Corpos estendidos no espaço em grupos

Carlos Shine

Vamos ver como conceitos de teoria dos números (especialmente números mod p) podem ser generalizados com conceitos de Álgebra.

1 Corpos

Em termos simples, corpos são conjuntos em que podemos somar, subtrair, multiplicar e dividir.

1.1 Definição

Um conjunto K munido das operações $+$ e $\cdot$ é um *corpo* quando:

- a operação $+$ é associativa, comutativa, tem elemento neutro 0 e oposto.
- a operação $\cdot$ é associativa, comutativa, tem elemento neutro 1 e inverso para todo elemento diferente do elemento neutro da adição.
- vale a distributiva da multiplicação com relação à adição.

Exemplos de corpos são $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e, especialmente, $\mathbb{Z}/p\mathbb{Z}$, os inteiros vistos módulo um primo p.

Exemplos de conjuntos que não são corpos são $\mathbb{Z}$, os inteiros módulo um composto e os polinômios com coeficientes em qualquer corpo.

1.2 Exercícios

1.1. Considere o conjunto $\mathbb{Z}/p\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}/p\mathbb{Z}\}$, em que p é primo e i é a unidade imaginária.

   (a) Mostre que se $p \equiv 3 \pmod 4$ então $\mathbb{Z}/p\mathbb{Z}[i]$ é um corpo.

   (b) Mostre que se $p \equiv 1 \pmod 4$ então $\mathbb{Z}/p\mathbb{Z}[i]$ não é um corpo.

   (c) O que acontece com o item anterior se trocarmos i por uma das "soluções" da congruência $x^2 = -1 \pmod p$? Por "solução" entendemos a solução em $\mathbb{Z}/p\mathbb{Z}$ se $p \equiv 1 \pmod 4$ e um símbolo formal se $p \equiv 3 \pmod 4$.

1.2. Seja $f(x)$ um polinômio de coeficientes racionais, irredutível em $\mathbb{Q}$. Sendo F o conjunto dos polinômios com coeficientes racionais vistos módulo $f(x)$ (ou seja, $P(x) \equiv Q(x) \pmod{f(x)} \iff f(x) \mid P(x) - Q(x)$), determine se F é um corpo.

1.3. O que acontece se, no exercício anterior, trocarmos os coeficientes de $\mathbb{Q}$ para $\mathbb{Z}/p\mathbb{Z}$? Considere o caso particular $f(x) = x^2 + 1$ e compare com o exercício 1.

2 Espaços vetoriais

Dado um corpo, podemos combinar elementos dele com outros conjuntos!

2.1 Definição

Dado um corpo K, um conjunto V munido de duas operações $+$ em V^2 (adição) e $\cdot$ em $K \times V$ (multiplicação por escalar) é um *espaço vetorial* sobre K quando, para todos $u, v \in V$ e α, β em K, $\alpha u + \beta v \in V$.

Os elementos de V são chamados *vetores* e os elementos de K são chamados *escalares*.

2.2 Combinações lineares, independência linear, base, dimensão

Espaços vetoriais, veremos em breve, funcionam bem com as chamadas *combinações lineares*, que são essencialmente uma extensão da conta $\alpha u + \beta v$ que vimos na definição: um vetor v é combinação linear de outros vetores $u_1, u_2, \ldots, u_m$ quando existem escalares $\alpha_1, \alpha_2, \ldots, \alpha_m$ tais que

$$v = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_m u_m.$$

Dada essa ideia, podemos definir *independência linear*: um conjunto de vetores $U = \{u_1, \ldots, u_k\}$ é *linearmente independente* (LI) quando nenhum dos elementos de U é combinação linear dos outros. Em outras palavras (ou, na verdade, símbolos): sendo $\alpha_1, \ldots, \alpha_k$ escalares, e $\vec{0}$ o vetor nulo,

$$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_k u_k = \vec{0} \iff \alpha_1 = \alpha_2 = \cdots = \alpha_k = 0.$$

Agora definiremos um conjunto que nos permite descrever espaços vetoriais de modo eficiente: primeiro, diremos que um conjunto W *gera* um espaço vetorial V quando todo elemento de V é combinação linear dos elementos de W. Se o conjunto W é também LI (ou seja, eliminamos as redundâncias), W é uma *base* de V. Com isso, podemos descrever os elementos de V a partir de uma de suas bases.

