Apêndice: Corpos Finitos

Um *corpo* é, grosso modo, um conjunto no qual podemos somar, subtrair, multiplicar e dividir por não nulo, no qual valem todas as propriedades usuais de tais operações, incluindo a comutativa da adição e da multiplicação. Exemplos de corpos são os racionais Q, os reais R, os complexos C e o conjunto dos inteiros vistos módulo p primo Z/pZ. Exemplos de conjuntos que não são corpos são os inteiros Z, os polinômios com coeficientes em R (estes dois exemplos são *anéis*), as matrizes quadradas de ordem n e o conjunto dos inteiros vistos módulo n composto Z/nZ.

Aqui, discutimos a existência de corpos finitos de ordem q. A *ordem* de um corpo finito é o seu número de elementos. A demonstração dada aqui é longa (e acho que daria um outro artigo e uma outra aula!), mas eu achei bastante bonita e instrutiva, de modo que julgo que vale a pena escrevê-la neste longo apêndice

Teorema 0.1. *Existem corpos de ordem q se, e somente se, q é uma potência de primo.*

Além disso, todos os corpos finitos de mesma ordem são isomorfos, isto é, para cada par de corpos K_1, K_2 de mesma ordem existe uma bijeção $\phi\colon K_1 \to K_2$, chamada *isomorfismo*, que mantém a estrutura algébrica dos corpos, ou seja, $\phi(xy) = \phi(x)\phi(y)$ e $\phi(x+y) = \phi(x) + \phi(y)$. Mas não demonstraremos isso aqui, a não ser para Z/pZ.

Demonstração

Demonstraremos esse fato com o auxílio de alguns lemas.

Lembre da definição de espaço vetorial que demos na seção sobre Álgebra Linear.

Lema 0.1. *Sejam $K \subset L$ corpos. Então L é um espaço vetorial sobre K.*

Demonstração

Fica para você, leitor. É só verificar que valem as propriedades da definição. ∎

Lema 0.2. *Seja F um corpo finito de q elementos e $F \subset K$, sendo K outro corpo finito. Então K tem q^n elementos, onde n é a dimensão do espaço vetorial de K sobre F.*

Demonstração

Sendo K e F finitos, a dimensão de K sobre F é claramente finita. Seja $\{u_1, u_2, \ldots, u_n\}$ uma base de K. Há q^n elementos em K: as expressões do tipo $\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$ (cada α_i pode ser escolhido de q maneiras). ∎

Antes de continuar, mais uma definição.

Definição 0.1. *A característica de um corpo K é o menor número inteiro positivo m tal que, sendo $a \in K$, $ma = \underbrace{a + a + \cdots + a}_{m \text{ vezes}} = 0$. Se tal m não existir, a característica do corpo é definida como zero.*

Por exemplo, Z/pZ é um corpo de característica p.

Agora, veremos porque corpos têm ordem potência de primo e não potência perfeita.

Lema 0.3. *A característica de um corpo é primo ou zero.*

Demonstração

Seja $m \neq 0$ a característica de um corpo. Seja 1 a unidade desse corpo e suponha que $m = pq$, p, q inteiros maiores que 1 (observe que se trocarmos a unidade 1 por outro elemento a do corpo, temos $ma = 0 \iff ma \cdot a^{-1} = 0 \iff m1 = 0$, ou seja, não perdemos generalidade). Ao desenvolvermos o produto

$$p1 \cdot q1 = \underbrace{(1 + 1 + \cdots + 1)}_{p \text{ vezes}} \cdot \underbrace{(1 + 1 + \cdots + 1)}_{q \text{ vezes}}$$

obtemos $m = pq$ uns. Logo $m1 = p1 \cdot q1 = 0 \iff p1 = 0$ ou $q1 = 0$, o que um absurdo, já que m é mínimo. ∎

Lema 0.4. *Seja p primo. Todos os corpos de ordem p são isomorfos a Z/pZ.*

Demonstração

Seja K um corpo de ordem p e 1 a sua unidade. Observe que, sendo K finito, admite característica finita, que só pode ser p. Defina o isomorfismo $\phi\colon Z/pZ \to K$, $\phi(m) = m1$ (somamos m vezes a unidade em K). Se $m1 = n1$ então $(m-n)1 = 0 \iff p | m - n \iff m = n$, pois $-p < m - n < p$. Logo os p números $0 \cdot 1 = 0$, 1, $2 \cdot 1, \ldots, (p-1)1$ são distintos e são os elementos de K. Logo ϕ é uma bijeção. Imitando a demonstração do lema anterior, podemos provar que ϕ mantém a estrutura algébrica de Z/pZ. Logo K e Z/pZ são isomorfos. ∎

Lema 0.5. *Seja F um corpo finito. Então F tem ordem potência de primo.*

Demonstração

Sendo o corpo finito, então admite característica finita: não é possível que se somarmos a unidade m vezes sempre resulte um número diferente; assim $m1 = t1$ para $m < t$. Daí, $(m-t)1 = 0$, ou seja, F tem uma característica (que é um divisor primo de $m - t$).

