Endomorfismos directos de grupos

por José Morgado
Instituto de Matemática, Universidade Federal de Pernambuco, Brasil

1. Introdução

Suponhamos que o grupo G é o produto directo dos subgrupos A e B, $G = A \times B$; isto significa, como é bem sabido, que cada elemento de G tem uma e uma só representação como produto de um elemento de A por um elemento de B e, além disso, A e B são subgrupos normais do grupo G.

Recordemos que, se, para cada $x \in G$, definirmos $\varphi(x)$ como o elemento de B que intervém na representação de x como produto de um elemento de A por um elemento de B, obtemos um *projector* φ de G, isto é, φ é um endomorfismo de G que satisfaz às duas condições seguintes:

a) φ *é idempotente*, quer dizer, $\varphi \circ \varphi = \varphi$;

b) φ *é normal*, quer dizer, φ comuta com todos os automorfismos internos de G; assim, se f_a designa o automorfismo interno determinado por $a \in G$, então tem-se

$$\varphi \circ f_a = f_a \circ \varphi \quad \text{para todo} \quad a \in G,$$

ou seja,

$$\varphi(a x a^{-1}) = a \varphi(x) a^{-1} \quad \text{para todos} \quad a, x \in G.$$

Os subgrupos normais A e B são, respectivamente, o núcleo de φ e a imagem de φ, $A = \mathrm{Ker}(\varphi)$ e $B = \mathrm{Im}(\varphi)$.

Inversamente, se φ é um projector do grupo G, então tem-se

$$G = \mathrm{Ker}(\varphi) \times \mathrm{Im}(\varphi).$$

Mas pode acontecer que um endomorfismo α do grupo G não seja um projector e, no entanto, se tenha

$$(1) \qquad G = \mathrm{Ker}(\alpha) \times \mathrm{Im}(\alpha).$$

Por exemplo, se G é o grupo cíclico de ordem 6,

$$G = \{1, a, a^2, a^3, a^4, a^5\},$$

e, se α é o endomorfismo definido por $\alpha(x) = x^2$ para todo $x \in G$, então

$$G = \mathrm{Ker}(\alpha) \times \mathrm{Im}(\alpha) = \{1, a^3\} \times \{1, a^2, a^4\}$$

e, no entanto, α não é um projector, visto que $\alpha(\alpha(a)) = a^4 \neq a^2 = \alpha(a)$.

Diremos que um endomorfismo α do grupo G é um *endomorfismo directo* de G, se é válida a igualdade (1).

O objectivo principal desta nota é precisamente dar uma caracterização dos endomorfismos directos de um grupo.

2. Preliminares

Comecemos por estabelecer a seguinte proposição:

I) *Se* α *é um endomorfismo directo do grupo* G, *então a restrição de* α *ao subgrupo normal* $Im(\alpha)$ *é um automorfismo.*

DEM. Com efeito, vejamos que se tem

$$(2) \qquad \mathrm{Ker}(\alpha) = \mathrm{Ker}(\alpha^2) \quad \text{e} \quad \mathrm{Im}(\alpha) = \mathrm{Im}(\alpha^2).$$

Da primeira destas igualdades vai resultar que, se

$$\alpha(\alpha(x)) = \alpha^2(x) = 1 \text{ (elemento neutro de } G),$$

então $\alpha(x)=1$ e, portanto, a restrição de α a $\mathrm{Im}(\alpha)$ é injectiva.

Da segunda destas igualdades vai resultar que, para todo $x \in G$, existe algum $y \in G$ tal que

$$\alpha(x)=\alpha^2(y)=\alpha(\alpha(y))$$

e, portanto, a restrição de α a $\mathrm{Im}(\alpha)$ é sobrejectiva.

Tudo se reduz, por consequência, a provar as igualdades (2).

Ora, como, para todo endomorfismo α de G, se tem

$$\mathrm{Ker}(\alpha) \subseteq \mathrm{Ker}(\alpha^2) \quad \text{e} \quad \mathrm{Im}(\alpha) \supseteq \mathrm{Im}(\alpha^2),$$

basta estabelecer as inclusões inversas.

