Aulas 13 a 15 — material complementar

As aulas 13 a 15 baseiam-se nas secções 3.1, 3.2 e 3.3 do livro de Dummit e Foote, e as presentes notas contêm material complementar.

I Classes laterais

§1. Definição. Seja G um grupo, $K \leq G$ e $g \in G$. Chama-se *classe lateral esquerda ("left coset") de K representada por g* ao conjunto

$$gK = \{gk \mid k \in K\}$$

e *classe lateral direita ("right coset") de K representada por g* ao conjunto

$$Kg = \{kg \mid k \in K\}.$$

§2. Nota. A classe lateral esquerda gK é a órbita de g para a acção regular à direita de K sobre G, e a classe lateral direita Kg é a órbita de g para a acção regular à esquerda de K sobre G. Portanto ambos os conjuntos

$$G/K := \{gK \mid g \in G\} \quad \text{e} \quad K\backslash G := \{Kg \mid g \in G\}$$

são partições de G:

$$\bigcup_{g\in G} gK = \bigcup_{g\in G} Kg = G$$

e, dados $g, h \in G$, tem-se $gK = hK$ ou $gK \cap hK = \emptyset$; e, de igual modo, $Kg = Kh$ ou $Kg \cap Kh = \emptyset$.

§3. Exercício. Prove que as condições seguintes são equivalentes:

1. $gK = hK$
2. $g^{-1}h \in K$

3. $h \in gK$.

Conclua que as condições seguintes são equivalentes:

1. $gK = K$
2. $g \in K$
3. $1 \in gK$.

§4. Nota. A função $\phi_g : K \to gK$ definida por $k \mapsto gk$ é uma bijecção cuja inversa $\phi_g^{-1} : gK \to K$ é definida por $\phi_g^{-1}(h) = g^{-1}h$, pois

$$\phi_g(\phi_g^{-1}(h)) = gg^{-1}h = h \quad \text{e} \quad \phi_g^{-1}(\phi_g(k)) = g^{-1}gk = k.$$

De igual modo existe uma bijecção $\psi_g : K \to Kg$, e portanto

$$|K| = |gK| = |Kg|.$$

No caso de G ser finito obtém-se o teorema de Lagrange e também que os seguintes cardinais são finitos e iguais:

$$|G/K| = |K\backslash G|.$$

No entanto, seja G finito ou não, os conjuntos G/K e $K\backslash G$ são em geral diferentes.

§5. Exercício. Encontre um grupo finito G e um subgrupo $K \leq G$ tais que $G/K \neq K\backslash G$.

§6. Definição. Seja G um grupo e $K \leq G$. Designa-se por *índice de K em G* o cardinal

$$|G : K| := |G/K|.$$

§7. Nota. Se G for finito então $|G : K| = |G|/|K|$.

§8. Nota. O índice pode ser finito mesmo que G seja infinito. Por exemplo, $|\mathbb{Z} : n\mathbb{Z}| = n$.

II Subgrupos normais

§9. Definição. Seja G um grupo e $K \leq G$. Diz-se que K é um *subgrupo normal* de G, e escreve-se $K \trianglelefteq G$, se para qualquer $g \in G$ as classes laterais esquerda e direita coincidem:

$$gK = Kg.$$

§10. Nota. Se G é um grupo abeliano então todos os subgrupos de G são normais.

§11. Exercício. Encontre todos os subgrupos normais de D_8 e de D_{10}.

O exercício anterior é parcialmente simplificado devido à proposição seguinte:

§12. Proposição. *Se $K \leq G$ e $|G : K| = 2$ então $K \trianglelefteq G$.*

Demonstração. Seja $g \in G - K$. Então $gK \cap K = Kg \cap K = \emptyset$. Como o índice de K é 2, existem apenas duas classes laterais, tanto esquerdas como direitas, pelo que G é a união disjunta $K \cup gK$ e também a união disjunta $K \cup Kg$. Logo, $gK = Kg = G - K$, e portanto K é normal. ∎

§13. Exemplo. $\langle r \rangle \trianglelefteq D_{2n}$.

§14. Exercício. Prove que um subgrupo de um subgrupo normal não é necessariamente normal.

§15. Exercício. Mostre que é normal qualquer subgrupo contido no centro $Z(G)$ de um grupo G.

§16. Exercício. Mostre que se $K \trianglelefteq G$ e $K \leq H \leq G$ então $K \trianglelefteq H$.