A quantidade de elementos de uma base de V é a *dimensão* de V. Por incrível que pareça, todas as bases de espaços vetoriais têm a mesma quantidade de elementos!

2.3 Exercícios

2.1. Mostre que $\mathbb{C}$ é um espaço vetorial sobre $\mathbb{R}$. Encontre uma base desse espaço vetorial.

2.2. Os polinômios com coeficientes em um corpo K formam um espaço vetorial sobre K? Se sim, determine sua dimensão.

2.3. Mostre que todas as bases de espaços vetoriais têm a mesma quantidade de elementos.

3 Extensões de corpos

Se um corpo K está contido em outro corpo L dizemos que K é um *subcorpo* de L. É bem fácil mostrar que, nesse caso, L é um espaço vetorial sobre KL (verifique!). Denotamos a dimensão desse espaço vetorial por $[L : K]$.

O seguinte teorema costuma ser bastante útil:

Teorema 1 (corpo intermediário)**.** *Se K, L e M são corpos com $K \subseteq L \subseteq M$ e $[L : K]$ e $[M : L]$ são finitos, então $[M : K]$ também é finito e*

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

Demonstração. Sejam $U = \{u_1, \ldots, u_m\}$ e $V = \{v_1, \ldots, v_n\}$ bases de L sobre K e M sobre L, respectivamente. Com isso, $[L : K] = m$ e $[M : L] = n$. Basta encontrar uma base de M sobre K com mn elementos.

Usando a definição de base, temos que todo elemento w de L pode ser escrito na forma

$$w = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_m u_m,$$

com $\alpha_1, \ldots, \alpha_m \in K$, e todo elemento x de M pode ser escrito na forma

$$x = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n,$$

com $\beta_1, \ldots, \beta_n \in L$.

Assim, para escrever $x \in M$ como combinação linear em K, podemos substituir as combinações lineares de β_i em L: sendo

$$\beta_i = \alpha_{i1}u_1 + \alpha_{i2}u_2 + \cdots + \alpha_{im}u_m,$$

temos

$$x = \sum_{i=1}^{n}\sum_{j=1}^{m} \alpha_{ij}v_iu_j,$$

e sendo $v_iu_j \in M$ e $\alpha_{ij} \in K$, escrevemos x como combinação linear de mn elementos de M, ou seja, o conjunto $B = \{v_iu_j, 1 \le i \le n, 1 \le j \le m\}$ gera M.

Falta provar que B é LI, ou seja, mostrar que nenhum elemento de B é combinação linear dos outros. Para isso, basta supor por absurdo: suponha, sem perdas, que

$$u_1v_1 = \sum_{i=2}^{n}\sum_{j=2}^{m} \theta_{ij}u_jv_i.$$

Lembrando que u_i, v_j são elementos de corpos, e que $u_i \neq 0$, podemos "isolar´´ v_1. Isso significa que v_1 pode ser escrito como combinação linear de $v_2, \ldots, v_n$ com coeficientes em L, o que contradiz a hipótese de que M é espaço vetorial sobre L.

Portanto B é base de M sobre K e a dimensão de M sobre K é

$$[M : K] = mn = [L : K] \cdot [M : L].$$

□

3.1 Extensões simples

Uma maneira de estender um corpo K (além de se deitar, é claro) é escolher um elemento $\zeta \notin K$ e obter o menor corpo $K(\zeta)$ que contém K e ζ. Isso é uma *extensão simples*. Nesse sentido, podemos dizer, por exemplo, que $\mathbb{C} = \mathbb{R}(i)$. Como podemos estender o corpo adicionando um elemento de cada vez, podemos só estudar extensões simples.

Polinômios acabam tendo um papel importante para descrever elementos dessas extensões.

Teorema 2 (Extensões simples algébricas)**.** *Seja K um corpo e $\zeta \notin K$ tal que existem um inteiro positivo n e elementos $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in K$ tais que*

$$\zeta^n = \alpha_0 + \alpha_1\zeta + \cdots + \alpha_{n-1}\zeta^{n-1}.$$

Em outras palavras, ζ é raiz de um polinômio f com coeficientes em K.

Suponha que f seja irredutível em K (se não for, fatore o polinômio em irredutíveis[1] e identifique aquele que tem ζ como raiz). Então os elementos de $K(\zeta)$ são os polinômios de grau menor ou igual a n. Dizendo de outra forma, tomamos os polinômios em K módulo f.

