Álgebra - Lic. C. Computação

Paula Marques Smith

DMA - UM

12 set'19

apresentação

identificação

Nome: Álgebra

Área Científica: Matemática

Departamento: Matemática

Docente: Paula Marques Smith psmith@math.uminho.pt ext: 604363

Escolaridade: 1^o semestre 3h (T) + 3h (TP) por semana 7,5 ECTS

45h + 45h de contacto - 130h trabalho independente

Período letivo:

aulas: 09 setembro a 21 dezembro (15 semanas)

aulas e exames: 09 setembro a 01 fevereiro

apresentação

Objetivos

- transmissão de conhecimentos específicos, básicos de Álgebra
  - ⋆ teoria de grupos; teoria de anéis; divisibilidade em domínios de integridade
- capacidade de aplicar os conhecimentos adquiridos em diversos contextos
- aptidões de raciocínio matemático, de modo a construir argumentos rigorosos;
- contribuição para a aquisição de um conjunto de competências:
  - ⋆ capacidade de assimilar informação e de a comunicar
  - ⋆ capacidade de expressão escrita
  - ⋆ capacidade de expressão oral
  - ⋆ capacidade de trabalhar em grupo
  - ⋆ capacidade de aprender de modo autónomo

apresentação

resultados de aprendizagem

1. Resolver problemas que envolvam os conceitos de subgrupo invariante e de congruência de grupo

2. Resolver problemas que envolvam os conceitos de ideal e de congruência de anel

3. Resolver problemas relativos a grupos e anéis quociente e a homomorfismos de grupo e de anel

4. Fatorizar elementos de um domínio de integridade como produto de elementos irredutíveis

5. Reconhecer um domínio de ideais principais como um domínio de fatorização única

6. Estruturar e redigir demonstrações de resultados básicos da Álgebra

pré-requisitos

Não existem

apresentação

docente

Email: psmith@math.uminho.pt

Telefone: 253 604363

Gabinete: ECUM - 4027 (Gualtar)

Horário de Atendimento:

sexta-feira: 09h:00 - 10h:00
16h:00 - 18h:00
outro, a combinar, atempadamente, com a docente

apresentação

programa resumido

Elementos da teoria de grupos

- Grupos e subgrupos
- Ordem de um elemento e Teorema de Lagrange
- Subgrupos normais, grupos quociente e homomorfismos de grupo
- Grupos cíclicos
- Grupos de permutações

Elementos da teoria de anéis

- domínios de integridade, anéis de divisão e corpos
- Ideais, ideais primos e ideais maximais
- Anéis quociente e homomorfismos de anel

Divisibilidade em domínios de integridade

O corpo das fracções de um domínio de integridade

apresentação

bibliografia

- Ficheiros pdf das aulas teóricas

- A. J. Monteiro e I. T. Matos, Álgebra, um primeiro curso. Escolar Editora, 2ª edição (2001)

- Durbin, J., Modern algebra - an introduction. John Wiley and Sons Inc. (2009)

- Grillet, P.A., Abstract algebra. Springer (2007)

- Marques Smith, P., Martins. P. Mendes, Roçadas, L., Álgebra, Exercícios resolvidos e exercícios propostos. Escolar Editora, (2015)

apresentação

Método de avaliação

Aprovados no quadro de avaliação periódica: alunos que, simultaneamente,

- tenham frequência a pelo menos 2/3 das aulas TP lecionadas;
- realizem dois testes e neles obtenham classificações t_1 e t_2, ambas iguais ou superiores a 7,5 valores, sendo que serão admitidos ao 2^o teste **apenas** os alunos que obtenham no 1^o teste classificação igual ou superior a 7,5 valores;
- obtenham a média aritmética $(t_1 + t_2)/2$ igual ou superior a 9,5 valores, sendo, neste caso, a classificação final igual a esse valor arredondado às unidades.

A classificação final pode ser acrescida (mas nunca diminuída) de 0,5 valores, com base no desempenho do aluno nas aulas TP.

Datas dos testes: 25 outubro e 13 dezembro

apresentação

Exame de recurso: Os alunos que não obtenham aprovação no quadro de avaliação periódica serão admitidos a exame de recurso, desde que tenham frequência a pelo menos 2/3 das aulas TP lecionadas.

Data do exame de recurso: a definir

O exame de recurso realiza-se ao abrigo do Regulamento Académico da Universidade do Minho (Despacho RT-41-2014).

regime de faltas: Será feito o controlo de presenças nas aulas teóricas (apenas para fins estatísticos) e nas aulas teórico-práticas.

página da unidade curricular:

- sumários: um sumário de cada aula estará on-line em tempo útil;
- os documentos da uc serão colocados na página da uc na plataforma Blackboard, na pasta *Conteúdos*.

Cap I. Elementos da teoria de grupos

Generalidades

Seja A um conjunto não vazio. Chama-se operação binária sobre A a qualquer aplicação de $A \times A$ em A.

Se $*$ for uma operação binária sobre A e $x, y \in A$, representamos por $x * y$ a imagem de (x, y) por $*$. De um modo geral, utilizam-se os símbolos $+$ (notação aditiva) e $\cdot$ ou $\times$ (notação multiplicativa) para representar uma operação binária.

Diz-se que uma operação binária, definida num conjunto não vazio A, satisfaz a:

- ⋆ *propriedade comutativa* se: $(\forall a, b \in A) \quad ab = ba$;
- ⋆ *propriedade associativa* se: $(\forall a, b, c \in A) \quad (ab)\,c = a\,(bc)$.

Cap I. Elementos da teoria de grupos

Generalidades

Diz-se que uma operação binária, definida num conjunto não vazio A, admite *elemento neutro* ou *elemento identidade* se

$$(\exists e \in A): \quad (\forall a \in A) \quad ae = ea = a.$$

Uma operação binária, definida num conjunto não vazio A, admite, no máximo, um elemento neutro único. (Porquê?) Existindo, este elemento representa-se por $1_{(A,\cdot)}$ ou simplesmente por 1_A.

Sejam A um conjunto não vazio, $\cdot$ uma operação binária em A que admite identidade e $x \in A$. Se existir $x' \in A$ tal que $xx' = x'x = 1_A$, diz-se que x é um elemento *invertível* e que x' é um *inverso* de x. Cada elemento $x \in A$ tem, no máximo, um inverso (porquê?): designa-se por *o inverso de* x e representa-se por x^{-1}.

Cap I. Elementos da teoria de grupos

Generalidades

Se A é um conjunto não vazio e $\cdot$ é uma operação binária sobre A, diz-se que o par $(A, \cdot)$ é um *grupóide*.

Sejam $(A, \cdot)$ um grupóide e B um subconjunto não vazio de A. Sempre que, dados $x, y \in B$, se tem $x \cdot y \in B$, diz-se que $(B, \cdot)$ é um *subgrupóide de* $(A, \cdot)$. Não havendo ambiguidade, representamos o grupóide $(A, \cdot)$ apenas por A.

Um grupóide no qual a operação binária é associativa diz-se um *semigrupo*. Um subgrupóide de um semigrupo S diz-se um *subsemigrupo de* S.

Um semigrupo no qual a operação binária é comutativa diz-se um *semigrupo comutativo*.

Um semigrupo com identidade diz-se um *monóide*.

Álgebra - Lic. C. Computação

Paula Marques Smith

DMA - UM

13 set'19

Cap I. Elementos da teoria de grupos

Generalidades

Sejam A um semigrupo com identidade 1_A,$a \in A$ e $n \in \mathbb{N}_0$. Chama-se *potência-n* de a, ou *potência de base a e expoente n*, e representa-se por a^n, ao elemento de A assim definido:

i. $a^0 = 1_A$;

ii. $a^1 = a$;

iii. $a^{n+1} = a^n a$, se $n > 0$.

Quando um semigrupo A não tem identidade, define-se apenas potência-n de a para $n \in \mathbb{N}$.

Num semigrupo (respetivamente, semigrupo com identidade) A, para as potências de expoente natural (respetivamente, inteiro não negativo), são válidas as seguintes propriedades:

Cap I. Elementos da teoria de grupos

Generalidades

Proposição. Sejam A um semigrupo.

1. Para qualquer $a \in A$ e quaisquer $m, n \in \mathbb{N}$ (respetivamente, $m, n \in \mathbb{N}_0$), tem-se $a^n a^m = a^{n+m}$ e $(a^n)^m = a^{nm}$;
2. Se $a, b \in A$ são tais que $ab = ba$, então, para qualquer $n \in \mathbb{N}$ (respetivamente, $n \in \mathbb{N}_0$), tem-se $ab^n = b^n a$ e $(ab)^n = a^n b^n$.

Dem. Exercício

Na linguagem aditiva, para um semigrupo $(A, +)$ com elemento neutro 0_A, a potência-n de $a \in A$ designa-se por *múltiplo-n de a*, representa-se por na e define-se do seguinte modo:

i. $0a = 0_A$;

ii. $1a = a$;

iii. $(n+1)a = na + a$, se $n > 0$.

As propriedades 1. e 2. enunciadas na proposição anterior são igualmente válidas para os múltiplos-n.

Um elemento e de um semigrupo S diz-se um *idempotente de S* se $e^2 = e$. Nem todos os semigrupos têm elementos idempotentes (encontre um exemplo). Um monóide tem pelo menos um idempotente: a sua identidade.

Um *grupo* é um monóide no qual cada elemento tem inverso.

Um grupo no qual a operação é comutativa diz-se um *grupo comutativo* ou *grupo abeliano*.

Exemplos.

1. $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$ são grupos abelianos mas $(\mathbb{R}, \times)$, $(\mathbb{Z}, \times)$ não são grupos.
2. $(\mathcal{M}_{p\times n}(\mathbb{R}), +)$ é um grupo comutativo.
3. $(\mathcal{M}_p^i(\mathbb{R}), \times)$ é um grupo que não é comutativo. (($\mathcal{M}_p^i(\mathbb{R})$: conjunto das matrizes invertíveis de ordem p.)

1. Um conjunto singular, $\{x\}$, algebrizado com a operação binária definida por $x * x = x$, é um grupo abeliano (designa-se por *grupo trivial*).
2. O conjunto $G = \{x, e\}$, algebrizado com a operação definida pela tabela

$$\begin{array}{c|cc} \cdot & e & x \\ \hline e & e & x \\ x & x & e \end{array},$$

é um grupo abeliano.

Proposição. Seja G um grupo. Então:

1. $1_G^{-1} = 1_G$;
2. $\left(a^{-1}\right)^{-1} = a, \quad \forall a \in G$;
3. $(ab)^{-1} = b^{-1}a^{-1}, \quad \forall a, b \in G$;
4. $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}, \quad (\forall n \in \mathbb{N}) \quad (\forall a_1, a_2, \ldots, a_n \in G)$.

Cap I. Elementos da teoria de grupos

Generalidades

Proposição. Seja G um semigrupo. Se G é um grupo, então as leis do corte são válidas em G, i.e., para $x, y, a \in G$,

$$ax = ay \Longrightarrow x = y \quad e \quad xa = ya \Longrightarrow x = y.$$

Demonstração. Sejam $a, x, y \in G$. Então,

$$\begin{aligned} ax = ay \quad &\Longrightarrow \quad a^{-1}(ax) = a^{-1}(ay) \\ &\Longrightarrow \quad \left(a^{-1}a\right)x = \left(a^{-1}a\right)y \\ &\Longrightarrow \quad 1_G x = 1_G y \\ &\Longrightarrow \quad x = y. \end{aligned}$$

A segunda implicação demonstra-se de modo análogo.

Cap I. Elementos da teoria de grupos

Generalidades

O exemplo que se segue mostra que a validade das leis do corte num qualquer semigrupo S não é condição suficiente para que o semigrupo seja grupo.

Exemplo. Seja $\mathbb{Z} \setminus \{0\}$ algebrizado com a multiplicação usual de inteiros. Este semigrupo comutativo com identidade satisfaz as leis do corte, mas não é um grupo, uma vez que os únicos elementos que admitem inverso são 1 e -1.

Questão: Que condição/condições deve um semigrupo com as leis do corte válidas satisfazer para que ele seja um grupo?

Comecemos por provar a seguinte caraterização de grupo:

Teorema. Um semigrupo S é um grupo se e só se as equações do tipo $ax = b$ e $ya = b$ têm solução única para quaisquer $a, b \in S$.

Generalidades

Demonstração.

Suponhamos que G é um grupo. Então, para $a, b \in G$, os elementos $a^{-1}b$ e ba^{-1} de G são soluções das equações $ax = b$ e $ya = b$, respectivamente. A unicidade destas soluções resulta do facto de as leis de corte serem válidas em G.

Reciprocamente, sejam S um semigrupo e $a \in S$. Por hipótese, existem soluções únicas das equações $ax = a$ e $ya = a$. Sejam e e e' essas soluções, respectivamente ($ae = a$ e $e'a = a$). Então, como para todo $b \in S$ existe um único $c \in S$ tal que $b = ca$, temos que

$$be = (ca)\,e = c\,(ae) = ca = b.$$

Logo, e satisfaz $be = b$, para todo $b \in S$. De modo análogo, provamos que e' satisfaz $e'b = b$, para todo $b \in S$. Assim, tomando $b = e'$ na 1^a igualdade e $b = e$ na 2^a igualdade , temos

$$e = e'e = e'$$

e, portanto, e é elemento neutro do semigrupo S.

Generalidades

Seja agora $a \in S$. Então, existem soluções únicas das equações $ax = e$ e $ya = e$. Sejam a' e a'' essas soluções, respectivamente. Temos então que $aa' = e$ e $a''a = e$. Logo,

$$a'' = a''e = a''\left(aa'\right) = \left(a''a\right)a' = ea' = a',$$

pelo que cada elemento $a \in S$ admite um inverso $a' \in S$. Portanto, S é um grupo.

Estamos agora em condições de responder à questão levantada anteriormente:

Proposição. Seja S um semigrupo **finito** que satisfaz as leis do corte. Então S é um grupo.

Demonstração.

Seja a um elemento qualquer de S. Então, as aplicações $\rho_a, \lambda_a : S \to S$ definidas por, respectivamente, $\rho_a(x) = xa$ e $\lambda_a(x) = ax$, $x \in S$, são injetivas.

Generalidades

De facto, para $x, y \in S$, tendo em conta as leis do corte,

$$\rho_a(x) = \rho_a(y) \Leftrightarrow xa = ya \Rightarrow x = y$$

e

$$\lambda_a(x) = \lambda_a(y) \Leftrightarrow ax = ay \Rightarrow x = y.$$

Logo, sendo S um conjunto finito, temos que as duas aplicações são também sobrejetivas, pelo que as duas equações

$$ax = b \text{ e } ya = b$$

têm soluções únicas em S. Assim, pela proposição anterior, o semigrupo S é um grupo.

Generalidades

Questão: Num grupo G, o conceito de *potência-n* de $a \in G$ poderá ser estendido para qualquer expoente **inteiro** n? Se sim, como fazer essa extensão?

Álgebra - Lic. C. Computação

Paula Marques Smith

DMA - UM

26 set'19

Cap I. Elementos da teoria de grupos

Generalidades

Questão: Num grupo G, o conceito de *potência-n* de $a \in G$ poderá ser estendido para qualquer expoente **inteiro** n? Se sim, como fazer essa extensão?

Sejam G um grupo, $a \in G$ e $n \in \mathbb{Z}$. Chama-se *potência-n* de a, ou *potência de base a e expoente n*, e representa-se por a^n, ao elemento de G assim definido:

i. $a^0 = 1_G$;
ii. $a^1 = a$;
iii. $a^{n+1} = a^n a$, se $n > 0$;
iv. $a^n = (a^{-n})^{-1}$, se $n < 0$.

Proposição. Sejam G um grupo, $x \in G$ e $m, n \in \mathbb{Z}$. Então,

1. $x^m x^n = x^{m+n}$;
2. $(x^m)^n = x^{mn}$.

Generalidades

Demonstração. Temos vários casos a considerar. Provemos quatro deles - dois dos restantes são triviais e os outros reduzem-se a um destes.