§17. Exercício. Encontre um grupo não abeliano finito cujos subgrupos são todos normais.

§18. Nota. Note-se que a condição $K \trianglelefteq G$ é equivalente a $N_G(K) = G$. No entanto, para verificar que um subgrupo $K \leq G$ é normal basta verificar uma das seguintes inclusões para todos os elementos $g \in G$:

$$gKg^{-1} \subset K \quad \text{ou} \quad gK \subset Kg \quad \text{ou} \quad Kg \subset gK.$$

(Exercício: porquê?)

III Núcleos

Já sabemos que o núcleo de um homomorfismo de grupos $\varphi : G \to H$ é um subgrupo $\operatorname{Nuc}\varphi \leq G$, mas agora veremos algo mais:

§19. PROPOSIÇÃO. *Seja $\varphi : G \to H$ um homomorfismo de grupos. Então* $\operatorname{Nuc}\varphi \trianglelefteq G$.

Demonstração. Seja $\varphi : G \to H$ um homomorfismo, e denotemos por K o núcleo $\operatorname{Nuc}\varphi$. Para cada $h \in H$ chamaremos ao conjunto

$$\varphi^{-1}(h) := \{g \in G \mid \varphi(g) = h\}$$

a *pré-imagem*, ou a *fibra*, de h por φ. Então a fibra de 1 é K. Claramente, tem-se $\varphi^{-1}(h) \neq \emptyset$ se e só se $h \in \varphi(G)$. Em particular, para cada $g \in G$ a fibra $\varphi^{-1}(\varphi(g))$ contém pelo menos o elemento g.

Agora verifiquemos que $\varphi^{-1}(\varphi(g)) = gK$. Primeiro, seja $k \in K$, de modo que gk é um elemento genérico de gK. Então $\varphi(gk) = \varphi(g)\varphi(k) = \varphi(g)1 = \varphi(g)$, e portanto $gk \in \varphi^{-1}(\varphi(g))$. Assim conclui-se que

$$gK \subset \varphi^{-1}(\varphi(g)).$$

Por outro lado, seja $x \in \varphi^{-1}(\varphi(g))$, ou seja,

$$\varphi(x) = \varphi(g).$$

Então $x = gg^{-1}x \in gK$ porque $g^{-1}x \in K$:

$$\varphi(g^{-1}x) = \varphi(g)^{-1}\varphi(x) = \varphi(g)^{-1}\varphi(g) = 1.$$

Portanto $\varphi^{-1}(\varphi(g)) \subset gK$. Assim, como pretendido, conclui-se que

$$gK = \varphi^{-1}(\varphi(g)).$$

Da mesma forma (verifique), conclui-se que

$$Kg = \varphi^{-1}(\varphi(g)).$$

Logo, $gK = Kg$ e portanto $K \trianglelefteq G$. ∎

IV Quocientes de grupos

Já vimos que todos os núcleos são subgrupos normais. Mas será que qualquer subgrupo normal é um núcleo? A proposição seguinte mostra que a resposta é afirmativa:

§20. Teorema. *Seja G um grupo e $K \trianglelefteq G$. O conjunto de classes laterais G/K tem estrutura de grupo cujas operações são definidas, para cada $g, h \in G$, por:*

$$\begin{aligned} (gK)(hK) &= ghK \\ (gK)^{-1} &= g^{-1}K \\ 1_{G/K} &= K. \end{aligned}$$

A função $q : G \to G/K$ que a cada $g \in G$ faz corresponder a classe gK é um homomorfismo sobrejectivo de grupos cujo núcleo é K.

Demonstração. Comecemos por examinar a definição da operação de multiplicação. Note-se que g é apenas um dos elementos da classe gK, e que h é apenas um dos elementos da classe hK. A definição do produto usa esses elementos, mas devemos interrogar-nos: se escolhermos outros elementos $g' \in gK$ e $h' \in hK$ a definição do produto mantém-se? Por outras palavras, a definição do produto depende dos *representantes* das classes ou só das classes? Na prática, temos de verificar que para quaisquer $g' \in gK$ e $h' \in hK$ se tem $ghK = g'h'K$. Sejam então g' e h' tais que

$$g' \in gK \quad \text{e} \quad h' \in hK.$$

Equivalentemente,

$$gK = g'K \quad \text{e} \quad hK = h'K.$$

Então, usando a normalidade de K, temos

$$ghK = g(hK) = g(h'K) = g(Kh') = (gK)h' = (g'K)h' = g'(Kh') = g'h'K.$$

Portanto o produto está bem definido. E é associativo, pois para quaisquer classes laterais g_1K, g_2K e g_3K tem-se

$$\begin{aligned} \big((g_1K)(g_2K)\big)(g_3K) &= (g_1g_2K)(g_3K) = (g_1g_2)g_3K = g_1(g_2g_3)K \\ &= (g_1K)\big((g_2K)(g_3K)\big). \end{aligned}$$

Ou seja, verificámos que a associatividade em G/K é consequência imediata da associatividade em G. Temos então uma estrutura de semigrupo em G/K.

