II SEMAT

O Teorema de Krull-Schmidt

Rodrigo Thomaz da Silva

Departamento de Matemática - Universidade Federal de São Carlos

Soma direta

Para começar, uma proposição que motiva a próxima definição.

Proposição 1. *Um grupo G é isomorfo a um produto direto $G_1 \times G_2$ de dois grupos G_1 e G_2 se, e somente se, G contém subgrupos normais $A \cong G_1$ e $B \cong G_2$ tais que $A \cap B = 1$ e $AB = G$.*

Neste trabalho entenderemos o conceito de *soma direta* como uma *soma direta interna*, isto é, os grupos a serem "somados"são, de antemão, subgrupos de um grupo maior.

Definição. Um grupo G é a *soma direta* (interna) $G = A \oplus B$ de dois subgrupos A e B quando $A, B \lhd G$, $A \cap B = 1$ e $AB = G$.

Com as devidas alterações a Proposição 1 pode ser generalizada para n grupos, donde a definição de soma direta pode ser estendida a n subgrupos de um grupo G.

Definição. Um grupo G é dito *indecomponível* se $G \neq 1$ e $G = A \oplus B$ implicar em $A = 1$ ou $B = 1$.

Definição. Um grupo G tem *comprimento finito* se toda cadeia de subgrupos normais de G é finita.

Proposição 2. *Todo grupo de comprimento finito pode ser escrito como soma direta de finitos subgrupos indecomponíveis.*

Endomorfismos normais

Lembremos que um *endomorfismo* é um homomorfismo de um grupo G em si mesmo. Denotaremos $E(G)$ o conjunto dos endomorfismos de G. Tal conjunto é um monoide com a composição de funções. Escreveremos todos os endomorfismos como operadores à esquerda.

Definição. Um endomorfismo η definido num grupo G é dito *normal* se vale $\eta(gxg^{-1}) = g(\eta x)g^{-1}$ para todo $x, g \in G$.

Note que da definição ambos $\operatorname{Im}\eta$ e $\operatorname{Ker}\eta$ são subgrupos normais de G.

A partir daqui apresentaremos diversos lemas necessários para a demonstração do resultado principal.

Lema 3. *Se G tem comprimento finito, então um endomorfismo normal de G é injetivo se, e somente se, ele é sobrejetivo (se, e somente se, é bijetivo).*

Lema 4. *Se G tem comprimento finito e η é um endomorfismo normal de G, então $G = \operatorname{Im}\eta^n \oplus \operatorname{Ker}\eta^n$ para algum $n > 0$.*

Definição. Um endomorfismo η é dito *nilpotente* se $\operatorname{Im}\eta^n = 1$ para algum $n > 0$.

Lema 5. *Se G é um grupo indecomponível de comprimento finito, então todo endomorfismo normal é ou nilpotente ou um automorfismo.*

A operação de G induz uma operação parcial $\bullet$ em $E(G)$: o *produto pontual* $\eta \bullet \zeta$ de $\eta, \zeta \in E(G)$ é definido em $E(G)$ se, e somente se, a função $\xi : x \mapsto (\eta x)(\zeta x)$ é um endomorfismo, e então $\eta \bullet \zeta = \xi$. As seguintes propriedades seguem sem dificuldade.

Lema 6. *Temos $\eta \bullet \zeta$ definido em $E(G)$ se, e somente se, ηx e ζy comutam para todo $x, y \in G$. Se η e ζ são normais e $\eta \bullet \zeta$ está definido, então $\eta \bullet \zeta$ é normal.*

Vale a generalização do lema anterior para n endomorfismos, com as devidas alterações. Também, vale a distributividade da composição sobre o produto pontual, quando este último estiver definido.