Caso 1: Sejam $m, n \in \mathbb{Z}^+$. O caso resulta imediatamente da definição.

Caso 2: Sejam $m, n \in \mathbb{Z}^-$. Então, $m = -l$ e $n = -k$ com $l, k > 0$, pelo que

$$x^m x^n = x^{-l} x^{-k} = \left(x^l\right)^{-1} \left(x^k\right)^{-1} = \left(x^k x^l\right)^{-1} = \left(x^{k+l}\right)^{-1} =$$

$$= x^{-(k+l)} = x^{-k-l} = x^{n+m}.$$

Por outro lado,

$$(x^m)^n = \left(x^{-l}\right)^{-k} = \left[\left(\left(x^{-1}\right)^l\right)^k\right]^{-1} = \left[\left(x^{-1}\right)^{lk}\right]^{-1} = \left[\left(x^{lk}\right)^{-1}\right]^{-1} =$$

$$= (x^{-lk})^{-1} = x^{lk} = x^{(-m)(-n)} = x^{mn}.$$

Caso 3: Sejam $m, n \in \mathbb{Z}$ tais que $m > 0$, $n < 0$ e $|m| > |n|$. Então, $n = -l$ com $m > l > 0$, pelo que

$$x^m x^n = x^{m-l+l} x^{-l} = x^{m-l} x^l \left(x^l\right)^{-1} = x^{m-l} 1_G = x^{m-l} = x^{m+n},$$

o que prova (i). Por outro lado,

$$(x^m)^n = (x^m)^{-l} = \left[(x^m)^l\right]^{-1} = \left(x^{ml}\right)^{-1} = x^{-ml} = x^{mn},$$

o que prova a condição (ii).

Caso 4. Sejam $m, n \in \mathbb{Z}$ tais que $m > 0$, $n < 0$ e $|m| < |n|$. Então, $n = -l$ com $l > m > 0$, pelo que

$$\begin{aligned} x^m x^n &= x^m x^{-l} = x^m \left(x^l\right)^{-1} = x^m \left(x^{l-m+m}\right)^{-1} = x^m \left(x^{l-m} x^m\right)^{-1} = \\ &= x^m \left(x^m\right)^{-1} \left(x^{l-m}\right)^{-1} = 1_G x^{-(l-m)} = x^{-l+m} = x^{n+m}. \end{aligned}$$

A demonstração de *(ii)* é análoga à do caso 3.

Subgrupos

Seja G um grupo. Um subconjunto não vazio H de G diz-se um *subgrupo de* G se H for grupo para a operação de G restringida a H. Neste caso escrevemos $H < G$.

Exemplo 1. O semigrupo $(\mathbb{Q}\setminus\{0\}, \times)$ é subgrupo de $(\mathbb{R}\setminus\{0\}, \times)$.

Exemplo 2. O semigrupo $(\mathbb{Q}\setminus\{0\}, \times)$ é um grupo mas não é um subgrupo de $(\mathbb{R}, +)$.

Exemplo 3. Seja $G = \{e, a, b, c\}$ o grupo de *4-Klein,* i.e., o grupo cuja operação é dada pela seguinte tabela

$$\begin{array}{c|cccc} \cdot & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array}.$$

Os subgrupos de G são: $\{e, a, b, c\}$, $\{e\}$, $\{e, a\}$, $\{e, b\}$ e $\{e, c\}$.

Subgrupos

Exemplo 4. Seja $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ o conjunto das classes módulo-4 algebrizado com a adição modular, i.e.,

$$\begin{array}{c|cccc} + & \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \hline \bar{0} & \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{1} & \bar{1} & \bar{2} & \bar{3} & \bar{0} \\ \bar{2} & \bar{2} & \bar{3} & \bar{0} & \bar{1} \\ \bar{3} & \bar{3} & \bar{0} & \bar{1} & \bar{2} \end{array}.$$

Então, $(\mathbb{Z}_4, +)$ é grupo e os seus subgrupos são: $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, $\{\bar{0}\}$ e $\{\bar{0}, \bar{2}\}$.

Observação. Um grupo G tem, pelo menos, dois subgrupos: $\{1_G\}$ (*subgrupo trivial*) e G (*subgrupo impróprio*).

Álgebra - Lic. C. Computação

Paula Marques Smith

DMA - UM

27 set'19

Cap I. Elementos da teoria de grupos

Subgrupos

Proposição. Sejam G um grupo e $H < G$. Então:

1. O elemento neutro de H, 1_H, é o mesmo que o elemento neutro de G, 1_G;
2. Para cada $h \in H$, o inverso de h em H é o mesmo que o inverso de h em G

Demonstração (1) Uma vez que 1_H é elemento neutro de H, temos

$$1_H 1_H = 1_H;$$

por outro lado, como 1_G é elemento neutro de G e $1_H \in G$, temos que

$$1_H 1_G = 1_H.$$

Logo,

$$1_H 1_H = 1_H 1_G,$$

pelo que, pela lei do corte,

$$1_H = 1_G.$$

Subgrupos

(2) Sejam $h \in H$, h^{-1} o inverso de h em G e h' o inverso de h em H. Então,

$$hh' = 1_H = 1_G = hh^{-1}.$$

Logo, pela lei do corte,

$$h' = h^{-1}.$$

Proposição. Sejam G um grupo e $H \subseteq G$. Então, $H < G$ se e só se são satisfeitas as seguintes condições:

1. $H \neq \emptyset$;
2. $x, y \in H \Rightarrow xy \in H$;
3. $x \in H \Rightarrow x^{-1} \in H$.

Subgrupos

Demonstração. Suponhamos que $H < G$. Então:

1. $H \neq \emptyset$, pois $1_G \in H$;
2. dados $x, y \in H$, como H é um grupóide, $xy \in H$;
3. dado $x \in H$, como todo o elemento de H admite inverso em H e este é igual ao inverso em G, então $x^{-1} \in H$.

Reciprocamente, suponhamos que $H \subseteq G$ satisfaz as condições (1), (2) e (3). Então,

(a) H é grupóide por (2);
(b) dado $x \in H$ (este elemento existe por (1)), $x^{-1} \in H$ (por (3)), pelo que $1_G = xx^{-1} \in H$ (por (2));
(c) qualquer elemento de H admite inverso em H (por (iii)).

Como a operação é associativa em G, também o é obviamente em H e, portanto, concluimos que $H < G$.

Cap I. Elementos da teoria de grupos

Subgrupos

Proposição. Sejam G um grupo e $H \subseteq G$. Então, $H < G$ se e só se são satisfeitas as seguintes condições:

1. $H \neq \emptyset$;
2. $x, y \in H \Rightarrow xy^{-1} \in H$.

Demonstração. Exercício.

Alguns subgrupos importantes de um grupo G

1. centralizador de $a \in G$ Representa-se por $C(a)$ e define-se por
$$C(a) = \{x \in G \mid ax = xa\}.$$
2. centro de G Representa-se por $Z(G)$ e define-se por
$$Z(G) = \{x \in G \mid ax = xa, \ (\forall a \in G)\}.$$

Subgrupos

Proposição. Sejam G um grupo e $H, K < G$. Então, $H \cap K < G$.

Demonstração. Sejam G um grupo e $H, K < G$. Então,

1. $H \cap K \neq \emptyset$, pois $1_G \in H$ e $1_G \in K$, pelo que $1_G \in H \cap K$;
2. dados $x, y \in H \cap K$, temos que $x, y \in H$ e $x, y \in K$, pelo que $xy \in H$ e $xy \in K$. Logo, $xy \in H \cap K$.
3. dado $x \in H \cap K$, temos que $x \in H$ e $x \in K$, pelo que $x^{-1} \in H$ e $x^{-1} \in K$ e, portanto, $x^{-1} \in H \cap K$.

Logo, $H \cap K < G$.

Proposição. Seja G um grupo. Então, a intersecção de uma família não vazia de subgrupos de G é ainda um subgrupo de G.

Subgrupos

O conceito de subgrupo gerado por um subconjunto de um grupo

Sejam G um grupo e $X \subseteq G$. Consideremos

$$\mathcal{H} = \{K \subseteq G : \; K < G \quad \text{e} \quad H \subseteq K\}$$

i.e., $\mathcal{H}$ é o conjunto de todos os subgrupos de G que contêm X. Então:

1. $\mathcal{H} \neq \emptyset$;
2. $\bigcap\limits_{K \in \mathcal{H}} K < G$;
3. $X \subseteq \bigcap\limits_{K \in \mathcal{H}} K$.
4. $J < G \; \wedge \; X \subseteq J \Rightarrow \bigcap\limits_{K \in \mathcal{H}} K \subseteq J$.

Assim, $\bigcap\limits_{K \in \mathcal{H}} K$ é **o** menor subgrupo de G que contém X.

Cap I. Elementos da teoria de grupos

Subgrupos

O menor subgrupo de G que contém X designa-se por *subgrupo de G gerado por X* e representa-se por $\langle X\rangle$.

Se $X=\{a\}$, então escrevemos $\langle a\rangle$ para representar $\langle X\rangle$ e falamos no *subgrupo de G gerado por a*.

Proposição. Sejam G um grupo e $a\in G$. Então, $\langle a\rangle=\{a^n \mid n\in\mathbb{Z}\}$.

Demonstração. Sejam G um grupo e $a\in G$. Seja

$$B=\{a^n \mid n\in\mathbb{Z}\}\,.$$

Mostramos que B é o menor subgrupo de G que contém a. (Exercício)

Cap I. Elementos da teoria de grupos

Ordem de um elemento de um grupo

Exemplo 1. Consideremos o grupo $(\mathbb{R} \setminus \{0\}, \times)$, cujo elemento neutro é 1. É claro que,

1. $1^1 = 1$
2. $(-1)^1 = -1 \neq 1$ mas $(-1)^2 = 1$
3. para qualquer $x \in \mathbb{R} \setminus \{1, -1\}$, não existe um inteiro positivo n ($n \in \mathbb{Z}^+$), tal que $x^n = 1$.

Exemplo 2. Consideremos o grupo 4-Klein G, cujo elemento neutro é e:

$$\begin{array}{c|cccc}
\cdot & e & a & b & c \\
\hline
e & e & a & b & c \\
a & a & e & c & b \\
b & b & c & e & a \\
c & c & b & a & e
\end{array}.$$

Facilmente se verifica que $e^1 = 1$ e para qualquer $x \in G \setminus \{e\}$, $x^1 \neq e$ e $x^2 = e$.

Exemplo 3. No grupo aditivo $(\mathbb{Z}_4, +)$, cujo elemento neutro é $\bar{0}$, temos:

1. $\bar{0} = \bar{0}$
2. $\bar{1} \neq \bar{0},\ \bar{1} + \bar{1} = \bar{2} \neq \bar{0},\ \bar{1} + \bar{1} + \bar{1} = \bar{3} \neq\ \bar{0}$ e $\bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{0}$
3. $\bar{2} \neq \bar{0}$ e $\bar{2} + \bar{2} = \bar{0}$
4. $\bar{3} \neq \bar{0},\ \bar{3} + \bar{3} = \bar{2} \neq \bar{0},\ \bar{3} + \bar{3} + \bar{3} = \bar{1} \neq \bar{0}$ e $\bar{3} + \bar{3} + \bar{3} + \bar{3} = \bar{0}$.

isto é

1. $1 \cdot \bar{0} = \bar{0}$
2. $1 \cdot \bar{1} \neq \bar{0},\ 2 \cdot \bar{1} = \bar{2} \neq \bar{0},\ 3 \cdot \bar{1} = \bar{3} \neq\ \bar{0}$ e $4 \cdot \bar{1} = \bar{0}$
3. $1 \cdot \bar{2} = \bar{2} \neq \bar{0}$ e $2 \cdot \bar{2} = \bar{4} = \bar{0}$
4. $1 \cdot \bar{3} \neq \bar{0},\ 2 \cdot \bar{3} = \bar{2} \neq \bar{0},\ 3 \cdot \bar{3} = \bar{1} \neq \bar{0}$ e $4 \cdot \bar{3} = \bar{0}$.

Ordem de um elemento de um grupo

Sejam G um grupo e $a \in G$.

(i) Diz-se que a tem *ordem infinita* se não existe qualquer $p \in \mathbb{N}$ tal que $a^p = 1_G$.

(ii) Diz-se que a tem *ordem finita* k, e escreve-se $o(a) = k$, se

$$\begin{array}{ll} (1) & k \in \mathbb{N}; \\ (2) & a^k = 1_G; \\ (3) & p \in \mathbb{N} \quad \text{e} \quad a^p = 1_G \Longrightarrow k \leq p. \end{array}$$

- $(\mathbb{R} \setminus \{0\}, \times)$: $o(1) = 1$, $o(-1) = 2$ e os restantes elementos têm ordem infinita.

- No grupo grupo 4-Klein , $o(e) = 1$ e $o(a) = o(b) = o(c) = 2$.

- No grupo $(\mathbb{Z}_4, +)$, $o(\bar{0}) = 1$, $o(\bar{2}) = 2$ e $o(\bar{1}) = o(\bar{3}) = 4$.

Cap I. Elementos da teoria de grupos

Ordem de um elemento de um grupo

Proposição. O elemento neutro de um grupo G é o único elemento de G que tem ordem igual a 1.

Demonstração. É claro que $o(1_G) = 1$. Suponhamos que $a \in G$ é tal que $o(a) = 1$. Então, $a^1 = 1_G$ i.e., $a = 1_G$.

Proposição. Sejam G um grupo e $a \in G$ um elemento com ordem infinita. Então, para quaisquer $m, n \in \mathbb{Z}$, se $m \neq n$, então $a^m \neq a^n$.

Demonstração. Sejam $m, n \in \mathbb{Z}$ tal que $a^m = a^n$. Então,

$$\begin{aligned}
a^m = a^n \quad &\Longrightarrow \quad a^m a^{-n} = a^n a^{-m} = 1_G \\
&\Longrightarrow \quad a^{m-n} = a^{n-m} = 1_G \\
&\Longrightarrow \quad a^{|m-n|} = 1_G \\
&\Longrightarrow \quad |m-n| = 0 \qquad\qquad (o\,(a)\text{ é infinita}) \\
&\Longrightarrow \quad m = n.
\end{aligned}$$

Logo, se $m \neq n$ então $a^m \neq a^n$.

Ordem de um elemento de um grupo

Tendo em conta que $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$, temos os dois seguintes corolários:

Corolário 1. Sejam G um grupo, se $a \in G$ tem ordem infinita, então o subgrupo $\langle a \rangle$ tem um número infinito de elementos.

Corolário 2. Num grupo finito nenhum elemento tem ordem infinita.

Proposição. Sejam G um grupo, $a \in G$ e $k \in \mathbb{N}$ tal que $o(a) = k$. Então,

1. se um inteiro n tem r como resto na divisão por k então $a^n = a^r$;
2. para $n \in \mathbb{Z}$, $a^n = 1_G \Leftrightarrow k \mid n$;
3. $\langle a \rangle = \left\{1_G, a^1, a^2, \ldots, a^{k-1}\right\}$;
4. $\langle a \rangle$ tem exactamente k elementos.

Demonstração.

1. Sejam $q, r \in \mathbb{Z}$ tais que $0 \leq r < k$ e $q \in \mathbb{Z}$ tal que $n = qk + r$. Então,

$$a^n = a^{qk+r} = a^{qk} a^r = \left(a^k\right)^q a^r = 1_G^q \, a^r = 1_G \, a^r = a^r.$$

2. Pretendemos provar que $a^m = 1_G \Leftrightarrow k \mid m$, ou seja, que

$$a^m = 1_G \Leftrightarrow m = kp \text{ para algum } p \in \mathbb{Z}.$$

   Suponhamos primeiro que $m = kp$, para algum $p \in \mathbb{Z}$. Então,

$$a^m = a^{kp} = \left(a^k\right)^p = 1_G^p = 1_G.$$

   Reciprocamente, suponhamos que $a^m = 1_G$. Pelo algoritmo da divisão, existem $p \in \mathbb{Z}$ e $0 \leq r < k$ tais que $m = kp + r$ e, portanto,

$$1_G = a^m = a^{kp+r} = \left(a^k\right)^p a^r = 1_G^p a^r = 1_G a^r = a^r.$$

   Como $o\,(a) = k$, temos que $r = 0$. Logo, $m = kp$.