Vamos ver que G/K é de facto um monóide cujo elemento neutro é a classe K (ou seja, a classe de 1):

$$(gK)K = (gK)(1K) = g1K = gK \quad \text{e} \quad K(gK) = (1K)(gK) = (1g)K = gK.$$

Ou seja, verificámos directamente que K é um elemento neutro porque 1 é elemento neutro de G.

Finalmente, vamos ver que G/K é um grupo com o inverso de uma classe calculado como descrito acima. Primeiro, tal como fizemos para o produto, vamos ver que a operação de inverso está bem definida. Ou seja, precisamos de mostrar que, para qualquer outro elemento $h \in gK$, se tem $g^{-1}K = h^{-1}K$. Seja então $gK = hK$. Então os conjuntos dos elementos inversos das classes gK e hK também coincidem:

$$\{(gk)^{-1} \mid k \in K\} = \{(hk)^{-1} \mid k \in K\}.$$

Mas temos, usando a normalidade de K,

$$\{(gk)^{-1} \mid k \in K\} = \{k^{-1}g^{-1} \mid k \in K\} = \{kg^{-1} \mid k \in K\} = Kg^{-1} = g^{-1}K$$

e, de igual modo,

$$\{(hk)^{-1} \mid k \in K\} = \{k^{-1}h^{-1} \mid k \in K\} = \{kh^{-1} \mid k \in K\} = Kh^{-1} = h^{-1}K,$$

e portanto $g^{-1}K = h^{-1}K$, tal como pretendido. Vamos agora ver que esta operação define um inverso de grupo em G/K:

$$(gK)(gK)^{-1} = (gK)(g^{-1}K) = gg^{-1}K = K$$

e

$$(gK)^{-1}(gK) = (g^{-1}K)(gK) = g^{-1}gK = K.$$

Tal como antes, verificámos que a propriedade algébrica do inverso em G/K resulta directamente da propriedade análoga em G.

Ficou assim demonstrado que G/K é um grupo. A função $q : G \to G/K$, definida por $q(g) = gK$ para cada $g \in G$, é obviamente um homomorfismo:

$$q(gh) = ghK = (gK)(hK) = q(g)q(h).$$

Além disso, é um homomorfismo sobrejectivo, pois qualquer classe gK é imagem por q de um elemento de G, uma vez que

$$gK = q(g).$$

Para concluir a demonstração vamos mostrar que $\mathrm{Nuc}\, q = K$, por meio das equivalências seguintes aplicadas a um elemento genérico $x \in G$:

$$x \in \mathrm{Nuc}\, q \iff q(x) = K \iff xK = K \iff x \in K. \quad \blacksquare$$

§21. Corolário. *Seja G um grupo e $K \leq G$. Então as condições seguintes são equivalentes:*

1. *$K \trianglelefteq G$.*
2. *$K = \mathrm{Nuc}\, \varphi$ para algum homomorfismo $\varphi : G \to H$.*
3. *$K = \mathrm{Nuc}\, \varphi$ para algum homomorfismo sobrejectivo $\varphi : G \to H$.*

§22. Exercício. Seja G um grupo. Sendo $N \trianglelefteq G$ e $x, y \in G$, mostre que o produto de classes laterais $(xN)(yN)$ definido no Teorema 20 coincide com o produto ponto a ponto: $(xN)(yN) = \{zw \mid z \in xN \text{ e } w \in yN\}$.

V Propriedade universal do quociente

§23. Teorema (Propriedade Universal do Quociente de Grupos). *Seja G um grupo, $K \trianglelefteq G$, e $q : G \to G/K$ o homomorfismo quociente (i.e., $q(g) = gK$ para cada $g \in G$). Para qualquer homomorfismo de grupos*

$$\varphi : G \to H$$

tal que $K \leq \operatorname{Nuc} \varphi$ existe um e um só homomorfismo

$$\overline{\varphi} : G/K \to H$$

tal que $\overline{\varphi} \circ q = \varphi$.

