corpo, mas $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos.
2. $\mathbb{Z}_n$ é um corpo se e somente se $n$ é primo.

Demonstração. Suponhamos que $\mathbb{Z}_n$ é um corpo com $n$ composto; digamos que $n = ab$ onde $1 < a, b < n$. Como $a \neq 0$, existe $\bar{a} \in \mathbb{Z}_n^*$ tal que $\bar{a}a = 1$. Assim,

$$b = 1 \cdot b = (\bar{a}a)b = \bar{a}(ab) = \bar{a}n = 0,$$

o que é uma contradição. Reciprocamente, seja $a \in \mathbb{Z}_n^*$ com $n$ primo. Então $\mathrm{mdc}(a, n) = 1$, isto é, existem inteiros $x$ e $y$ tais que $ax + ny = 1$. Logo $ax \equiv 1 \pmod{n}$. □

Daniel Panario | Introdução aos Corpos Finitos: Parte I | 16-17 de janeiro de 2020 | 17 / 77

## Uma outra operação

Sejam $R$ um anel, $a \in R$ e $n \in \mathbb{Z}$. Definimos:

$$na = \begin{cases} 0 & \text{se } n = 0 \\ \underbrace{a + \cdots + a}_{n \text{ vezes}} & \text{se } n > 0 \\ -((-n)a) & \text{se } n < 0. \end{cases}$$

Propriedade: $(ma)(nb) = (mn)(ab)$ para todo $m, n \in \mathbb{Z}$ e para todo $a, b \in R$.



## Característica de um anel

**Definição**

*Seja $R$ um anel para o qual existe um inteiro positivo $n$ tal que*

$$n \cdot 1 = \underbrace{1 + \cdots + 1}_{n \text{ vezes}} = 0.$$

*O menor tal inteiro positivo $n$ é chamado a característica (positiva) de $R$ e denotado por $\mathrm{car}(R)$. Em particular, se $n$ é primo, então dizemos que $R$ tem característica prima. Se $R$ não tem característica positiva, dizemos que $R$ tem característica zero.*

Exemplo: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ têm característica zero, enquanto $\mathbb{Z}_n$ tem característica $n$ quando $n \geq 2$.

## Característica de um anel

**Definição**

*Seja $R$ um anel para o qual existe um inteiro positivo $n$ tal que*

$$n \cdot 1 = \underbrace{1 + \cdots + 1}_{n \text{ vezes}} = 0.$$

*O menor tal inteiro positivo $n$ é chamado a característica (positiva) de $R$ e denotado por $\mathrm{car}(R)$. Em particular, se $n$ é primo, então dizemos que $R$ tem característica prima. Se $R$ não tem característica positiva, dizemos que $R$ tem característica zero.*

Exemplo: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ têm característica zero, enquanto $\mathbb{Z}_n$ tem característica $n$ quando $n \geq 2$.



## Extensão de corpos

$F$ corpo, $K \subseteq F$

Se $K$ também é um corpo sob as operações de $F$, dizemos que $K$ é um subcorpo de $F$ e que $F$ é uma extensão de $K$.

Exemplo: $\mathbb{Q}$ é um subcorpo de $\mathbb{R}$ e $\mathbb{C}$; $\mathbb{R}$ é um subcorpo de $\mathbb{C}$.

## Extensão de corpos

$F$ corpo, $K \subseteq F$

Se $K$ também é um corpo sob as operações de $F$, dizemos que $K$ é um subcorpo de $F$ e que $F$ é uma extensão de $K$.

Exemplo: $\mathbb{Q}$ é um subcorpo de $\mathbb{R}$ e $\mathbb{C}$; $\mathbb{R}$ é um subcorpo de $\mathbb{C}$.

$$\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{R} \\ | \\ \mathbb{Q} \end{array}$$



## Corpos finitos e espaços vetoriais

Se $L$ é um corpo de extensão de $K$, então $L$ pode ser visto como um espaço vetorial sobre $K$:

⋆ $(L, +)$ é um grupo abeliano

⋆ $K \times L \to L$ satisfaz, para todo $r, s \in K$ e para todo $\alpha, \beta \in L$,
$(r, \alpha) \mapsto r\alpha$

$$\begin{aligned} r(\alpha + \beta) &= r\alpha + r\beta, \\ (r + s)\alpha &= r\alpha + s\alpha, \\ (rs)\alpha &= r(s\alpha), \\ 1_K \cdot \alpha &= \alpha. \end{aligned}$$

Quando $\dim_K L < \infty$, dizemos que $L$ é uma extensão finita de $K$ cujo grau é $[L : K] = \dim_K L$.

Exemplo: bases polinomiais e normais.

**Teorema**

*Se $M$ é uma extensão finita de $L$ e $L$ é uma extensão finita de $K$, então $M$ é uma extensão finita de $K$ com*

$$[M : K] = [M : L][L : K].$$




## Representações de elementos em corpos finitos

Consideramos corpos finitos da forma $\mathbb{F}_q$ onde $q = p^n, n \geq 1$.

- Corpos primos: $q = p$. Neste caso $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$, usando as operações módulo $p$.
- Extensões finitas: $q = p^n, n \geq 2$.
  - Usando polinômios: $\mathbb{F}_q \cong \mathbb{F}_p[x]/(f)$ onde $f \in \mathbb{F}_p[x]$ é irredutível sobre $\mathbb{F}_p$ de grau $n$, e operamos módulo $f$.
  - Usando bases normais (próxima aula).
  - Juntando uma raiz: seja $f \in \mathbb{F}_p[x]$ um polinômio irredutível de grau $n$, e seja $\alpha$ uma raiz em $\mathbb{F}_q$. Então $\mathbb{F}_q = \mathbb{F}_p(\alpha)$.

    Exemplo: $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ onde $\alpha$ é uma raiz do polinômio irredutível $x^2 + 1 \in \mathbb{F}_3[x]$. Os elementos de $\mathbb{F}_9$ são: $\{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$.

## Corpos primos: $\mathbb{F}_p$

Escrevemos $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$, isto é como $\mathbb{Z}_p$, e as operações são consideradas módulo $p$.

- Seja $p$ um número primo e suponhamos que os inteiros $x_1, x_2, y_1, y_2$ verificam $x_1 \equiv x_2 \pmod{p}$ and $y_1 \equiv y_2 \pmod{p}$. Então

$$x_1 + y_1 \equiv x_2 + y_2 \pmod{p} \quad \text{e} \quad x_1 y_1 \equiv x_2 y_2 \pmod{p}.$$

- Soma e produto são calculados modulo $p$.

Quando $p$ é muito grande (de interesse em criptografia), $p$ pode ser maior que o tamanho de uma palavra de máquina. Neste caso operamos com inteiros longos; ver, por exemplo, o livro de Knuth The Art of Computer Programming, vol. 2.



## Modelo computacional

Neste curso consideramos o caso mais geral de contar as operações em $\mathbb{F}_{q^n}$ em função das operações em $\mathbb{F}_q$. Em particular, $q$ pode ser um número primo, que é o caso considerado acima.

Nossa medida de custo sera o número de operações no corpo finito. Por exemplo, se trabalhamos em $\mathbb{F}_{p^n}$ representado por um polinômio irredutível sobre $\mathbb{F}_p$ de grau $n$, então o custo das operações com polinômios depende do grau $n$ e do primo $p$.