Cap I. Elementos da teoria de grupos

Ordem de um elemento de um grupo

3. Pretendemos mostrar que

$$\langle a\rangle = \left\{1_G, a^1, a^2, \ldots, a^{k-1}\right\}.$$

Sabemos que $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$. É claro que $\left\{1_G, a, a^2, a^3, \ldots, a^{k-1}\right\} \subseteq \langle a\rangle$.

Relativamente à outra inclusão, seja $x \in \langle a\rangle$. Então $x = a^p$, para algum $p \in \mathbb{Z}$.

Se $p \in \{0, 1, 2, 3, \ldots, k-1\}$, $x \in \left\{1_G, a, a^2, a^3, \ldots, a^{k-1}\right\}$.

Se $p \notin \{0, 1, 2, 3, \ldots, k-1\}$, dividimos p por k, consideramos o resto r desta divisão, o qual satisfaz $0 \leq r \leq k-1$, e sabemos, por (1), que $a^p = a^r$.

Logo, $\langle a\rangle \subseteq \left\{e, a, a^2, a^3, \ldots, a^{k-1}\right\}$ e a igualdade indicada é verdadeira.

Ordem de um elemento de um grupo

4. Pretendemos mostrar que $\langle a \rangle$ tem exactamente k elementos.

Suponhamos que na lista $1_G, a, a^2, a^3, \ldots, a^{k-1}$ há repetição de elementos:

$$a^p = a^q, \quad \text{para certos} \quad 0 \leq q < p \leq k-1.$$

Então, $p - q > 0$ e

$$a^{p-q} = a^p a^{-q} = a^q a^{-q} = 1_G,$$

pelo que $p - q \leq k - 1$. Como $o(a) = k$, temos que $k \leq p - q$ pelo que obtemos $k \leq p - q \leq k - 1$, o que é impossível.

Logo, não há qualquer repetição e o subgrupo $\langle a \rangle$ tem exactamente k elementos.

Álgebra - Lic. C. Computação

Paula Marques Smith

DMAT - UM

3 out'19

Cap I. Elementos da teoria de grupos

O Teorema de Lagrange

Sejam G um grupo e $H < G$. Para cada $a \in G$, os subconjuntos

$$aH = \{ax : x \in H\} \qquad \text{e} \qquad Ha = \{xa : x \in H\}$$

designam-se por *classe lateral esquerda de a módulo H* e *classe lateral direita de a módulo H*, respetivamente.

Proposição. Sejam G um grupo e $H < G$. Tem-se:

1. $G = \bigcup_{x \in G} xH \qquad (G = \bigcup_{x \in G} Hx)$;
2. $xH \cap yH \neq \emptyset \iff xH = yH \qquad (Hx \cap Hy \neq \emptyset \iff Hx = Hx)$.

Demonstração. Exercício.

Corolário. Sejam G um grupo e $H < G$. Então $\{xH\}_{x \in G}$, $(\{Hx\}_{x \in G})$, constitui uma partição de G.

O Teorema de Lagrange

Proposição. Sejam G um grupo e $H < G$. Se H é finito então cada classe lateral módulo H tem a mesma cardinalidade que H.

Demonstração Sejam G um grupo e $a \in G$. As aplicações

$$\begin{array}{rcl} \lambda_a : G & \longrightarrow & G \\ x & \longmapsto & ax \end{array} \quad \text{e} \quad \begin{array}{rcl} \rho_a : G & \longrightarrow & G \\ x & \longmapsto & xa \end{array}$$

são bijeções de G em G (porquê?). Como H é finito, $\lambda_a|_H$ e $\rho_a|_H$ são bijeções de H em $\lambda_a(H) = aH$ e de H em $\rho_a(H) = Ha$, respectivamente (porquê?). Assim,

$$\sharp(aH) = \sharp H = \sharp(Ha).$$

Cap I. Elementos da teoria de grupos

O Teorema de Lagrange

Exemplo 1. No grupo *4-Klein*,

$$\begin{array}{c|cccc} \cdot & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array},$$

considerando o subgrupo $H = \{e, a\}$, as classes laterais esquerdas módulo H são

$$eH = H = aH \qquad \text{e} \qquad bH = \{b, c\} = cH$$

e as classes laterais direitas módulo H são iguais já que o grupo é comutativo.

Exemplo 2. No grupo $G = \{e, p, q, a, b, c\}$, cuja operação é dada pela tabela

$$\begin{array}{c|cccccc}
\cdot & e & p & q & a & b & c \\
\hline
e & e & p & q & a & b & c \\
p & p & q & e & c & a & b \\
q & q & e & p & b & c & a \\
a & a & b & c & e & p & q \\
b & b & c & a & q & e & p \\
c & c & a & b & p & q & e
\end{array},$$

considerando o subgrupo $H = \{e, a\}$, as classes laterais esquerdas módulo H são

$$eH = H = aH, \quad bH = \{b, q\} = qH \quad \text{e} \quad cH = \{c, p\} = pH$$

e as classes laterais direitas módulo H são

$$He = H = Ha, \quad Hb = \{b, p\} = Hp \quad \text{e} \quad Hc = \{c, q\} = Hq.$$

O Teorema de Lagrange

Proposição. Sejam G um grupo finito e $H < G$. Se $a_1H, a_2H, \ldots, a_rH$ forem, exactamente, as classes laterais esquerdas módulo H ($a_1, a_2, \ldots, a_r \in G$), então, $Ha_1^{-1}, Ha_2^{-1}, \ldots, Ha_r^{-1}$ são exactamente as classes laterais direitas módulo H.

Demonstração. Cada elemento de G pertence exactamente a uma e uma só classe lateral esquerda $a_1H, a_2H, \ldots, a_rH$. Sejam $x \in G$ e $1 \leq i \leq r$. Então,

$$\begin{aligned} x \in Ha_i^{-1} &\iff x\left(a_i^{-1}\right)^{-1} \in H \\ &\iff xa_i \in H \\ &\iff \left(x^{-1}\right)^{-1} a_i \in H \\ &\iff x^{-1} \in a_iH. \end{aligned}$$

Como a condição $x^{-1} \in a_iH$ é verdadeira para exactamente um valor de i, então também a expressão $x \in Ha_i^{-1}$ é verdadeira para exactamente um valor de i.

Cap I. Elementos da teoria de grupos

O Teorema de Lagrange

Sejam G um grupo **finito** e $H < G$. Chama-se:

(i) *ordem do grupo* G, e representa-se por $|G|$, ao cardinal de G;

(ii) *índice de* H *em* G, e representa-se por $|G : H|$, ao número de classes laterais esquerdas (ou direitas) módulo H.

Teroema **(de Lagrange)** Sejam G um grupo finito e $H < G$. Então,

$$|G| = |G : H| \times |H| \,.$$

Demonstração. Imediata, tendo em conta o Corolário anterior : $\{xH\}_{x \in G}$ é uma partição de G, e o facto do grupo G ser finito.

O Teorema de Lagrange

Corolário. Num grupo finito G, a ordem de cada elemento divide a ordem do grupo.

Demonstração. Imediata, tendo em conta que $o\,(a) = |\langle a \rangle|$, para todo $a \in G$.

Corolário. Sejam G um grupo finito e p um número primo tal que $|G| = p$. Então, existe $b \in G$ tal que $G = \langle b \rangle$.

Demonstração. Como p é primo, $p \neq 1$, pelo que $G \neq \{1_G\}$. Seja $x \in G$ tal que $x \neq 1_G$. Então,

$$o\,(x) \mid p \Longrightarrow o\,(x) = p \Longrightarrow |\langle x \rangle| = p \Longleftrightarrow G = \langle x \rangle\,.$$

Observação: O inverso do Teorema de Lagrange não é verdadeiro, i.e., o facto de a ordem de um grupo G admitir um determinado factor, não garante que existe um subgrupo de G cuja ordem é esse factor.

Álgebra - Lic. C. Computação

Paula Marques Smith

DMAT - UM

04 out'19

subgrupos normais, relações de congruência e grupo quociente

Sejam G um grupo e $H < G$. Diz-se que H é *subgrupo invariante* ou *normal* de G, e escreve-se $H \lhd G$, se

$$(\forall x \in G) \quad xH = Hx.$$

Assim, um subgrupo H de G é invariante se, para cada $x \in G$ e $h_1 \in H$, existe $h_2 \in H$ tal que

$$xh_1 = h_2x.$$

Exemplos.

1. Dado um grupo G, $\{1_G\}$ e G são subgrupos normais de G.
2. O centro $Z(G)$ de um grupo G é um subgrupo normal de G.
3. Todo o subgrupo de um grupo abeliano é um subgrupo normal.

Elementos da teoria de grupos

Proposição. Sejam G um grupo e $H < G$ tal que $|G : H| = 2$. Então, $H \lhd G$.

Dem. Seja $H < G$ tal que $|G : H| = 2$. Então,

$$\{H, xH\}_{x \in G:\, H \neq xH} \qquad \text{e} \qquad \{H, Hx\}_{x \in G:\, H \neq Hx}$$

são partições de G, pelo que $xH = G \setminus H = Hx$, para qualquer $x \in G \setminus H$. Portanto, para todo $y \in G$, como

$$yH = \begin{cases} H & \text{se } y \in H \\ G \setminus H & \text{se } y \notin H \end{cases}$$

e

$$Hy = \begin{cases} H & \text{se } y \in H \\ G \setminus H & \text{se } y \notin H, \end{cases}$$

temos que $yH = Hy$, qualquer que seja $y \in G$.

Proposição. Sejam G um grupo e $H < G$. Então,

$$H \lhd G \Longleftrightarrow (\forall x \in G) \;\; (\forall h \in H) \quad xhx^{-1} \in H.$$

Dem. Suponhamos que $H \lhd G$. Então, para todo $x \in G$, $xH = Hx$. Sejam $g \in G$ e $h \in H$:

$$ghg^{-1} = (gh)\,g^{-1} = \left(h'g\right) g^{-1} = h'\left(gg^{-1}\right) = h' \in H.$$

Reciprocamente, suponhamos que, para quaisquer $x \in G$ e $h \in H$, se tem $xhx^{-1} \in H$ e seja $g \in G$. Então,

$$\begin{aligned} y \in gH \quad & \Leftrightarrow \quad (\exists h' \in H) \quad y = gh' \\ & \Leftrightarrow \quad (\exists h' \in H) \quad y = gh'\left(g^{-1}g\right) \\ & \Leftrightarrow \quad (\exists h' \in H) \quad y = \left(gh'g^{-1}\right) g \\ & \Rightarrow \quad y \in Hg \qquad \textit{por hipótese}, \end{aligned}$$

pelo que $gH \subseteq Hg$. Analogamente, $Hg \subseteq gH$ e, portanto, $Hg = gH$.

Elementos da teoria de grupos

subgrupos normais, relações de congruência e grupo quociente

Se G admite um subgrupo normal H, a relação $\equiv (mod\, H)$ definida por :

$$x \equiv y\, (mod\, H) \Leftrightarrow x^{-1}y \in H$$

é uma relação de equivalência que satisfaz:

$$x \equiv y\, (mod\, H) \ \wedge \ a \equiv b\, (mod\, H) \Rightarrow xa \equiv yb\, (mod\, H) \ \wedge \ ax \equiv by\, (mod\, H)$$

(Verifique)

O respetivo conjunto quociente representa-se por G/H, tendo-se:

$$G/H = \{xH : x \in G\} = \{Hx : x \in G\}.$$

(Verifique)

Proposição. Sejam G um grupo e H um subgrupo normal de G. Então

$$x \equiv y\, (mod\, H) \Leftrightarrow yx^{-1} \in H.$$

Elementos da teoria de grupos

subgrupos normais, relações de congruência e grupo quociente

Algebrização de G/H: multiplicação de subconjuntos de G:

$$(xH)\,(yH) = x(Hy)H = x(yH)H = (xy)(HH) = xyH.$$

Teorema. Sejam G um grupo e $H \lhd G$. Então, G/H é grupo para a multiplicação de subconjuntos de G.

Demonstração: exercício

$$1_{G/H} = H : \quad (H)\,(xH) = (1_G H)\,(xH) = (1_G x)H = xH$$

$$(xH)^{-1} = x^{-1}H : \quad (xH)\,(x^{-1}H) = (xx^{-1})H = H.$$

O grupo G/H designa-se por *grupo quociente determinado por H em G*.

Elementos da teoria de grupos

subgrupos normais, relações de congruência e grupo quociente

Proposição. Sejam G um grupo e θ uma relação de congruência definida em G. Então,

1. a classe de congruência do elemento identidade, $[1_G]_\theta$, é um subgrupo normal de G;
2. para quaisquer $x, y \in G$,
$$x\theta y \iff x^{-1}y \in [1_G]_\theta \,.$$

Demonstração: exercício

Recorde que

$$[1_G]_\theta = \{x \in G : x\theta 1_G\}.$$

Sejam G_1, G_2 grupos. Uma aplicação $\psi : G_1 \longrightarrow G_2$ diz-se um *morfismo* ou *homomorfismo* de grupos se

$$(\forall x, y \in G_1) \qquad \psi(xy) = \psi(x)\,\psi(y)\,.$$

Um morfismo de grupos $\psi : G_1 \longrightarrow G_2$ diz-se um

- *epimorfismo* se for uma aplicação sobrejetiva;
- *monomorfismo* se for uma aplicação injetiva
- *isomorfismo* se for uma aplicação bijetiva;
- *endomorfismo* se $G_1 = G_2$;
- *automorfismo* se $G_1 = G_2$ e ψ for uma aplicação bijetiva.

Sempre que exista um isomorfismo $\psi : G_1 \longrightarrow G_2$, diz-se que G_1 é isomorfo a G_2 e escreve-se $G_1 \cong G_2$. Como

$$G_1 \cong G_2 \implies G_2 \cong G_1,$$

podemos falar, sem ambiguidade, em *grupos isomorfos*.

Elementos da teoria de grupos

Exemplos. Para quaisquer grupos G e H,

- a aplicação identidade $id_G : G \to G$, definida por $id_G(x) = x$, para todo $x \in G$, é um automorfismo de G. Designa-se por *morfismo identidade*.

- a aplicação $\varphi : G \to H$, definida por $\varphi(x) = 1_H$, para todo $x \in G$, é um morfismo. Designa-se por *morfismo nulo*.

Proposição. Sejam G_1 e G_2 grupos e $\psi : G_1 \longrightarrow G_2$ um morfismo. Então:

- $\psi(1_{G_1}) = 1_{G_2}$;
- $[\psi(x)]^{-1} = \psi\left(x^{-1}\right)$, para qualquer $x \in G_1$.

Dem. De $1_{G_1} 1_{G_1} = 1_{G_1}$, obtemos

$$\psi(1_{G_1})\,\psi(1_{G_1}) = \psi(1_{G_1} 1_{G_1}) = \psi(1_{G_1}) = \psi(1_{G_1})\,1_{G_2}.$$

Logo,

$$\psi(1_{G_1})\,\psi(1_{G_1}) = \psi(1_{G_1})\,1_{G_2},$$

e, então, pela lei do corte,

$$\psi(1_{G_1}) = 1_{G_2}.$$

Elementos da teoria de grupos

Seja $x \in G_1$. Então,

$$\psi(x)\,\psi\left(x^{-1}\right) = \psi\left(xx^{-1}\right) = \psi(1_{G_1}) = 1_{G_2}$$

e

$$\psi\left(x^{-1}\right)\psi(x) = \psi\left(x^{-1}x\right) = \psi(1_{G_1}) = 1_{G_2}.$$

Portanto, $[\psi(x)]^{-1} = \psi\left(x^{-1}\right)$.

