NOTAS DE AULA DE ELEMENTOS DE ÁLGEBRA

TIAGO MACEDO

Aula 4

Geradores e relações

Da discussão acima, nós observamos que todos os elementos de D_{2n} podem ser obtidos como produtos finitos dos elementos r e s. Por isso, dizemos que D_{2n} é gerado por $\{r, s\}$, ou que r, s são geradores de D_{2n}. Mas nem todos os produtos de r com s são distintos. Por exemplo, nós vimos que $r^2 = s^n = \mathrm{id}_{\Delta_n}$. Essas identidades são chamadas de relações. Todo grupo pode ser descrito através de um conjunto de geradores satisfazendo um conjunto de relações. (Esse não é um resultado imediato.) Uma descrição de um grupo G dessa forma,

$$G = \langle \text{geradores} \mid \text{relações} \rangle$$

é chamada de presentação de G.

A presentação de um grupo, em geral, não é única. Mas, dada uma presentação de um grupo G, deve ser possível escrever todos os elementos de G como produtos finitos dos elementos do conjunto de geradores, e deduzir todas as relações entre elementos de G a partir do conjunto de relações.

Exemplo 4.1. Uma presentação de D_{2n} é $\langle r, s \mid r^2 = s^n = e, rs = sr^{-1} \rangle$.

Exemplo 4.2. Uma presentação de $(\mathbb{Z}, +)$ é $\langle 1 \mid \emptyset \rangle$, ou simplesmente $\langle 1 \rangle$.

Exemplo 4.3. Uma presentação de $\mathbb{Z}_n$ é $\langle \bar{1} \mid n\bar{1} = \bar{0} \rangle$.

Exemplo 4.4. Uma presentação de $\mathbb{H} = Q_8$ é $\langle i, j \mid i^4 = 1, i^2 = j^2, iji = j \rangle$.

Exemplo 4.5. Uma presentação de S_n é

$$\langle s_1, \ldots, s_{n-1} \mid s_i^2 = e,\ (s_i s_{i+1})^3 = e,\ s_i s_j = s_j s_i\ (j \neq i \pm 1) \rangle.$$

1.6. Homomorfismos e isomorfimos

Definição 4.6. Sejam (G, m_G) e (H, m_H) dois grupos. Um homomorfismo de grupos de G para H é uma função $f\colon G \to H$ satisfazendo:

(i) $f(m_G(g_1, g_2)) = m_H(f(g_1), f(g_2))$ para todos $g_1, g_2 \in G$,
(ii) $f(e_G) = e_H$.

Um isomorfismo de grupos é um homomorfismo de grupos que é bijetor. Dizemos que o grupo G é isomorfo ao grupo H quando existe algum isomorfismo de grupos $f\colon G \to H$. Neste caso, denotamos $G \cong H$.

Um homomorfismo entre dois grupos é uma função que preserva a estrutura importante que esses conjuntos têm, a de grupo. Quando existe um isomorfismo entre dois grupos, isso significa que a estrutura de grupo de um pode ser transferida para o outro sem perder informação. Ou seja, quando dois grupos são isomorfos, eles são, de certa forma, idênticos. O próximo resultado mostra algumas evidências disso.

Lema 4.7. *Sejam G e H dois grupos.*

(a) Se $f\colon G \to H$ é um homomorfismo de grupos, então $f(g^n) = f(g)^n$ para todo $n \in \mathbb{Z}$. Em particular, $f(g^{-1}) = f(g)^{-1}$ para todo $g \in G$.
(b) Se $G \cong H$, então $|G| = |H|$ (os dois conjuntos têm a mesma cardinalidade).
(c) Se $G \cong H$ e G é abeliano, então H é abeliano.
(d) Se $f \cong G \to H$ for um isomorfismo, então $o(f(g)) = o(g)$ para todo $g \in G$.