Para a análise assintótica do custo das operações aritméticas, usaremos a seguinte definição. Sejam $f$ e $g$ funções de $\mathbb{N}$ em $\mathbb{R}$. Dizemos que $f$ é $O(g)$ se existem constantes $C \in \mathbb{R}^+$ e $n_0 \in \mathbb{N}$ tais que $|f(x)| \leq C|g(x)|$ para todo $x \geq n_0$.
Exemplos: $7000n$ é $O(n^2)$, e $n \log n$ é $O(n^2)$.

# Polinômios

## Definição

*Sejam $R$ um anel e $a_0, a_1, \ldots, a_n$ elementos em $R$ com $a_n \neq 0$. Um polinômio $f$ sobre $R$ é uma expressão da forma*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

*Neste caso, dizemos que cada $a_i$ é um coeficiente de $f$, $a_n$ é o coeficiente do termo dominante de $f$ e o grau de $f$ é $n$. O polinômio nulo tem todos os coeficientes iguais a zero e neste caso, por convenção, o grau é $-\infty$ (ou o grau é $-1$). Quando o coeficiente do termo dominante de $f$ é $1$, dizemos que $f$ é mônico.*



# Soma e produto de polinômios

## Definição

*Dados dois polinômios $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{j=0}^{m} b_j x^j$ sobre $R$ com $m \leq n$, definimos a soma $f(x) + g(x)$ e o produto $f(x)g(x)$ da seguinte maneira:*

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i \quad e \quad f(x)g(x) = \sum_{i=0}^{n+m} c_k x^k,$$

*onde $b_{m+1} = b_{m+2} = \cdots = b_n = 0$, e*

$$c_k = \sum_{\substack{0 \leq i \leq n \\ 0 \leq j \leq m \\ k = i+j}} a_i b_j.$$

*O conjunto de todos os polinômios sobre $R$ com essas duas operações é o anel dos polinômios sobre $R$ denotado por $R[x]$.*

## Produto de polinômios

Além do método clássico de multiplicação de polinômios, há outros métodos que são mais eficientes quando os graus dos polinômios são grandes.

O método de Karatsuba (1962) reduz o custo de $O(n^2)$ a $O(n^{\log_2 3})$.
É um método eficiente não só assintoticamente, mas também na prática (hoje em dia mais em software que em hardware).

Um método ainda mais rápido é baseado na transformada rápida de Fourier (FFT), que a seguir comentamos brevemente.



## Mutiplicação baseada no FFT

Sejam $f, g \in \mathbb{F}_q[x]$ dois polinômios de grau $n$ com $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{i=0}^{n} b_i x^i$. Consideremos elementos $u_i, i = 0, \ldots 2n$, dois a dois distintos.

O polinômio $f$ pode ser descrito usando a sua representação por valores: $f(u_0), \ldots, f(u_n)$. De fato podemos usar interpolação para reconstruir o polinômio $f$.

Se dois polinômios $f$ e $g$ são dados pelas suas representações por valores, então podemos multiplicar os polinômios rapidamente (tempo linear) multiplicando as imagens segundo as funções induzidas pelos polinômios $f$ e $g$:

$$f(u_0)g(u_0), \ldots, f(u_{2n})g(u_{2n}).$$

Método:

1. avaliar os dois polinômios;
2. multiplicar os resultados segundo as funções induzidas pelos polinômios;
3. interpolar para obter o produto dos polinômios.

O método mais rápido para avaliar um polinômio $f$ num ponto particular $u$ é o método de Horner:

$$f(u) = (\cdots((a_n u + a_{n-1})\, u + a_{n-2})\cdots)\, u + a_0,$$

que requer $O(n)$ operações em $\mathbb{F}_q$. Se aplicarmos o método de Horner para calcular os valores dos polinômios $f$ e $g$ nos pontos $u_0, \ldots, u_{2n}$, teríamos um custo total de $O(n^2)$ operações em $\mathbb{F}_q$.



Além disso, uma implementação direta do algoritmo de interpolação de Lagrange também produziria um custo de $O(n^2)$. Assim, não teríamos nenhuma vantagem sobre a multiplicação clássica.

Podemos melhorar este custo? Precisamos de um método rápido para calcular os valores de um polinômio em vários pontos.

Schönhage e Strassen (1971) dão um método rápido de avaliar polinômios baseado nas potências de uma raiz $n$-ésima primitiva da unidade, digamos, $\omega$, e o algoritmo FFT (Transformada Rápida de Fourier). O passo de interpolação também pode ser executado rapidamente usando o algoritmo FFT com $\omega^{-1}$ ao invés de $\omega$. Para mais detalhes sobre o assunto, veja, por exemplo, o livro de von zur Gathen e Gerhard (2003).

Não é claro a partir de que valores o método baseado na FFT é prático.

O custo de executar a FFT é $O(n \log n \log\log n)$. Logo, podemos multiplicar dois polinômios de grau $n$ usando $O(n \log n \log\log n)$ operações em $\mathbb{F}_q$. Usando métodos rápidos de multiplicação, o tempo assintótico de uma divisão de polinômios passa a ser $O(n \log n \log\log n)$.

Os métodos FFT também podem ser usados para calcular o $\mathrm{mdc}$ e o inverso, usando $O(n \log^2 n \log\log n)$ operações em $\mathbb{F}_q$.

Observamos que o famoso método de Strassen para multiplicação de matrizes $n \times n$ em $O(n^{\log 7})$ é baseado em idéias similares às do método de Karatsuba.



## Divisibilidade de polinômios

Sejam $f$ e $g$ polinômios sobre um anel $R$. Dizemos que $g$ divide $f$, se existe $h \in R[x]$ tal que $f = gh$. Neste caso, também dizemos que $g$ é um divisor de $f$.

Mais geralmente, temos o seguinte resultado.

**Teorema (Algoritmo da divisão)**

*Sejam $F$ um corpo e $f, g \in F[x]$ com $g \neq 0$. Existem únicos polinômios $h$, $r \in F[x]$ tais que $f = gh + r$ e $\mathrm{grau}(r) < \mathrm{grau}(g)$.*

Seja $R$ um anel. Para que o algoritmo da divisão seja válido em $R[x]$, é necessário que o coeficiente do termo dominante de $g$ seja inversível em $R$.

## Máximo divisor comum (MDC) de polinômios

**Definição**

*Seja $F$ um corpo. Dados $f$ e $g \in F[x]$, existe um único polinômio mônico $d \in F[x]$ tal que*

(a) *$d$ divide $f$ e $g$,*

(b) *qualquer polinômio $h \in F[x]$ dividindo ambos $f$ e $g$ divide também $d$.*

*Este polinômio $d$ é o máximo divisor comum de $f$ e $g$, denotado por* $\mathrm{mdc}(f, g)$.

Observamos que o $\mathrm{mdc}(f, g)$ é o polinômio mônico de maior grau dentre os polinômios que dividem ambos $f$ e $g$ em $F[x]$.

Veremos que $f$ e $g$ têm um divisor comum $d$ tal que $d = af + bg$ para certos $a, b \in F[x]$. Desta expressão, resulta que qualquer divisor comum de $f$ e $g$ divide $d$.



## Algoritmo de Euclides

A fim de encontrar o $\mathrm{mdc}(f, g)$, apresentaremos agora o algoritmo euclideano, que é baseado em várias aplicações do algoritmo da divisão. Começamos com a divisão de $f$ por $g$, supondo que o resto desta divisão seja $r_1$. A próxima divisão é a de $g$ por $r_1$ com resto $r_2$, digamos. Dividindo $r_1$ por $r_2$ e continuando com este processo, obtemos:

$$\begin{aligned} f &= q_1 g + r_1 \\ g &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{s-3} &= q_{s-1} r_{s-2} + r_{s-1} \\ r_{s-2} &= q_s r_{s-1} + r_s \\ r_{s-1} &= q_{s+1} r_s + 0, \end{aligned} \tag{1}$$

onde $q_1, \ldots, q_{s+1}, r_1, \ldots, r_s$ são polinômios sobre $F$.

