Grupos

Prof. Eanes Torres Pereira

FMCC2

Roteiro

Grupos - Introdução

- **Definição 1**. Um conjunto não-vazio G sobre o qual uma operação $\circ$ é definida é chamado de grupo em relação a essa operação desde que, para valores arbitrários a, b, $c \in \mathrm{G}$, as seguintes propriedades sejam válidas:
  1. $(a \circ b) \circ c = a \circ (b \circ c)$.
  2. Existe $u \in \mathrm{G}$ tal que $a \circ u = u \circ a = a$ para todo $a \in \mathrm{G}$.
  3. Para cada $a \in \mathrm{G}$ existe $a^{-1} \in \mathrm{G}$ tal que $a \circ a^{-1} = a^{-1} \circ a = u$.
- **Exemplo 1**. O conjunto Z de todos os inteiros forma um grupo em relação à adição?

Grupos - Introdução

- **Definição 1**. Um conjunto não-vazio G sobre o qual uma operação $\circ$ é definida é chamado de grupo em relação a essa operação desde que, para valores arbitrários a, b, $c \in \mathrm{G}$, as seguintes propriedades sejam válidas:
  1. $(a \circ b) \circ c = a \circ (b \circ c)$.
  2. Existe $u \in \mathrm{G}$ tal que $a \circ u = u \circ a = a$ para todo $a \in \mathrm{G}$.
  3. Para cada $a \in \mathrm{G}$ existe $a^{-1} \in \mathrm{G}$ tal que $a \circ a^{-1} = a^{-1} \circ a = u$.
- **Exemplo 1**. O conjunto Z de todos os inteiros forma um grupo em relação à adição?

  Solução. Sim, o elemento identidade é o 0 e o inverso de $a \in \mathrm{Z}$ é $-a$. Portanto, podemos falar do grupo aditivo Z.
- **Exemplo 2**. O conjunto Z de todos os inteiros forma um grupo em relação à multiplicação?

Grupos - Introdução

- **Definição 1**. Um conjunto não-vazio G sobre o qual uma operação $\circ$ é definida é chamado de grupo em relação a essa operação desde que, para valores arbitrários a, b, $c \in \mathrm{G}$, as seguintes propriedades sejam válidas:
  1. $(a \circ b) \circ c = a \circ (b \circ c)$.
  2. Existe $u \in \mathrm{G}$ tal que $a \circ u = u \circ a = a$ para todo $a \in \mathrm{G}$.
  3. Para cada $a \in \mathrm{G}$ existe $a^{-1} \in \mathrm{G}$ tal que $a \circ a^{-1} = a^{-1} \circ a = u$.
- **Exemplo 1**. O conjunto Z de todos os inteiros forma um grupo em relação à adição?

  Solução. Sim, o elemento identidade é o 0 e o inverso de $a \in \mathrm{Z}$ é $-a$. Portanto, podemos falar do grupo aditivo Z.
- **Exemplo 2**. O conjunto Z de todos os inteiros forma um grupo em relação à multiplicação?

  Solução. Não, pois, por exemplo, nem 0 nem 2 tem inverso multiplicativo.

Grupos - Propriedades

1. **Teorema 1**. Se a, b, $c \in \mathrm{G}$, então $a \circ b = a \circ c$ implica $b = c$.
2. **Teorema 2**. Para a, $b \in \mathrm{G}$, cada uma das equações $a \circ x = b$ e $y \circ a = b$ tem uma solução única.
3. **Teorema 3**. Para todo $a \in \mathrm{G}$, o inverso do inverso de a é a, isto é, $(a^{-1})^{-1} = a$.
4. **Teorema 4**. Para todo a, $b \in \mathrm{G}$, $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.
5. **Teorema 5**. Para todo a, b, ..., p, $q \in \mathrm{G}$, $(a \circ b \circ \ldots \circ p \circ q)^{-1} = q^{-1} \circ q^{-1} \circ \ldots \circ b^{-1} \circ a^{-1}$.

