Aulas 11 e 12 — material complementar

As aulas 11 e 12 baseiam-se nas secções 2.4 e 2.5 do livro de Dummit e Foote, e as presentes notas contêm material complementar.

I Reticulados

Recorde que uma *ordem parcial* sobre um conjunto L é uma relação binária $\leq \subset L \times L$ com as seguintes propriedades:

Reflexividade: $x \leq x$ para qualquer $x \in L$;

Transitividades: $x \leq y$ e $y \leq z$ implica $x \leq z$, para quaisquer $x, y, z \in L$;

Anti-simetria: $x \leq y$ e $y \leq x$ implica $x = y$, para quaisquer $x, y \in L$.

Um conjunto L equipado com uma ordem parcial $\leq$ diz-se um *conjunto parcialmente ordenado*. Por vezes usa-se a terminologia *poset* (motivada pelo inglês *partially ordered set*).

As definições de supremo e ínfimo, familiares do estudo dos números reais, são análogas no caso de um poset L: dado um subconjunto $S \subset L$,

- o *máximo* de S, se existir, é o (necessariamente único, devido à anti-simetria) elemento $y \in S$ tal que $x \leq y$ para qualquer $x \in S$;
- o *mínimo* de S, se existir, é o (necessariamente único, devido à anti-simetria) elemento $x \in S$ tal que $x \leq y$ para qualquer $y \in S$;
- um *elemento maximal* de S é um elemento $x \in S$ para o qual a condição $x \leq y$, com $y \in S$, implica $x = y$;
- um *elemento minimal* de S é um elemento $y \in S$ para o qual a condição $x \leq y$, com $x \in S$, implica $x = y$;

- um *majorante* de S é um elemento $y \in L$ tal que $x \leq y$ para qualquer $x \in S$, e denotamos por S^u o conjunto de todos os majorantes de S ("u" de "upper bound");

- um *minorante* de S é um elemento $x \in L$ tal que $x \leq y$ para qualquer $y \in S$, e denotamos por S_ℓ o conjunto de todos os minorantes de S ("ℓ" de "lower bound");

- diz-se que S *tem supremo* se S^u tem mínimo, o qual nesse caso se denota por $\sup S$ ou $\bigvee S$ e se designa por *supremo* de S;

- diz-se que S *tem ínfimo* se S_ℓ tem máximo, o qual nesse caso se denota por $\inf S$ ou $\bigwedge S$ e se designa por *ínfimo* de S.

§1. Definição. Um *reticulado* é um conjunto L equipado com uma ordem parcial $\leq$ tal que para quaisquer $x, y \in L$ existe o supremo de $\{x, y\}$, que se denota por $\sup(x, y)$ ou $x \vee y$, e o ínfimo de $\{x, y\}$, que se denota por $\inf(x, y)$ ou $x \wedge y$.

§2. Exercício. Demonstre as seguintes afirmações a respeito de um poset L:

1. $\bigvee \emptyset$, se existir, é o mínimo de L — nesse caso denota-se esse elemento por 0_L ou simplesmente 0;

2. $\bigwedge \emptyset$, se existir, é o máximo de L — nesse caso denota-se esse elemento por 1_L ou simplesmente 1;

3. $\bigvee L$, se existir, é igual a 1;

4. $\bigwedge L$, se existir, é igual a 0.

§3. Exercício. Demonstre as seguintes afirmações a respeito de um reticulado L:

1. $(L, \vee)$ e $(L, \wedge)$ são semigrupos idempotentes e comutativos;

2. $(L, \vee)$ é um monóide se e só se L tem mínimo;

3. $(L, \wedge)$ é um monóide se e só se L tem máximo;

4. Para quaisquer $x, y \in L$ tem-se $x \wedge (x \vee y) = x$ e $x \vee (x \wedge y) = x$ (leis de *absorção*).

§4. Exercício. Diz-se que um semigrupo idempotente e comutativo L é um *semireticulado*. Demonstre que, se num semireticulado L definirmos $x \leq y$ pela condição $xy = x$, então $\leq$ é uma ordem parcial e para quaisquer $x, y \in L$ o ínfimo $x \wedge y$ existe e é igual a xy. Demonstre que, se definirmos $x \leq y$ pela condição $xy = y$ então para quaisquer $x, y \in L$ o supremo $x \vee y$ existe e é igual a xy.