## Algoritmo de Euclides (cont.)

Temos que

$$\text{grau}(g) > \text{grau}(r_1) > \text{grau}(r_2) > \cdots > \text{grau}(r_{s-1}) > \text{grau}(r_s) \geq 0.$$

Como $\text{grau}(g)$ é finito, este processo de divisões sempre termina com uma divisão exata. Quando isso acontece, temos que

$$\text{mdc}(f, g) = a^{-1} r_s,$$

onde $a$ é o coeficiente do termo dominante do último resto não nulo $r_s$. Esta multiplicação de $r_s$ por $a^{-1}$ é realizada para que tenhamos um polinômio mônico.



## Exemplo: MDC de polinômios

1. Sejam $f(x) = x^3 + 3$ e $g(x) = 2x^2 + 2$ onde $f, g \in \mathbb{F}_5[x]$. Temos que

$$\begin{aligned} x^3 + 3 &= 3x(2x^2 + 2) + (4x + 3) \\ 2x^2 + 2 &= (3x + 4)(4x + 3) + 0. \end{aligned}$$

   Então $\text{mdc}(x^3 + 3, 2x^2 + 2) = (4^{-1})(4x + 3) = 4(4x + 3) = x + 2$.

2. Sejam $f(x) = 2x^6 + x^3 + x^2 + 2$ e $g(x) = x^4 + x^2 + 2x$ onde $f, g \in \mathbb{F}_3[x]$. Temos que

$$\begin{aligned} 2x^6 + x^3 + x^2 + 2 &= (2x^2 + 1)(x^4 + x^2 + 2x) + (x + 2) \\ x^4 + x^2 + 2x &= (x^3 + x^2 + 2x + 1)(x + 2) + 1 \\ x + 2 &= (x + 2)(1) + 0. \end{aligned}$$

   Então $\text{mdc}(f, g) = 1$.

Se $\text{mdc}(f, g) = 1$, dizemos que $f$ e $g$ são polinômios coprimos.

## Algoritmo estendido de Euclides

É possível escrever o $\mathrm{mdc}(f, g)$ como uma combinação linear de $f$ e $g$, no sentido de que $\mathrm{mdc}(f, g) = af + bg$ para certos polinômios $a$ e $b$ em $F[x]$.

Esta representação é muito útil como veremos mais tarde. Vamos ver agora como encontrar tais polinômios $a$ e $b$ usando o algoritmo euclideano estendido. Como o próprio nome sugere, estaremos usando dados das divisões efetuadas no algoritmo euclideano.

Escrevemos o resto de cada divisão, em termos dos outros polinômios envolvidos em cada expressão de (1). Começando de baixo para cima, pela penúltima expressão, obtemos que:



## Algoritmo estendido de Euclides (cont.)

$$\begin{aligned} r_s &= r_{s-2} - q_s r_{s-1} \\ r_{s-1} &= r_{s-3} - q_{s-1} r_{s-2} \\ &\vdots \\ r_3 &= r_1 - q_3 r_2 \\ r_2 &= g - q_2 r_1 \\ r_1 &= f - q_1 g. \end{aligned}$$

Por simplicidade, suponhamos que $s = 3$. Combinamos as expressões acima da seguinte maneira:

$$\begin{aligned} r_3 &= r_1 - q_3 r_2 = r_1 - q_3(g - q_2 r_1) \\ &= r_1(1 + q_2 q_3) - q_3 g = (f - q_1 g)(1 + q_2 q_3) - q_3 g \\ &= f(1 + q_2 q_3) + g(-q_1 - q_1 q_2 q_3 - q_3). \end{aligned}$$

Portanto, $a = 1 + q_2 q_3$ e $b = -q_1 - q_1 q_2 q_3 - q_3$. No caso geral, procedemos de forma análoga com esta série de substituições para encontrar os polinômios $a$ e $b$.

# Exemplo: algoritmo estendido de Euclides para polinômios

## Exemplo

*Sejam* $f(x) = 2x^{10} + x^7 + x^2 + 1$ *e* $g(x) = x^7 + 1$ *em* $\mathbb{F}_3[x]$. *Vamos escrever o* $\mathrm{mdc}(f, g)$ *como combinação linear de* $f$ *e* $g$. *Pelo algoritmo euclideano, temos as seguintes expressões:*

$$\begin{aligned} 2x^{10} + x^7 + x^2 + 1 &= (2x^3 + 1)(x^7 + 1) + (x^3 + x^2) \\ x^7 + 1 &= (x^4 + 2x^3 + x^2 + 2x + 1)(x^3 + x^2) + (2x^2 + 1) \\ x^3 + x^2 &= (2x + 2)(2x^2 + 1) + (x + 1) \\ 2x^2 + 1 &= (2x + 1)(x + 1) + 0. \end{aligned}$$



# Exemplo: algoritmo estendido de Euclides (cont.)

## Exemplo

*Logo* $\mathrm{mdc}(f, g) = x + 1$. *Além disso, temos*

$$\begin{aligned} & x + 1 \\ = \; & (x^3 + x^2) - (2x + 2)(2x^2 + 1) \\ = \; & (x^3 + x^2) - (2x + 2)((x^7 + 1) - (x^4 + 2x^3 + x^2 + 2x + 1)(x^3 + x^2)) \\ = \; & (2x^5)(x^3 + x^2) + (x + 1)(x^7 + 1) \\ = \; & (2x^5)((2x^{10} + x^7 + x^2 + 1) - (2x^3 + 1)(x^7 + 1)) + (x + 1)(x^7 + 1) \\ = \; & 2x^5(2x^{10} + x^7 + x^2 + 1) + (2x^8 + x^5 + x + 1)(x^7 + 1). \end{aligned}$$

*Assim, obtemos que* $\mathrm{mdc}(f, g) = (2x^5)f + (2x^8 + x^5 + x + 1)g$.

## Resumo: aritmética polinomial

Custo: operações em $\mathbb{F}_q$.

Dois polinômios de grau no máximo $n$ em $\mathbb{F}_q[x]$ podem ser multiplicados em

- $O(n^2)$ usando métodos diretos,
- $O(n^{\log 3})$ usando o algoritmo de Karatsuba, ou com
- $O(n \log n \log\log n)$ usando métodos baseados na FFT.

Uma divisão com resto pode ser calculada com o mesmo número de operações em $\mathbb{F}_q$ usadas numa multiplicação.



## Resumo: aritmética polinomial (cont.)

O mdc de dois polinômios de grau no máximo $n$ em $\mathbb{F}_q[x]$ pode ser calculado com

- $O(n^2)$ usando métodos diretos, ou com
- $O(n \log^2 n \log\log n)$ usando métodos baseados na FFT.

Para polinômios $f, g \in \mathbb{F}_q[x]$, $\text{grau}(f) = n$, $\text{grau}(g) < n$ e $e < q^n$, o cálculo de $g^e \pmod f$ pode ser feito usando o método da repetição de quadrados com, no máximo, $O(n \log q)$ multiplicações em $\mathbb{F}_q[x]$ módulo $f$, ou seja,

- $O(n^3 \log q)$ usando métodos diretos, ou
- $O(n^2 \log q \log n \log\log n)$ usando métodos baseados na FFT.