   Para qualquer $q \in \mathrm{G}$ e $m \in \mathrm{Z}^+$, definimos:

   $a^m = a \circ a \circ a \circ \ldots \circ$, com m fatores.

   $a^0 = u$, o elemento identidade.

   $a^{-m} = (a^{-1})^m = a^{-1} \circ a^{-1} \circ a^{-1} \ldots \circ a^{-1}$, a m fatores.
6. **Teorema 6**. Para qualquer $a \in \mathrm{G}$, (i) $a^m \circ a^n = a^{m+n}$ e $(a^m)^n = a^{mn}$, em que m, $n \in \mathrm{Z}$.

Grupos - Exercícios

1. Prove o Teorema 1.
2. Prove o Teorema 2.
3. Prove o Teorema 3.

Grupos

- **Definição**. A ordem de um grupo é definida pela quantidade de elementos do grupo.
- **Exemplo 3**. Qual é a ordem do grupo aditivo $\mathbb{Z}$?

Grupos

- **Definição**. A ordem de um grupo é definida pela quantidade de elementos do grupo.
- **Exemplo 3**. Qual é a ordem do grupo aditivo $\mathbb{Z}$?

  Resposta: É de ordem infinita.
- **Exemplo 4**. O conjunto $A = \{1, -1, i, -i\}$, em relação à multiplicação no conjunto dos números complexos, forma um grupo?

Grupos

- **Definição**. A ordem de um grupo é definida pela quantidade de elementos do grupo.
- **Exemplo 3**. Qual é a ordem do grupo aditivo $\mathbb{Z}$?

  Resposta: É de ordem infinita.
- **Exemplo 4**. O conjunto $A = \{1, -1, i, -i\}$, em relação à multiplicação no conjunto dos números complexos, forma um grupo?

  Resposta: Sim.
- **Exemplo 5**. Qual é a ordem do grupo do Exemplo 4?

Grupos

- **Definição**. A ordem de um grupo é definida pela quantidade de elementos do grupo.
- **Exemplo 3**. Qual é a ordem do grupo aditivo $\mathbb{Z}$?

  Resposta: É de ordem infinita.
- **Exemplo 4**. O conjunto $A = \{1, -1, i, -i\}$, em relação à multiplicação no conjunto dos números complexos, forma um grupo?

  Resposta: Sim.
- **Exemplo 5**. Qual é a ordem do grupo do Exemplo 4?

  Resposta: 4.

Grupos

- **Definição**. A *ordem de um elemento* $a \in \mathrm{G}$ é o menor inteiro positivo n, se existir, para o qual $a^n = u$, o elemento identidade de G.
- **Definição**. Se $a \neq 0$ é um elemento do grupo aditivo Z, então $na \neq 0$ para todo $n > 0$ e a é definido como sendo de ordem infinita.
- **Exemplo 6**. Qual é a ordem do elemento -1 do exemplo 4?

Grupos

- **Definição**. A *ordem de um elemento* $a \in \mathrm{G}$ é o menor inteiro positivo n, se existir, para o qual $a^n = u$, o elemento identidade de G.
- **Definição**. Se $a \neq 0$ é um elemento do grupo aditivo Z, então $na \neq 0$ para todo $n > 0$ e a é definido como sendo de ordem infinita.
- **Exemplo 6**. Qual é a ordem do elemento -1 do exemplo 4?

  Resposta. A ordem é 2 já que $(-1)^2 = 1$.
- **Exemplo 7**. Qual é a ordem do elemento i do exemplo 4?

Grupos

- **Definição**. A *ordem de um elemento* $a \in \mathrm{G}$ é o menor inteiro positivo n, se existir, para o qual $a^n = u$, o elemento identidade de G.
- **Definição**. Se $a \neq 0$ é um elemento do grupo aditivo Z, então $na \neq 0$ para todo $n > 0$ e a é definido como sendo de ordem infinita.
- **Exemplo 6**. Qual é a ordem do elemento -1 do exemplo 4?

  Resposta. A ordem é 2 já que $(-1)^2 = 1$.
- **Exemplo 7**. Qual é a ordem do elemento i do exemplo 4?