Seja então $a \in \mathrm{Ker}(\alpha^2)$.

De $\alpha^2(a)=1$, resulta que $\alpha(a) \in \mathrm{Ker}(\alpha)$ e, como se tem evidentemente $\alpha(a) \in \mathrm{Im}(\alpha)$, conclui-se que $\alpha(a)=1$, visto que $\mathrm{Ker}(\alpha) \cap \mathrm{Im}(\alpha)=\{1\}$, em virtude de, por hipótese, ser válida a igualdade (1).

Isto mostra que $\mathrm{Ker}(\alpha^2) \subseteq \mathrm{Ker}(\alpha)$ e, portanto, verifica-se a primeira das igualdades (2).

Seja agora $a \in \mathrm{Im}(\alpha)$, isto é, $a=\alpha(x)$ para algum $x \in G$.

Como se tem

$$x=bc, \quad \text{onde } b \in \mathrm{Ker}(\alpha) \text{ e } c \in \mathrm{Im}(\alpha),$$

pode-se escrever

$$x=b\,\alpha(d) \quad \text{para algum } d \in G,$$

donde

$$a=\alpha(x)=\alpha(b)\,\alpha^2(d)=\alpha^2(d),$$

o que mostra ter-se $\mathrm{Im}(\alpha) \subseteq \mathrm{Im}(\alpha^2)$ e, portanto, verifica-se a segunda igualdade (2).

II) *Se α é um endomorfismo directo do grupo* G, *então existe um automorfismo σ de* G *tal que*

$$\sigma \circ \alpha = \alpha^2 = \alpha \circ \sigma. \tag{3}$$

DEM. Com efeito, designemos por τ o automorfismo induzido por α no subgrupo normal $\mathrm{Im}(\alpha)$ e seja

$$x=yz, \quad \text{onde } y \in \mathrm{Ker}(\alpha) \text{ e } z \in \mathrm{Im}(\alpha). \tag{4}$$

Como a representação (4) de x é única, pondo

$$\sigma(x)=y\,\tau(z), \tag{5}$$

define-se uma aplicação σ de G em G; é claro que, se $x \in \mathrm{Im}(\alpha)$, então $\sigma(x)=\tau(x)=\alpha(x)$ e, se $x \in \mathrm{Ker}(\alpha)$, então $\sigma(x)=x$.

Vejamos que σ é um automorfismo de G.

Seja

$$t=uv, \quad \text{onde } u \in \mathrm{Ker}(\alpha) \text{ e } v \in \mathrm{Im}(\alpha)$$

e, portanto,

$$\sigma(t)=u\,\tau(v).$$

De (1) resulta que cada elemento de $\mathrm{Ker}(\alpha)$ comuta com cada elemente de $\mathrm{Im}(\alpha)$, sendo, por consequência,

$$xt=yz\cdot uv=yu\cdot zv, \quad \text{onde } yu \in \mathrm{Ker}(\alpha) \text{ e } zv \in \mathrm{Im}(\alpha)$$

e daqui resulta

$$\sigma(xt)=yu\,\tau(zv)=yu\,\tau(z)\,\tau(v)= \\ =y\,\tau(z)\,u\,\tau(v)=\sigma(x)\,\sigma(t),$$

quer dizer, σ é um endomorfismo de G.

O endomorfismo σ é injectivo Na verdade, se $\sigma(x)=1$, então de (4) e (5) conclui-se que

$$\tau(z)=y^{-1} \in \mathrm{Ker}(\alpha) \cap \mathrm{Im}(\alpha)=\{1\},$$

e, como τ é um automorfismo de $\mathrm{Im}(\alpha)$, resulta $z=1=y$, o que implica $x=1$.

O endomorfismo σ é sobrejectivo. Na verdade, seja $a \in G$ e vejamos que existe algum $x \in G$ tal que $\sigma(x)=a$.