§5. Exercício. Mostre que um reticulado L é o mesmo que um conjunto L equipado com duas operações binárias $\wedge$ e $\vee$ tais que $(L, \wedge)$ e $(L, \vee)$ são semireticulados e as leis de absorção são satisfeitas.

§6. Definição. Um *reticulado completo* é um poset L tal que qualquer subconjunto $S \subset L$ tem ínfimo $\bigwedge S$ e supremo $\bigvee S$.

§7. Exercício. Demonstre que:

1. Um poset L é um reticulado completo se e só se qualquer subconjunto $S \subset L$ tem supremo $\bigvee S$;
2. Um poset L é um reticulado completo se e só se qualquer subconjunto $S \subset L$ tem ínfimo $\bigwedge S$;
3. Qualquer reticulado completo é um reticulado.

§8. Exemplos.

1. O conjunto $\mathbb{R}$, com a ordenação habitual, é um conjunto *totalmente* ordenado, ou seja, é um poset tal que para quaisquer $x, y \in \mathbb{R}$ se tem $x \leq y$ ou $y \leq x$.
2. Qualquer conjunto totalmente ordenado L é um reticulado tal que para quaisquer $x, y \in L$ se tem $x \vee y = \max(x, y)$ e $x \wedge y = \min(x, y)$.
3. $\mathbb{Z}_{\geq 1}$, equipado com a ordem de divisibilidade,[1] é um reticulado, sem máximo e com mínimo igual a 1, no qual se tem $m \vee n = \mathrm{mmc}(m, n)$ e $m \wedge n = \mathrm{mdc}(m, n)$.
4. Seja $n \in \mathbb{Z}_{\geq 1}$. O conjunto dos divisores de n, novamente equipado com a ordem de divisibilidade, é um reticulado com máximo n e mínimo 1.

[1] m é "menor ou igual" a n se e só se $m \mid n$.

5. Dado um conjunto X, o conjunto das partes de X, denotado por $\mathcal{P}(X)$, é um reticulado completo cuja ordem parcial é a inclusão de subconjuntos: $Y \leq Z$ se e só se $Y \subset Z$. Em particular, dados dois subconjuntos $Y, Z \subset X$, tem-se $X \vee Y = X \cup Y$ e $X \wedge Y = X \cap Y$. Mais geralmente, dado um conjunto $\mathcal{S}$ de subconjuntos de X, $\bigvee \mathcal{S}$ é a união de todos os elementos de $\mathcal{S}$, que denotamos por $\bigcup \mathcal{S}$; e $\bigwedge \mathcal{S}$ é a intersecção de todos os elementos de $\mathcal{S}$, que denotamos por $\bigcap \mathcal{S}$.

6. Dado um conjunto infinito X, o conjunto das partes finitas de X é um reticulado mas não um reticulado completo (porquê?).

7. Dado um grupo G, o conjunto $\mathrm{Sub}(G)$ dos subgrupos de G, ordenado pela relação de inclusão, é um reticulado completo.