## Fatoração única de polinômios

Consideramos umas das propriedades mais importantes de $F[x]$: a *fatoração única de polinômios*.

**Teorema (Fatoração única de polinômios)**

*Seja $F$ um corpo. Qualquer polinômio $f \in F[x]$ de grau positivo pode ser escrito como*

$$f = a f_1^{e_1} f_2^{e_2} \dots f_k^{e_k},$$

*onde $a \in F$, $e_1, e_2, \dots, e_k \in \mathbb{N}$ e $f_1, f_2, \dots, f_k$ são polinômios mônicos irredutíveis sobre $F$. Além disso, esta fatoração é única a menos da ordem dos fatores.*

A prova deste teorema, que será omitida, não é construtiva, uma vez que não fornece um algoritmo para fatorar polinômios. Veremos métodos para fatorar polinômios sobre um corpo finito.



## Representação polinomial

O próximo teorema é fundamental na teoria dos corpos finitos.

**Teorema**

*Seja $q = p^n$. Se $f$ é um polinômio irredutível sobre $\mathbb{F}_p$ de grau $n$ então $\mathbb{F}_q \cong \mathbb{F}_p[x]/(f)$.*

Em geral, para $q = p^n$, $\mathbb{F}_{q^m} \cong \mathbb{F}_q[x]/(f)$, onde $f$ é um polinômio irredutível de grau $m$ sobre $\mathbb{F}_q$. Assim, um elemento em $\mathbb{F}_{q^m}$ pode ser representado por um polinômio em $\mathbb{F}_q[x]$ de grau menor que $m$.

**Exemplo:** Como $f(x) = x^2 + x + 1$ tem grau 2 e não possui raízes em $\mathbb{F}_2$, $f$ é irredutível sobre $\mathbb{F}_2$. Temos que $\mathbb{F}_4$ e $\mathbb{F}_2[x]/(f)$ são isomorfos. Os elementos de $\mathbb{F}_4$, representados em termos de polinômios, são 0, 1, $x$ e $x + 1$. As tabelas completas de adição e de multiplicação para $\mathbb{F}_4$ são:

## Representação polinomial

O próximo teorema é fundamental na teoria dos corpos finitos.

**Teorema**

*Seja $q = p^n$. Se $f$ é um polinômio irredutível sobre $\mathbb{F}_p$ de grau $n$ então $\mathbb{F}_q \cong \mathbb{F}_p[x]/(f)$.*

Em geral, para $q = p^n$, $\mathbb{F}_{q^m} \cong \mathbb{F}_q[x]/(f)$, onde $f$ é um polinômio irredutível de grau $m$ sobre $\mathbb{F}_q$. Assim, um elemento em $\mathbb{F}_{q^m}$ pode ser representado por um polinômio em $\mathbb{F}_q[x]$ de grau menor que $m$.

**Exemplo:** Como $f(x) = x^2 + x + 1$ tem grau 2 e não possui raízes em $\mathbb{F}_2$, $f$ é irredutível sobre $\mathbb{F}_2$. Temos que $\mathbb{F}_4$ e $\mathbb{F}_2[x]/(f)$ são isomorfos. Os elementos de $\mathbb{F}_4$, representados em termos de polinômios, são 0, 1, $x$ e $x+1$. As tabelas completas de adição e de multiplicação para $\mathbb{F}_4$ são:



## Exemplo: $\mathbb{F}_4$

| $+$ | $0$ | $1$ | $x$ | $x+1$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $x$ | $x+1$ |
| $1$ | $1$ | $0$ | $x+1$ | $x$ |
| $x$ | $x$ | $x+1$ | $0$ | $1$ |
| $x+1$ | $x+1$ | $x$ | $1$ | $0$ |

| $\cdot$ | $0$ | $1$ | $x$ | $x+1$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $x$ | $x+1$ |
| $x$ | $0$ | $x$ | $x+1$ | $1$ |
| $x+1$ | $0$ | $x+1$ | $1$ | $x$ |

□

Podemos substituir $x$ por um elemento $a$ em $\mathbb{F}_4$ (mas não em $\mathbb{F}_2$!) desde que as regras de operação sejam como nas tabelas acima.

$\mathbb{F}_2$ esta contido em $\mathbb{F}_4$ (ver primeira e segunda linha e coluna).

A seguinte tabela mostra a adição e a multiplicação em $\mathbb{F}_8$ visto como $\mathbb{F}_2[x]/(x^3+x+1)$. O polinômio $x^3+x+1$ é irredutível sobre $\mathbb{F}_2$, pois tem grau 3 e não possui raízes em $\mathbb{F}_2$.

Observação: nas tabelas a seguir eliminamos as colunas do 0 e do 1 para que caibam na pÃ¡gina.

Verificar que $\mathbb{F}_2$ está contido em $\mathbb{F}_8$, mas $\mathbb{F}_4$ não está contido em $\mathbb{F}_8$!



# Exemplo: $\mathbb{F}_8$

| $+$ | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $x^2+x+1$ |
|---|---|---|---|---|---|---|
| 0 | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $x^2+x+1$ |
| 1 | $x+1$ | $x$ | $x^2+1$ | $x^2$ | $x^2+x+1$ | $x^2+x$ |
| $x$ | 0 | 1 | $x^2+x$ | $x^2+x+1$ | $x^2$ | $x^2+1$ |
| $x+1$ | 1 | 0 | $x^2+x+1$ | $x^2+x$ | $x^2+1$ | $x^2$ |
| $x^2$ | $x^2+x$ | $x^2+x+1$ | 0 | 1 | $x$ | $x+1$ |
| $x^2+1$ | $x^2+x+1$ | $x^2+x$ | 1 | 0 | $x+1$ | $x$ |
| $x^2+x$ | $x^2$ | $x^2+1$ | $x$ | $x+1$ | 0 | 1 |
| $x^2+x+1$ | $x^2+1$ | $x^2$ | $x+1$ | $x$ | 1 | 0 |

| $\cdot$ | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $x^2+x+1$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $x^2+x+1$ |
| $x$ | $x^2$ | $x^2+x$ | $x+1$ | 1 | $x^2+x+1$ | $x^2+1$ |
| $x+1$ | $x^2+x$ | $x^2+1$ | $x^2+x+1$ | $x^2$ | 1 | $x$ |
| $x^2$ | $x+1$ | $x^2+x+1$ | $x^2+x$ | $x$ | $x^2+1$ | 1 |
| $x^2+1$ | 1 | $x^2$ | $x$ | $x^2+x+1$ | $x+1$ | $x^2+x$ |
| $x^2+x$ | $x^2+x+1$ | 1 | $x^2+1$ | $x+1$ | $x$ | $x^2$ |
| $x^2+x+1$ | $x^2+1$ | $x$ | 1 | $x^2+x$ | $x^2$ | $x+1$ |

# Estruturas e Propriedades dos Corpos Finitos



## Corpos Finitos

Seja $F$ um corpo onde $\#F = q < \infty$. Então $F$ é um corpo finito e $q$ é a *ordem* de $F$.

**Teorema**

*A característica de um corpo finito é prima.*

**Demonstração.**

Existem inteiros $m$ e $n$ tais que $1 \leq m < n$ e $n \cdot 1 = m \cdot 1$. Portanto, $(n-m) \cdot 1 = 0$ e, logo, $F$ tem característica positiva. Suponhamos que $\mathrm{car}(F) = ab$ com $1 < a, b < \mathrm{car}(F)$. Então $(a \cdot 1)(b \cdot 1) = 0$. Como $F$ é um corpo, temos que $a \cdot 1 = 0$ ou $b \cdot 1 = 0$, o que é uma contradição. □

Obs.: Se $\mathrm{car}(F) = p$, então $F$ contém uma cópia de $\mathbb{Z}_p$ $(= \mathbb{F}_p)$. Exemplo: $\mathbb{F}_2$ esta em $\mathbb{F}_{2^2}$.