Supondo que

$$a = b\,c\,, \text{ com } b \in \mathrm{Ker}(\alpha) \text{ e } c \in \mathrm{Im}(\alpha),$$

e pondo $x = b\,\tau^{-1}(c)$, vem

$$\sigma(x) = b\,\tau(\tau^{-1}(c)) = b\,c = a\,,$$

como se pretendia.

Vejamos agora que o automorfismo σ verifica as condições (3).

Já observámos que, se $z \in \mathrm{Im}(\alpha)$, então $\sigma(z) = \tau(z) = \alpha(z)$, resultando, por consequência, que

$$(\sigma \circ \alpha)(x) = \sigma(\alpha(x)) = \tau(\alpha(x)) = \\ = \alpha(\alpha(x)) = \alpha^2(x).$$

Por outro lado, tem-se

$$(\alpha \circ \sigma)(x) = \alpha(\sigma(y\,z)) = \alpha(y\,\tau(z)) = \alpha(\tau(z)) = \\ = \alpha(\alpha(z)) = \alpha^2(z) = \alpha^2(y)\,\alpha^2(z) = \\ = \alpha^2(y\,z) = \alpha^2(x).$$

Isto mostra que, de facto, σ verifica as condições (3).

3. Caracterização dos endomorfismos directos

Recordemos que, se f e g são aplicações do grupo G em si mesmo, então a diferença $f-g$ define-se pela condição

$$(f-g)(x) = f(x)\,g(x^{-1}) \quad \text{para todo} \quad x \in G.$$

Se f e g são endomorfismos de G, então a diferença $f-g$ não é necessàriamente um endomorfismo de G.

No entanto, se α é um endomorfismo directo de G e σ é o automorfismo construido acima, é fácil ver que a diferença $\sigma - \alpha$ é um endomorfismo de G.

De facto, suponhamos que $x = y\,z$ e $t = u\,v$, com $y, u \in \mathrm{Ker}(\alpha)$ e $z, v \in \mathrm{Im}(\alpha)$.

Então, tem-se evidentemente

$$(\sigma - \alpha)(x\,t) = \sigma(x\,t)\,\alpha((x\,t)^{-1}) = \\ = \sigma(x)\,\sigma(t)\,\alpha(t^{-1})\,\alpha(x^{-1}) = \\ = y\,\tau(z)\,u\,\tau(v)\,\alpha(v^{-1}u^{-1})\,\alpha(z^{-1}y^{-1}) = \\ = y\,\tau(z)\,u\,\tau(v)\,\alpha(v^{-1})\,\alpha(z^{-1}) = \\ = y\,\tau(z)\,u\,\alpha(z^{-1}) = \\ = y\,u\,.$$

Por outro lado, tem-se também

$$(\sigma - \alpha)(x) \cdot (\sigma - \alpha)(t) = \sigma(x)\,\alpha(x^{-1})\,\sigma(t)\,\alpha(t^{-1}) = \\ = y\,\tau(z)\,\alpha(z^{-1}y^{-1})\,u\,\tau(v)\,\alpha(v^{-1}u^{-1}) = \\ = y\,\tau(z)\,\alpha(z^{-1})\,u\,\tau(v)\,\alpha(v^{-1}) = \\ = y\,u\,,$$

o que prova que $\sigma - \alpha$ é um endomorfismo de G.

Suponhamos agora que α é um endomorfismo do grupo G, tal que existe um automorfismo σ de G satisfazendo à condição (3) e $\sigma - \alpha$ é um endomorfismo de G.

Tem-se trivialmente

$$x = x\,\alpha(\sigma^{-1}(x^{-1})) \cdot \alpha(\sigma^{-1}(x))$$

para todo $x \in G$.