   Demonstração. Já vimos que, para qualquer colecção não vazia de subgrupos $(H_i)_{i \in I}$, a intersecção $\bigcap_{i \in I} H_i$ é um subgrupo de G, e portanto tem-se $\bigwedge_{i \in I} H_i = \bigcap_{i \in I} H_i$. Por outro lado, o ínfimo da família vazia $\bigwedge \emptyset$ existe porque $\mathrm{Sub}(G)$ tem máximo, ou seja, tem-se $\bigwedge \emptyset = G$. Portanto qualquer colecção de subgrupos tem ínfimo, e por isso $\mathrm{Sub}(G)$ é um reticulado completo. ∎

8. Dado um espaço vectorial complexo V, o conjunto $\mathrm{Sub}(V)$ dos subespaços lineares de V, ordenado pela relação de inclusão, é um reticulado completo. Tal como no caso dos subgrupos, tem-se $\bigwedge \emptyset = V$ e o ínfimo de qualquer colecção não vazia de subespaços é igual à intersecção desses subespaços.

§9. Exercício. Justifique que o supremo de uma família não vazia $(H_i)_{i \in I}$ de subgrupos de G é igual a $\bigcap\left((\bigcup_{i \in I} H_i)^u\right)$. Ou, usando outra notação,

$$\bigvee_{i \in I} H_i = \bigcap_{K \leq G,\ \forall_i (H_i \leq K)} K.$$

§10. Exercício. Mostre que se $\mathcal{S} \subset \mathrm{Sub}(G)$ for uma colecção totalmente ordenada de subgrupos de G então $\bigvee \mathcal{S} = \bigcup \mathcal{S}$.

§11. Exercício. Mostre que se $\mathcal{S} \subset \mathrm{Sub}(V)$ for uma colecção totalmente ordenada de subespaços lineares de um espaço vectorial complexo V então $\bigvee \mathcal{S} = \bigcup \mathcal{S}$.

§12. Exercício. Mostre que se V e W forem dois subespaços lineares de um espaço vectorial U sobre um corpo qualquer, então $V \vee W = V + W$. (Recorde que $V + W = \{x + y \mid x \in V,\ y \in W\}$.)

§13. EXERCÍCIO. Mostre que se A e B forem dois subgrupos de um grupo abeliano G, então $A \vee B = A + B$, onde se define $A+B = \{a+b \mid a \in A,\ b \in B\}$.)

II Geradores de subgrupos

Seja G um grupo e $A \subset G$. O *subgrupo de G gerado por A* é

$$\langle A \rangle = \bigcap_{H \leq G,\ A \subset H} H.$$

Por outras palavras, $\langle A \rangle$ é o menor subgrupo de G que contém A. Se A for um conjunto finito $\{a_1, \ldots, a_k\}$, então omitimos as chavetas e denotamos $\langle A \rangle$ por $\langle a_1, \ldots, a_k \rangle$. Em particular, se $A = \{a\}$ escrevemos $\langle a \rangle$; este é o *subgrupo cíclico gerado por a*, e recordemos que um grupo G é *cíclico* se existir $a \in G$ tal que $G = \langle a \rangle$.

§14. EXEMPLO. $\langle \emptyset \rangle$ é o subgrupo trivial $\{1\}$.

Como sabemos, o subgrupo cíclico $\langle a \rangle$ contém exactamente os elementos a^n com $n \in \mathbb{Z}$. De igual modo, podemos sempre obter uma expressão explícita para os elementos de $\langle A \rangle$, para qualquer conjunto $A \subset G$:

§15. DEFINIÇÃO. Seja G um grupo e $A \subset G$ um conjunto. Define-se o conjunto $\overline{A} \subset G$ da seguinte forma: um elemento $g \in G$ pertence a $\overline{A}$ se e só se $g = 1$ ou então existem $k \in \mathbb{Z}_{\geq 1}$ e elementos $a_1, \ldots, a_k \in A$, e inteiros $n_1, \ldots, n_k \in \{-1, 1\}$, tais que $g = a_1^{n_1} \cdots a_k^{n_k}$.