## Corpos Finitos

Seja $F$ um corpo onde $\#F = q < \infty$. Então $F$ é um corpo finito e $q$ é a *ordem* de $F$.

**Teorema**

*A característica de um corpo finito é prima.*

**Demonstração.**

Existem inteiros $m$ e $n$ tais que $1 \leq m < n$ e $n \cdot 1 = m \cdot 1$. Portanto, $(n-m) \cdot 1 = 0$ e, logo, $F$ tem característica positiva. Suponhamos que $\mathrm{car}(F) = ab$ com $1 < a, b < \mathrm{car}(F)$. Então $(a \cdot 1)(b \cdot 1) = 0$. Como $F$ é um corpo, temos que $a \cdot 1 = 0$ ou $b \cdot 1 = 0$, o que é uma contradição. □

Obs.: Se $\mathrm{car}(F) = p$, então $F$ contém uma cópia de $\mathbb{Z}_p$ $(= \mathbb{F}_p)$. Exemplo: $\mathbb{F}_2$ esta em $\mathbb{F}_{2^2}$.



## Corpos Finitos

Seja $F$ um corpo onde $\#F = q < \infty$. Então $F$ é um corpo finito e $q$ é a *ordem* de $F$.

**Teorema**

*A característica de um corpo finito é prima.*

**Demonstração.**

Existem inteiros $m$ e $n$ tais que $1 \leq m < n$ e $n \cdot 1 = m \cdot 1$. Portanto, $(n-m) \cdot 1 = 0$ e, logo, $F$ tem característica positiva. Suponhamos que $\mathrm{car}(F) = ab$ com $1 < a, b < \mathrm{car}(F)$. Então $(a \cdot 1)(b \cdot 1) = 0$. Como $F$ é um corpo, temos que $a \cdot 1 = 0$ ou $b \cdot 1 = 0$, o que é uma contradição. □

Obs.: Se $\mathrm{car}(F) = p$, então $F$ contém uma cópia de $\mathbb{Z}_p$ $(= \mathbb{F}_p)$. Exemplo: $\mathbb{F}_2$ esta em $\mathbb{F}_{2^2}$.

**Teorema**

*Sejam $K$ um corpo finito de ordem $q$ e $F$ uma extensão finita de $K$ de grau $n$. Então, a ordem de $F$ é $q^n$.*

**Demonstração.**

Seja $\{\beta_1, \beta_2, \ldots, \beta_n\}$ uma base para o espaço vetorial $F$ sobre $K$. Qualquer elemento em $F$ tem uma expressão única da forma

$$a_1\beta_1 + a_2\beta_2 + \cdots + a_n\beta_n$$

com $a_1, a_2, \ldots, a_n \in K$. Há $q$ valores possíveis para cada $a_i$, logo o número total de elementos em $F$ é $q^n$. □

Em particular, se $F$ é um corpo finito de ordem $q$ e característica $p$, então $F$ contém o corpo $\mathbb{F}_p$ e $q = p^n$, onde $n$ é o grau da extensão de $F$ sobre $\mathbb{F}_p$.



**Teorema**

*Sejam $K$ um corpo finito de ordem $q$ e $F$ uma extensão finita de $K$ de grau $n$. Então, a ordem de $F$ é $q^n$.*

**Demonstração.**

Seja $\{\beta_1, \beta_2, \ldots, \beta_n\}$ uma base para o espaço vetorial $F$ sobre $K$. Qualquer elemento em $F$ tem uma expressão única da forma

$$a_1\beta_1 + a_2\beta_2 + \cdots + a_n\beta_n$$

com $a_1, a_2, \ldots, a_n \in K$. Há $q$ valores possíveis para cada $a_i$, logo o número total de elementos em $F$ é $q^n$. □

Em particular, se $F$ é um corpo finito de ordem $q$ e característica $p$, então $F$ contém o corpo $\mathbb{F}_p$ e $q = p^n$, onde $n$ é o grau da extensão de $F$ sobre $\mathbb{F}_p$.

## Duas perguntas naturais

⋆ Existe um corpo de ordem $p^n$ para cada primo $p$ e cada inteiro positivo $n$?

⋆ Se sim, ele é único?



## Duas perguntas naturais

⋆ Existe um corpo de ordem $p^n$ para cada primo $p$ e cada inteiro positivo $n$?

⋆ Se sim, ele é único?

Respostas: Sim, existe e é único (a menos de isomorfismos).
Precisamos de alguns resultados para provar esse teorema.

**Lema**

*Num corpo finito $F$ de ordem $q$, qualquer $a \in F$ satisfaz $a^q = a$.*

**Demonstração.**

Isto é trivial se $a = 0$. Caso contrário, como $F^* = F \setminus \{0\}$ é um grupo multiplicativo de ordem $q - 1$, segue que $a^{q-1} = 1$ para todo $a \neq 0$. □

Então, se $a \neq 0$, $a^{q-1} = 1$ para todo $a \in \mathbb{F}_q$.

**Definição**

*Sejam $F$ e $K$ corpos, onde $F$ é uma extensão de $K$. O corpo $F$ é um corpo de decomposição do polinômio $f \in K[x]$, se $f$ é um produto de fatores lineares em $F[x]$ e se $f$ não é um produto de fatores lineares sobre qualquer subcorpo próprio de $F$ contendo $K$.*



**Lema**

*Num corpo finito $F$ de ordem $q$, qualquer $a \in F$ satisfaz $a^q = a$.*

**Demonstração.**

Isto é trivial se $a = 0$. Caso contrário, como $F^* = F \setminus \{0\}$ é um grupo multiplicativo de ordem $q - 1$, segue que $a^{q-1} = 1$ para todo $a \neq 0$. □

Então, se $a \neq 0$, $a^{q-1} = 1$ para todo $a \in \mathbb{F}_q$.

**Definição**

*Sejam $F$ e $K$ corpos, onde $F$ é uma extensão de $K$. O corpo $F$ é um corpo de decomposição do polinômio $f \in K[x]$, se $f$ é um produto de fatores lineares em $F[x]$ e se $f$ não é um produto de fatores lineares sobre qualquer subcorpo próprio de $F$ contendo $K$.*

**Lema**

*Num corpo finito $F$ de ordem $q$, qualquer $a \in F$ satisfaz $a^q = a$.*

**Demonstração.**

Isto é trivial se $a = 0$. Caso contrário, como $F^* = F \setminus \{0\}$ é um grupo multiplicativo de ordem $q - 1$, segue que $a^{q-1} = 1$ para todo $a \neq 0$. □

Então, se $a \neq 0$, $a^{q-1} = 1$ para todo $a \in \mathbb{F}_q$.