§24. Nota: É comum escrever a última afirmação da seguinte forma: *Para qualquer homomorfismo de grupos $\varphi : G \to H$ tal que $K \leq \operatorname{Nuc} \varphi$ existe um e um só homomorfismo $\overline{\varphi} : G/K \to H$ tal que o diagrama seguinte é comutativo (ou dizemos apenas que o diagrama comuta):*

$$\begin{tikzcd} G \arrow[r, "q"] \arrow[dr, "\varphi"'] & G/K \arrow[d, dotted, "\overline{\varphi}"] \\ & H. \end{tikzcd}$$

(A seta ponteada indica o facto de $\overline{\varphi}$ ser único para a condição dada.)

§25. Nota. Podemos ainda resumir a afirmação do teorema dizendo que estabelece uma bijecção de conjuntos

$$\left\{ \begin{matrix} \text{Homomorfismos } \varphi : G \to H \\ \text{tais que } K \leq \operatorname{Nuc} \varphi \end{matrix} \right\} \cong \left\{ \begin{matrix} \text{Homomorfismos} \\ \overline{\varphi} : G/K \to H \end{matrix} \right\}$$

que, explicitamente da direita para a esquerda, é a função que a cada $\overline{\varphi}$ faz corresponder $\overline{\varphi} \circ q$.

Demonstração. Primeiro vamos demonstrar a unicidade de $\overline{\varphi}$. Esta resulta apenas do facto de q ser uma função sobrejectiva, pois dadas duas funções quaisquer $f, g : G/K \to H$ tais que $f \circ q = g \circ q$ tem-se necessariamente $f = g$ (exercício: verifique). Logo, pode existir no máximo um homomorfismo $\overline{\varphi} : G/K \to H$ tal que $\overline{\varphi} \circ q = \varphi$.

Vamos então demonstrar a existência de $\overline{\varphi}$ no caso em que φ é um homomorfismo cujo núcleo contém K. A condição $\overline{\varphi} \circ q = \varphi$ significa precisamente que para cada $x \in G$ se tem a fórmula

$$\overline{\varphi}(xK) = \varphi(x).$$

Isto significa que $\overline{\varphi}$ está a ser definido nas classes laterais em função de representantes das classes. Tal como quando verificámos que o produto em G/K está bem definido, é necessário verificar que esta definição de $\overline{\varphi}$ faz sentido, ou seja, que não muda quando se mudam os representantes das classes. Por outras palavras, queremos verificar que se $xK = yK$ então necessariamente $\varphi(x) = \varphi(y)$. Mas a condição $xK = yK$ é equivalente a $y^{-1}x \in K$, e portanto por hipótese implica $y^{-1}x \in \operatorname{Nuc}\varphi$, que por sua vez significa que $\varphi(y^{-1}x) = 1$, ou seja, que $\varphi(x) = \varphi(y)$.

Assim verificámos que existe uma única função $\overline{\varphi} : G/K \to H$ tal que $\varphi = \overline{\varphi} \circ q$ e, para concluir a demonstração, falta verificar que $\overline{\varphi}$ é um homomorfismo. Sejam xK e yK duas classes. Então

$$\overline{\varphi}((xH)(yH)) = \overline{\varphi}(xyH) = \varphi(xy) = \varphi(x)\varphi(y) = \overline{\varphi}(xH)\overline{\varphi}(yH). \quad \blacksquare$$

§26. Nota. O teorema diz que $q : G \to G/K$, que tem a propriedade $K \leq \operatorname{Nuc} q$, é "especial" na colecção de todos os homomorfismos $\varphi : G \to H$ que têm a mesma propriedade (i.e., $K \leq \operatorname{Nuc}\varphi$), na medida em que qualquer desses homomorfismos tem uma *factorização única através de* q: qualquer um desses homomorfismos φ pode ser factorizado como uma composição $\varphi = \overline{\varphi} \circ q$ para um único $\overline{\varphi}$. É esta propriedade especial de q que se designa por *propriedade universal do quociente* G/K. Mais precisamente, esta propriedade universal diz respeito ao homomorfismo quociente q, cujo codomínio é G/K, e não apenas ao grupo quociente G/K.