Proposição. Sejam G_1 e G_2 grupos, $H \subseteq G_1$ e $\psi : G_1 \longrightarrow G_2$ um morfismo de grupos. Então,

$$H < G_1 \Longrightarrow \psi(H) < G_2.$$

Dem. Seja $H < G_1$. Então:

(i) Como $H < G_1$, $1_{G_1} \in H$, pelo que $\psi(1_{G_1}) \in \psi(H)$. Pela proposição anterior, $\psi(1_{G_1}) = 1_{G_2}$. Portanto, $1_{G_2} \in \psi(H)$.

(ii) Sejam $a, b \in \psi(H)$. Então,

$$(\exists x, y \in H) \quad a = \psi(x) \quad \text{e} \quad b = \psi(y).$$

Portanto, $ab = \psi(x)\,\psi(y) = \psi(xy)$, pelo que $ab \in \psi(H)$;

Elementos da teoria de grupos

(iii) Seja $a \in \psi(H)$. Então,

$$a = \psi(x), \text{ para certo } x \in H \Rightarrow a^{-1} = [\psi(x)]^{-1} = \psi\left(x^{-1}\right) \text{ onde } x^{-1} \in H.$$

Logo, $a^{-1} \in \psi(H)$.

De (i), (ii) e (iii) concluimos que $\psi(H) < G$.

Corolário. Seja $\psi : G_1 \longrightarrow G_2$ um morfismo de grupos. Se ψ é um monomorfismo então

$$G_1 \cong \psi(G_1).$$

Sejam G_1 e G_2 grupos e $\varphi : G_1 \to G_2$ um morfismo de grupos. O subgrupo $\varphi(G_1)$ de G_2 designa-se por *imagem de* φ, e representa-se por $\mathcal{I}m\,\varphi$ ou por $\varphi(G_1)$.

Elementos da teoria de grupos

Proposição. A imagem epimorfa de um subgrupo invariante de um grupo é um subgrupo invariante.

Dem. G_1, G_2 grupos, $H \subseteq G_1$ e $\psi : G_1 \longrightarrow G_2$ um epimorfismo. Pretendemos mostrar que

$$H \lhd G_1 \Longrightarrow \psi(H) \lhd G_2.$$

Tendo em conta a proposição anterior, falta apenas provar que, para $g \in G_2$ e $a \in \psi(H)$ se tem que $gag^{-1} \in \psi(H)$. Como ψ é um epimorfismo, tem-se:

$$\begin{aligned}
g \in G_2,\ a \in \psi(H) &\Longrightarrow (\exists x \in G_1)(\exists h \in H)\ \ g = \psi(x),\ a = \psi(h) \\
&\Longrightarrow gag^{-1} = \psi(x)\psi(h)[\psi(x)]^{-1} \\
&\Longrightarrow gag^{-1} = \psi\left(xhx^{-1}\right),\ onde\ xhx^{-1} \in H \\
&\Longrightarrow gag^{-1} \in \psi(H).
\end{aligned}$$

Assim, $\psi(H) \lhd G_2$.

Elementos da teoria de grupos

Para fazer:

1. Sejam G_1 e G_2 grupos, $H' \subseteq G_2$ e $\psi : G_1 \longrightarrow G_2$ um morfismo de grupos. Prove que
   - $H' < G_2 \Longrightarrow \psi^{\leftarrow}(H') < G_1$.
   - $H' \lhd G_2 \Longrightarrow \psi^{\leftarrow}(H') \lhd G_1$.
   - $\psi^{\leftarrow}(\{1_{G_2}\}) \lhd G_1$.

2. - Justifique que dois grupos finitos isomorfos têm a mesma ordem.
   - Enuncie a proposição recíproca da proposição anterior e prove que ela é uma proposição falsa. (*sugestão: considere o grupo 4-Klein e o grupo aditivo* $\mathbb{Z}_4$.)

Álgebra - Lic C. Computação

Paula Marques Smith

DMA - UM

11 out'19

Cap I. Elementos da teoria de grupos

morfismos

Seja $\psi : G_1 \longrightarrow G_2$ um morfimo de grupos. Chama-se *núcleo* (ou *kernel*) de ψ, e representa-se por $\mathrm{Nuc}\,\psi$ (ou $\ker\psi$) ao subconjunto de G_1 definido por

$$\mathrm{Nuc}\,\psi = \psi^{\leftarrow}\left(\{1_{G_2}\}\right) = \{x \in G_1 \mid \psi(x) = 1_{G_2}\}\,.$$

Assim,

- $\mathrm{Nuc}\,\psi$ é um subgrupo invariante de G_1;
- $\mathrm{Nuc}\,\psi$ define uma relação de congruência em G_1:

$$\begin{aligned} x \equiv y \,(\mathrm{mod}\ \mathrm{Nuc}\,\psi) &\iff xy^{-1} \in \mathrm{Nuc}\,\psi \\ &\iff \psi\left(xy^{-1}\right) = 1_{G_2} \\ &\iff \psi(x)\,[\psi(y)]^{-1} = 1_{G_2} \\ &\iff \psi(x) = \psi(y)\,. \end{aligned}$$

Proposição. Sejam G um grupo e $H \lhd G$. Então,

$$\begin{array}{rcl} \pi : G & \longrightarrow & G/H \\ x & \longmapsto & xH \end{array}$$

é um epimorfismo tal que $\mathrm{Nuc}\,\pi = H$.

Dem. Sejam G um grupo e $H \lhd G$. Para quaisquer $x, y \in G$,

$$\psi(xy) = (xy)H = xHyH = \psi(x)\psi(y),$$

pelo que π é um morfismo. Além disso, como cada elemento de G/H é uma classe de equivalência, ele é imagem, por π, de qualquer um dos seus elementos. Portanto, π é sobrejetiva. Finalmente,

$$\begin{array}{rcl} x \in \mathrm{Nuc}\,\pi & \Longleftrightarrow & \pi(x) = H \\ & \Longleftrightarrow & xH = H \\ & \Longleftrightarrow & x \in H. \end{array}$$

O morfismo π designa-se por *epimorfismo canónico*.

Cap I. Elementos da teoria de grupos

morfismos

Observação

- qualquer morfismo de grupos determina um subgrupo normal do seu domínio, a saber, o seu núcleo;
- qualquer subgrupo invariante de um grupo, determina um morfismo cujo núcleo é esse mesmo subgrupo.
- estes dois processos são inversos um do outro.

Cap I. Elementos da teoria de grupos

morfismos

Teorema Fundamental do Homomorfismo. Seja $\theta : G \longrightarrow G'$ um morfismo de grupos. Então,

$$\mathrm{Im}\,\theta \;\cong\; G/_{\mathrm{Nuc}\,\theta}.$$

Dem. Seja $\phi : G/_{\mathrm{Nuc}\,\theta} \longrightarrow G'$ tal que

$$(\forall x \in G) \quad \phi\left(x\,\mathrm{Nuc}\,\theta\right) = \theta\left(x\right).$$

- ϕ está bem definida:
  - para qualquer $xK \in G/\mathrm{Nuc}\,\theta$, $x \in G$ e, portanto, existe $\theta(x) \in G'$.
  - para $x, y \in G$,

$$\begin{aligned} x\,\mathrm{Nuc}\,\theta = y\,\mathrm{Nuc}\,\theta \quad &\Longrightarrow \quad x^{-1}y \in \mathrm{Nuc}\,\theta \\ &\Longrightarrow \quad \theta\left(x^{-1}y\right) = 1_{G'} \\ &\Longrightarrow \quad \theta\left(x\right) = \theta\left(y\right), \end{aligned}$$

  i.e., se $x\,\mathrm{Nuc}\,\theta = y\,\mathrm{Nuc}\,\theta$ então $\theta\left(x\right) = \theta\left(y\right)$.

Cap I. Elementos da teoria de grupos

morfismos

- ϕ é injectiva:

$$\begin{aligned}\phi\left(x\mathrm{Nuc}\,\theta\right)=\phi\left(y\mathrm{Nuc}\,\theta\right) &\implies \theta\left(x\right)=\theta\left(y\right)\\ &\implies \theta\left(x^{-1}y\right)=1_{G'}\\ &\implies x^{-1}y\in\mathrm{Nuc}\,\theta\\ &\implies x\,\mathrm{Nuc}\,\theta=y\,\mathrm{Nuc}\,\theta\end{aligned}$$

- $\mathrm{Im}\,\phi=\{\phi\left(\mathrm{x}\,\mathrm{Nuc}\,\theta\right):\mathrm{x}\in\mathrm{G}\}=\{\theta\left(\mathrm{x}\right):\mathrm{x}\in\mathrm{G}\}=\mathrm{Im}\,\theta.$

- ϕ é um morfismo:

$$\begin{aligned}\phi\left(\left(x\,\mathrm{Nuc}\,\theta\right)\,\left(y\,\mathrm{Nuc}\,\theta\right)\right) &= \phi\left(\left(xy\right)\mathrm{Nuc}\,\theta\right)\\ &= \theta\left(xy\right)\\ &= \theta\left(x\right)\theta\left(y\right)\\ &= \phi\left(x\,\mathrm{Nuc}\,\theta\right)\;\phi\left(y\,\mathrm{Nuc}\,\theta\right).\end{aligned}$$

teoremas de isomorfismo

Lema. Sejam $\psi : G \to G'$ um morfismo de grupos e $K < G$. Então,

$$\mathrm{Nuc}\,\psi \subseteq K \Longrightarrow \psi^{\leftarrow}(\psi(K)) = K.$$

Dem. Exercício

Teorema 1. Sejam G e G' grupos e $\psi : G \longrightarrow G'$ um epimorfismo. Seja $K \lhd G$ tal que $\mathrm{Nuc}\,\psi \subseteq K$. Então

$$G/_K \cong G'/_{\psi(K)}.$$

Dem. Exercício

(i) Recorde que: $K \lhd G \Rightarrow \psi(K) \lhd G'$

(ii) Mostre que a correspondência $xK \longmapsto \psi(x)\psi(K)$ de $G/_K$ em $G'/_{\psi(K)}$ é um isomorfismo de grupos.

teoremas de isomorfismo

Teorema 2. Sejam G um grupo e $H, T < G$ tal que $T \lhd G$. Então,

$$(HT)/_T \cong H/_{(H\cap T)}.$$

Dem. Exercício

- Mostre que HT é um grupo;
- Mostre que T é um subgrupo normal de HT;
- Mostre que $H \cap T$ é um subgrupo normal de H;
- Considere o epimorfismo canónico $\pi : HT \longrightarrow HT/_T$ e aplique o Teorema Fundamental do Homomorfismo a π;
- Conclua que $(HT)/_T \cong H/_{(H\cap T)}$.

Cap I. Elementos da teoria de grupos

grupos cíclicos

- O grupo $(\mathbb{Z}, +)$ é tal que $\mathbb{Z} = \langle 1 \rangle$, uma vez que
$$(\forall n \in \mathbb{Z}) \quad n = n \cdot 1.$$
- O grupo $(\mathbb{Z}_4, +)$ é tal que $\mathbb{Z}_4 = \langle \bar{1} \rangle = \langle \bar{3} \rangle$, pois
$$\begin{aligned} \bar{0} &= 0 \cdot \bar{1} = 0 \cdot \bar{3} \\ \bar{1} &= 1 \cdot \bar{1} = 3 \cdot \bar{3} \\ \bar{2} &= 2 \cdot \bar{1} = 2 \cdot \bar{3} \\ \bar{3} &= 3 \cdot \bar{1} = 1 \cdot \bar{3} \end{aligned}$$
- A situação anterior não se aplica ao grupo $(\mathbb{R}, +)$.

Os grupos $(\mathbb{Z}, +)$ e $(\mathbb{Z}_4, +)$ dizem-se grupos cíclicos.

- Um grupo G diz-se *grupo cíclico* se
$$(\exists a \in G) \quad G = \langle a \rangle.$$

O grupo $(\mathbb{R}, +)$ não é cíclico.

Cap I. Elementos da teoria de grupos

grupos cíclicos

- Para qualquer $n \in \mathbb{N}$, temos que $(\mathbb{Z}_n, +)$ é cíclico, já que $\mathbb{Z}_n = \langle [1]_n \rangle$.

- O conjunto $G = \{i, -i, 1, -1\}$, quando algebrizado com a multiplicação usual de complexos, é um grupo cíclico: $G = \langle i \rangle$.

- O grupo trivial $G = \{1_G\}$ é um grupo cíclico. Em qualquer grupo G, $\langle 1_G \rangle = \{1_G\}$.

Proposição. Todo o grupo cíclico é abeliano.

Demonstração. Sejam $G = \langle a \rangle$ e $x, y \in G$. Então, existem $n, m \in \mathbb{Z}$ tais que $x = a^n$ e $y = a^m$. assim,

$$xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx.$$

Obs. O recíproco do teorema anterir não é verdadeiro: o grupo 4-Klein é abeliano mas não é cíclico, porque $\langle 1_G \rangle = \{1_G\} \neq G$, $\langle a \rangle = \{1_G, a\} \neq G$, $\langle b \rangle = \{1_G, b\} \neq G$ e $\langle c \rangle = \{1_G, c\} \neq G$. Não existe, pois, $x \in G$ tal que $G = \langle x \rangle$.

Álgebra - Lic Ciências de Computação

Paula Marques Smith

DMA - UM

17 out'19

grupos cíclicos

Teorema: Qualquer subgrupo de um grupo cíclico é cíclico.

Demonstração. Sejam $G = \langle a \rangle$, para algum $a \in G$, e $H < G$.

Se $H = \{1_G\}$, então $H = \langle 1_G \rangle$ e, portanto, H é cíclico.

Se $H \neq \{1_G\}$, então, existe $x = a^n \in G$ $(n \neq 0)$ tal que $x \in H$. Então, H tem pelo menos uma potência positiva de a. Seja d o menor inteiro positivo tal que $a^d \in H$.

Provamos que $H = \left\langle a^d \right\rangle$:

(i) Por um lado $a^d \in H$, logo $\left\langle a^d \right\rangle \subseteq H$;

(ii) Por outro lado, dado $y \in H$, como $y \in G$, $y = a^m$ para algum $m \in \mathbb{Z} \setminus \{0\}$.

Cap I. Elementos da teoria de grupos

grupos cíclicos

Então, existem $q, r \in \mathbb{Z}$ com $0 \leq r < d$, tais que

$$y = a^m = a^{dq+r} = a^{qd} a^r.$$

Assim,

$$a^r = \left(a^d\right)^{-q} a^m \in H,$$

pelo que $r = 0$ ($0 \leq r < d$). Logo,

$$a^m = a^{qd} \in \left\langle a^d \right\rangle,$$

e, portanto, $H = \left\langle a^d \right\rangle$.

- $\mathbb{Z}_4 = \langle \bar{1} \rangle = \langle \bar{3} \rangle$ e $o\left(\bar{1}\right) = o\left(\bar{3}\right) = 4$.

Proposição. Qualquer gerador de um grupo cíclico finito tem ordem igual à ordem do grupo.

Cap I. Elementos da teoria de grupos

grupos cíclicos

Proposição. Seja $G = \langle a \rangle$ um grupo infinito e $H = \left\langle a^d \right\rangle$, para algum $d \in \mathbb{N}$. Então,

$$H, aH, a^2H, ..., a^{d-1}H$$

é a lista completa de elementos de G/H.

Demonstração.

- para todo $x \in G$, $xH = a^r H$, $\quad$ para algum $r \in \{0, 1, 2, ..., d-1\}$:

se $x \in G = \langle a \rangle$, então existe $p \in \mathbb{Z}$ tal que $x = a^p$. Assim, $p = qd + r$, para certos $q \in \mathbb{Z}$ e $0 \leq r \leq d - 1$ e, portanto,

$$a^p = a^{qd+r} = a^r \cdot \left(a^d\right)^q \in a^r H.$$

Logo, $a^p H = a^r H$.