  Resposta. A ordem é 4 já que $i^2 = -1$, $i^3 = -i$ e $i^4 = 1$.

Roteiro

Subgrupos

- **Definição**. Seja $\mathrm{G} = \{a, b, c, \ldots\}$ um grupo com relação a $\circ$. Qualquer subconjunto G' de G é chamado de *subgrupo* de G se G' é um grupo em relação a $\circ$.
- **Definição**. *Subgrupo impróprio*: $\mathrm{G}' = \{u\}$. Todos os outros subgrupos, se existirem, são chamados de subgrupos próprios.
- **Exemplo 8**. Um subgrupo próprio do grupo $\mathrm{G} = \{1, -1, i, -i\}$ é $\mathrm{G}' = \{1, -1\}$.
- **Teorema 7**. Um subconjunto não-vazio G' de um grupo G é um subgrupo de G se, e somente se: (i) G' é fechado em relação a $\circ$, (ii) G' contém o inverso de cada um de seus elementos.

  Prova. Suponha que G' é um subgrupo de G. Se a, $b \in \mathrm{G}'$, então $a^{-1} \in \mathrm{G}'$ e, pela Lei do Fechamento, $a^{-1} \circ b \in \mathrm{G}'$.

Subgrupos

- **Teorema 8**. Um subconjunto não-vazio G' de um grupo G é um subgrupo de G se, e somente se, para todo a, $b \in \mathrm{G}'$, $a^{-1} \circ b \in \mathrm{G}'$.
- **Teorema 9**. Seja a um elemento de um grupo G. O conjunto $\mathrm{G}' = \{a^n : n \in \mathrm{Z}\}$ de todas as potências inteiras de a é um subgrupo de G.
- **Teorema 10**. Se S é qualquer conjunto de subgrupos de G, a interseção desses subgrupos também é um subgrupo de G.
- **Exercício**. Prove o Teorema 8.
- **Exercício**. Prove o Teorema 10.

Roteiro

Grupos Cíclicos

- **Definição**. Um grupo G é chamado de *cíclico* se, para algum $a \in \mathrm{G}$, todo $x \in \mathrm{G}$ é da forma a^m, em que $m \in \mathrm{Z}$. O elemento a é, então, chamado de um *gerador* de G.
- **Exemplo 9**. O grupo aditivo Z é cíclico com gerador $a = 1$?

Grupos Cíclicos

- **Definição**. Um grupo G é chamado de *cíclico* se, para algum $a \in \mathrm{G}$, todo $x \in \mathrm{G}$ é da forma a^m, em que $m \in \mathrm{Z}$. O elemento a é, então, chamado de um *gerador* de G.
- **Exemplo 9**. O grupo aditivo Z é cíclico com gerador $a = 1$?

  Reposta. Sim, pois para todo $m \in \mathrm{Z}$, $a^m = ma = m$. Obs.: ver Teorema 5.
- **Exemplo 10**. O grupo $\mathrm{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ sob adição módulo 8 é cíclico?

Grupos Cíclicos

- **Definição**. Um grupo G é chamado de *cíclico* se, para algum $a \in \mathrm{G}$, todo $x \in \mathrm{G}$ é da forma a^m, em que $m \in \mathrm{Z}$. O elemento a é, então, chamado de um *gerador* de G.
- **Exemplo 9**. O grupo aditivo Z é cíclico com gerador $a = 1$?

  Reposta. Sim, pois para todo $m \in \mathrm{Z}$, $a^m = ma = m$. Obs.: ver Teorema 5.
- **Exemplo 10**. O grupo $\mathrm{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ sob adição módulo 8 é cíclico?

  Resposta. Sim, este grupo pode ser gerado por 1, 3, 5 ou 7.
- **Exercício**. Prove que 1, 3, 5 ou 7 são geradores do grupo do exemplo 10, mas 2, 4 e 6 não são geradores.

Grupos Cíclicos

- **Teorema 11**. Qualquer elemento a^t de um grupo G cíclico finito de ordem n é um gerador de G se, e somente se, $mdc(n, t) = 1$.
- **Teorema 12**. Todo subgrupo de um grupo cíclico é um grupo cíclico.
- **Exercício**. Prove o Teorema 12.