Seja p a característica de F. Usando a definição de ϕ do lema anterior, construímos um subcorpo $F_0 \subset F$ isomorfo a Z/pZ. Do lema 0.2, F tem p^n elementos, sendo n a dimensão de F sobre F_0. ∎

Pois bem, provamos a ida. Mas quem garante a existência de corpos finitos de ordem igual a **qualquer** potência de primo? Vamos construir um corpo de ordem p^n, p primo.

Uma maneira de construir um corpo de ordem p^n (que é utilizada para construir os corpos utilizados em códigos) é tomarmos um polinômio $p(x)$ irredutível de grau n com coeficientes em Z/pZ e tomarmos como elementos desse corpo os polinômios visto $\operatorname{mód} p(x)$. A soma é a soma de polinômios e é claro que valem todas as propriedades usuais de adição e multiplicação. E a divisão? Pelo teorema de Bezóut, para $q(x) \not\equiv 0$ (mód. $p(x)$) existem polinômios $a(x)$ e $b(x)$ tais que $a(x) \cdot q(x) + b(x) \cdot p(x) = 1$. Vendo $\operatorname{mód} p(x)$ nota-se que $a(x) = \big(q(x)\big)^{-1}$, de modo que qualquer elemento não nulo admite inverso.

Perceba agora que a existência do corpo depende unicamente da existência de polinômios irredutíveis de grau arbitrário em Z/pZ. Para isso usamos o

Lema 0.6. *Existem polinômios irredutíveis de grau arbitrário em Z/pZ.*

Demonstração

A prova que daremos aqui é combinatória! Contaremos o número a_n de polinômios irredutíveis em Z/pZ de grau n, utilizando algumas técnicas de contagem. Depois é só provar que $a_n > 0$ sempre.

Em [3], foi demonstrado que certos anéis são domínios de fatoração única

Considere todos os polinômios mônicos $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ de grau n, $a_i \in Z/pZ$, $i = 0, 1, \ldots, n-1$. Há p escolhas para cada a_i, logo há p^n polinômios desse tipo. Cada polinômio $p(x)$ fatora unicamente em irredutíveis. Suponha que m_i desses polinômios têm grau i, $i = 1, 2, \ldots, n$. Somando os graus dos fatores irredutíveis, obtemos $m_1 + 2m_2 + \cdots + nm_n = n$.

Observando do lado dos polinômios irredutíveis, podemos escolher m_k de a_k polinômios irredutíveis, permitindo repetições. O número de tais escolhas é igual ao número de soluções inteiras de $x_1 + x_2 + \cdots + x_{a_k} = m_k$, que é $\binom{m_k + a_k - 1}{m_k}$. Assim, todos os possíveis produtos de m_1 fatores irredutíveis de grau 1, m_2 fatores irredutíveis de grau 2, etc, são em total de

$$\prod_{1 \le k \le n} \binom{m_k + a_k - 1}{m_k}$$

Assim, considerando todas as soluções possíveis de $m_1 + 2m_2 + \cdots + nm_n = n$, temos todas as fatorações de todos os p^n polinômios, ou seja,

$$\sum_{m_1 + 2m_2 + \cdots + nm_n = n} \prod_{1 \le k \le n} \binom{m_k + a_k - 1}{m_k} = p^n \qquad (*)$$

Isso já define uma recorrência para a_n, mas muito complicada. Calculemos valores pequenos para $p = 2$: de

$$\begin{aligned} a_1 &= 2 \\ a_2 + \binom{a_1 + 1}{2} &= 4 \\ a_3 + a_1 a_2 + \binom{a_1 + 2}{3} &= 8 \\ a_4 + a_1 a_3 + \binom{a_2 + 1}{2} + \binom{a_1 + 3}{4} &= 16 \end{aligned}$$

obtemos $a_1 = 2$, $a_2 = 1$, $a_3 = 2$ e $a_4 = 3$.

Vamos simplificar significantemente essa recorrência, encontrando, eventualmente, uma fórmula fechada ppara a_n.