**Definição**

*Sejam $F$ e $K$ corpos, onde $F$ é uma extensão de $K$. O corpo $F$ é um corpo de decomposição do polinômio $f \in K[x]$, se $f$ é um produto de fatores lineares em $F[x]$ e se $f$ não é um produto de fatores lineares sobre qualquer subcorpo próprio de $F$ contendo $K$.*



**Lema**

*Seja $F$ um corpo de ordem $q$ e característica $p$. Então o polinômio $x^q - x$ fatora-se em $F[x]$ como*

$$x^q - x = \prod_{a \in F} (x - a).$$

*Além disso, $F$ é um corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$.*

**Demonstração.**

O polinômio $x^q - x$ tem no máximo $q$ raízes em $F$. Pelo lema anterior, qualquer $a \in F$ é uma raiz de $x^q - x$ e assim $x^q - x$ fatora-se sobre $F$, mas isto não acontece sobre qualquer outro subcorpo de $F$. □

**Lema**

*Seja $F$ um corpo de ordem $q$ e característica $p$. Então o polinômio $x^q - x$ fatora-se em $F[x]$ como*

$$x^q - x = \prod_{a \in F} (x - a).$$

*Além disso, $F$ é um corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$.*

**Demonstração.**

O polinômio $x^q - x$ tem no máximo $q$ raízes em $F$. Pelo lema anterior, qualquer $a \in F$ é uma raiz de $x^q - x$ e assim $x^q - x$ fatora-se sobre $F$, mas isto não acontece sobre qualquer outro subcorpo de $F$. □



## Exemplos do lema

- $q = 2$: $x(x-1) = x^2 - x$;
- $q = 3$:
  $x(x-1)(x-2) = (x^2 - x)(x-2) = x^3 - 2x^2 - x^2 + 2x = x^3 - x$;
- $q = 4$: usando a tabela de $\mathbb{F}_4$ e o fato que a característica é 2 temos

$$\begin{aligned} & x(x-1)(x-a)(x-(a+1)) \\ = \; & (x^2 - x)(x^2 - ax - ax - x + a(a+1)) \\ = \; & (x^2 - x)(x^2 - x + a(a+1)) \\ = \; & x^4 - x^3 - x^3 + x^2 + a(a+1)x^2 - a(a+1)x \\ = \; & x^4 + (a(a+1) + 1)x^2 - a(a+1)x \\ = \; & x^4 - x. \end{aligned}$$

□

**Lema**

*Seja $F$ um corpo de característica $p$. Então, para qualquer inteiro $n \geq 0$, temos que $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.*

**Demonstração por indução.**

Para $n = 1$, observamos que todo coeficiente binomial $\binom{p}{i}$ com $0 < i < p$ na expansão de $(a+b)^p$ é zero, já que

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{i!} \equiv 0 \pmod{p}.$$

Segue da hipótese de indução que

$$(a+b)^{p^{n+1}} = ((a+b)^{p^n})^p = (a^{p^n} + b^{p^n})^p = a^{p^{n+1}} + b^{p^{n+1}}.$$

Portanto, $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ para todo $n \geq 0$. □



**Lema**

*Seja $F$ um corpo de característica $p$. Então, para qualquer inteiro $n \geq 0$, temos que $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.*

**Demonstração por indução.**

Para $n = 1$, observamos que todo coeficiente binomial $\binom{p}{i}$ com $0 < i < p$ na expansão de $(a+b)^p$ é zero, já que

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{i!} \equiv 0 \pmod{p}.$$

Segue da hipótese de indução que

$$(a+b)^{p^{n+1}} = ((a+b)^{p^n})^p = (a^{p^n} + b^{p^n})^p = a^{p^{n+1}} + b^{p^{n+1}}.$$

Portanto, $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ para todo $n \geq 0$. □

## Exemplo do lema

O lema é válido somente para potências da característica $p$ mas pode ser usado para simplificar os cálculos. Por exemplo, suponha que tenhamos que calcular $(a+b)^{33}$ em $\mathbb{F}_2$; então:

$$\begin{aligned}(a+b)^{33} &= (a+b)^{32}(a+b) = (a+b)^{2^5}(a+b)\\ &= \left(a^{2^5}+b^{2^5}\right)(a+b)\\ &= \left(a^{32}+b^{32}\right)(a+b)\\ &= a^{33}+a^{32}b+ab^{32}+b^{33}.\end{aligned}$$

□



## Existência e unicidade de corpos finitos

**Teorema**

*Para qualquer primo $p$ e qualquer inteiro positivo $n$, existe um corpo finito com $p^n$ elementos. Além disso, qualquer corpo finito com $p^n$ elementos é isomorfo ao corpo de decomposição de $x^{p^n}-x$ sobre $\mathbb{F}_p$.*

Demonstração.

Suponhamos $q=p^n$. Seja $F$ o corpo de decomposição de $x^q-x$ sobre $\mathbb{F}_p$. Todas as raízes de $x^q-x$ em $F$ são distintas. De fato,

$$\operatorname{mdc}(x^q-x,(x^q-x)') = \operatorname{mdc}(x^q-x, qx^{q-1}-1) = 1.$$

# Existência e unicidade de corpos finitos

**Teorema**

*Para qualquer primo $p$ e qualquer inteiro positivo $n$, existe um corpo finito com $p^n$ elementos. Além disso, qualquer corpo finito com $p^n$ elementos é isomorfo ao corpo de decomposição de $x^{p^n} - x$ sobre $\mathbb{F}_p$.*

Demonstração.
Suponhamos $q = p^n$. Seja $F$ o corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Todas as raízes de $x^q - x$ em $F$ são distintas. De fato,

$$\mathrm{mdc}(x^q - x, (x^q - x)') = \mathrm{mdc}(x^q - x, qx^{q-1} - 1) = 1.$$



Demonstração (cont.). Seja $S = \{a \in F : a^q = a\}$. Temos que

- $S$ tem $q$ elementos;
- $S$ é um subconjunto de $F$ que contém 0 e 1;
- se $a, b \in S$ então

$$(a - b)^q = a^q + (-b)^q = a^q - b^q = a - b$$

  implica que $a - b \in S$;
- para $b \neq 0$, temos

$$(ab^{-1})^q = a^q(b^q)^{-1} = ab^{-1},$$

  isto é, $ab^{-1} \in S$.

Logo $S$ é um corpo e contém todas as raízes de $x^q - x$. Portanto, $S = F$ e $F$ é um corpo finito com $q$ elementos.

Demonstração (cont.).
Para mostrar a unicidade, seja $F$ um corpo finito com $q = p^n$ elementos. Então, $F$ tem característica $p$ e contém $\mathbb{F}_p$ como um subcorpo primo. Então, $F$ é um corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Como quaisquer dois corpos de decomposição são isomorfos, completamos assim esta prova. □



## Outras caracterizações

**Teorema**

*Seja $q = p^n$. Se $f$ é um polinômio irredutível sobre $\mathbb{F}_p$ de grau $n$, então $\mathbb{F}_q \cong \mathbb{F}_p[x]/(f)$.*

**Teorema**

*Seja $f \in \mathbb{F}_q[x]$ irredutível sobre $\mathbb{F}_q$. Então, existe uma extensão simples de $\mathbb{F}_q$ sendo definida por uma raiz de $f$. Além disso, se $\theta$ é uma raiz de $f$, então $\mathbb{F}_q(\theta) \cong \mathbb{F}_q[x]/(f)$.*

## Outras caracterizações

**Teorema**

*Seja $q = p^n$. Se $f$ é um polinômio irredutível sobre $\mathbb{F}_p$ de grau $n$, então $\mathbb{F}_q \cong \mathbb{F}_p[x]/(f)$.*

**Teorema**

*Seja $f \in \mathbb{F}_q[x]$ irredutível sobre $\mathbb{F}_q$. Então, existe uma extensão simples de $\mathbb{F}_q$ sendo definida por uma raiz de $f$. Além disso, se $\theta$ é uma raiz de $f$, então $\mathbb{F}_q(\theta) \cong \mathbb{F}_q[x]/(f)$.*



## Subcorpos de um corpo finito

**Teorema**

*Seja $\mathbb{F}_q$ um corpo finito com $q = p^n$ elementos. Então, todo subcorpo de $\mathbb{F}_q$ tem ordem $p^m$, onde $m$ é um divisor positivo de $n$. Reciprocamente, se $m$ é um divisor positivo de $n$, então existe exatamente um subcorpo de $\mathbb{F}_q$ com $p^m$ elementos.*

Demonstração. Se $q = p^n$, então qualquer subcorpo $F$ de $\mathbb{F}_q$ tem ordem $p^m$ com $0 < m \leq n$. Se $[\mathbb{F}_q : F] = \ell$, então $p^n = (p^m)^\ell = p^{m\ell}$, e assim $m \mid n$.