Cap I. Elementos da teoria de grupos

grupos cíclicos

- Provemos agora que, para $0 \leq i, j \leq d-1$ se tem

$$i \neq j \Longrightarrow a^i H \neq a^j H. \qquad (\star)$$

Suponhamos que $i < j$. Então, $0 \leq j - i \leq d-1$, pelo que

$$\begin{aligned} a^i H = a^j H &\iff \left(a^i\right)^{-1} a^j \in H \\ &\iff a^{j-i} \in H \\ &\iff j - i = kd, \text{ para algum } k \in \mathbb{Z} \\ &\iff j - i = 0 \\ &\iff j = i. \end{aligned}$$

Logo, a implicação $(\star)$ verifica-se e, portanto,

$$G/_H = \left\{H, aH, ..., a^{d-1}H\right\}.$$

Cap I. Elementos da teoria de grupos

grupos cíclicos

Proposição. Dois grupos cíclicos finitos são isomorfos se e só se tiverem a mesma ordem.

Demonstração. Sejam $G = \langle a \rangle$ e $T = \langle b \rangle$ dois grupos cíclicos e finitos.

- Se $G \cong T$, então G e T têm a mesma ordem.

- Se G e T têm a mesma ordem n, então, $o(a) = o(b) = n$ e

$$\begin{array}{rcl} G & = & \left\{1_G, a, a^2, ..., a^{n-1}, a^n\right\} \\ & & \text{e} \\ T & = & \left\{1_T, b, b^2, ..., b^{n-1}, b^n\right\}. \end{array}$$

A aplicação $\psi : G \longrightarrow T$ definida por

$$\psi = \left(\begin{array}{cccccc} 1_G & a & a^2 & \cdots & a^{n-1} & a^n \\ 1_T & b & b^2 & \cdots & b^{n-1} & b^n \end{array} \right)$$

é claramente um isomorfismo. (Verifique)+

grupos cíclicos

Corolário. Sejam $n \in \mathbb{N}$ e G um grupo cíclico de ordem n. Então, $G \cong \mathbb{Z}_n$.

- Se G é um grupo e $a \in G$ é um elemento de ordem infinita, então, para $m, n \in \mathbb{Z}$

$$m \neq n \Longrightarrow a^m \neq a^n.$$

Assim, se G é infinito e cíclico, temos que $G = \langle a \rangle$, para algum $a \in G$ com ordem infinita, pelo que

$$G = \left\{ \ldots, a^{-2}, a^{-1}, 1_G, a, a^2, a^3, \ldots \right\}.$$

Portanto,

Proposição. Se G é um grupo cíclico infinito, então, $G \cong \mathbb{Z}$.

$\psi : G \longrightarrow \mathbb{Z}$ definida por $\psi(a^p) = p$ é um isomorfismo. (Verifique)

Álgebra - Lic Ciências de Computação

Paula Marques Smith

DMA - UM

24 out'19

O grupo simétrico $\mathcal{S}_n$

Seja A um conjunto não vazio. Uma *permutação* de A é uma aplicação bijectiva de A em A.

Teorema. *O conjunto das permutações de um conjunto X é um grupo para a composição de aplicações.*

Este grupo designa-se por *grupo simétrico sobre A* e representa-se por $\mathcal{S}_A$. Chama-se *grupo de permutações de A* a qualquer subgrupo de $\mathcal{S}_A$.

Para cada $n \in \mathbb{N}$, o grupo simétrico sobre o conjunto $\{p \in \mathbb{N} : p \leq n\}$ designa-se por *grupo simétrico de grau n* e representa-se por $\mathcal{S}_n$.

O grupo simétrico $\mathcal{S}_n$

- Se A é um conjunto finito com n elementos ($n \in \mathbb{N}$), digamos $A = \{a_1, a_2, ..., a_n\}$, podemos estabelecer uma bijecção entre A e o conjunto $\{1, 2, ..., n\}$: $a_i \mapsto i$.

Adoptamos a seguinte notação para qualquer conjunto com n elementos - dizemos, por exemplo, que

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

é uma permutação de um conjunto com 4 elementos.

- Se A é um conjunto finito com n elementos ($n \in \mathbb{N}$), existem exatamente $n!$ permutações de A.

Exemplos

I. O grupo simétrico S_1 é o grupo trivial.

II. Considerando um conjunto com dois elementos,

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\};$$

que é, claramente, um grupo isomorfo a $(\mathbb{Z}_2, +)$. Verifique.

III. Se considerarmos um conjunto com 3 elementos, então

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\theta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \theta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \theta_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

é a lista de todos os elementos de S_3.

O grupo simétrico $\mathcal{S}_n$

A tabela de Cayley de $\mathcal{S}_3$ é

$\circ$	ρ_1	ρ_2	ρ_3	θ_1	θ_2	θ_3
ρ_1	ρ_1	ρ_2	ρ_3	θ_1	θ_2	θ_3
ρ_2	ρ_2	ρ_3	ρ_1	θ_3	θ_1	θ_2
ρ_3	ρ_3	ρ_1	ρ_2	θ_2	θ_3	θ_1
θ_1	θ_1	θ_2	θ_3	ρ_1	ρ_2	ρ_3
θ_2	θ_2	θ_3	θ_1	ρ_3	ρ_1	ρ_2
θ_3	θ_3	θ_1	θ_2	ρ_2	ρ_3	ρ_1

Cap I. Elementos da teoria de grupos

O grupo simétrico $\mathcal{S}_n$

IV. Se considerarmos um conjunto com 4 elementos, então

$$
\begin{aligned}
S_4 \quad = \quad & \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \right. \\
& \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \\
& \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \\
& \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \\
& \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \\
& \left. \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \right\}.
\end{aligned}
$$

Cap I. Elementos da teoria de grupos

O grupo simétrico $\mathcal{S}_n$

Os grupos simétricos S_1 e S_2 são abelianos. No entanto, facilmente que verifica que o grupo simétrico S_3 não é comutativo. De facto,

$$\theta_1\theta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\theta_2\theta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Teorema. Seja $n \in \mathbb{N}$. O grupo simétrico S_n é não comutativo para $n \geq 3$.

Dem. Para $n = 3$ o resultado foi já demonstrado. Sejam $n > 3$ e $\alpha, \beta \in S_n$ definidas por:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix}, \qquad \beta == \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 2 & 1 & 4 & \cdots & n \end{pmatrix}.$$

Então, $\alpha\beta \neq \beta\alpha$ e, portanto, S_n é não comutativo.

Cap I. Elementos da teoria de grupos

Ciclos

Uma permutação σ de um conjunto finito A diz-se um ciclo de comprimento n se existirem

$$a_1, a_2, \ldots, a_n \in A$$

tais que

$$\sigma(a_1) = a_2, \quad \sigma(a_2) = a_3, \ldots, \quad \sigma(a_{n-1}) = a_n, \quad \sigma(a_n) = a_1$$

e se

$$\sigma(x) = x, \qquad \forall x \in A \backslash \{a_1, a_2, ..., a_n\}.$$

Neste caso, representa-se este facto por $\sigma = \begin{pmatrix} a_1 & a_2 & \ldots & a_{n-1} & a_n \end{pmatrix}$.

Exemplo. Tomando $A = \{1, 2, 3, 4, 5\}$, temos que

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 3 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 3 & 5 \end{pmatrix}, \end{aligned}$$

pelo que σ tem cumprimento 4.

Ciclos

O produto de dois ciclos nem sempre é um ciclo. Por exemplo, em S_6,

$$\begin{pmatrix} 1 & 4 & 5 & 6 \end{pmatrix}\begin{pmatrix} 2 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}$$

não é um ciclo.

Dado um conjunto A finito, diz-se que dois ciclos são *disjuntos* se não existir qualquer elemento de A que apareça simultaneamente na notação desses ciclos, i.e., se nenhum elemento de A for movido simultaneamente pelos dois ciclos.

Embora não seja um ciclo, a permutação σ é o produto de (dois) ciclos disjuntos:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1 \quad 6)\,(2 \quad 5 \quad 3)\,.$$

Teorema. Toda a permutação σ de um conjunto finito é um produto de ciclos disjuntos.

Teorema. Dois quaisquer ciclos disjuntos de um conjunto finito comutam.

Dem. Sejam σ e τ ciclos disjuntos de um conjunto finito A e seja $x \in A$. Duas situações podem ocorrer.

- x aparece na notação de σ
  Então x não aparece na notação de τ e $\sigma(x)$ aparece na notação de σ mas não aparece na notação de τ. Deste modo,
  $$\tau(\sigma(x)) = \sigma(x) \qquad \sigma(\tau(x)) = \sigma(x).$$
- x não aparece na notação de σ
  Então $\sigma(x) = x$. Se x aparece na notação de τ, então $\tau(x)$ aparece na notação de τ e não aparece na notação de σ. Portanto,
  $$\tau(\sigma(x)) = \tau(x) \qquad \sigma(\tau(x)) = \tau(x).$$
  Se x não aparece na notação de τ, então $\tau(x) = x$. Portanto,
  $$\sigma(\tau(x)) = \sigma(x) = x = \tau(x) = \tau(\sigma(x)).$$

Cap I. Elementos da teoria de grupos

Ciclos

Proposição. Seja σ uma permutação de um conjunto finito A. Tem-se:

1. se σ é um ciclo, então $\circ(\sigma)$ é igual ao comprimento do ciclo;
2. se σ é um produto de pelo menos dois ciclos **disjuntos**, então $\circ(\sigma)$ é igual ao m.m.c. dos comprimentos dos ciclos envolvidos no referido produto.

Exemplo 1. Em S_8,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 4 & 3 & 7 & 6 & 1 & 8 \end{pmatrix} = (1 \quad 2 \quad 5 \quad 7)\,(3 \quad 4);$$

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 3 & 4 & 1 & 6 & 2 & 8 \end{pmatrix}, \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 1 & 4 & 3 & 2 & 6 & 5 & 8 \end{pmatrix} \text{ e}$$

$\sigma^4 = id$.

Logo, $\circ(\sigma) = 4$.

Ciclos

Exemplo 2. Em S_8,

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 1 & 7 & 8 & 5 & 6 \end{pmatrix} = (1 \quad 3 \quad 4)\,(5 \quad 7)\,(6 \quad 8),$$

temos que $\circ\,(\phi) = 6$.

Exercício Considere, no grupo S_7, as permutações

$$\beta = (1\,3\,2\,4)\,(7\,3\,2) \qquad \text{e} \qquad \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 2 & 3 & 4 & 1 & 7 \end{pmatrix}.$$

1. Exprima β com produto de ciclos disjuntos e calcule β^{40} e β^{-25}.
2. Determine, em extensão, o subgrupo $< \beta^{40} >$.
3. Sem efectuar o produto $\alpha^{-1}\beta^3\alpha$, diga qual é a ordem da permutação $\alpha^{-1}\beta^3\alpha$.

Álgebra - Lic Ciências de Computação

Paula Marques Smith

DMA - UM

31 out'19

O grupo alterno

Chama-se *transposição* a qualquer ciclo de comprimento 2.

Proposição. *Qualquer ciclo de um conjunto finito é produto de transposições.*

Dem. Basta ter em conta que

$$(a_1 \quad a_2 \quad a_3 \quad \cdots \quad a_n) = (a_1 \quad a_n)\,(a_1 \quad a_{n-1}) \cdots (a_1 \quad a_3)\,(a_1 \quad a_2)\,.$$

Qualquer permutação pode ser decomposta no produto de transposições.

$$\begin{aligned}(1 \quad 2 \quad 3 \quad 4 \quad 5) &= (1 \quad 5)\,(1 \quad 4)\,(1 \quad 3)\,(1 \quad 2)\\ &= (4 \quad 5)\,(1 \quad 4)\,(1 \quad 2)\,(3 \quad 5)\,(4 \quad 5)\,(2 \quad 4)\end{aligned}$$

Teorema 1. *Nenhuma permutação de um conjunto finito pode ser expressa simultaneamente como produto de um número par de transposições e como produto de um número ímpar de transposições.*

Cap I. Elementos da teoria de grupos

Uma permutação diz-se *par* se se escreve como o produto de um número par de transposições. Uma permutação diz-se *ímpar* se se escreve como produto de um número ímpar de permutações.

Em S_n (qualquer $n \in \mathbb{N}$), a aplicação identidade é uma permutação par:

$$id = (a_i \quad a_j)\,(a_i \quad a_j)\,,$$

para quaisquer $a_i, a_j \in \{1, 2, ..., n\}$.

Teorema. *Seja $n \in \mathbb{N}$ e $n \geq 2$. O subconjunto das permutações pares de S_n é um subgrupo de S_n de ordem $\frac{n!}{2}$.*

Dem. Seja $A = \{\sigma \in S_n : \sigma \text{ é uma permutação par}\}$. É claro que $A < S_n$.

Sejam $\tau \in S_n$ uma transposição e B o conjunto das permutações ímpares de S_n. A aplicação $\phi_\tau : A \longrightarrow B$ definida por $\phi_\tau(\sigma) = \tau\sigma$ é bijectiva. Assim, $\#\,(A) = \#\,(B)$ e, como $\#\,(A) + \#\,(B) = \#\,(S_n) = n!$, obtemos que $|A| = \frac{n!}{2}$.

Cap I. Elementos da teoria de grupos

Dado um conjunto X com n elementos, chama-se *grupo alterno de* X, e representa-se por $\mathcal{A}_n$, ao subgrupo de S_n constituído pelas permutações pares.

Grupos diedrais

Chama-se *simetria do plano* a toda a transformação do plano que, aplicada a uma qualquer figura do plano, permite obter uma figura que, colocada sobre a figura inicial, com ela coincide.

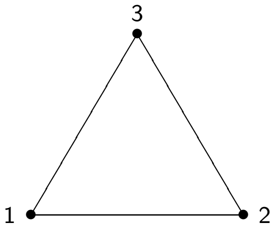
O conjunto das simetrias de um polígono regular de n lados, algebrizado com a composição de simetrias, constitui um grupo. Designa-se por grupo diedral de ordem n e representa-se por $\mathcal{D}_n$.

Estudamos dois grupos diedrais: os grupos $\mathcal{D}_3$ e $\mathcal{D}_4$

Cap I. Elementos da teoria de grupos

Grupos diedrais

O grupo diedral $\mathcal{D}_3$:



As simetrias do triângulo equilátero são:

(i) as rotações de 0^o, 120^o e 240^o, respectivamente,

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ e } \rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix};$$

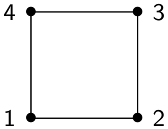
(ii) as simetrias em relação às bissectrizes dos ângulos 1, 2 e 3, respectivamente,

$$\theta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \theta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ e } \theta_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Neste caso, $\mathcal{D}_3 = \mathcal{S}_3$.

Cap I. Elementos da teoria de grupos

O grupo diedral $\mathcal{D}_4$: as simetrias do quadrado são:



(i) as rotações de 0^o, 90^o, 180^o e 270^o, respectivamente:

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \text{ e } \rho_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix};$$

(ii) as simetrias em relação às bissectrizes $[1,3]$ e $[2,4]$, respectivamente:

$$\theta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ e } \theta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix};$$

(iii) as simetrias em relação às mediatrizes do lado $[1,2]$ e do lado $[2,3]$, respectivamente:

$$\theta_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \text{ e } \theta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

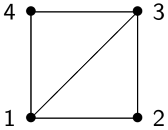
Cap I. Elementos da teoria de grupos

Grupos diedrais

Assim, o grupo $\mathcal{D}_4$ tem apenas 8 dos 24 elementos que $\mathcal{S}_4$ contém. Portanto, $\mathcal{D}_4$ é um subgrupo **próprio** de $\mathcal{S}_4$.

- um grupo de simetrias (não diedral), subgrupo de $\mathcal{D}_4$:

O grupo das simetrias da figura



composto pelas permutações

$$\phi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \phi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

$$\phi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ e } \phi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

o teorema de representação de Cayley

Teorema de representação de Cayley. Todo o grupo é isomorfo a um grupo de permutações.

Dem. Seja G um grupo. Para cada $x \in G$, a aplicação

$$\begin{array}{rcl} \lambda_x : G & \longrightarrow & G \\ a & \longmapsto & \lambda_x(a) = xa, \end{array}$$

é uma permutação em G. (Verifique)

Seja S é o grupo das permutações de G e θ a função

$$\begin{array}{rcl} \theta : G & \longrightarrow & S \\ x & \longmapsto & \lambda_x. \end{array}$$

o teorema de representação de Cayley

Então, para $x, y, g \in G$,

$$(\lambda_x \circ \lambda_y)(g) = \lambda_x(\lambda_y(g)) = \lambda_x(yg) = x(yg) = (xy)g = \lambda_{xy}(g),$$

pelo que

$$\theta(x) \circ \theta(y) = \theta(xy),$$

i.e., θ é um morfismo.