Roteiro

Grupos de Permutação

- Seja $S = \{1, 2, 3, \ldots, n\}$ e considere o conjunto S_n das $n!$ permutações desses símbolos.
- Uma permutação de um conjunto S é uam função injetora de S em S.
- Sejam i_1, i_2, i_3, ..., i_n uma disposição de elementos de S. Usamos a seguinte notação de duas linhas:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix}$$

- De modo similar, se j_1, j_2, j_3, ..., j_n é outro arranjo de elementos de S, escrevemos:

$$\beta = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ j_1 & j_2 & i_3 & \ldots & i_n \end{pmatrix}$$

Grupos de Permutação

- **Exemplo 11**. Sejam:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$$

- 3 das 5! permutações no conjunto S_5 de todas as permutações em $S = \{1, 2, 3, 4, 5\}$.
- $\circ$ é a operação *permutação*.
- Como a ordem dos elementos da permutação não importa. $\beta \circ \alpha$:

$$\begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

- Ou seja, $\beta \circ \alpha(1) = \beta(\alpha(1)) = \beta(2) = 3$

Grupos de Permutação

- Se reescrevermos α como:

$$\begin{pmatrix} 1 & 3 & 2 & 5 & 4 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$$

- obtemos:

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$$

- Portanto $\circ$ não é comutativo.
- **Exercício**. Escrevendo γ como

$$\begin{pmatrix} 3 & 2 & 5 & 4 & 1 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$$

determine se a operação $\circ$ é associativa fazendo:
$(\gamma \circ \beta) \circ \alpha = \gamma \circ (\beta \circ \alpha)$

Grupos de Permutação

- **Exercício**. Mostre que I é a permutação identidade de $\circ$, fazendo $\mathrm{I} \circ \alpha = \alpha \circ \mathrm{I} = \alpha$.

$$\mathrm{I} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

- **Exercício**. Mostre que alternar as linhas de α gera α^{-1}, fazendo $\alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = \mathrm{I}$.

$$\alpha = \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

Grupos de Permutação

- α do exemplo da página 12 pode ser escrito em notação *cíclica* como (12345) em que o ciclo (12345) é interpretado como: 1 é substituído por 2, 2 é substituído por 3, 3 é substituído por 4, 4 é substituído por 5 e 5 é substituído por 1.
- Uma permutação como (12), (25), ... que envolve a troca de apenas dois dos n símbolos de $S = \{1, 2, 3, 4, \ldots, n\}$ é chamada de *transposição*.
- **Exemplo 12**. Expresse a permutação (23) em $S_n = \{1, 2, 3, 4, 5\}$ como produtos de transposições.

Grupos de Permutação

- α do exemplo da página 12 pode ser escrito em notação *cíclica* como (12345) em que o ciclo (12345) é interpretado como: 1 é substituído por 2, 2 é substituído por 3, 3 é substituído por 4, 4 é substituído por 5 e 5 é substituído por 1.
- Uma permutação como (12), (25), ... que envolve a troca de apenas dois dos n símbolos de $S = \{1, 2, 3, 4, \ldots, n\}$ é chamada de *transposição*.
- **Exemplo 12**. Expresse a permutação (23) em $S_n = \{1, 2, 3, 4, 5\}$ como produtos de transposições.

  Solução. Se $\alpha = (12)$, $\beta = (23)$, $\gamma = (13)$, então $(23) = \alpha \circ \beta \circ \gamma$. Pois $\alpha \circ \beta = (123)$ e $(\alpha \circ \beta) \circ \gamma = (23)$.

Grupos de Permutação

- Qualquer permutação pode ser expressa, mas não unicamente, como um produto de transposições.
- **Exemplo 13**. Mostre que $(23) = (12) \circ (13) \circ (12)$.
- S_n é um grupo em relação às operações de permutação $\circ$.
- S_n não é um grupo abeliano, pois $\circ$ não é comutativo.
- S_n é chamado de *grupo simétrico* de n símbolos.
- Qualquer subgrupo de S_n é chamado de *grupo de permutação* em n símbolos.