Utilizaremos agora um pouco de funções geratrizes. Você pode encontrar km

$$^{k} = \frac{1}{1 - pt}$$

Colocamos um apóstrofo para indicar que a soma é sobre seqüências com um número finito de termos não nulos.

Agora, o ponto crucial de nossos cálculos. Vamos classificar os termos da forma $\binom{m+a_k-1}{m}t^{km}$. Note que a soma acima é sobre **todas** as seqüências $(m_1, m_2, \ldots)$ com um número finito de termos não nulos. Seqüências desse tipo e produtórios como o que aparece acima caracterizam um desenvolvimento de um produto de somas. Por exemplo, vamos voltar nosso foco ao primeiro termo m_1 da seqüência. multiplicando termos da $\binom{m+a_1-1}{m}t^m$ (aqui trocamos m_1 por m). Logo

$$\begin{aligned}
&\sum_{(m_1,m_2,\ldots)}{}' \prod_{k\geq 1} \binom{m_k+a_k-1}{m_k} t^{km_k} \\
&= \binom{0+a_1-1}{0} t^0 \sum_{(m_2,\ldots)}{}' \prod_{k\geq 2} \binom{m_k+a_k-1}{m_k} t^{km_k} + \\
&\quad \binom{1+a_1-1}{2} t^1 \sum_{(m_2,\ldots)}{}' \prod_{k\geq 2} \binom{m_k+a_k-1}{m_k} t^{km_k} + \\
&\quad \binom{2+a_1-1}{2} t^2 \sum_{(m_2,\ldots)}{}' \prod_{k\geq 2} \binom{m_k+a_k-1}{m_k} t^{km_k} + \\
&\quad \ldots \\
&= \left(\binom{0+a_1-1}{0} t^0 + \binom{1+a_1-1}{1} t^1 + \binom{2+a_1-1}{1} t^2 + \cdots \right) \sum_{(m_2,\ldots)}{}' \prod_{k\geq 2} \binom{m_k+a_k-1}{m_k} t^{km_k} \\
&= \sum_{m\geq 0} \binom{m+a_1-1}{m} t^{m\cdot 1} \sum_{(m_2,\ldots)}{}' \prod_{k\geq 2} \binom{m_k+a_k-1}{m_k} t^{km_k}
\end{aligned}$$

Indutivamente, podemos concluir que

$$\sum_{(m_1,m_2,\ldots)}{}' \prod_{k\geq 1} \binom{m_k+a_k-1}{m_k} t^{km_k} = \prod_{k\geq 1} \sum_{m\geq 0} \binom{m+a_k-1}{m} t^{m\cdot k} = \frac{1}{1-pt}$$

Utilizando o conceito de binomial generalizado, ou seja,

$$\binom{a}{n} = \frac{a(a-1)\cdots(a-n+1)}{n!} \quad \text{para } a \text{ real e } n \text{ natural,}$$

temos

$$\begin{aligned}
\binom{m+a-1}{m} &= \frac{(m+a-1)(m+a-2)(m+a-3)\cdots a}{m!} \\
&= (-1)^m \frac{-a(-a-1)\cdots(-a-m+1)}{m!} = (-1)^m \binom{-a}{m}
\end{aligned}$$

e, pelo binômio de Newton generalizado,

$$\sum_{m\geq 0} \binom{m+a_k-1}{m} t^{m\cdot k} = \sum_{m\geq 0} (-1)^m \binom{-a_k}{m} (t^k)^m = (1-t^k)^{-a_k}$$

Logo

$$\prod_{k\geq 1} (1-t^k)^{-a_k} = \frac{1}{1-pt}$$

Poderíamos ter chegado nessa identidade um pouco mais rápido, na verdade. O Humberto Silva Naves e eu estávamos discutindo para ver se conseguíamos provar essa identidade sem fazer tanta conta e chegamos nesse atalho (valeu Humberto!): considere a soma $\sum_{i \geq 0} p^i t^i$. O termo em t^i indica a quantidade de polinômios mônicos de grau i, que são fatorados de forma única em irredutíveis mônicos. Assim, t^i é um marcador do grau dos polinômios. Agora, considere $(1 + t^k + t^{2k} + \cdots)^a_k$. Ao desenvolvermos esse produto, tomamos o termo t^{mk} do i-ésimo fator quando tomamos o i-ésimo irredutível de grau k (que são em total de a_k). Logo, considerando todos os graus,

$$\prod_{k \geq 1} (1 + t^k + t^{2k} + \cdots)^a_k = \sum_{i \geq 0} p^i t^i \iff \prod_{k \geq 1} (1 - t^k)^{-a_k} = \frac{1}{1 - pt}$$

Mas, de qualquer forma, é importante saber manipular algebricamente essas expressões, logo resolvi deixar os cálculos anteriores no artigo.