Alternativamente, escrevendo

$$A^{-1} = \{a^{-1} \mid a \in A\} \quad e \quad AB = \{ab \mid a \in A,\ b \in B\}$$

para quaisquer subconjuntos $A, B \subset G$, e usando a notação $A^1 = A$, $A^2 = AA$, $A^3 = AAA$, etc., temos

$$\overline{A} = \{1\} \cup \bigcup_{n \in \mathbb{Z}_{\geq 1}} (A \cup A^{-1})^n.$$

§16. PROPOSIÇÃO. *Seja $A \subset G$, para um grupo G. Então $\langle A \rangle = \overline{A}$.*

Demonstração. Primeiro, se $H \leq G$ e $A \subset H$ então é claro que $1 \in H$, $A^{-1} \subset H$, $(A \cup A^{-1})^2 \subset H$, $(A \cup A^{-1})^3 \subset H$, etc., ou seja, $\overline{A} \subset H$. Portanto $\overline{A} \subset \langle A \rangle$. Para verificar que na verdade há uma igualdade $\overline{A} = \langle A \rangle$ é suficiente verificar que $\overline{A}$ é um subgrupo (pois por construção temos $A \subset \overline{A}$). Em primeiro lugar, por construção temos $1 \in \overline{A}$. E dado um elemento arbitrário $g = a_1^{n_1} \cdots a_k^{n_k}$ o seu inverso é $a_k^{-n_k} \cdots a_1^{-n_1}$, que também é um elemento de $\overline{A}$. Finalmente, dado outro elemento de A, $h = b_1^{m_1} \cdots b_k^{m_k}$, o produto gh é

$$a_1^{n_1} \cdots a_k^{n_k} b_1^{m_1} \cdots b_k^{m_k},$$

que também é um elemento de $\overline{A}$. Logo, $\overline{A} \leq G$ e portanto $\overline{A} = \langle A \rangle$. ∎

§17. Corolário. *Seja G um grupo e $H, K \subset G$. O supremo de H e K é dado pela fórmula*

$$H \vee K = \langle H \cup K \rangle.$$

De igual modo, dada uma família de subgrupos $(H_i)_{i \in I}$,

$$\bigvee_{i \in I} H_i = \left\langle \bigcup_{i \in I} H_i \right\rangle,$$

onde se convenciona que $\bigcup_{i \in \emptyset} H_i = \emptyset$, e portanto $\bigvee_{i \in \emptyset} H_i = \{1\}$.

§18. Exercício. Calcule todos os elementos dos seguintes subgrupos de D_8:

1. $\langle s, r \rangle$
2. $\langle s, r^2 \rangle$
3. $\langle sr^2, r^2 \rangle$
4. $\langle sr, r^2 \rangle$.

III Diagramas de Hasse

Dado um poset finito L, representa-se diagramaticamente a ordem de L por meio de um *diagrama de Hasse*. Cada elemento de L é representado por um símbolo, que pode ser o símbolo genérico $\circ$, e cada relação $x \leq y$ é representada por um segmento de recta que sobe de x para y, omitindo-se os segmentos que são redundantes por resultarem da transitividade de $\leq$.

Por exemplo, $L = \{0, a, b, c, 1\}$, com mínimo 0 e máximo 1, e a, b e c não comparáveis entre si, representa-se pelo seguinte diagrama de Hasse:

$$\begin{tikzcd}
 & 1 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
a \arrow[dr, dash] & b \arrow[d, dash] & c \arrow[dl, dash] \\
 & 0 &
\end{tikzcd}$$

IV Exemplos com grupos finitos

Na aula anterior vimos exemplos de diagramas de Hasse para reticulados de subgrupos de grupos cíclicos finitos, nomeadamente $\mathbb{Z}/12\mathbb{Z}$, Z_{36} e Z_{30}.

§19. Exercício. Mostre que o reticulado de subgrupos de $\mathbb{Z}/12\mathbb{Z}$ é isomorfo ao reticulado de divisores de 12 equipado com a ordem oposta da ordem de divisibilidade, ou seja, tal que m é "menor que" n se $n \mid m$. Justifique que para cada par de divisores m e n de 12 se tem $\langle\overline{m}\rangle \vee \langle\overline{n}\rangle = \langle \mathrm{mdc}(m, n)\rangle$ e $\langle\overline{m}\rangle \wedge \langle\overline{n}\rangle = \langle \mathrm{mmc}(m, n)\rangle$.