Ora, como $\alpha(\sigma^{-1}(x)) \in \mathrm{Im}(\alpha)$ e, além disso,

$$\alpha(x\,\alpha(\sigma^{-1}(x^{-1}))) = \alpha(x)\,\alpha^2(\sigma^{-1}(x^{-1})) = \\ = \alpha(x) \cdot (\alpha \circ \sigma)(\sigma^{-1}(x^{-1})) = \\ = \alpha(x)\,\alpha(\sigma(\sigma^{-1}(x^{-1}))) = \\ = 1\,,$$

isto é, $x\,\alpha(\sigma^{-1}(x^{-1})) \in \mathrm{Ker}(\alpha)$, conclui-se que o grupo G é o produto dos subgrupos $\mathrm{Ker}(\alpha)$ e $\mathrm{Im}(\alpha)$.

Vamos ver que este produto é directo.

Com efeito, mostremos primeiramente que a representação de um elemento de G como produto de um elemento de $\mathrm{Ker}(\alpha)$ por um elemento de $\mathrm{Im}(\alpha)$ é única.

Realmente, se $yz = uv$, com $y, u \in \mathrm{Ker}(\alpha)$ e $z, v \in \mathrm{Im}(\alpha)$, então

$$u^{-1} y = v z^{-1} \in \mathrm{Ker}(\alpha) \cap \mathrm{Im}(\alpha).$$

Ora é fácil ver que a intersecção destes subgrupos é $\{1\}$.

Na verdade, se x é um elemento qualquer daquela intersecção, então tem-se $\alpha(x) = 1$ e $x = \alpha(t)$ para algum $t \in G$, donde resulta $\alpha^2(t) = 1$, ou seja, $\sigma(\alpha(t)) = 1$. Como σ é um automorfismo de G, tem-se necessàriamente $1 = \alpha(t) = x$.

Por consequência,

$$u^{-1} y = v z^{-1} = 1$$

isto é, $y = u$ e $z = v$.

Para podermos concluir que se tem

$$G = \mathrm{Ker}(\alpha) \times \mathrm{Im}(\alpha),$$

basta agora provar que o subgrupo $\mathrm{Im}(\alpha)$ é normal.

Para isso, temos de mostrar que

$$a\,\alpha(x)\,a^{-1} \in \mathrm{Im}(\alpha) \text{ para todos } a, x \in G,$$

o que é equivalente a mostrar que

(6) $$\sigma(b)\,\alpha(x)\,\sigma(b^{-1}) \in \mathrm{Im}(\alpha) \quad \text{para todos } b, x \in G,$$

em virtude de σ ser um automorfismo de G.

Ora, por hipótese, $\sigma - \alpha$ é um endomorfismo de G e isto significa que se tem

$$\sigma(u)\,\sigma(v)\,\alpha(v^{-1})\,\alpha(u^{-1}) = \sigma(u)\,\alpha(u^{-1})\,\sigma(v)\,\alpha(v^{-1})$$

para todos $u, v \in G$.

Daqui resulta

$$\sigma(v^{-1})\,\alpha(u^{-1})\,\sigma(v) = \alpha(v^{-1})\,\alpha(u^{-1})\,\alpha(v)$$

para todos $u, v \in G$.

Fazendo $u = x^{-1}$ e $v = b^{-1}$, resulta

$$\sigma(b)\,\alpha(x)\,\sigma(b^{-1}) = \alpha(b\,x\,b^{-1}),$$

o que prova a relação (6).

Ficou, portanto, provado o seguinte

TEOREMA 1. *Um endomorfismo α de um grupo G é um endomorfismo directo, se e só se existe algum automorfismo σ de G que satisfaça às seguintes condições:*

(i) $\sigma \circ \alpha = \alpha^2 = \alpha \circ \sigma$

(ii) *$\sigma - \alpha$ é um endomorfismo de G.*

OBSERVAÇÃO. Se α é um endomorfismo directo do grupo G, então deve existir um projector φ de G tal que

$$\mathrm{Ker}(\varphi) = \mathrm{Ker}(\alpha) \text{ e } \mathrm{Im}(\varphi) = \mathrm{Im}(\alpha).$$