Além disso,

$$x \in \mathrm{Nuc}\,\theta \Leftrightarrow \theta(x) = id_G \Leftrightarrow \lambda_x = id_G \Rightarrow x = \lambda_x(1_G) = id_G(1_G) = 1_G,$$

e, portanto,

$$\mathrm{Nuc}\,\theta = \{1_G\}.$$

Logo, θ é um monomorfismo, pelo que $G \cong \mathrm{Im}\theta < S$.

Exemplo.

Seja $G = \mathbb{Z}_4$. Como para quaisquer $a, x \in \mathbb{Z}_4$, se tem

$$\lambda_a(x) = a + x,$$

temos:

$$\begin{aligned}
\lambda_{\bar{0}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{0} & \bar{1} & \bar{2} & \bar{3} \end{pmatrix} = id \\
\lambda_{\bar{1}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{1} & \bar{2} & \bar{3} & \bar{0} \end{pmatrix} = (\bar{0} \quad \bar{1} \quad \bar{2} \quad \bar{3}) \\
\lambda_{\bar{2}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{2} & \bar{3} & \bar{0} & \bar{1} \end{pmatrix} = (\bar{0} \quad \bar{2})\,(\bar{1} \quad \bar{3}) \\
\lambda_{\bar{3}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{3} & \bar{0} & \bar{1} & \bar{2} \end{pmatrix} = (\bar{0} \quad \bar{3} \quad \bar{2} \quad \bar{1})\,.
\end{aligned}$$

Assim, $\mathbb{Z}_4 \cong \{\lambda_{\bar{0}}, \lambda_{\bar{1}}, \lambda_{\bar{2}}, \lambda_{\bar{3}}\}$.

Álgebra - Lic Ciências de Computação

Paula Marques Smith

DMA - UM

7 nov'19

Cap II. Elementos da teoria de anéis

Generalidades

Seja A um conjunto não vazio e $+$ e $\cdot$ duas operações binárias nele definidas. O triplo $(A, +, \cdot)$ diz-se um *anel* se

1. $(A, +)$ é um grupo comutativo (também designado por *módulo*);
2. $(A, \cdot)$ é um semigrupo;
3. A operação $\cdot$ é *distributiva* em relação à operação $+$, i.e., para quaisquer $a, b, c \in A$,

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{e} \qquad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Referimo-nos à operação $+$ como *adição* e à operação $\cdot$ como *multiplicação*.

Não havendo ambiguidade, falamos no anel A sempre que nos referirmos ao anel $(A, +, \cdot)$ e omitimos o sinal da multiplicação (i.e., para quaisquer $a, b \in A$, ab significará $a \cdot b$).

Cap II. Elementos da teoria de anéis

Generalidades

O elemento identidade do grupo $(A, +)$ designa-se por *zero do anel* e representa-se por 0_A.

Para cada $a \in A$, $-a$ representa o *simétrico de a* no grupo $(A, +)$.

Se a multiplicação for comutativa, o anel A diz-se um *anel comutativo.*

Se a multiplicação admitir elemento identidade, ele designa-se por *a identidade do anel* e representa-se por 1_A. Nesta situação, existirão elementos invertíveis (pelo menos 1_A) e, para cada elemento invertível $a \in A$, a^{-1} representa o inverso de a.

Cap II. Elementos da teoria de anéis

Generalidades

Exemplos:

1. Seja $A = \{a\}$. Então, $(A, +, \cdot)$, onde $a + a = a$ e $a \cdot a = a$, é um anel comutativo com identidade. Designa-se por *anel nulo* e representa-se por $A = \{0_A\}$.

2. $(\mathbb{Z}, +, \times)$ é um anel comutativo com identidade.

3. $(\mathbb{R}, +, \times)$ é um anel comutativo com identidade.

4.$(2\mathbb{Z}, +, \times)$ é um anel comutativo sem identidade.

5. $(\mathcal{M}_2(\mathbb{R}), +, \times)$ é um anel não comutativo com identidade.

6. O conjunto $A = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{R} \right\}$, algebrizado com a adição e multiplicação usuais de matrizes, é um anel não comutativo e sem identidade.

Tarefa Elaborar um diagrama que apresente, de modo fundamentado, a relação entre as classes dos anéis, a dos anéis comutativos e a dos anéis com identidade.

Cap II. Elementos da teoria de anéis

Generalidades

Proposição. Seja A um anel. Então, para todo $x \in A$,

$$0_A\, x = x\, 0_A = 0_A.$$

Dem. Seja $x \in A$. Pela distributividade,

$$0_A\, x + 0_A\, x = (0_A + 0_A)\, x$$

e, então

$$\begin{aligned} 0_A x + 0_A x = (0_A + 0_A)\, x \quad &\Leftrightarrow 0_A x + 0_A x = 0_A x \\ &\Leftrightarrow 0_A x + 0_A x = 0_A x + 0_A \\ &\Leftrightarrow 0_A x = 0_A. \end{aligned}$$

Logo, $0_A x = 0_A$. Analogamente se prova que $x 0_A = 0_A$.

Proposição. Se $A \neq \{0_A\}$ é um anel com identidade, então $1_A \neq 0_A$.

Dem. Se 0_A fosse a identidade do anel, então, para qualquer $x \neq 0_A$ (estes elementos existem porque, por hipótese, o anel A não é nulo), teríamos $x = 0_A\, x$ pelo que, pela proposição anterior, $x = 0_A$, uma contradição. Logo $1_A \neq 0_A$.

Cap II. Elementos da teoria de anéis

Generalidades

Proposição. Sejam A um anel e $x, y \in A$. Então:

(i) $(-x)\,y = x\,(-y) = -(xy)$;

(ii) $(-x)\,(-y) = xy$.

Dem. Exercício

Proposiç ao (*Propriedade distributiva generalizada*). Sejam A um anel, $n \in \mathbb{N}$ e $a, b_1, b_2, ..., b_n \in A$. Então,

(i) $a\,(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n$;

(ii) $(b_1 + b_2 + \cdots + b_n)\,a = b_1a + b_2a + \cdots + b_na$.

Dem. Exercício

Cap II. Elementos da teoria de anéis

Generalidades

Dado um anel $(A, +, \cdot)$, como $(A, +)$ é grupo, temos definido o conceito de *potências de expoente inteiro de* $a \in A$. Na linguagem aditiva, este conceito designa-se por *múltiplo inteiro* n *de* a. **Recordemos** a definição:

(i) $0a = 0_A$;

(ii) $(n+1)\,a = na + a$, para todo $n \in \mathbb{N}_0$;

(iii) $na = -\left((-n)a\right)$, para todo $n \in \mathbb{Z}^-$.

Proposição. Sejam A, um anel, $a, b \in A$ e $m, n \in \mathbb{Z}$. Então,

(i) $(m+n)\,a = ma + na$;

(ii) $n\,(ma) = (nm)\,a$;

(iii) $n\,(a+b) = na + nb$.

Cap II. Elementos da teoria de anéis

Generalidades

Proposição. Sejam A um anel, $a, b \in A$ e $n \in \mathbb{Z}$. Então,

$$n\,(ab) = (na)\,b = a\,(nb)\,.$$

Dem. Há, exatamente, três casos a considerar:

(i) $n = 0$; (trivial)

(ii) $n > 0$; (Método de Indução Matemática - exercício)

(iii) $n < 0$.

$$n\,(ab) = -\left((-n)\,(ab)\right) = -\left[((-n)\,a)\,b\right] = \left[-\left(-\,(na)\right)\right]b = (na)\,b$$

e

$$n\,(ab) = -\left((-n)\,ab\right) = -\left[a\,((-n)\,b)\right] = a\left[-\,(-n)\,b\right] = a\,(nb)\,.$$

Cap II. Elementos da teoria de anéis

Generalidades

Dado um anel $(A, +, \cdot)$, como $(A, \cdot)$ é semigrupo, temos definido o conceito de *potências de expoente natural de* $a \in A$. **Recordemos** a definição:

(i) $a^1 = a$;

(ii) $a^{n+1} = a^n \cdot a$, para todo $n \in \mathbb{N}$.

Proposição. Sejam A um anel, $a \in A$ e $m, n \in \mathbb{N}$. Então,

(i) $(a^n)^m = a^{nm}$;

(ii) $a^n a^m = a^{n+m}$.

Cap II. Elementos da teoria de anéis

Generalidades

Seja A um anel com identidade 1_A. Um elemento $a \in A$ diz-se uma *unidade* se for invertível (i.e., se admitir um inverso em A). O conjunto das unidades de um anel com identidade representa-se por $\mathcal{U}_A$. É claro que, para qualquer anel A com identidade, $\mathcal{U}_A \neq \emptyset$.

1. No anel $(\mathbb{Z}, +, \times)$, $\mathcal{U}_{\mathbb{Z}} = \{-1, 1\}$.
2. No anel $(\mathbb{R}, +, \times)$, $\mathcal{U}_{\mathbb{R}} = \mathbb{R} \setminus \{0\}$.
3. No anel $(\mathcal{M}_2(\mathbb{R}), +, \times)$,

$$\mathcal{U}_{\mathcal{M}_2(\mathbb{R})} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{M}_2(\mathbb{R}) : ad - bc \neq 0 \right\}.$$

Generalidades

Seja A um anel. Um elemento $a \in A$ diz-se *simplificável* se, para quaisquer $x, y \in A$,

$$xa = ya \quad ou \quad ax = ay \Longrightarrow x = y.$$

- Nos anéis $(\mathbb{Z}, +, \times)$ e $(\mathbb{R}, +, \times)$, qualquer elemento não nulo é simplificável.

- No anel $(\mathcal{M}_2(\mathbb{R}), +, \times)$, o elemento $\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}$ não é simplificável:

$$\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ -1 & -2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ -3 & -2 \end{bmatrix}$$

e

$$\begin{bmatrix} 1 & 2 \\ -1 & -2 \end{bmatrix} \neq \begin{bmatrix} 3 & 2 \\ -3 & -2 \end{bmatrix}.$$

Cap II. Elementos da teoria de anéis

Generalidades

Um elemento a de um anel A diz-se um *divisor de zero* se existe $b \in A \setminus \{0_A\}$ tal que

$$ab = 0_A \quad \text{ou} \quad ba = 0_A.$$

Questão O zero de um anel é divisor de zero?

- No anel $(\mathbb{Z}, +, \times)$, o único divisor de zero existente é o elemento 0.

- No anel $(\mathbb{R}, +, \times)$, o único divisor de zero é o elemento 0.

- No anel $(\mathcal{M}_2(\mathbb{R}), +, \times)$, a matriz $\begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix}$ é um divisor de zero, uma vez que

$$\begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} -1 & -1 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Prova-se que qualquer matriz $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ de $\mathcal{M}_2(\mathbb{R})$ tal que $ad - bc = 0$ é divisor de zero.

Generalidades

De facto,

(i) se $a = b = c = d = 0$, para qualquer matriz $M \in \mathcal{M}_2(\mathbb{R})$, temos:

$$M \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix};$$

(ii) se $d \neq 0$ ou $c \neq 0$, temos:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} d & d \\ -c & -c \end{bmatrix} = \begin{bmatrix} ad - bc & ad - bc \\ cd - dc & cd - dc \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix};$$

(iii) se $a \neq 0$ ou $b \neq 0$, temos:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} -b & -b \\ a & a \end{bmatrix} = \begin{bmatrix} -ab + ba & -ab + ba \\ -cb + da & -cb + da \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Cap II. Elementos da teoria de anéis

Generalidades

Um anel comutativo com identidade A diz-se um *domínio* (ou *anel*) *de integridade* se o elemento zero do anel for o único divisor de zero de A.

- Os anéis $(\mathbb{Z}, +, \times)$ e $(\mathbb{R}, +, \times)$ são domínios de integridade.

- O anel das matrizes quadradas de ordem 2 não é um domínio de integridade.

- O anel $(\mathbb{Z}_3, +, \times)$ é domínio de integridade e o anel $(\mathbb{Z}_8, +, \times)$ não é domínio de integridade.

Obs. Se A é um domínio de integridade, então, $A \neq \{0_A\}$.

Exercício 1. Seja A um anel comutativo com identidade. Então A é domínio de integridade se e só se $A \setminus \{0_A\} \neq \emptyset$ e todo o elemento de $A \setminus \{0_A\}$ é simplificável.

Exercício 2. Seja A um anel comutativo com identidade. Então A é domínio de integridade se e só se $A \setminus \{0_A\} \neq \emptyset$ e $A \setminus \{0_A\}$ é subsemigrupo de A relativamente à multiplicação.

Cap II. Elementos da teoria de anéis

Generalidades

Um anel A diz-se um *anel de divisão* se $(A\setminus\{0_A\},\cdot)$ é um grupo. Um anel de divisão comutativo diz-se um *corpo*.

Resulta da definição que qualquer corpo é um domínio de integridade. No entanto, nem todos os domínios de integridade são corpos. Analisemos o seguinte exemplo.

- O domínio de integridade $(\mathbb{Z},+,\times)$ não é um anel de divisão, uma vez que $(\mathbb{Z}\setminus\{0\},\times)$ não é grupo.

- O domínio de integridade $(\mathbb{R},+,\times)$ é um corpo e, portanto, um anel de divisão.

- O anel $(\mathbb{Z}_6,+,\times)$ não é um anel de divisão, uma vez que $[2]_6$ não é invertível.

Questão para que valores de n é o anel $(\mathbb{Z}_n,+,\times)$

(i) domínio de integridade?

(ii) anel de divisão?

Cap II. Elementos da teoria de anéis

Generalidades

- Seja $\mathcal{Q} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$, onde $i^2 = j^2 = k^2 = -1$, $ij = -ji = k, ki = -ik = j, jk = -kj = i$. Considere em $\mathcal{Q}$ as operações de adição e de multiplicação definidas por

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = a + a' + (b + b')i + (c + c')j + (d + d')k$$

e

$$\begin{aligned}(a + bi + cj + dk) \times (a' + b'i + c'j + d'k) = \\ aa' - bb' - cc' - dd' + (ab' + a'b + cd' - c'd)i + \\ (ac' - bd' + a'c + b'd)j + (ad' + bc' - b'c + a'd)k,\end{aligned}$$

onde as somas dos elementos $a, a', b, b', c, c', d, d'$ são efectuadas em $\mathbb{R}$.
O triplo $(\mathcal{Q}, +, \times)$ é um anel de divisão não comutativo. Este anel designa-se por *Anel dos Quarteniões.*

Tarefa Completar o diagrama elaborado no início do capítulo de modo a incluir a classes dos domínios de integridade e a dos corpos.

Álgebra - Lic Ciências de Computação

Paula Marques Smith

DMA - UM

8 nov'19

Cap II. Elementos da teoria de anéis

Caraterística de um anel

Seja A um anel. Considerando os múltiplos de elementos de A, duas situações podem ocorrer:

(i) $(\exists m \in \mathbb{Z}\setminus \{0\})\ (\forall a \in A) \quad ma = 0_A$;

(ii) $(\forall m \in \mathbb{Z}\setminus \{0\})\,(\exists b \in A) \quad mb \neq 0_A \quad$ (i.e., $(\forall b \in A)\ nb = 0_A \implies n = 0$).

- É exemplo da situação (i) o anel $(\mathbb{Z}_4, +, \cdot)$:

$$4[0]_4 = [0]_4; 4[1]_4 = [0]_4; 4[2]_4 = [0]_4; 4[3]_4 = [0]_4.$$

- São exemplos da situação (ii) o anel dos números reais e o anel dos números inteiros.

Caraterística de um anel

Seja A um anel.