VI Mais propriedades universais

§27. Lema. *Seja G um grupo, $K \trianglelefteq G$, $q : G \to G/K$ o homomorfismo quociente, $\varphi : G \to H$ um homomorfismo de grupos tal que $K \leq \operatorname{Nuc}\varphi$, e $\overline{\varphi} : G/K \to H$ o homomorfismo único tal que $\overline{\varphi} \circ q = \varphi$. Então*

$$\operatorname{Nuc}\overline{\varphi} = q(\operatorname{Nuc}\varphi).$$

Demonstração. Seja $x \in G$. Então

$$x \in \operatorname{Nuc}\varphi \iff \varphi(x) = 1 \iff \overline{\varphi}(xK) = 1 \iff xK \in \operatorname{Nuc}\overline{\varphi}.$$

Logo, $\operatorname{Nuc}\overline{\varphi} = \{xK \mid x \in \operatorname{Nuc}\varphi\} = q(\operatorname{Nuc}\varphi)$, como pretendido. ∎

Vamos agora ver que a bijecção da Nota 25 se restringe à bijecção seguinte, em que a desigualdade $K \leq \operatorname{Nuc}\varphi$ é substituída pela igualdade $K = \operatorname{Nuc}\varphi$ e os homomorfismos $\overline{\varphi}$ são injectivos:

$$\left\{\begin{matrix} \text{Homomorfismos } \varphi : G \to H \\ \text{tais que } K = \operatorname{Nuc}\varphi \end{matrix}\right\} \cong \left\{\begin{matrix} \text{Homomorfismos injectivos} \\ \overline{\varphi} : G/K \to H \end{matrix}\right\}$$

Por outras palavras:

§28. Corolário. *Seja G um grupo, $K \trianglelefteq G$, $q : G \to G/K$ o homomorfismo quociente, $\varphi : G \to H$ um homomorfismo de grupos tal que $K \leq \operatorname{Nuc}\varphi$, e $\overline{\varphi} : G/K \to H$ o homomorfismo único tal que $\overline{\varphi} \circ q = \varphi$. Então $\overline{\varphi}$ é injectivo se e só se $K = \operatorname{Nuc}\varphi$.*

Demonstração. Pelo lema sabemos que $\operatorname{Nuc}\overline{\varphi} = q(\operatorname{Nuc}\varphi)$. Portanto $\overline{\varphi}$ é injectivo se e só se $q(\operatorname{Nuc}\varphi) = K$. Isto significa que $xK = K$ para qualquer $x \in \operatorname{Nuc}\varphi$, ou seja, significa que $\operatorname{Nuc}\varphi \leq K$, e portanto $\operatorname{Nuc}\varphi = K$. ∎

§29. Corolário. *Seja G um grupo, $K \trianglelefteq G$, $q : G \to G/K$ o homomorfismo quociente, $\varphi : G \to H$ um homomorfismo de grupos tal que $K \leq \operatorname{Nuc}\varphi$, e $\overline{\varphi} : G/K \to H$ o homomorfismo único tal que $\overline{\varphi} \circ q = \varphi$. Então $\overline{\varphi}$ é sobrejectivo se e só se φ é sobrejectivo.*

Demonstração. Visto que q é sobrejectivo e $\varphi = \overline{\varphi} \circ q$, é imediato que φ é sobrejectivo se e só se $\overline{\varphi}$ é. ∎

§30. Corolário. *Seja G um grupo, $K \trianglelefteq G$, $q : G \to G/K$ o homomorfismo quociente, $\varphi : G \to H$ um homomorfismo de grupos tal que $K \leq \operatorname{Nuc}\varphi$, e $\overline{\varphi} : G/K \to H$ o homomorfismo único tal que $\overline{\varphi} \circ q = \varphi$. Então $\overline{\varphi}$ é um isomorfismo se e só se φ é sobrejectivo e $K = \operatorname{Nuc}\varphi$.*

Demonstração. Imediato dos dois corolários anteriores. ∎

§31. Corolário (Primeiro Teorema do Isomorfismo). *Seja*

$$\varphi : G \to H$$

um homomorfismo de grupos. Então

$$\varphi(G) \cong G/\operatorname{Nuc}\varphi.$$

Demonstração. Exercício. ∎

§32. Exercício. Considere o grupo diedral D_{16} e o subgrupo normal $K = \langle r^4 \rangle$. Prove que $D_{16}/K \cong D_8$. (Sugestão: defina um homomorfismo sobrejectivo $\varphi : D_{16} \to D_8$ cujo núcleo é K.)