

1 Corpos finitos

Os corpos finitos são fundamentais em várias áreas da matemática e da ciência da computação, incluindo teoria dos números, geometria algébrica, teoria de Galois, geometria finita, criptografia e teoria de codificação.

Nosso objetivo nessas notas será definir e caracterizar os corpos finitos.

Relembraremos o seguinte:

Exemplo 1. O anel $F_p = \mathbb{Z}/\mathbb{Z}_p$ é um corpo finito. De fato, os elementos em $\mathbb{Z}/\mathbb{Z}_p$ são os inteiros resto da divisão por p $\{0, \dots, p-1\}$, é claro que $\mathbb{Z}/\mathbb{Z}_p$ é um anel comutativo com unidade, e seja $a \in \mathbb{Z}/\mathbb{Z}_p$, vamos provar que a admite inverso multiplicativo. Pelo *pequeno teorema de Fermat* temos que para todo $a \in \mathbb{Z}/\mathbb{Z}_p$, vale que $a^{p-1} = 1$ (em $\mathbb{Z}/\mathbb{Z}_p$). Assim, $a \cdot a^{p-2} = 1$ e portanto $a^{-1} = a^{p-2}$. Assim, $\mathbb{Z}/\mathbb{Z}_p$ é um corpo, que denotaremos por $\mathbb{F}_p$.

Em um corpo finito F , para todo elemento $a \in F$, existirá $m \in \mathbb{Z}$ positivo, tal que $m \cdot a := \underbrace{a + \dots + a}_{m \text{ vezes}} = 0$. Isto motiva a seguinte definição.

Definição 1. Seja F um corpo. Chamamos de **característica de F** o menor inteiro m tal que $m \cdot a = 0$ para todo $a \in F$, e denotamos $\text{char}(F) = m$. Caso este inteiro não exista diremos que F possui característica zero, e escreveremos $\text{char}(F) = 0$.

Nosso objetivo será entender quais os possíveis valores para a característica de um corpo, para isso vamos investigar a relação do anel dos inteiros com corpos. Seja F um corpo. Considere o homomorfismo $f : \mathbb{Z} \rightarrow F$ tal que $f(n) = n \cdot 1_F$. É claro que f é um homomorfismo e temos duas possibilidades:

Caso 1: f é injetivo Neste caso $\mathbb{Z}$ pode ser mergulhado em F , e $\mathbb{Q}$ também pode ser mergulhado em F . De tado, defina $g : \mathbb{Q} \rightarrow F$ tal que $g(\frac{a}{b}) = f(a)f(b)^{-1}$. É claro que g é injetivo, e portanto $\mathbb{Q}$ pode ser mergulhado em F . Veremos agora que $\text{Char}(F) = 0$. De fato, como $\mathbb{Q}$ é subcorpo de F segue que não existe inteiro tal que n tal que $n \cdot 1_F = 0$, e portanto $\text{Char}(F) = 0$.

Caso 2: f não é injetivo Neste caso, $\ker f$ é um ideal de $\mathbb{Z}$ e como $\mathbb{Z}$ é domínio de ideais principais, segue que existe $m \in \mathbb{Z}$ tal que $\ker f = (m)$.

Vamos ver que m é um número primo. De fato, suponha que existam $a, b \in \mathbb{Z}$ tal que $m = ab$. Assim, $0 = f(m) = f(a)f(b)$ em F , logo $f(a) = 0$ ou $f(b) = 0$, sem perda de generalidade suponha $f(a) = 0$. Assim $a \in (m)$, logo m divide a logo $m \leq a$ e como $m = ab$ segue que $m \geq a$, então $a = m$, e $b = 1$, e portanto m é primo. Veremos agora que $\text{Char}(F) = m$. De fato, seja $n = \text{char}(F)$. Por definição $n \cdot 1_F = 0$ e assim $n \in \ker f = (m)$ assim m/n , como $m \cdot 1_F = 0$, temos pela minimalidade de $\text{char}(F)$ que $m = n$.

Isto mostra em particular que a característica de um corpo ou é zero, ou é prima.

Assim temos o seguinte resultado.

Teorema 2. *Seja F um corpo. Então a característica de F é zero, e neste caso $\mathbb{Q} \subset F$, ou é um número primo e neste caso $\mathbb{F}_p \subset F$. Em particular, se F é um corpo finito, então $\text{char}(F) = p$, para algum primo p .*

Nosso próximo objetivo será estudar quais os possíveis número de elementos que um corpo finito possui. Para isso, precisaremos da noção de extensão de corpos.