1. Diz-se que o anel A tem *caraterística* 0, e escreve-se $c(A)=0$, se
$$(\forall b \in A \;\; nb = 0_A) \Rightarrow n = 0;$$
2. Diz-se que o anel A tem *caraterística* q, $q \in \mathbb{N}$, e escreve-se $c(A)=q$, se
$$(\exists m \in \mathbb{Z} \setminus \{0\}): \;\; (\forall a \in A) \;\; ma = 0_A$$
e $q = \min\{n \in \mathbb{N} : na = 0_A \;\forall a \in A\}$.

Questão No ponto 2 da definição anterior, por que é que podemos falar no elemento $\min\{n \in \mathbb{N} : na = 0_A \;\forall a \in A\}$?

Cap II. Elementos da teoria de anéis

Caraterística de um anel

Sejam A um anel e $a \in A$. Como $(A, +)$ é um grupo, temos definido o conceito de ordem do elemento a. Recordemos:

- a tem *ordem infinita* se $pa \neq 0_A$, para todo o $p \in \mathbb{N}$;

- a tem *ordem finita* $p \in \mathbb{N}$ se p é o menor natural tal que $pa = 0_A (= 1_{(A,+)}$.

Assim, se A tem caraterística $q \in \mathbb{N}$, então, cada $x \in A$ tem ordem finita, digamos p, e p é um divisor de q. Deste modo, a caraterística $q \in \mathbb{N}$ de A é o m.m.c. das ordens de todos os elementos de A.

Se o anel A tiver identidade, então a caraterística de A é determinada pela ordem de 1_A:

Proposição. Sejam $A \neq \{0_A\}$ um anel com identidade 1_A e $n \in \mathbb{N}$. Então, $c(A) = n$ se e só se a ordem de 1_A é n.

Caraterística de um anel

Demonstração ($\Rightarrow$) Por hipótese, temos que $c(A) = n$, i.e., temos que:

(i) $\forall a \in A \quad na = 0_A$;

(ii) $(\exists p \in \mathbb{N} : \quad \forall a \in A \quad pa = 0_A) \Longrightarrow n \mid p$.

Queremos provar que $o(1_A) = n$, i.e., queremos provar que:

(a) $n1_A = 0_A$;

(b) $(\exists p \in \mathbb{N} : p1_A = 0_A) \Longrightarrow n \mid p$.

Claramente, (a) resulta de (i). Provemos (b): suponhamos que existe $p \in \mathbb{N}$ tal que $p1_A = 0_A$. Então, para qualquer $a \in A$, temos:

$$pa = p(1_A a) = (p1_A)a = 0_A a = 0_A.$$

Assim, por (ii), obtemos $n \mid p$. Logo, (b) verifica-se.

Caraterística de um anel

($\Leftarrow$) Suponhamos agora que $o(1_A) = n$. Queremos provar que o anel satisfaz (i) e (ii):

(i) Para todo $a \in A$, temos que

$$na = n(1_A a) = (n1_A)a = 0_A a = 0_A.$$

(ii) Seja $p \in \mathbb{N}$ tal que, para todo $a \in A$, $pa = 0_A$. Em particular, como $1_A \in A$, temos que $p1_A = 0_A$. Então, por (b), concluimos que $n \mid p$.

Exemplo 1. Seja $n \in \mathbb{N}$. Como, em $\mathbb{Z}_n$, $o([1]_n) = n$, concluimos que $c(\mathbb{Z}_n) = n$.

Exemplo 2. O anel dos números inteiros e o anel dos números reais são anéis de caraterística 0.

Álgebra - Lic Ciências de Computação

Paula Marques Smith

DMA - UM

14 e 15 nov'19

Cap II. Elementos da teoria de anéis

Subanéis

Seja A um anel. Um subconjunto B de A diz-se um *subanel de A* se:

1. $0_A \in B$;
2. $(\forall x, y \in A) \quad x, y \in B \Longrightarrow x - y \in B$;
3. $(\forall x, y \in A) \quad x, y \in B \Longrightarrow x\,y \in B$.

Obs. Repare-se que a conjunção de (1) e (2) é equivalente à afirmação de que $(B, +)$ é um subgrupo de $(A, +)$ e que (3) é equivalente à afirmação de que $(B, \cdot)$ é um subsemigrupo de $(A, \cdot)$

Um subanel A' de um domínio de integridade (respectivamente, anel de divisão, corpo) A diz-se um *subdomínio de integridade (respectivamente, subanel de divisão, subcorpo) de A* se for um domínio de integridade (respectivamente, anel de divisão, corpo) relativamente às restrições das operações de adição e multiplicação de A a A'.

Cap II. Elementos da teoria de anéis

ideais e relações de congruência num anel

Seja A um anel. Um subconjunto I de A diz-se um *ideal direito* (respectivamente, *ideal esquerdo*) de A se:

(i) $(I, +) < (A, +)$;

(ii) $(\forall a \in A)\ (\forall x \in I) \quad xa \in I$ (respectivamente, $ax \in I$)

Se I for simultaneamente ideal esquerdo de A e ideal direito de A, então, I diz-se um *ideal de A*.

Exemplo 1. O subconjunto $2\mathbb{Z}$ do anel $(\mathbb{Z}, +, \times)$ é um ideal pois $(2\mathbb{Z}, +) < (\mathbb{Z}, +)$ e o produto de um inteiro qualquer por um inteiro par é um inteiro par.

Exemplo 2. O subconjunto $\{\bar{0}, \bar{2}\}$ do anel $(\mathbb{Z}_4, +, \cdot)$, é um ideal pois

$$(\{\bar{0}, \bar{2}\}, +) < (\mathbb{Z}_4, +) \quad \text{e}$$

$$\begin{array}{l} \bar{0} \cdot \bar{0} = \bar{0} \cdot \bar{1} = \bar{0} \cdot \bar{2} = \bar{0} \cdot \bar{3} = \bar{0} \in \{\bar{0}, \bar{2}\} \\ \bar{2} \cdot \bar{0} = \bar{2} \cdot \bar{2} = \bar{0} \in \{\bar{0}, \bar{2}\} \quad e \quad \bar{2} \cdot \bar{1} = \bar{2} \cdot \bar{3} = \bar{2} \in \{\bar{0}, \bar{2}\}. \end{array}$$

Como o anel em questão é comutativo, concluimos que $\{\bar{0}, \bar{2}\}$ é um ideal de $\mathbb{Z}_4$.

ideais e relações de congruência num anel

Exemplo 3. Seja A um anel. Então, $\{0_A\}$ é um ideal de A. Designa-se por *ideal trivial de A*.

Exemplo 4. Um anel A é um ideal de si próprio. Este ideal designa-se por *ideal impróprio de A*.

Proposição. Todo o ideal de um anel A é um subanel de A.

Dem. Exercício.

Questão Analisar a veracidade do recíproco da proposição anterior.

Proposição. A intersecção de uma família de ideais de um anel A é um ideal de A.

Dem. Exercício.

Cap II. Elementos da teoria de anéis

ideais e relações de congruência num anel

Proposição. Num anel A, com identidade, todo o ideal que contém 1_A é impróprio.

Dem. Sejam A um anel com identidade 1_A e I um ideal de A tal que $1_A \in I$. Então,

$$\forall a \in A, \qquad a = a \cdot 1_A \in I.$$

Logo, $A \subseteq I$. Como, por definição, $I \subseteq A$, segue-se que $I = A$.

Proposição. Num anel de divisão existem apenas dois ideais: o trivial e o impróprio.

Dem.

- ★ $\{0_A\}$ e A são ideais de qualquer anel A.
- ★ A anel de divisão e $I \neq \{0_A\}$ um ideal de A.

Então, existe $x \in A \setminus \{0_A\}$ tal que $x \in I$. Como $(A \setminus \{0_A\}, \cdot)$ é um grupo, temos que $x^{-1} \in A \setminus \{0_A\} \subseteq A$ e como I é um ideal de A, segue-se que $xx^{-1} \in I$, i.e., $1_A \in I$. Logo $I = A$.

ideais e relações de congruência num anel

Sejam A um anel e $a \in A$. A interseção de todos os ideais direitos de A que contêm a é o menor ideal direito de A que contém a (Verifique). Este ideal designa-se por *ideal principal direito gerado por a* e representa-se por $(a)_d$.

Analogamente, se definem:

- o *ideal principal esquerdo gerado por a*, que se representa por $(a)_e$: o menor ideal esquerdo de A que contém a;

- o *ideal principal gerado por a*, que se representa por (a): o menor ideal de A que contém a.

ideais e relações de congruência num anel

Exemplo. Consideremos o anel $\mathbb{Z}_4$. Como o anel é comutativo, todos os ideais esquerdos são ideais direitos e vice-versa, pelo que podemos falar simplesmente em ideais. Os ideais de $\mathbb{Z}_4$ são:

$$(\bar{0}) = \{\bar{0}\}$$

$$(\bar{2}) = \{\bar{0}, \bar{2}\}$$

$$(\bar{1}) = \mathbb{Z}_4 = (\bar{3})$$

Proposição. Sejam A um anel com identidade e $b \in A$. Então, $(b)_d = bA$ e $(b)_e = Ab$.

Dem. Exercício. (Para mostrar que $(b)_d = bA$, terá que ter em conta que $bA = \{bx : x \in A\}$ e provar que bA é o menor ideal direito de A que contém b. Analogamente para mostrar que $(b)_e = Ab$).

Corolário: Sejam A um anel comutativo com identidade e $b \in A$. Então, $(b) = Ab = bA$.

Cap II. Elementos da teoria de anéis

ideais e relações de congruência num anel

Seja A um anel. Uma relação de equivalência ρ definida em A diz-se uma *relação de congruência* se, para quaisquer $x, x', y, y' \in A$,

$$x \,\rho\, x' \quad \text{e} \quad y \,\rho\, y' \Longrightarrow (x+y)\ \rho\ \left(x'+y'\right) \quad \text{e} \quad (xy)\ \rho\ \left(x'y'\right).$$

Exemplo: Consideremos, no anel $\mathbb{Z}$, a relação

$$a \,\rho\, b \Longleftrightarrow a-b \in 2\mathbb{Z}.$$

A relação ρ é de equivalência e é tal que

$$\begin{aligned}
a \,\rho\, b \quad \text{e} \quad a' \,\rho\, b' \quad & \Longleftrightarrow \quad a-b,\ a'-b' \in 2\mathbb{Z} \\
& \Longrightarrow \quad a+a'-\left(b+b'\right) \in 2\mathbb{Z} \quad \text{e} \\
& \qquad\ \ aa'-bb' = aa'-ba'+ba'-bb' = (a-b)\,a'+b\left(a'-b'\right) \in 2\mathbb{Z} \\
& \Longleftrightarrow \quad \left(a+a'\right)\ \rho\ \left(b+b'\right) \quad \text{e} \quad aa' \,\rho\, bb',
\end{aligned}$$

Portanto, ρ é uma relação de congruência no anel dos inteiros.

ideais e relações de congruência num anel

A proposição seguinte generaliza o exemplo anterior e mostra que, em qualquer anel A, cada ideal de A determina uma relação de congruência em A.

Proposição. Sejam A um anel e I um ideal de A. Então, a relação definida em A por

$$a \, \rho_I \, b \Longleftrightarrow a - b \in I$$

é uma relação de congruência.

Dem. Exercício.

Mostramos, de seguida, que, em qualquer anel A, a cada relação de congruência definida em A corresponde um ideal de A.

Proposição. Seja ρ uma relação de congruência definida num anel A. Então:

(i) a classe $[0_A]_\rho$ é um ideal de A;
(ii) $a \, \rho \, b \Longleftrightarrow a - b \in [0_A]_\rho$, i.e., $\rho = \rho_I$, para $I = [0_A]_\rho$;
(iii) $(\forall a \in A) \quad [a]_\rho = a + [0_A]_\rho \, (= \{a + x \in A \mid x \, \rho \, 0_A\})$.

Cap II. Elementos da teoria de anéis

anel quociente

Seja ρ uma relação de congruência num anel A. Sendo uma relação de equivalência, podemos falar no conjunto quociente determinado por ρ:

$$A/\rho = \left\{ [a]_\rho \mid a \in A \right\}.$$

Consideremos as seguintes igualdades para quaisquer $a, b \in A$:

$$\text{(i)} \quad [a]_\rho + [b]_\rho = [a+b]_\rho \,;$$

$$\text{(ii)} \quad [a]_\rho \, [b]_\rho = [ab]_\rho \,.$$

e mostremos que elas definem duas operações binárias, não dependendo, por isso, da escolha do representante de cada uma das classes.

Cap II. Elementos da teoria de anéis

anel quociente

Se $[a]_\rho = [a']_\rho$ e $[b]_\rho = [b']_\rho$, temos que

$$a\,\rho\,a' \text{ e } b\,\rho\,b',$$

pelo que

$$(a+b)\,\rho\,(a'+b') \quad \text{e} \quad (ab)\,\rho\,(a'b')$$

e, portanto

$$[a]_\rho + [b]_\rho = [a+b]_\rho = [a'+b']_\rho = [a']_\rho + [b']_\rho$$

e

$$[a]_\rho\,[b]_\rho = [ab]_\rho = [a'b']_\rho = [a']_\rho\,[b']_\rho\,.$$

Teorema. Sejam A um anel e ρ uma relação de congruência definida em A. Então, para a adição e multiplicação definidas por

$$[a]_\rho + [b]_\rho = [a+b]_\rho \quad \text{e} \quad [a]_\rho\,[b]_\rho = [ab]_\rho\,,$$

$(A/\rho, +, \cdot)$ é um anel.

anel quociente

Dado que qualquer relação de congruência ρ em A é do tipo ρ_I, para certo ideal I de A, representaremos o anel quociente $(A/\rho, +, \cdot)$ por $(A/I, +, \cdot)$. Tendo em conta que $I = [0_A]_\rho$, temos que $[x]_{\rho_I} = x + I$ (verifique), pelo que

$$A/I = \{x + I : x \in A\}$$

e

$$y \in x + I \iff y - x \in I.$$

As operações definidas em A/I são dadas por

$$(x + I) + (y + I) = (x + y) + I$$

e

$$(x + I)\,(y + I) = xy + I,$$

para quaisquer $x, y \in A$.

Álgebra - Lic Ciências de Computação

Paula Marques Smith

DMA - UM

22 nov'19

ideais primos e ideais maximais

Seja A um anel comutativo com identidade. Um ideal I de A diz-se *maximal* se $I \neq A$ e não existir um ideal K de A tal que

$$I \subsetneqq K \subsetneqq A.$$

Exemplo. O ideal $2\mathbb{Z}$ do anel $\mathbb{Z}$ é maximal. O ideal $4\mathbb{Z}$ não é maximal pois

$$4\mathbb{Z} \subsetneqq 2\mathbb{Z} \subsetneqq \mathbb{Z}.$$

Seja A um anel comutativo com identidade. Um ideal I de A diz-se *primo* se $A \backslash I \neq \emptyset$ e, para cada $x, y \in A \backslash I$, $xy \in A \backslash I$.

Exemplo. O ideal $2\mathbb{Z}$ do anel $\mathbb{Z}$ é primo: $\mathbb{Z} \backslash 2\mathbb{Z} = 2\mathbb{Z} + 1 \neq \emptyset$ e

$$(2n+1)(2m+1) = 2(n+m+2nm) + 1,$$

para quaisquer $n, m \in \mathbb{Z}$.

Cap II. Elementos da teoria de anéis

ideais primos e ideais maximais

Sejam A um anel comutativo com identidade e I um ideal de A. Então, as seguintes afirmações são equivalentes :

1. (i) I é maximal;
2. ii) A/I é corpo.

Dem. $[(i) \Rightarrow (ii)]$

Como A é um anel comutativo com identidade, temos que A/I é um anel comutativo com identidade. Mostramos agora que todo o elemento não nulo $x + I \in A/I$ admite um inverso.