Grupos de Permutação - Exercícios

- Seja $S_4 = \{(1), (12), (13), (14), (23), (24), (34), \alpha = (123), \alpha^2, \beta = (124), \beta^2, \gamma = (134), \gamma^2, \delta = (234), \delta^2, \theta = (1234), \theta^2, \theta^3, \sigma = (1234), \sigma^2, \sigma^3, \tau = (1324), \tau^2, \tau^3\}$
- Quais os valores de: δ^2, θ^2, σ^2, σ^3, τ^2 e τ^3?

Grupos de Permutação - Exercícios

- Seja $S_4 = \{(1), (12), (13), (14), (23), (24), (34), \alpha = (123), \alpha^2, \beta = (124), \beta^2, \gamma = (134), \gamma^2, \delta = (234), \delta^2, \theta = (1234), \theta^2, \theta^3, \sigma = (1234), \sigma^2, \sigma^3, \tau = (1324), \tau^2, \tau^3\}$
- Quais os valores de: δ^2, θ^2, σ^2, σ^3, τ^2 e τ^3?

  Resp.: $\delta^2 = (243)$, $\theta^2 = (13)(24)$, $\theta^3 = (1432)$, $\sigma^2 = (14)(23)$, $\sigma^3 = (1342)$, $\tau^2 = (12)(34)$, $\tau^3 = (1423)$.

Roteiro

Homomorfismos

- **Definição**. Seja G, com operação $\circ$, e G', com operação $\square$, dois grupos. Um *homomorfismo* de G em G' é um mapeamento

$$\theta : \mathrm{G} \to \mathrm{G}'$$

tal que $\theta(g) = g'$ e

1. todo $g \in \mathrm{G}$ tem uma única imagem $g' \in \mathrm{G}$;
2. se $\theta(a) = a'$ e $\theta(b) = b'$, então $\theta(a \circ b) = \theta(a) \square \theta(b) = a' \square b'$.
   - se, além disso, o mapeamento satisfaz:
3. todo $g' \in \mathrm{G}'$ é uma imagem
   - nós temos um homomorfismo de G em G' e chamamos G' de uma *imagem homomórfica* de G.

Homomorfismos

- **Exemplo 14**. Considere o grupo cíclico $\mathrm{G} = \{a, a^2, a^3, \ldots, a^{12} = \mathbf{u}\}$ e seu subgrupo $\mathrm{G}'\{a^2, a^4, a^6, \ldots, a^{12}\}$.
- O mapeamento $a^n \to a^{2n}$ é um homomorfismo de G em G'?

Homomorfismos

- **Exemplo 14**. Considere o grupo cíclico $\mathrm{G} = \{a, a^2, a^3, \ldots, a^{12} = \mathbf{u}\}$ e seu subgrupo $\mathrm{G}'\{a^2, a^4, a^6, \ldots, a^{12}\}$.
- O mapeamento $a^n \to a^{2n}$ é um homomorfismo de G em G'?

  Resposta: sim, pois os critérios (1) e (2) da definição de homomorfismo são atendidos.
- O mapeamento $a^n \to a^n$ é um homomorfismo de G' em G?

Homomorfismos

- **Exemplo 14**. Considere o grupo cíclico $\mathrm{G} = \{a, a^2, a^3, \ldots, a^{12} = \mathbf{u}\}$ e seu subgrupo $\mathrm{G}'\{a^2, a^4, a^6, \ldots, a^{12}\}$.
- O mapeamento $a^n \to a^{2n}$ é um homomorfismo de G em G'?

  Resposta: sim, pois os critérios (1) e (2) da definição de homomorfismo são atendidos.
- O mapeamento $a^n \to a^n$ é um homomorfismo de G' em G?

  Resposta: sim, pois os critérios (1) e (2) da definição de homomorfismo são atendidos.

Referência

- Theory and Problems in Abstract Algebra - Frank Ayres and Lloyd R. Jaisingh.