Demonstração. É imediato que podemos somar, subtrair e multiplicar módulo $f(x)$. Falta provar a existência de inverso para todo $g(x) \not\equiv 0 \pmod{f(x)}$.

Como f é irredutível em K, pelo teorema de Bézout, para qualquer polinômio g que não é divisível por K existem polinômios a e b tais que

$$a(x)f(x) + b(x)g(x) = 1 \implies b(x)g(x) \equiv 1 \pmod{f(x)}$$

e podemos tomar $b = g^{-1}$. □

Note também que $[K(\zeta) : K] = \partial f$, o grau de f.

Podemos resolver essas ferramentas para resolver alguns problemas bacanas de polinômios.

Exemplo 1. *Seja f um polinômio irredutível em $\mathbb{Q}$ e seja n seu grau. Sendo g um polinômio qualquer com coeficientes racionais, prove que todo fator irredutível de $f(g(x))$ tem grau múltiplo de n.*

[1] Pode-se provar que os polinômios em K têm fatoração única, mas isso fica para outra ocasião! Mas se você quiser pensar, comece definindo divisão euclidiana, prove Bezóut, defina mdc e chegue a algo equivalente ao teorema fundamental da aritmética.

Solução: Seja $p(x)$ um fator irredutível de $f(g(x))$ e α uma raiz de p. Seja também $\beta = g(\alpha)$. Note que $p \mid f \circ g \implies f(g(\alpha)) = 0 \iff f(\beta) = 0$, de modo que:

- $\beta = g(\alpha)$ quer dizer que $\beta = \sum a_n \alpha^n$, ou seja, $\beta \in \mathbb{Q}(\alpha)$. Isso implica $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$, pois qualquer combinação linear de β^i's pode ser escrita como uma combinação linear de α^j's.

- $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \partial p$ e $[\mathbb{Q}(\beta) : \mathbb{Q}] = n$.

Feito isso, o problema essencialmente acabou: temos $\mathbb{Q} \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$ e pelo teorema do corpo intermediário,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] \implies [\mathbb{Q}(\beta) : \mathbb{Q}] \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] \iff n \mid \partial p,$$

como queríamos demonstrar.

3.2 Exercícios

3.1. Nessa seção mostramos que se $K \subseteq L$ são corpos então L é um espaço vetorial sobre K. Prove que a recíproca não é verdadeira, ou seja, exiba um exemplo de espaço vetorial V sobre um corpo K tal que V não é um corpo.

3.2. Mostre que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ (para obter $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, estendemos colocando $\sqrt{2}$ e $\sqrt{3}$).

3.3. Seja $p(x) \in \mathbb{Z}[x]$ um polinômio mônico e irredutível tal que $|p(0)|$ não é quadrado perfeito. Prove que $p(x^2)$ é irredutível em $\mathbb{Q}$.

4 Grupos

Grupos têm regras mais simples do que corpos, mas por causa disso tem menos estrutura e os teoremas são um pouco mais complexos.

4.1 Definição

Um conjunto G munido de uma operação $*$ é um grupo se satisfaz as seguintes propriedades:

- (Fechado) para todos $a, b \in G$, $a * b \in G$;
- (Associativa) $a * (b * c) = (a * b) * c$ para todos $a, b, c \in G$;
- (Elemento neutro) existe $e \in G$ tal que $a * e = e * a = a$ para todo $a \in G$;
- (Inverso) para todo $a \in G$ existe $b \in G$ tal que $a * b = b * a = e$.

Note que não necessariamente vale $a * b = b * a$. Se isso acontece, dizemos que o grupo é *abeliano*. Temos vários exemplos de grupos:

- Inteiros com soma: note que $e = 0$ e o inverso de a é o oposto $-a$.
- Inteiros módulo n com soma.
- Inteiros módulo p primo, tirando $0 \bmod p$, com multiplicação.
- Matrizes quadradas inversíveis de mesmo tamanho com multiplicação.
- Conjuntos com a diferença simétrica $A \,\Delta\, B = (A \setminus B) \cup (B \setminus A)$.
- Funções bijetoras de A em A (permutações) com composição.

A partir de agora, para grupos gerais representaremos $a * b = ab$.