Uma maneira de transformar produtórios em somatórios é tirar logaritmos dos dois lados. Aqui, log indica logaritmo natural. Obtemos então

$$-\sum_{k \geq 1} a_k \log(1 - t^k) = -\log(1 - pt)$$

O desenvolvimento de $\log(1 - x)$ em série de potências é

$$\log(1 - x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots = \sum_{i \geq 1} \frac{x^i}{i}$$

Portanto

$$\sum_{k \geq 1} a_k \sum_{i \geq 1} \frac{t^{ik}}{i} = \sum_{i \geq 1} \frac{(pt)^i}{i}$$

Basta, agora, comparar os termos em t^n. No segundo membro é p^n/n. No primeiro, aparece sempre que $ik = n \iff i = n/k$, ou seja, quando k divide n. Logo

$$\sum_{k|n} \frac{a_k}{n/k} = \frac{p^n}{n} \iff \sum_{k|n} k a_k = p^n,$$

que é uma recorrência bem mais tratável. Vamos rever os casos pequenos que estudamos antes, com $p = 2$:

$$\begin{aligned} a_1 &= 2 \\ a_1 + 2a_2 &= 4 \\ a_1 + 3a_3 &= 8 \\ a_1 + 2a_2 + 4a_4 &= 16 \end{aligned}$$

Agora, provemos que $a_n > 0$. Considere a soma $\sum_{k|n} k a_k$. Fora $n a_n$, todos os outros no máximo $n - 1$ termos são menores que $q^{n/2}$, pois já apareceram em somas anteriores. Deste modo,

$$\sum_{k|n} k a_k < (n-1) q^{n/2} + n a_n \iff q^n < (n-1) q^{n/2} + n a_n \iff n a_n > q^{n/2}(q^{n/2} - n + 1) > 0$$

∎

Podemos encontrar uma fórmula fechada para a_n a partir da *fórmula de inversão de Möbius* (cuja demonstração pode ser encontrada em [5]):

$$f(n) = \sum_{d|n} g(d), \text{ para todo } n \in Z_+^* \iff g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right), \text{ para todo } n \in Z_+^*$$

onde

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \\ (-1)^r & \text{se } n \text{ é o produto de } r \text{ primos distintos} \\ 0 & \text{caso contrário} \end{cases}$$

é a *função de Möbius.*

Temos

$$a_n = \sum_{d|n} \mu(n) p^{n/d}$$

1. Referências bibliográficas

[1] I. N. Herstein. *Topics in Algebra*, Wiley. Um livro de Álgebra Abstrata para quem quer aprender o básico e mais um pouco dessa fascinante e importantíssima área da Matemática. Parte da demonstração do teorema sobre corpos finitos (a ida) foi retirada do Capítulo 7 (cujo título é “Selected Topics”!) deste livro.

[2] Peter J. Cameron. *Combinatorics: Topics, Techniques, Algorithms*, Cambridge Press. Um livro de Combinatória. Não o li o suficiente, mas a volta do teorema sobre corpos finitos foi retirada deste livro, do Capítulo 4, sobre recorrências e funções geratrizes.

[3] Guilherme Fujiwara. *Inteiros de Gauss e Inteiros de Eisenstein*, in: Revista Eureka! 14. Acho que é o primeiro artigo que fala de aplicações da Álgebra Abstrata fora dos tradicionais números módulo m. A referência [1] também fala de inteiros dde Gauss, mas essa referência é claramente mais acessível e mais didática, além de conter fatos bem mais interessante para o público “olímpico”.

[4] Eduardo Tengan. *Séries Formais*, in: Revista Eureka! 11. Um ótimo artigo para quem quer começar a estudar funções geratrizes. Lá tem um resultado importante sobre partições e um método para encontrar termos gerais de recorrências como, por exemplo, Fibonacci. Recomendo também o fantástico livro *Concrete Mathematics*, do grande Donald E. Knuth e, para calcular certos somatórios, o livro $A = B$, de Marko Petkovšek, Herbert S. Wilf e Doron Zeilberger. Aliás, este livro pode ser baixado em

`http://www.math.upenn.edu/~wilf/AeqB.pdf`

ou `http://www.math.temple.edu/~zeilberg/AeqB.pdf`

[5] José Plínio de Oliveira Santos. *Introdução à Teoria dos Números*, IMPA. Um bom livro introdutório para teoria dos números. Vai um pouco além de congruências, Euler-Fermat e raízes primitivaas, falando sobre funções aritméticas e partições.