Demonstração. (a) Fixe $g \in G$. Se $n = 0$, então $f(g^0) = f(e_G) = e_H = f(g)^0$. Vamos usar indução para $n > 0$. O caso $n = 1$ é óbvio, então suponha que $f(g^{n-1}) = f(g)^{n-1}$. Como f é um homomorfismo de grupos, pela hipótese de indução, nós temos que

$$f(g^n) = f(gg^{n-1}) = f(g)f(g^{n-1}) = f(g)f(g)^{n-1} = f(g)^n.$$

Isso prova o caso $n \geq 0$. Para $n = -1$, observe que $f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$ e $f(g^{-1})f(g) = f(g^{-1}g) = f(e_G) = e_H$. Portanto $f(g^{-1})$ é o inverso de $f(g)$. Para completar a demonstração, use indução para $n < 0$.

(b) Se $G \cong H$, então exite um isomorfismo $f\colon G \to H$. Em particular, f é uma bijeção entre os conjuntos G e H. Portanto $|G| = |H|$.

(c) Seja $f\colon G \to H$ um isomorfismo. Em particular, f é sobrejetora, ou seja, para cada $h \in H$, existe $g \in G$ tal que $f(g) = h$. Dados $h_1, h_2 \in H$, tome $g_1, g_2 \in G$ tais que $f(g_1) = h_1$ e $f(g_2) = h_2$. Como$f$ é um homomorfismo de grupos e G é abeliano, então

$$h_1h_2 = f(g_1)f(g_2) = f(g_1g_2) = f(g_2g_1) = f(g_2)f(g_1) = h_2h_1.$$

Isso mostra que H é abeliano.

(d) Dado $g \in G$, denote $o(g) = n$ e lembre que $g^n = e_G$ e $e_G \notin \{g, g^2, \ldots, g^{n-1}\}$. Como f é um isomorfismo, em particular, $f(e_G) = e_H$ e f é injetora. Logo, $f(g) = e_H$ se, e somente se, $g = e_G$. Portanto $f(g)^n = f(g^n) = f(e_G) = e_H$ e $e_H \notin \{f(g), f(g)^2, \ldots, f(g)^{n-1}\}$. Isso mostra que $o(f(g)) = n$. □

Exercício 4.8. Sejam G, H e K três grupos.

(a) Mostre que $\mathrm{id}_G\colon G \to G$ é um isomorfismo de grupos.
(b) Se $f\colon G \to H$ é um isomorfismo de grupos, mostre que $f^{-1}\colon H \to G$ também é um isomorfismo de grupos.
(c) Se $\phi\colon G \to H$ e $\psi\colon H \to K$ forem homomorfismos (resp. isomorfismos) de grupos, mostre que $(\psi \circ \phi)\colon G \to K$ é um homomorfismo (resp. isomorfismo) de grupos.
(d) Conclua que $\cong$ (isomorfismo de grupos) é uma relação de equivalência.

Um exemplo de homomorfismo de grupos que já é familiar é o seguinte.

Exemplo 4.9. Considere dois $\mathbb{R}$-espaços vetoriais $(V, +_V, \cdot_V)$ e $(W, +_W, \cdot_W)$. Pela definição, toda transformação linear $T\colon V \to W$ é um homomorfismo do grupo $(V, +_V)$ para o grupo $(W, +_W)$. Além disso, todo isomorfismo linear $T\colon V \to W$ é um isomorfismo do grupo $(V, +_V)$ para o grupo $(W, +_W)$.

Um caso particular do exemplo anterior é o seguinte.

Exemplo 4.10. Considere o grupo aditivo $\mathbb{R}$, o grupo multiplicativo $\mathbb{R}_{>0} = \{\alpha \in R \mid \alpha > 0\}$ e a função $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$ dada por $\exp(a) = e^a$. Vamos mostrar que exp é um isomorfismo de grupos.

(i) $\exp(a + b) = e^{a+b} = e^ae^b = \exp(a) \cdot \exp(b)$ para todos $a, b \in \mathbb{R}$.
(ii) $\exp(0) = e^0 = 1$

Isso mostra que exp é um homomorfismo de grupos. Além disso, $\ln\colon \mathbb{R}_{>0} \to \mathbb{R}$ é a inversa de exp. Portanto, exp é uma bijeção, e consequentemente, um isomorfismo de grupos.