Teorema 3. *Sejam F um corpo finito, e p um número primo tal que $p = \text{char}(F)$. Então $|F| = p^n$ para algum n inteiro positivo.*

Demonstração. Seja F um corpo finito. Temos que existe p um número primo, tal que $p = \text{char}(F)$. Além disso temos que $F|\mathbb{F}_p$ é uma extensão de corpos, e daí segue que $\dim_{\mathbb{F}_p} F = [F : \mathbb{F}_p]$. Seja $n := [F : \mathbb{F}_p] = \dim_{\mathbb{F}_p} F$. Como F é um conjunto de cardinalidade finita, a dimensão n de F sobre $\mathbb{F}_p$ é finita. Se $\{v_1, \dots, v_n\}$ é uma base de F sobre $\mathbb{F}_p$ então todo elemento de F pode ser escrito de maneira única como $a_1 v_1 + \dots + a_n v_n$ com $a_1, \dots, a_n \in \mathbb{F}_p$. Como existem exatamente p escolhas para todo a_i segue que $|F| = p^n$. $\square$

Em particular, por exemplo, não existem corpos de cardinalidade 12 (pois 12 não é uma potência de um primo).

A próxima pergunta natural que gostaríamos de responder é a seguinte, dados p um número primo, e n um número inteiro positivo, é possível construir um corpo com p^n elementos?

Nossa ideia para construir um corpo com p^n elementos será realizá-lo como corpo de adjunção de alguns elementos.

Teorema 4. *Sejam p um primo e $n \geq 1$. Então existe um corpo $\mathbb{F}_{p^n}$ com p^n elementos.*

Demonstração. Seja $\overline{\mathbb{F}_p}$ o fecho algébrico de $\mathbb{F}_p$. Considere o conjunto

$$\mathbb{F}_{p^n} := \{x \in \overline{\mathbb{F}_p} : x^{p^n} = x\}$$

. Vamos mostrar que $\mathbb{F}_{p^n}$ é um corpo. Para verificar isso, os pontos essenciais a se checar são se $\mathbb{F}_{p^n}$ é fechado sob multiplicação, adição e inversa multiplicativa;

- Adição: Sejam $x, y \in \mathbb{F}_{p^n}$. Então $(x+y)^{p^n} = x+y$ pelo teorema “sonho do estudante” (Lembre que $x^{p^n} = x$ e que $y^{p^n} = y$).
- Multiplicação: Sejam $x, y \in \mathbb{F}_{p^n}$. Então $(xy)^{p^n} = xy$ isto é claro pela comutatividade de $\overline{\mathbb{F}_p}$.
- Inverso multiplicativo: Seja $x \in \mathbb{F}_{p^n}$. Vamos mostrar que x^{-1} (que existe em $\overline{\mathbb{F}_p}$) está em $\mathbb{F}_{p^n}$. Mas como $(x^{-1})^{p^n} = (x^{p^n})^{-1} = x^{-1}$ Para ver que $\mathbb{F}_{p^n}$ possui p^n elementos, note que $\mathbb{F}_{p^n}$ foi construído de modo a ser o conjunto das raízes de $f(t) = t^{p^n} - t$. Como $f'(t) = -1$ em $\mathbb{F}_{p^n}$, segue que $f(t)$ não possui raízes repetidas, logo, $|\mathbb{F}_{p^n}| = p^n$

□

A próxima pergunta que gostaríamos de responder é a seguinte, se F é outro corpo com p^n elementos qual a relação de F e $\mathbb{F}_{p^n}$?

Teorema 5. *Quaisquer dois corpos de ordem p^n são isomorfos*

Demonstração. Seja F um corpo com p^n elementos. Então $F|\mathbb{F}_p$ é uma extensão finita de corpos. Seja $\overline{\mathbb{F}_p}$ o fecho algébrico de $\mathbb{F}_p$ então $\overline{\mathbb{F}_p}$ também é um fecho algébrico para F . Seja $\varphi: F \rightarrow \overline{\mathbb{F}_p}$ um homomorfismo de corpos,

Afirmção : $\varphi(F) \subseteq \mathbb{F}_{p^n}$

Para isso é suficiente mostrar que $\varphi(x)^{p^n} = \varphi(x)$ para todo $x \in F$, mas então é suficiente mostrar que $x^{p^n} = x$ para todo $x \in F$. A igualdade é óbvia se $x = 0$. Para $x \neq 0$, queremos mostrar que $x^{p^n-1} = 1$. Mas como $F^* := F \setminus \{0\}$ é um grupo abeliano multiplicativo de ordem $p^n - 1$, temos pelo Teorema de Lagrange que a ordem de qualquer elemento de F^* divide a ordem de F^* que é $p^n - 1$. Assim para todo $x \in F^*$ existe m tal que $x^m = 1$ e $m/p^n - 1$, logo $x^{p^n-1} = 1$. E portanto $\varphi(F) \subseteq \mathbb{F}_{p^n}$. Logo $\varphi : F \rightarrow \mathbb{F}_{p^n}$ é um homomorfismo injetivo, e como $|F| = |\mathbb{F}_{p^n}| = p^n$, segue que φ é um isomorfismo. $\square$

Pergunta: Você consegue pensar em um corpo de característica positiva que seja infinito? Dica: Corpos algebricamente fechados podem ser finitos? Se não, qual é a característica do fecho algébrico de um corpo de característica positiva?