É fácil ver que $\varphi = \sigma^{-1} \circ \alpha$ é um tal projector. De facto, de (i) resulta

$$\alpha \circ \sigma^{-1} = \sigma^{-1} \circ \alpha \text{ e } \sigma^{-1} \circ \alpha^2 = \alpha,$$

donde

$$\varphi \circ \varphi = (\sigma^{-1} \circ \alpha) \circ (\sigma^{-1} \circ \alpha) = \\ = \sigma^{-1} \circ (\sigma^{-1} \circ \alpha \circ \alpha) = \sigma^{-1} \circ \alpha = \varphi,$$

o que mostra a idempotência do endomorfismo φ. Por outro lado, como $\sigma - \alpha$ é um endomorfismo, também

$$\varepsilon - \sigma^{-1} \circ \alpha = (\sigma^{-1} \circ \sigma) - (\sigma^{-1} \circ \alpha) = \sigma^{-1} \circ (\sigma - \alpha)$$

onde ε é o automorfismo idêntico, é um endomorfismo. Ora, sabe-se ([2], teorema 1) que o endomorfismo β é um endomorfismo normal, se e sòmente se $\varepsilon - \beta$ é um endomorfismo. Por conseguinte, $\sigma^{-1} \circ \alpha$, sendo um endomorfismo idempotente e normal, é um projector, que tem o mesmo núcleo e a mesma imagem que α.

Podemos dar outra forma à condição (ii) do Teorema 1.

Com efeito, pelo que acima vimos, $\sigma - \alpha$ é um endomorfismo, se e só se

(7) $$\sigma(b)\,\alpha(x)\,\sigma(b^{-1}) = \alpha(b\,x\,b^{-1}) \quad \text{para todos } b, x \in G.$$

Como σ é um automorfismo de G, que comuta com α, a condição (7) é equivalente à condição

$$\sigma(b\,\alpha(y)\,b^{-1}) = \alpha(b\,\sigma(y)\,b^{-1})$$
$$\text{para todos } b, y \in G,$$

ou seja,

$$\sigma \circ \gamma \circ \alpha = \alpha \circ \gamma \circ \sigma$$

para todo automorfismo interno γ do grupo G.

É válido, portanto, o seguinte

Teorema 2. *O endomorfismo α do grupo G é um endomorfismo directo, se e só se existe um automorfismo σ de G que satisfaça às seguintes condições:*

(I) $\sigma \circ \alpha = \alpha^2 = \alpha \circ \sigma$

(II) $\sigma \circ \gamma \circ \alpha = \alpha \circ \gamma \circ \sigma$

para todo automorfismo interno γ de G.

4. Endomorfismos normais de ordem finita

É claro que o conjunto $\mathrm{End}(G)$, formado por todos os endomorfismos do grupo G, constitui um semigrupo (mais precisamente, um monoide) com respeito à operação de composição. Se o subsemigrupo $<\alpha>$ de $\mathrm{End}(G)$, gerado pelo endomorfismo α, é finito, diz-se que a ordem de α é finita e é igual ao número de elementos de $<\alpha>$.

Mostraremos que, para todo endomorfismo normal de ordem finita, existe alguma sua potência que é um endomorfismo directo.

Antes, porém, vamos estabelecer o seguinte

Teorema 3. *Se α é um endomorfismo normal do grupo G cuja restrição à imagem de α^n é um automorfismo, então α^n é um endomorfismo directo.*

Dem. Com efeito, designemos por τ o automorfismo induzido por α em $\mathrm{Im}(\alpha^n)$.

Tem-se evidentemente, para todo $x \in G$,

$$x = x\,\tau^{-n}(\alpha^n(x^{-1})) \cdot \tau^{-n}(\alpha^n(x)).$$

Ora

$$\tau^{-n}(\alpha^n(x)) \in \mathrm{Im}(\alpha^n),$$

porque τ^{-n} é um automorfismo de $\mathrm{Im}(\alpha^n)$; e

$$x\,\tau^{-n}(\alpha^n(x^{-1})) \in \mathrm{Ker}(\alpha^n),$$

porque

$$\alpha^n(x)\,\alpha^n(\tau^{-n}(\alpha^n(x^{-1}))) = \alpha^n(x)\,\alpha^n(x^{-1}) = 1.$$

Isto significa que $G = \mathrm{Ker}(\alpha^n)\,\mathrm{Im}(\alpha^n)$.