O próximo exemplo mostra que, dados quaisquer dois grupos, sempre existe algum homomorfismo entre eles.

Exemplo 4.11. Sejam G e H dois grupos. Verifique que a função $f\colon G \to H$ dada por $f(g) = e_H$ para todo $g \in G$ é um homorfismo de grupos. Esse homomorfismo é chamado de homomorfismo trivial. Observe que esse homomorfismo é um isomorfismo se, e somente se, $G = H = \{e\}$.

Exemplo 4.12. Seja $n \geq 3$. Verifique que a função $\vartheta\colon D_{2n} \to S_n$ definida na Seção 1.2 (Aula 3) é um homomorfismo de grupos. Além disso, mostre que ϑ é um isomorfismo se, e somente se, $n = 3$.

Nos próximos exemplos, vamos usar geradores e relações para construir homomorfismo de grupos.

Exemplo 4.13. Considere os grupos abelianos $\mathbb{Z}$ e $\mathbb{Z}_n$ ($n \geq 2$). Para cada $k \in \mathbb{Z}$, podemos definir um único homomorfimo de grupos $f_k\colon \mathbb{Z} \to \mathbb{Z}_n$ satisfazendo $f_k(1) = \overline{k}$. De fato, como 1 gera $\mathbb{Z}$ e queremos que f_k seja um homomorfismo de grupos, então $f_k(\ell) = k\ell$ para todo $\ell \in \mathbb{Z}$. Em particular, se escolhermos $k = 0$, obteremos o homoorfismo trivial; e se escolhermos $k = 1$, obteremos um homomorfismo chamado de projeção canônica.

Exemplo 4.14. Considere agora os grupos aditivos $\mathbb{Z}_2$ e $\mathbb{Z}_6$. Assim como no exemplo anterior, para cada $k \in \mathbb{Z}$, vamos tentar construir um homomorfismo de grupos $f_k\colon \mathbb{Z}_2 \to \mathbb{Z}_6$. Se definirmos $f_k(\overline{1}) = \overline{k}$, como queremos que f_k seja um homomorfismo de grupos, teremos que:

$$f_k(\overline{0}) = f_k(\overline{1} + \overline{1}) = f_k(\overline{1}) + f_k(\overline{1}) = \overline{2k} = \overline{0}.$$

Mas, observe que $\overline{2k} = \overline{0}$ se, e somente se, $\overline{k} \in \{\overline{0}, \overline{3}\}$. Em particular, $f_1(\overline{1}) = \overline{1}$ **não** induz um homomorfismo de grupos.

Mas se, assim como $\mathbb{Z}$, o grupo $\mathbb{Z}_2$ é gerado por um único elemento, qual é a diferença desse exemplo para o anterior? A diferença é que o gerador $\overline{1} \in \mathbb{Z}_2$ satisfaz a relação $2\overline{1} = \overline{0}$ (enquanto o gerador $1 \in \mathbb{Z}$ não satisfaz relação nenhuma). Então, no caso de $\mathbb{Z}_2$, nós podemos definir f_k só no gerador $\overline{1}$, mas nós temos que verificar que $f_k(\overline{1})$ também satisfaz a relação $2f_k(\overline{1}) = \overline{0}$.

Vamos usar a idéia do exemplo anterior no próximo exemplo.

Exemplo 4.15. Sejam $n \geq 2$ e $f\colon \mathbb{Z}_n \to \mathbb{Z}$ um homomorfismo de grupos. Como $\mathbb{Z}_n$ é gerado por $\overline{1}$, então f é únicamente determinado por $f(\overline{1})$. Ou seja, se $f(\overline{1}) = k$, então $f(\overline{\ell}) = \overline{k\ell}$ para todo $\overline{\ell} \in \mathbb{Z}_n$. Agora, como $f(\overline{1}) = k$ deve satisfazer a relação $nk = 0$ e $n \neq 0$, concluímos que $k = 0$. Ou seja, não existe nenhum homomorfismo de grupos $f\colon \mathbb{Z}_n \to \mathbb{Z}$ além do trivial.