4.2 Subgrupos, coclasses, relações de equivalência e teorema de Lagrange

Se $H \subseteq G$ são grupos (com a mesma operação) dizemos que H é *subgrupo* de G. Dado um subgrupo H de G, e $a \in G$, definimos a *coclasse esquerda* por

$$aH = \{ah, h \in H\}.$$

Nem sempre o conjunto aH é um grupo. Por exemplo, usando a soma como operação, se $G = \mathbb{Z}$ e $H = 2\mathbb{Z}$ é o conjunto dos números pares, H é um subgrupo e $1H = \{1 + h, h \in H\}$ não é um grupo (de fato, a soma não é fechada nos ímpares).

As coclasses induzem uma *relação de equivalência*. Diremos que aH e bH são equivalentes quando $aH = bH$. Relações de equivalência são aquelas $\sim$ com as seguintes propriedades: $a \sim a$ (reflexiva) $a \sim b \iff b \sim a$ (simétrica) e $a \sim b$ e $b \sim c \implies a \sim c$ (transitiva). Relações de equivalência não aparecem somente em teoria dos grupos, mas induzem partições, em que elementos do mesmo conjunto estão relacionados.

Usando os inteiros $\mathbb{Z}$ com a soma, e o subgrupo $n\mathbb{Z}$ dos múltiplos de n, as partições são $m + n\mathbb{Z} = \{m + nk, k \in \mathbb{Z}\}$, ou seja, as classes de conguência módulo n! De fato, podemos até escrever, em geral, $aH = bH \iff a \equiv b \pmod{H}$.

Feito isso, podemos provar o seguinte teorema:

Teorema 3 (Lagrange)**.** *Sendo H um subgrupo de G, $|H|$ divide $|G|$.*

Demonstração. Considere a partição induzida por H. Todas as coclasses têm $|H|$ elementos pois $ah_1 = ah_2 \implies h_1 = h_2$ – basta aplicar o inverso de a à esquerda. Como G é a união disjunta de coclasses de H, $|H|$ divide $|G|$. □

4.3 Ordem, menor divide

Agora vamos trabalhar com grupos finitos. Seja e o elemento neutro de G. Dado um elemento $g \in G$, a *ordem* de g é o menor inteiro positivo k tal que $g^k = \underbrace{g \dots g}_{k\ g's} = e$.

Note que k sempre existe pois $g, g^2, g^3, \dots$ assume uma quantidade finita de valores, e ocorre $g^m = g^n$ para alguns $m > n$, e tomamos $k = m - n$.

O teorema do *menor divide* continua válido: se $g^n = e$ então a ordem de g divide n.

É bem fácil ver que o conjunto $\langle g \rangle = \{e, g, \dots, g^{k-1}\}$ é um grupo. Com isso, a ordem de g é a cardinalidade $|\langle g \rangle|$. Pelo teorema de Lagrange, essa ordem divide $|G|$. Logo temos

Teorema 4 ("Euler-Fermat")**.** *Para todo $g \in G$, $g^{|G|} = e$.* □

4.4 Relação com $\mathbb{Z}/p\mathbb{Z}$

Tomemos $G = \mathbb{Z}/p\mathbb{Z}^*$ com a multiplicação. Podemos traduzir alguns resultados da teoria dos números na linguagem de grupos:

- O último teorema nos dá $a^{p-1} \equiv 1 \pmod{p}$.
- Os resíduos quadráticos formam um grupo de tamanho $(p-1)/2$ (que divide $p - 1$). Isso é óbvio, mas $r^{(p-1)/2} \equiv 1 \pmod{p}$.
- Existe um elemento g tal que $\langle g \rangle = \mathbb{Z}/p\mathbb{Z}^*$ (raiz primitiva).

4.5 Usando em extensões de corpos

As coisas ficam mais interessantes quando trabalhamos com extensões de corpos. Para obter um grupo de um corpo, basta ignorar uma das operações do corpo!

Exemplo 2. *Considere os* inteiros de Gauss*, ou seja,* $\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\}$*. Usamos* [] *no lugar de* () *porque* $\mathbb{Z}[i]$ *não é um corpo (é um* anel*, que é tipo os inteiros – nem todo mundo tem inverso).*

Seja π *um primo de* $\mathbb{Z}[i]$*. Então os inteiros de Gauss módulo* π *formam um corpo.*

(a) Quantos elementos esse corpo tem?

(b) Enuncie o equivalente a Euler-Fermat nesse corpo.

Solução: Antes de ir para a solução em si, definimos a *norma* $N(\pi) = \pi \cdot \overline{\pi}$, e a divisão euclidiana da seguinte forma: sendo q o quociente e r o resto da divisão de a por b, $a = bq + r$, com $r = 0$ ou $N(r) < N(b)$. Pode-se provar que r é único nessa situação.