Pretendemos provar que este produto é directo.

É imediato que se tem

$$\mathrm{Ker}(\alpha^n) \cap \mathrm{Im}(\alpha^n) = \{1\},$$

porque, se x é um elemento qualquer desta intersecção, então $\alpha^n(x) = 1$ e $x = \alpha^n(t)$ para algum $t \in G$, donde $\alpha^{2n}(t) = 1$. Ora, por τ ser um automorfismo de $\mathrm{Im}(\alpha^n)$, tem-se evidentemente

$$\mathrm{Ker}(\alpha^n) = \mathrm{Ker}(\tau \circ \alpha^n) = \mathrm{Ker}(\alpha^{n+1}) = \cdots = \mathrm{Ker}(\alpha^{2n}) = \cdots$$

e, anàlogamente,

$$\mathrm{Im}(\alpha^n) = \mathrm{Im}(\tau \circ \alpha^n) = \mathrm{Im}(\alpha^{n+1}) = \cdots = \mathrm{Im}(\alpha^{2n}) = \cdots.$$

Assim, $t \in \mathrm{Ker}(\alpha^n)$, donde resulta

$$x = \alpha^n(t) = 1.$$

Para concluir que aquele produto é directo, basta notar que o subgrupo $\mathrm{Im}(\alpha^n)$ é normal, visto α^n ser um endomorfismo normal.

Logo, α^n é um endomorfismo directo do grupo G.

Corolário. *Se α é um endomorfismo normal de ordem finita do grupo G, então há pelo menos uma potência de α que é um endomorfismo directo do grupo G.*

Na verdade, se α é de ordem finita, então o subsemigrupo de $\mathrm{End}(G)$,

$$<\alpha> = \{\alpha, \alpha^2, \alpha^3, \cdots, \alpha^n, \cdots\}$$

tem sòmente um número finito de elementos, quer dizer, há potências de α que são iguais e têm expoentes distintos.

Seja α^m a primeira potência de α que é igual a alguma potência de expoente $n < m$. Então os elementos de $<\alpha>$ são

$$\alpha, \alpha^2, \cdots, \alpha^n, \cdots, \alpha^{m-1}.$$

É imediato que α induz um automorfismo em $\mathrm{Im}(\alpha^n)$ e, pelo Teorema 3, α^n é um endomorfismo directo de G.

É interessante observar que o conjunto

$$\{\alpha^n, \alpha^{n+1}, \cdots, \alpha^{m-1}\}$$

é um subgrupo do semigrupo $<\alpha>$. O elemento neutro é o elemento α^r, onde r é o único múltiplo de $m-n$ existente no conjunto

$$\{n, n+1, \cdots, m-1\}$$

([4], pp. 19-20).

Todos os elementos daquele subgrupo são endomorfismos directos do grupo G.

O elemento neutro α^r é a única potência de α que é um projector.

Uma outra consequência imediata do Teorema 3 é o conhecido Lema de Fitting ([1], p. 327): Se o grupo G satisfaz às duas condições de cadeia e α é um endomorfismo normal de G, então tem-se

$$G = \mathrm{Ker}(\alpha^n) \times \mathrm{Im}(\alpha^n)$$

para algum inteiro positivo n; α induz um automorfismo em $\mathrm{Im}(\alpha^n)$.

BIBLIOGRAFIA

[1] A. Almeida Costa, *Cours d'Algèbre Générale*, vol. I, Fundação Calouste Gulbenkian, Lisboa, 1964.

[2] José Morgado, *A note on the normal endomorphisms of a group*, Gazeta de Matemática, n.º 109-112 (1968), pp. 6-8.

[3] ————, *A note on the endomorphisms associated to semi-direct decompositions of a group*, em publicação na «Portugaliae Mathematica».

[4] A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups*, I, Mathematical Surveys, Am. Math. Soc., 1961.