§20. Exercício. Desenhe diagramas de Hasse para $\mathrm{Sub}(G)$ nos casos seguintes:

1. $G = D_8$;
2. $G = D_{10}$;
3. $G = Q_8$;
4. $G = S_3$.

V Funções entre reticulados

§21. Definição. Dados dois posets P e Q, uma *função monótona*

$$f : P \to Q$$

é uma função tal que $f(x) \leq f(y)$ sempre que $x \leq y$. Se a função monótona f for bijectiva e a sua inversa $f^{-1} : Q \to P$ também for monótona então f diz-se um *isomorfismo de ordem*.

Dois posets P e Q dizem-se *isomorfos*, e escrevemos $P \cong Q$, se existir um isomorfismo de ordem $f : P \to Q$.

§22. Exercício. Dê um exemplo de dois posets P e Q e de uma função monótona bijectiva $f : P \to Q$ que não é um isomorfismo de ordem.

§23. Exercício. Prove que se $f : P \to Q$ for um isomorfismo de ordem então para qualquer $S \subset P$ o conjunto $f(S)$ tem supremo se e só se S tiver supremo, e que nesse caso se tem

$$\bigvee f(S) = f(\bigvee S).$$

Verifique que a mesma afirmação é válida se substituirmos supremos por ínfimos.

§24. Exercício. Seja $\varphi : G \to H$ um homomorfismo de grupos. Mostre que a função $\overline{\varphi} : \mathrm{Sub}(G) \to \mathrm{Sub}(H)$ que a cada subgrupo $K \leq G$ faz corresponder o contradomínio $\varphi(K)$ é monótona.

§25. Exercício. Mostre que se $\varphi : G \to H$ for um isomorfismo de grupos então $\overline{\varphi} : \mathrm{Sub}(G) \to \mathrm{Sub}(H)$ é um isomorfismo de ordem.

§26. Exercício. Dê um exemplo de um par de grupos finitos G e H não isomorfos cujos reticulados de subgrupos são isomorfos (v. exercícios 12–14 da secção 2.5 do livro).

§27. Definição. Sejam P e Q dois posets. Uma função $f : P \to Q$ diz-se um *mergulho de ordem* se para quaisquer $x, y \in P$ se tiver a equivalência

$$x \leq y \iff f(x) \leq f(y).$$

§28. Exercício. Mostre que:

1. Qualquer mergulho de ordem é uma função injectiva;

2. Um isomorfismo de ordem é o mesmo que um mergulho de ordem sobrejectivo.

§29. Exercício. Mostre que se $\varphi : G \to H$ for um homomorfismo injectivo de grupos então $\overline{\varphi} : \mathrm{Sub}(G) \to \mathrm{Sub}(H)$ é um mergulho de ordem.

VI Alguns exercícios da secção 2.5 do livro

1. (Exercício 4) Observando o diagrama de Hasse do reticulado de subgrupos de D_8, obtenha todos os pares de elementos de D_8 que geram todo o grupo (há doze pares).

2. (Exercício 6) Use os reticulados de subgrupos para encontrar todos os centralizadores de cada elemento de cada um dos grupos seguintes:
   (a) D_8
   (b) Q_8
   (c) S_3
   (d) D_{16}.

3. (Exercício 8) Em cada um dos grupos seguintes, encontre o normalizador de cada subgrupo:
   (a) S_3
   (b) Q_8.

