ELEMENTOS DE ÁLGEBRA

TIAGO MACEDO

Aula 2

Avisos: A página da disciplina é http://ict.unifesp.br/tmacedo/elementos_algebra, e ela vai conter a ementa da disciplina, fotos das aulas e notas de aula.

Notação 2.1. Dado um grupo (G, m), a partir de agora, vamos denotar:

- $m(g, , h)$ por gh para quaisquer $g, h \in G$,
- $gg \cdots g$ (k vezes) por g^k para quaisquer $g \in G$ e $k > 0$,
- $\tilde{g}$ por g^{-1} para qualquer $g \in G$,
- $g^{-1}g^{-1} \cdots g^{-1}$ (k vezes) por g^{-k} para quaisquer $g \in G$ e $k > 0$,
- g^0 por e para qualquer $g \in G$.

Além disso, quando não gerar confusão, nós vamos omitir a operação binária m e denotar o grupo (G, m) simplesmente por G.

Exemplo 2.2. O conjunto com um único elemento $\{e\}$ munido da única operação binária $m\colon \{e\} \times \{e\} \to \{e\}$ (dada por $m(e, e) = e$) é um grupo (abeliano). Esse grupo é chamado de grupo trivial.

Exercício 2.3. Dado um grupo G, mostre que $e^k = e$ para todo $k \in \mathbb{Z}$. (Sugestão: mostre que $e^{-1} = e$ e use indução duas vezes, para $k > 0$ e para $k < 0$.)

Definição 2.4. Dados um grupo G, definimos a ordem de G como $|G|$. Dado um elemento $g \in G$, definimos a ordem de g como o menor inteiro positivo o tal que $g^o = e$, se tal inteiro existir; e como infinito, se tal inteiro não existir. Denote a ordem de g em G por $|g|$ ou por $o(g)$.

Exemplo 2.5. Considere o conjunto $\mathbb{C}\backslash\{0\}$ munido da operação binária dada pela multiplicação usual de números complexos. Verifique que $(\mathbb{C}\backslash\{0\}, \cdot)$ é um grupo abeliano, cujo elemento neutro é 1 e o elemento inverso de $z \in \mathbb{C} \setminus \{0\}$ é $z^{-1} = \frac{\overline{z}}{\|z\|}$.

Se $z = e^{\frac{\pi}{3}}$, a raiz sexta primitiva da unidade, então $o(z) = 6$. De fato,

$$z^2 = e^{\frac{2\pi}{3}} \neq 1, \quad z^3 = e^{\pi} \neq 1, \quad z^4 = e^{\frac{4\pi}{3}} \neq 1, \quad z^5 = e^{\frac{5\pi}{3}} \neq 1 \quad \text{e} \quad z^6 = e^{2\pi} = 1.$$

Verifique também que $o\left(e^{\pi}\right) = 2$, $o\left(e^{\frac{2\pi}{3}}\right) = o\left(e^{\frac{4\pi}{3}}\right) = 3$ e $o\left(e^{\frac{5\pi}{3}}\right) = 6$.

Exemplo 2.6. Considere o grupo abeliano $(\mathbb{Z}, +)$. Observe que a ordem do elemento 0 é 1. Além disso, a ordem de todo elemento $n \neq 0$ é infinita. De fato, se a ordem de n fosse $k > 0$, então teríamos que $kn = 0$. Como $n \neq 0$ e $k \neq 0$, isso é impossível.

A seguir, nós vamos dar outros exemplos de grupos e, em particular, calcular as ordens de alguns de seus elementos.

0.3. Inteiros módulo n

Durante toda essa seção, fixe um inteiro positivo n. Considere o conjunto $\mathbb{Z}_n$ formado pelos símbolos $\{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. Para definir a operação binária $m\colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, vamos explicar o que esses símbolos representam.

Considere a relação no conjunto $\mathbb{Z}$ dada por

$$a \sim b \qquad \text{se, e somente se,} \qquad n \text{ divide } a - b \quad (\text{denotado } n|(a-b)).$$

Observe que essa é uma relação de equivalência. De fato:

- Para todo $a \in \mathbb{Z}$, temos que $a \sim a$, pois $n|0 = a - a$;
- Se $a, b \in \mathbb{Z}$ e $a \sim b$, ou seja, $n|(a-b)$, então $n|(b-a)$, ou seja, $b \sim a$;
- Se $a, b, c \in \mathbb{Z}$, $a \sim b$ e $b \sim c$, isso significa que existem $k, \ell \in \mathbb{Z}$ tais que $kn = (a-b)$ e $\ell n = (b-c)$. Então temos que $(a-c) = (a-b) + (b-c) = kn + \ell n = (k+l)n$, ou seja, $n|(a-c)$. Portanto $a \sim c$.

As classes de equivalência desta relação $\sim$ (ou seja, os subconjuntos disjuntos de $\mathbb{Z}$ dentro dos quais todos os elementos são equivalentes entre si) serão denotados por $\overline{k}$ ($k \in \mathbb{Z}$). Observe que essas classes de equivalência podem ser representadas pelos restos das divisões dos inteiros por n. De fato, se $k \in \mathbb{Z}$ for escrito como $k = qn + r$ (onde q é o quociente e r é o resto da divisão), então $(k - r) = qn$, ou seja, $k \sim r$, ou equivalentemente, $\overline{k} = \overline{r}$. Como $0 \leq r < n$ e n não divide $a - b$ quando $a, b \in \{0, \dots, n-1\}$, então o conjunto $\mathbb{Z}_n$ é formado exatamente pelas classes de equivalência dos inteiros pela relação $\sim$.

Agora defina uma operação binária $m\colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ da seguinte forma $m(\overline{a}, \overline{b}) = \overline{(a+b)}$. Primeiro, vamos verificar que m está bem definida (ou seja, que ela não depende dos representantes que nós pegamos para $\overline{a}$ e $\overline{b}$). Lembre que os elementos da classe de equivalência $\overline{a}$ (respectivamente, $\overline{b}$) são da forma $a + nz$ (resp. $b + nz$) para algum $z \in \mathbb{Z}$. Para quaisquer $z, w \in \mathbb{Z}$, pela definição, temos que $m(\overline{a+nz}, \overline{b+nw}) = \overline{(a+b+n(z+w))} = \overline{(a+b)} = m(\overline{a}, \overline{b})$. Portanto m está bem definida.

Exercício 2.7. Verifique que $(\mathbb{Z}_n, m)$ é um grupo abeliano (finito). Além disso, mostre que

$$o(\overline{k}) = \frac{\mathrm{mmc}(k,n)}{k} = \frac{n}{\mathrm{mdc}(k,n)} \qquad \text{para todo } k \in \{1, \dots, n-1\}.$$