Lema 7. *Sejam $\eta_1, \ldots, \eta_n$ endomorfismos normais de um grupo indecomponível G de comprimento finito. Se $\eta_i x$ comuta com $\eta_j y$ para todo $x, y \in G$ e todo $i \neq j$, e todo η_i é nilpotente, então $\eta_1 \bullet \cdots \bullet \eta_n$ é nilpotente.*

Decomposições em somas diretas vêm com endomorfismos normais. Seja $G = G_1 \oplus \cdots \oplus G_m$, então todo $x \in G$ pode ser escrito unicamente na forma $x = x_1 x_2 \cdots x_m$ com $x_i \in G_i$ para todo i. Para todo k seja η_k a função $\eta_k : x_1 x_2 \cdots x_n \mapsto x_k \in G$. Tal função é um endomorfismo de G (composição de homomorfismos), o k-ésimo *endomorfismo projeção* da soma direta $G = G_1 \oplus \cdots \oplus G_m$. Valem as seguintes propriedades:

Lema 8. *Em qualquer decomposição em soma direta $G = G_1 \oplus \cdots \oplus G_m$, os endomorfismos projeção $\eta_1, \ldots, \eta_m$ são endomorfismos normais; $\operatorname{Im}\eta_k = G_k$; $\eta_k x = x$ para todo $x \in G_k$; $\eta_k x = 1$ para todo $x \in G_i$ se $i \neq k$; $\eta_i x$ comuta com $\eta_j y$ para todo $x, y \in G$ e todo $i \neq j$; $\eta_1 \bullet \cdots \bullet \eta_m$ é definido em $E(G)$; e $\eta_1 \bullet \cdots \bullet \eta_m = 1_G$.*

Lema 9. *Seja $G = A \oplus B$. Todo subgrupo normal de A é um subgrupo normal de G. Se η é um endomorfismo normal de G e $\eta A \subset A$, então a restrição $\eta_{|A}$ é um endomorfismo normal de A.*

Teorema de Krull-Schmidt

Com este arsenal, estamos prontos para provar o Teorema de Krull-Schmidt.

Teorema. *Se um grupo G de comprimento finito é a soma direta*

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_m = H_1 \oplus H_2 \oplus \cdots \oplus H_n$$

de subgrupos indecomponíveis, então $m = n$ e $H_1, \ldots, H_n$ podem ser reindexados de forma que $H_i \cong G_i$ para todo $i \leq n$ e

$$G = G_1 \oplus \cdots \oplus G_k \oplus H_{k+1} \oplus \cdots \oplus H_n$$

para todo $k < n$.

Demonstração. Vamos fazer indução em k para provar o seguinte para todo $k \leq n$:

(1) $k \leq m$, e $H_1, \ldots, H_n$ podem ser reindexados de forma que

(2) $H_i \cong G_i$ para todo $i \leq k$ e

(3) $G = G_1 \oplus \cdots \oplus G_k \oplus H_{k+1} \oplus \cdots \oplus H_n$.

Para $k = 0$ não há nada para provar. Seja $0 < k \leq n$ e suponha que (1), (2) e (3) valem para $k - 1$. Pelo Lema 9, todos G_i e H_j têm comprimento finito. Sejam $\eta_1, \ldots, \eta_m$ as projeções da soma dos G's e $\zeta_1, \ldots, \zeta_n$ as projeções da soma $G = G_1 \oplus \cdots \oplus G_{k-1} \oplus H_k \oplus \cdots \oplus H_n$ da hipótese de indução.

Pelo Lema 8, $\eta_1 \bullet \cdots \bullet \eta_m = 1_G$. Portanto, $\zeta_k = \zeta_k(1_G) = \zeta_k\eta_1 \bullet \cdots \bullet \zeta_k\eta_m$. Se $k > m$, então $\eta_i x \in G_i$ para todo $x \in G$ e $\operatorname{Im}\zeta_k\eta_i = 1$ para todo $i \leq m < k$, pelo Lema 8; logo $H_k = \operatorname{Im}\zeta_k = 1$, uma contradição com H_k ser indecomponível. Portanto $k \leq m$ e (1) vale para k.

De maneira similar, $\zeta_1 \bullet \cdots \bullet \zeta_n = 1_G$, $\eta_k\zeta_j G_k \subset G_k$ para todo j, e $\operatorname{Im}\eta_k\zeta_j = 1$ para todo $j < k$, porque $\zeta_j x \in G_j$ para todo $x \in G$. Portanto, $\eta_k = \eta_k(1_G) = \eta_k\zeta_1 \bullet \cdots \bullet \eta_k\zeta_n = \eta_k\zeta_k \bullet \cdots \bullet \eta_k\zeta_n$.