(a) Como $N(r)$ pode assumir os valores de 1 a $N(\pi) - 1$, a quantidade de elementos é no máximo $N(\pi) - 1$. Agora, considerando os inteiros (de Gauss) $1, 2, \ldots, N(\pi) - 1$, eles são distintos módulo π porque se $i \equiv j \pmod{\pi}$ então $\pi \mid i - j$ e $\overline{\pi} \mid \overline{i - j} \iff \overline{\pi} \mid i - j$, e sendo $\text{mdc}(\pi, \overline{\pi}) = 1$ (pois π é primo), temos $\pi\overline{\pi} \mid i - j \iff N(\pi) \mid i - j$. Como $|i - j| < N(\pi)$, $i = j$. Logo esse grupo tem $N(\pi) - 1$ elementos.

(b) $a^{N(\pi)-1} \equiv 1 \pmod{\pi}$.

Só para complementar, façamos um caso particular: seja $\pi = 2 + 3i$. Sendo $N(\pi) = 2^2 + 3^2 = 13$, acabamos de afirmar que os restos são $0, 1, 2, \ldots, 12$. Note que $13 \equiv 0 \pmod{2+3i}$ pois $13 = (2+3i)(2-3i) \implies 2 + 3i \mid 13$. Agora, podemos reduzir para inteiros racionais da seguinte forma: usamos primeiro $i(2 + 3i) = -3 + 2i$, que também é múltiplo de $2 + 3i$. Se $a + bi$ tem b par, subtraímos $(-3 + 2i)b/2$ de $a + bi$ e obtemos um inteiro racional; se $a + bi$ é ímpar, subtraímos $2 + 3i + (3 - 2i)(b - 3)/2$ de $a + bi$ e obtemos um inteiro racional.

Exemplo 3. *Faça o mesmo que o exemplo anterior para o corpo* $\mathbb{Z}/p\mathbb{Z}(\sqrt{2})$*. Suponha que* $\sqrt{2} \notin \mathbb{Z}/p\mathbb{Z}$ *(ou seja,* 2 *não é resíduo quadrático módulo* p*).*

Solução:

(a) Os elementos de $\mathbb{Z}/p\mathbb{Z}(\sqrt{2})$ são da forma $a + b\sqrt{2}$, com $a, b \in \mathbb{Z}/p\mathbb{Z}$. Em princípio, temos $p^2 - 1$ elementos no grupo multiplicativo (eliminamos o zero). Agora, $p \mid a + b\sqrt{2} - (c + d\sqrt{2}) \iff \exists k, \ell \in \mathbb{Z} : (a - c) + (b - d)\sqrt{2} = p(k + \ell\sqrt{2}) \iff p \mid a - c$ e $p \mid b - d \iff a = c$ e $b = d$, logo não há repetições.

(b) $a^{p^2-1} \equiv 1 \pmod{p}$.

4.6 Exercícios

4.1. Seja S a sequência definida por $S_0 = 4$ e $S_{k+1} = S_k^2 - 2$ para $k \geq 0$. Para $n > 2$, prove que $M_n = 2^n - 1$ é primo se, e somente se, S_{n-2} é múltiplo de M_n.[2]

4.2. (OBM 2017) Seja a inteiro positivo e p um divisor primo de $a^3 - 3a + 1$ com $p \neq 3$. Prove que p é da forma $9k + 1$ ou $9k - 1$, sendo k inteiro.

4.3. (IMO Shortlist 2003) A sequência $a_0, a_1, \ldots$ é definido por $a_0 = 2$, $a_{k+1} = 2a_k^2 - 1$ para $k \geq 0$. Prove que se um primo ímpar p divide a_n então 2^{n+3} divide $p^2 - 1$.

4.4. (IMO Shortlist 2004) Seja k um inteiro fixado maior do que 1, e defina $m = 4k^2 - 5$. Prove que existem inteiros positivos a e b tais que a sequência (x_k) definida por

$$x_0 = a, \quad x_1 = b, \quad x_{n+2} = x_{n+1} + x_n, n = 0, 1, 2, \ldots$$

tem todos os seus termos primos com m.

[2]Retirado do livro *Primos de Mersenne (e outros primos muito grandes)*, de Carlos Gustavo T. A. Moreira (Gugu), e Nicolau C. Saldanha