# Subcorpos de um corpo finito

**Teorema**

*Seja $\mathbb{F}_q$ um corpo finito com $q = p^n$ elementos. Então, todo subcorpo de $\mathbb{F}_q$ tem ordem $p^m$, onde $m$ é um divisor positivo de $n$. Reciprocamente, se $m$ é um divisor positivo de $n$, então existe exatamente um subcorpo de $\mathbb{F}_q$ com $p^m$ elementos.*

Demonstração. Se $q = p^n$, então qualquer subcorpo $F$ de $\mathbb{F}_q$ tem ordem $p^m$ com $0 < m \leq n$. Se $[\mathbb{F}_q : F] = \ell$, então $p^n = (p^m)^\ell = p^{m\ell}$, e assim $m \mid n$.



Reciprocamente, se $m \in \mathbb{N}$ e $m \mid n$, temos que $(p^m - 1) \mid (p^n - 1)$ e assim

$$(x^{p^m-1} - 1) \mid (x^{p^n-1} - 1),$$

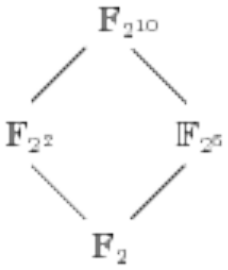
em $\mathbb{F}_p[x]$, i.e.

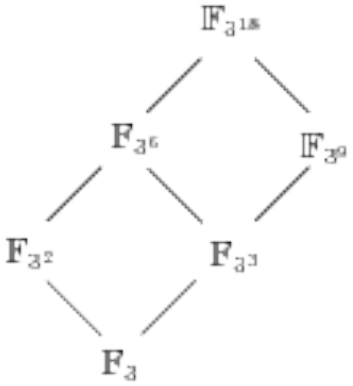
$$\{a \colon a^{p^m} - a = 0\} \subseteq \{a \colon a^{p^n} - a = 0\} = \mathbb{F}_q.$$

Logo $\mathbb{F}_q$ deve conter um corpo de decomposição de $x^{p^m} - x$ sobre $\mathbb{F}_p$. O resultado é então concluído pelo teorema de existência e unicidade de corpos finitos. □

Exemplos:

1. Como os divisores positivos de 10 são 1, 2, 5 e 10, os subcorpos de $\mathbb{F}_{2^{10}}$ são $\mathbb{F}_2$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^5}$ e $\mathbb{F}_{2^{10}}$.
2. $\mathbb{F}_{3^{18}}$ tem cinco subcorpos próprios: $\mathbb{F}_3$, $\mathbb{F}_{3^2}$, $\mathbb{F}_{3^3}$, $\mathbb{F}_{3^6}$ e $\mathbb{F}_{3^9}$.






## Elementos primitivos

**Teorema**

*O grupo multiplicativo de qualquer corpo finito $(\mathbb{F}_q^*, \cdot)$ é cíclico.*

**Definição**

*Um gerador de $\mathbb{F}_q^*$ é chamado um elemento primitivo.*

O teorema anterior fornece uma maneira conveniente de representar os elementos não nulos de um corpo finito: se $\alpha$ é um elemento primitivo de $\mathbb{F}_q$, então $\mathbb{F}_q^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$.

Para encontrarmos elementos primitivos, podemos usar o algoritmo de Gauss que é eficiente para $q$ pequeno. Este algoritmo fornece uma seqüência de elementos $\alpha_1, \alpha_2, \ldots, \alpha_i \in \mathbb{F}_q$ tais que

$$\mathrm{ord}(\alpha_1) < \mathrm{ord}(\alpha_2) < \cdots < \mathrm{ord}(\alpha_i) = q - 1.$$

Exemplo. O elemento $\gamma$ correspondente ao polinômio $1 + x$ é um elemento primitivo em $\mathbb{F}_{16} \cong \mathbb{F}_2[x]/(x^4 + x + 1)$:

| potência de $\gamma$ | polinômio |
|---|---|
| 1 | 1 |
| $\gamma$ | $x + 1$ |
| $\gamma^2$ | $x^2 + 1$ |
| $\gamma^3$ | $x^3 + x^2 + x + 1$ |
| $\gamma^4$ | $x$ |
| $\gamma^5$ | $x^2 + x$ |
| $\gamma^6$ | $x^3 + x$ |
| $\gamma^7$ | $x^3 + x^2 + 1$ |
| $\gamma^8$ | $x^2$ |
| $\gamma^9$ | $x^3 + x^2$ |
| $\gamma^{10}$ | $x^2 + x + 1$ |
| $\gamma^{11}$ | $x^3 + 1$ |
| $\gamma^{12}$ | $x^3$ |
| $\gamma^{13}$ | $x^3 + x + 1$ |
| $\gamma^{14}$ | $x^3 + x^2 + x$ |



Para ilustrarmos as operações aritméticas usando o elemento primitivo $\gamma$, calculamos:

1. $\gamma^7 \gamma^{14} = \gamma^{21} = \gamma^6$; isto é muito mais rápido do que calcular $[(x^3 + x^2 + 1)(x^3 + x^2 + x)] \pmod{x^4 + x + 1}$;
2. $(\gamma^{13})^{-1} = \gamma^{-13} = \gamma^2$; isto é muito mais rápido do que calcular $(x^3 + x + 1)^{-1} \pmod{x^4 + x + 1}$ usando o algoritmo euclideano estendido;
3. $\gamma^i = \gamma^3$ para todo $i$ tal que $i \equiv 3 \pmod{15}$; isto é muito mais rápido do que calcular $(x + 1)^{318} \pmod{x^4 + x + 1}$, por exemplo.

Porém, somas $\gamma^i + \gamma^j$ não são fáceis de calcular em corpos grandes.

Problema difícil: não se conhece um algoritmo de tempo polinomial para o problema de encontrar elementos primitivos.

Uma vez que encontramos tal $\alpha$, teremos encontrado todos os elementos primitivos, a saber, qualquer $\alpha^i$, onde $i$ e $q-1$ são relativamente primos. Há $\phi(q-1)$ elementos primitivos, onde $\phi$ é a função de Euler.

**Definição**

*A função de Euler é uma função $\phi\colon \mathbb{N} \to \mathbb{N}$, onde $\phi(n)$ é definido como sendo o número de inteiros $m$, $1 \leq m \leq n$, com a propriedade de que $m$ e $n$ são relativamente primos.*

**Exemplo**

*Em $\mathbb{F}_{13}$, temos que 2 é um elemento primitivo*

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 3, \quad 2^5 = 6, \quad 2^6 = 12,$$

$$2^7 = 11, \quad 2^8 = 9, \quad 2^9 = 5, \quad 2^{10} = 10, \quad 2^{11} = 7, \quad 2^{12} = 1.$$

*Temos que $\phi(12) = 4$ dado que 1, 5, 7 e 11 são coprimos com 12. Então há três outros elementos primitivos de $\mathbb{F}_{13}$ além de $2^1$: $2^5 = 6$, $2^7 = 11$ e $2^{11} = 7$. (Exercício: verificar que 6, 7 e 11 são elementos primitivos.)*



## Elementos normais

Podemos ver $\mathbb{F}_{q^n}$ como um espaço vectorial de dimensão $n$ sobre $\mathbb{F}_q$. Então, qualquer base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ pode ser usada para representar os elementos de $\mathbb{F}_{q^n}$.