Agora, todo $(\eta_k\zeta_j)_{|G_k}$ é um endomorfismo normal de G_k, pelo Lema 9, e $(\eta_k\zeta_k)_{|G_k} \bullet \cdots \bullet (\eta_k\zeta_n)_{|G_k}$ é a identidade em G_k e não é nilpotente; pelo Lema 7, $(\zeta_k\zeta_j)_{|G_k}$ não é nilpotente para algum $j \geq k$. Os grupos $H_k, \ldots, H_n$ podem ser indexados de forma que $(\eta_k\zeta_k)_{|G_k}$ não seja nilpotente.

Mostraremos que $G_k \cong H_k$. Pelo Lema 5, $(\eta_k\zeta_k)_{|G_k}$ é um automorfismo de G_k. Portanto $\eta_k\zeta_k$ não é nilpotente. Então $\operatorname{Im}\eta_k(\zeta_k\eta_k)^p\zeta_k = \operatorname{Im}(\eta_k\zeta_k)^{p+1} \neq 1$ para todo p, logo $\zeta_k\eta_k$ não é nilpotente. Portanto $(\zeta_k\eta_k)_{|H_k}$ não é nilpotente, pois se tivéssemos $(\zeta_k\eta_k)^n x = 1$ para todo $x \in H_k$, valeria $(\zeta_k\eta_k)^n\zeta_k\eta_k x = 1$ para todo $x \in G$; donde $(\zeta_k\eta_k)_{|H_k}$ é um automorfismo de H_k. Assim, como $\zeta_k G_k \supset \zeta_k\eta_k H_k = H_k$, temos que $\eta_{k|H_k}$ é injetivo e $\zeta_k G_k = H_k$. Analogamente, $\zeta_{k|G_k}$ é injetivo e $\eta_k H_k = G_k$. Portanto $\eta_{k|H_k}$ é um isomorfismo de H_k sobre G_k (e $\zeta_{k|G_k}$ é um isomorfismo de G_k sobre H_k). Concluímos que (2) vale para k.

Para provar (3), defina $K = G_1 \cdots G_{k-1} H_{k+1} \cdots H_n$. Como $G = G_1 \oplus \cdots \oplus G_{k-1} \oplus H_k \oplus \cdots \oplus H_n$ pela hipótese de indução, temos $K = G_1 \oplus \cdots \oplus G_{k-1} \oplus H_{k+1} \oplus \cdots \oplus H_n$. Também, $\zeta_k K = 1$. Do fato de $\zeta_{k|G_k}$ ser injetivo, temos que $K \cap G_k = 1$. Logo, $KG_k = K \oplus G_k$.

Agora, $\eta_{k|H_k}$ é um isomorfismo, e $\eta_k x = 1$ para $x \in G_i$ ou $x \in H_j$, $i < k < j$. Portanto $\theta = \zeta_1 \bullet \cdots \bullet \zeta_{k-1} \bullet \eta_k \bullet \zeta_{k+1} \bullet \cdots \bullet \zeta_n$ é um isomorfismo

$$\begin{aligned} \theta : G &= G_1 \oplus \cdots \oplus G_{k-1} \oplus H_k \oplus H_{k+1} \oplus \cdots \oplus H_n \\ &\to G_1 \oplus \cdots \oplus G_{k-1} \oplus G_k \oplus H_{k+1} \oplus \cdots \oplus H_n = KG_k. \end{aligned}$$

Visto como um endomorfismo de G, θ é normal e injetivo; portanto θ é bijetivo (pelo Lema 3), $G = KG_k$, e (3) vale para k. ■

Referências

[1] P. A. GRILLET, *Abstract Algebra*, 2ed., Graduate Texts in Mathematics, 2007, pp. 43-54

Agradecimentos

Agradeço ao meu orientador Francisco Braun, que mesmo entre dificuldades me incentiva e dá apoio para seguir estudando e produzindo.