VII Produtos ponto a ponto de subgrupos

Num exercício acima já verificámos que se G for um grupo abeliano e $A, B \leq G$, então $A \vee B = A + B$. Ou, em notação multiplicativa,

$$A \vee B = AB = \{ab \mid a \in A,\ b \in B\}.$$

De igual modo, para um grupo arbitrário G, abeliano ou não, define-se o *produto (ponto a ponto)* de dois subgrupos H e K da seguinte forma:

$$HK = \{hk \mid h \in H, k \in K\}.$$

Contudo, ao contrário do que se passa se G for abeliano, HK não tem de ser um subgrupo de G.

§30. LEMMA. *Seja G um grupo e $H_1, H_2, K \leq G$. Então as condições seguintes são equivalentes:*

1. $H_1 \leq K$ *e* $H_2 \leq K$.

2. $H_1 \vee H_2 \leq K$.

3. $H_1H_2 \subset K$.

Em particular, temos

$$H_1 \cup H_2 \subset H_1H_2 \subset H_1 \vee H_2.$$

Demonstração. 1 e 2 são equivalentes pela definição de supremo. Uma vez que $H_1 \vee H_2$ tem de conter, em particular, os produtos h_1h_2 com $h_1 \in H_1$ e $h_2 \in H_2$, conclui-se que $H_1H_2 \subset H_1 \vee H_2$, e portanto 2 implica 3. Finalmente, 3 implica 1 porque $H_1 \subset H_1H_2$ (porque $1 \in H_2$) e $H_2 \subset H_1H_2$ (porque $1 \in H_1$). A conclusão $H_1 \cup H_2 \subset H_1H_2 \subset H_1 \vee H_2$ é imediata. ∎

§31. Proposição. *Seja G um grupo e $H, K \leq G$. Então as condições seguintes são equivalentes:*

1. $HK \leq G$;
2. $HK = KH$;
3. $HK = H \vee K$.

Demonstração. ($1 \Rightarrow 2$) Assuma-se que HK é um subgrupo de G. Então

$$\begin{aligned} HK &= (HK)^{-1} = \{(hk)^{-1} \mid h \in H,\ k \in K\} \\ &= \{k^{-1}h^{-1} \mid h \in H,\ k \in K\} = KH. \end{aligned}$$

($2 \Rightarrow 1$) Assuma-se que $HK = KH$. Vamos ver que $HK \leq G$:

- $1 \in HK$ — Isto é evidente, pois $1 \in H$ e $1 \in K$.
- $(HK)^{-1} \subset HK$ — Seja hk um elemento genérico de HK ($h \in H$ e $k \in K$). Então $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$.
- $HKHK \subset HK$ — Sejam $h_1, h_2 \in H$ e $k_1, k_2 \in K$, de modo que h_1k_1 e h_2k_2 são elementos arbitrários de HK. Uma vez que $HK = KH$, o elemento k_1h_2 é igual a h_3k_3 para algum par de elementos $h_3 \in H$ e $k_3 \in K$, pelo que

  $$(h_1k_1)(h_2k_2) = h_1h_3k_3k_2 \in HK.$$

  ($1 \Rightarrow 3$) Pelo lema anterior temos $H \cup K \subset HK \subset H \vee K$. Logo, se $HK \leq G$, pela definição de supremo temos $HK = H \vee K$ porque $H \vee K$ é o menor subgrupo de G que contém H e K.

  ($3 \Rightarrow 2$) Imediato, pois $\vee$ é uma operação comutativa. ∎

§32. PROPOSIÇÃO. *Seja G um grupo e $H, K \leq G$. Então*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Demonstração. Será feita nas aulas (ver Proposição 13 da secção 3.2 do livro). ∎

§33. NOTA. Repare-se na semelhança da fórmula acima com as seguintes, para subconjuntos finitos $X, Y \subset Z$ e subespaços vectoriais de dimensão finita $V, W \subset U$:

$$\begin{aligned} |X \cup Y| &= |X| + |Y| - |X \cap Y| \\ \dim(V + W) &= \dim(V) + \dim(W) - \dim(V \cap W). \end{aligned}$$