Um elemento $\alpha \in \mathbb{F}_{q^n}$ é chamado normal se

$$\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$$

é uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Neste caso, a base é chamada uma base normal.

Os elementos $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ são chamados de conjugados de $\alpha$.

Convenção: definimos $\alpha_i = \alpha^{q^i}$ para todo $i = 0, 1, \ldots, n-1$.

## Exemplos

Os polinômios $x^3 + x + 1$ e $x^3 + x^2 + 1$ são irredutíveis sobre $\mathbb{F}_2$. Então, eles podem ser usados para construir $\mathbb{F}_{2^3}$. Seja $\alpha \in \mathbb{F}_{2^3}$. Consideremos primeiro $\alpha$ tal que $\alpha^3 + \alpha + 1 = 0$. Então,

$$\{\alpha, \alpha^2, \alpha^{2^2}\} = \{\alpha, \alpha^2, \alpha + \alpha^2\}.$$

Esse é um conjunto de 3 elementos em $\mathbb{F}_{2^3}$ que não é linearmente independente. Então, $\alpha$ não é um elemento normal em $\mathbb{F}_{2^3}$.

Consideremos agora $\alpha$ tal que $\alpha^3 + \alpha^2 + 1 = 0$. Então,

$$\{\alpha, \alpha^2, \alpha^{2^2}\} = \{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}.$$

Esses sim são linearmente independentes em $\mathbb{F}_{2^3}$, e assim $\alpha$ é um elemento normal em $\mathbb{F}_{2^3}$.



## O teorema da base normal

Teorema (Hensel 1888). Para qualquer $q$, potência de um número primo, e qualquer número inteiro positivo $n$, existe uma base normal para $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Esse teorema foi conjecturado por Eisenstein (1850) e parcialmente provado por Schönemann (1851). A prova completa é de Hensel (1888).

O teorema foi depois generalizado para qualquer extensão de Galois por Noether (1934). Independentemente, Ore (1934) provou esse resultado usando "linearized polynomials".

Foi também provada a existência de elementos ao mesmo tempo primitivos e normais. A prova é de Lenstra and Schoof (1986).

# A funcão traço

A soma e o produto dos conjugados de $\alpha$ produzem duas funcões especiais muito usadas em aplicacões.

**Definição**

*Para cada $\alpha \in \mathbb{F}_{q^m}$, a função traço de $\alpha$ sobre $\mathbb{F}_q$ é definida por*

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}.$$

Observamos que

$$\begin{aligned} f(x) &= (x-\alpha)(x-\alpha^q)\ldots(x-\alpha^{q^{n-1}}) \\ &= x^n - (\alpha + \alpha^q + \cdots + \alpha^{q^{n-1}})x^{n-1} + \cdots + (-1)^n \alpha\alpha^q \ldots \alpha^{q^{n-1}}, \end{aligned}$$

então $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = -a_{n-1}$.



**Teorema**

*Sejam $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$, $\alpha, \beta \in \mathbb{F}_{q^m}$ e $a, b \in \mathbb{F}_q$. Então,*

1. $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$;
2. $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\alpha + b\beta) = a\,\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) + b\,\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)$;
3. $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ *é uma transformacão linear de $\mathbb{F}_{q^m}$ em $\mathbb{F}_q$, onde $\mathbb{F}_{q^m}$ e $\mathbb{F}_q$ são vistos como espaços vetoriais sobre $\mathbb{F}_q$;*
4. $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) = ma$;
5. $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^q) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$.

A demonstração desta proposição fica como exercício.

Podemos definir o traço de $\mathbb{F}_{q^n}$ sobre um subcorpo $\mathbb{F}_{q^m}$:

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^m}}(x) = x + x^{q^m} + \cdots + \left(x^{q^m}\right)^{\frac{n-1}{m}}.$$

Quando temos uma cadeia de extensões de corpos, podemos calcular a composição de traços.

**Teorema**

*Seja $K$ um corpo finito, $F$ uma extensão de $K$ e $E$ uma extensão de $F$. Então, para $\alpha \in E$,*

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_{F/K}\left(\mathrm{Tr}_{E/F}(\alpha)\right).$$



Demonstração. Seja $K = \mathbb{F}_q$, $[F : K] = n$, $[E : F] = m$ e então $[E : K] = mn$. Para $\alpha \in E$ temos

$$\begin{aligned}\mathrm{Tr}_{F/K}\left(\mathrm{Tr}_{E/F}(\alpha)\right) &= \sum_{i=0}^{n-1}\left(\mathrm{Tr}_{E/K}(\alpha)\right)^{q^i} = \sum_{i=0}^{n-1}\left(\sum_{j=0}^{m-1}\alpha^{(q^n)^j}\right)^{q^i} \\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\alpha^{q^{nj+i}} = \sum_{k=0}^{mn-1}\alpha^{q^k} = \mathrm{Tr}_{E/K}(\alpha). \qquad \square\end{aligned}$$

A funcão traço $\mathrm{Tr}_{F/K}$ para uma extensão $F$ de $K$ é uma transformação linear de $F$ em $K$ que dá todas as possíveis transformações de $F$ em $K$ (funcionais lineares de $F$).

**Teorema**

*Seja $F$ um corpo, extensão finita do corpo finito $K$. As transformações lineares de $F$ em $K$ são funções $L_\beta$, $\beta \in F$, onde $L_\beta(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha)$ para todo $\alpha \in F$. Alem disso, temos $L_\beta \neq L_\gamma$ quando $\beta$ e $\gamma$ são elementos distintos de $F$.*

# A função norma

## Definição

*Para $\alpha \in \mathbb{F}_{q^n}$, a norma $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ sobre $\mathbb{F}_q$ é definida como*

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha\alpha^q \dots \alpha^{q^{n-1}} = \alpha^{\frac{q^n-1}{q-1}}.$$

Como para a função traço, se $f(x) = (x-\alpha)\dots(x-\alpha^{q^{n-1}}) = \sum_{i=0}^{n} a_i x^i$, então

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = (-1)^n a_0.$$



## Teorema

*A função norma de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ satisfaz*

(a) $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha\beta) = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta)$ *para todo* $\alpha, \beta \in \mathbb{F}_{q^n}$;

(b) $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ *leva* $\mathbb{F}_{q^n}$ *em* $\mathbb{F}_q$ *e* $\mathbb{F}_q^*$ *em* $\mathbb{F}_q^*$;

(c) $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha^n$, *para todo* $\alpha \in \mathbb{F}_q$;

(d) $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^q) = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$, *para todo* $\alpha \in \mathbb{F}_{q^n}$.

(e) *Transitividade da norma: Se $K$ é uma extensão de um corpo finito $K$ e $E$ é uma extensão de um corpo finito $F$, então* $\mathrm{N}_{E/K}(\alpha) = \mathrm{N}_{F/K}\left(\mathrm{N}_{E/F}(\alpha)\right)$, *para todo* $\alpha \in E$.

Demonstração deixada como exercício.