Seja $a + I \in A/I$ tal que $a + I \neq I$. Então,

$$K = \{i + xa \in A \mid i \in I \text{ e } x \in A\}$$

é um ideal de A. (Verifique). O ideal K é tal que

$$I \subsetneq K :$$

$$i \in I \Rightarrow i = i + 0_A a \Rightarrow i \in K, \qquad a = 0_A + 1_A a \in K \ \text{ e } \ a \notin I.$$

ideais primos e ideais maximais

Como I é um ideal maximal, obtemos $K = A$. Então, $1_A \in K$, i.e., existem $i_1 \in I$ e $x_1 \in A$ tais que

$$1_A = i_1 + x_1 a,$$

ou seja

$$1_A - x_1 a = i_1 \in I.$$

Logo,

$$(1_A - x_1 a) + I = I.$$

Temos:

$$(1_A - x_1 a) + I = I \Longleftrightarrow x_1 a + I = 1_A + I \Longleftrightarrow (x_1 + I)\,(a + I) = 1_A + I.$$

Portanto, $a + I$ é invertível e

$$(a + I)^{-1} = x_1 + I.$$

ideais primos e ideais maximais

$[(ii) \Rightarrow (i)]$

Seja agora I um ideal de A tal que A/I é um corpo.

Suponhamos que existe um ideal K de A, tal que $I \subsetneq K \subseteq A$. De $I \subsetneq K$, obtemos

$$(\exists x \in K) \qquad x \notin I.$$

Logo, $x + I \neq I$. Como A/I é corpo,

$$\begin{aligned}
x + I \neq I \quad & \Longrightarrow \quad \big(\exists x' + I \in (A/I) \setminus \{I\}\big) \quad (x+I)\left(x'+I\right) = 1_A + I \\
& \Longrightarrow \quad \big(\exists x' \in A \backslash I\big) \quad xx' + I = 1_A + I \\
& \Longrightarrow \quad \big(\exists x' \in A \backslash I\big) \quad xx' - 1_A = i \in I \\
& \Longrightarrow \quad \big(\exists x' \in A\big) \quad 1_A = xx' - i, \quad \text{com } i, x \in K, \\
& \Longrightarrow \quad 1_A \in K.
\end{aligned}$$

Assim, $K = A$ e, portanto, I é maximal.

Exemplo. Considerando o anel $\mathbb{Z}$, sabemos $\mathbb{Z}_p$ é corpo se e só se p for primo. Portanto, um ideal de $\mathbb{Z}$ é maximal se e só se é do tipo $p\mathbb{Z}$, com p primo.

Teorema. Sejam A um anel comutativo com identidade e I um ideal de A. Então, as seguintes afirmações são equivalentes :

1. (i) I é ideal primo;
2. (ii) A/I é um domínio de integridade.

Dem. $[(ii) \Rightarrow (i)]$

Sejam A um anel e I um ideal de A tais que A/I é um domínio de integridade. Então, $A/I \neq \{I\}$ e, portanto, $A \neq I$ isto é $A \backslash I \neq \emptyset$.

Sejam $a, b \in A \backslash I$. Pretendemos provar que $ab \in A \backslash I$. Suponhamos que $ab \in I$. Então, $ab + I = I$. Logo,

$$(a + I)(b + I) = I \Longrightarrow a + I = I \text{ ou } b + I = I,$$

o que contradiz a hipótese de se ter $a, b \in A \backslash I$.

ideais primos e ideais maximais

$[(i) \Rightarrow (ii)]$

Como A é um anel comutativo com identidade, A/I é também um anel comutativo com identidade e, como I é primo, $A \backslash I \neq \emptyset$. Portanto, $A/I \neq \{I\}$. Mostramos que I é o único divisor de zero de A/I, i.e., que

$$(x+I)\,(y+I) = I \Longrightarrow x+I = I \text{ ou } y+I = I.$$

Temos:

$$\begin{aligned}
(x+I)\,(y+I) = I \quad &\Longleftrightarrow \quad xy + I = I \\
&\Longleftrightarrow \quad xy \in I \\
&\Longrightarrow \quad x \in I \text{ ou } y \in I \qquad (I \text{ ideal primo}) \\
&\Longleftrightarrow \quad x+I = I \text{ ou } y+I = I.
\end{aligned}$$

ideais primos e ideais maximais

Corolário: Qualquer anel maximal de um anel comutativo com identidade é ideal primo.

Dem. A demonstração é trivial, tendo em conta que todo o corpo é um domínio de integridade. Assim,

$$I \text{ ideal maximal} \Longleftrightarrow A/I \text{ corpo} \Longrightarrow A/I \text{ domínio de integridade} \Longleftrightarrow I \text{ ideal primo.}$$

O recíproco do Corolário anterior é falso. Porquê?

Cap II. Elementos da teoria de anéis

morfismos

Sejam A e A' dois anéis. Uma aplicação $\varphi : A \to A'$ diz-se um *morfismo* (ou *homomorfismode anéis*) se satisfaz:

(i) $(\forall a, b \in A) \qquad \varphi(a+b) = \varphi(a) + \varphi(b)$;

(ii) $(\forall a, b \in A) \qquad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Um morfismo diz-se um *monomorfismo* (respectivamente, *epimorfismo, isomorfismo*) se for injetivo (respectivamente, sobrejetivo, bijetivo)

Um morfismo diz-se um *endomorfismo* se $A = A'$. Um endomorfismo bijetivo diz-se um *automorfismo.*

Exemplo1. Sejam A e A' anéis. A aplicação $\varphi_0 : A \to A'$, definida por $\varphi_0(x) = 0_{A'}$, para todo $x \in A$, é um morfismo. Designa-se por *morfismo nulo.*

Exemplo 2. Seja A um anel. Então, a aplicação identidade em A é um automorfismo. Designa-se por *morfismo identidade.*

morfismos

Proposição. Sejam A e A' dois anéis e $\varphi : A \rightarrow A'$ um morfismo de anéis. Então:

(i) $\varphi(0_A) = 0_{A'}$;

(ii) $(\forall a \in A) \quad \varphi(-a) = -\varphi(a)$;

(iii) $(\forall a \in A)(\forall k \in \mathbb{Z}) \quad \varphi(ka) = k\varphi(a)$.

Dem. Exercício

Proposição. Sejam $\varphi : A \rightarrow A'$ um morfismo de anéis e B um subanel de A. Então, $\varphi(B)$ é um subanel de A'.

Dem. Exercício

Proposição. Sejam $\varphi : A \rightarrow A'$ um epimorfismo de anéis e I um ideal de A. Então, $\varphi(I)$ é um ideal de A'.

Dem. Exercício

morfismos

Proposição. Sejam $\varphi : A \to A'$ um morfismo de anéis e B' um subanel de A'. Então,

$$\varphi^{\leftarrow}(B') = \{x \in A \mid \varphi(x) \in B'\}$$

é um subanel de A.

Dem. Exercício

Proposição. Sejam $\varphi : A \to A'$ um morfismo de anéis e I' um ideal de A'. Então,

$$\varphi^{\leftarrow}(I') = \{x \in A \mid \varphi(x) \in I'\}$$

é um ideal de A.

Dem. Exercício

morfismos

Seja $\varphi : A \to A'$ um morfismo de anéis.

(i) Chama-se *Núcleo de* φ (ou *kernel de* φ), e representa-se por $\mathrm{Nuc}\,\varphi$ (ou $\mathrm{Ker}\,\varphi$), ao subconjunto de A definido por

$$\mathrm{Nuc}\,\varphi = \{x \in A : \varphi(x) = 0_{A'}\};$$

(ii) Chama-se *imagem de* φ, e representa-se por $\mathrm{Im}\,\varphi$ ou $\varphi(A)$, ao subconjunto de A' definido por

$$\mathrm{Im}\,\varphi = \{\varphi(x) : x \in A\}.$$

Proposição. Seja $\varphi : A \to A'$ um morfismo de anéis. Então,

(i) $\mathrm{Nuc}\,\varphi$ é um ideal de A;

(ii) $\mathrm{Im}\,\varphi$ é um subanel de A'.

Dem. Exercício

o teorema fundamental do homomorfismo

Proposição. Sejam A um anel e I um ideal de A. Então, a aplicação $\pi : A \to A/I$ definida por $\pi(x) = x + I \ (x \in A)$, é um epimorfismo. Designa-se por *epimorfismo canónico*.

Teorema fundamental do homomorfismo Seja $\varphi : A \to A'$ um morfismo de anéis. Então, existe um ideal I de A tal que

$$A/I \cong \varphi(A).$$

Dem (linhas gerais). Comece por considerar o ideal $\mathrm{Nuc}\,\varphi$ de A e o epimorfismo canónico $\pi : A \to A/\mathrm{Nuc}\,\varphi$.

Mostre que a correspondência que a cada elemento $x + \mathrm{Nuc}\,\varphi$ de $A/\mathrm{Nuc}\,\varphi$ faz corresponder o elemento $\varphi(x)$ de A' é um monomorfismo.

Conclua que

$$A/\mathrm{Nuc}\,\varphi \cong \varphi(A).$$

Álgebra - Lic Ciências de Computação

Paula Marques Smith

DMA - UM

28 nov'19

Divisibilidade

Conceitos básicos

D: domínio de integridade (anel comutativo com identidade no qual 0_D é o único divisor de zero)

Como 0_D é divisor de zero, $D \neq \{0_D\}$ e, portanto, $1_D \neq 0_D$.

$\mathcal{U}_D$: grupo das unidades de D (o grupo dos elementos $u \in D$ para os quais existe $u^{-1} \in D$)

Divisibilidade

Exemplo. Consideremos o domínio de integridade $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$, onde as operações são definidas por: para todos $a, b, c, d \in \mathbb{Z}$,

$$(a + b\sqrt{-3}) + (c + d\sqrt{-3}) = (a + c) + (b + d)\sqrt{-3},$$

$$(a + b\sqrt{-3})(c + d\sqrt{-3}) = (ac - 3bd) + (ad + bc)\sqrt{-3}.$$

$\mathcal{U}_{\mathbb{Z}[\sqrt{-3}]} = \mathcal{U}_{\mathbb{Z}}$. De facto, suponhamos que

$$(a + b\sqrt{-3})(c + d\sqrt{-3}) = 1. \qquad (i)$$

Sendo dois números complexos iguais, os quadrados dos seus módulos também são iguais . Assim,

$$(a^2 + 3b^2)(c^2 + 3d^2) = 1.$$

Como $a, b, c, d \in \mathbb{Z}$, segue-se que $a = \pm 1$, $c = \pm 1$ e $b = d = 0$. Substituindo em (i), obtemos $a = c = \pm 1$ e $b = d = 0$. Logo,

$$\mathcal{U}_{\mathbb{Z}[\sqrt{-3}]} = \{1, -1\} = \mathcal{U}_{\mathbb{Z}}.$$

Divisibilidade

Definição Dados $x, y \in D$, diz-se que x *divide* y (ou que x *é factor de* y ou que y *é divisível por* x), e escreve-se $x \mid y$, se

$$\exists q \in D: \ \ y = qx.$$

Neste caso, diz-se também que qx é uma *factorização* (ou *decomposição em factores*) *de* y.

Exemplo. Em $\mathbb{Z}$, temos que $-2 \mid 4$, mas $2 \nmid 3$.

Como consequência da definição, provam-se algumas propriedades básicas que passamos a referir.

Proposição Sejam $x, y \in D$. Então,

(i) $x \mid 0_D$;

(ii) $1_D \mid x$;

(iii) $\forall u \in \mathcal{U}_D \quad u \mid x$;

(iv) $x \mid y$ e $y \mid x$ se e só se $y = ux$ para algum $u \in \mathcal{U}_D$ (e, consequentemente, $x = u^{-1}y$).

Divisibilidade

Proposição Sejam D um domínio de integridade, $a, b, c, d \in D$ e $u, u' \in \mathcal{U}_D$. Então,

(i) $a \mid b \Longrightarrow a \mid bc$;

(ii) $a \mid b \Longleftrightarrow au \mid b$;

(iii) $a \mid b \Longleftrightarrow au \mid bu'$;

(iv) $a \mid b,\ c \mid d \Longrightarrow ac \mid bd$;

(v) $a \mid b,\ a \mid c \Longrightarrow a \mid (b + c)$;

(vi) $a \mid b,\ b \mid c \Longrightarrow a \mid c$.

Definição Dois elementos x e y de um domínio de integridade D dizem-se *associados* se $x \mid y$ e $y \mid x$.

Proposição Sejam $x, y \in D$. Então, as seguintes afirmações são equivalentes:

(i) x e y são associados;

(ii) $x \in y\mathcal{U}_D$;

(iii) $y \in x\mathcal{U}_D$.

Divisibilidade

Definição Um elemento $p \in D$ diz-se *irredutível em D* se satisfizer

(i) $p \neq 0_D$ e $p \notin \mathcal{U}_D$ e

(ii) $p = ab \Longrightarrow a \in \mathcal{U}_D$ *ou* $b \in \mathcal{U}_D$.

Exemplo. Em $\mathbb{Z}$, os elementos irredutíveis são os números primos e os seus simétricos.

Definição Um elemento $p \in D$ diz-se *primo* se satisfizer

(i) $p \neq 0_D$ e $p \notin \mathcal{U}_D$ e

(ii) $p \mid ab \Longrightarrow p \mid a$ *ou* $p \mid b$.

Proposição Seja p um elemento não nulo de D. Então,

(i) p é primo se e só se (p) é ideal primo de D;

(ii) p é irredutível se e só se (p) é ideal maximal na classe dos ideais principais de D.

Divisibilidade

Demonstração.

Como D é um anel comutativo com identidade, temos que $(p) = pD$.

(i) Suponhamos que p é primo.

- Então $p \notin \mathcal{U}_D$, pelo que $1_D \notin pD$ e, portanto, $D \backslash (p) \neq \emptyset$.
- Sejam $a, b \in D$ tais que $ab \in pD$. Então, $p \mid ab$. Como p é primo, segue-se que $p \mid a$ ou $p \mid b$ e, portanto, $a \in pD$ ou $b \in pD$. Logo, pD é ideal primo de D.

Reciprocamente, suponhamos que o ideal $(p) = pD$ é primo.

- Então, $pD \neq D$, pelo que $1_D \notin pD$ e, portanto, p não é unidade de D.
- Sejam $a, b \in D$ tais que $p \mid ab$. Então, $ab \in (p)$. Como (p) é ideal primo, concluimos que $a \in (p)$ ou $b \in (p)$. Assim, $p \mid a$ ou $p \mid b$. Portanto, p é primo.

(ii) Exercício

Divisibilidade

Proposição Todo o elemento primo de D é um elemento irredutível.

Demonstração.

Sejam p um elemento primo e $a, b \in D$ tais que $p = ab$. Então, $p \notin \mathcal{U}_D \cup \{0_D\}$ é tal que $p \mid ab$ e, portanto, $p \mid a$ ou $p \mid b$. Se $p \mid a$, temos que $a = px$, para algum $x \in D$. Logo,

$$p = ab = pxb.$$

Assim, pela lei de corte,

$$1_D = xb,$$

pelo que $b \in \mathcal{U}_D$.

Analogamente, supondo que $p \mid b$, obtemos $a \in \mathcal{U}_D$. Logo, p é irredutível

O exemplo que se segue mostra que o recíproco desta proposição não é verdadeiro.

Divisibilidade

Exemplo. Consideremos o domínio de integridade $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$.

O elemento $x = 1 + \sqrt{-3}$ é irredutível, mas não é primo.

$1 + \sqrt{-3}$ **é irredutível em** $\mathbb{Z}[\sqrt{-3}]$

1. $1 + \sqrt{-3}$ não é nulo e não é unidade
2. Se $1 + \sqrt{-3} = (a + b\sqrt{-3})(c + d\sqrt{-3})$, um dos dois fatores é uma unidade:

   Sejam $a + b\sqrt{-3}, c + d\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ tais que

   $$1 + \sqrt{-3} = (a + b\sqrt{-3})(c + d\sqrt{-3}).$$

   Então os quadrados dos módulos destes dois complexos também são iguais, i.e.,

   $$4 = (a^2 + 3b^2)(c^2 + 3d^2).$$

   Tendo em conta que os factores são não negativos, as únicas factorizações possíveis são, a menos da ordem dos factores, 2×2 e 1×4. Como a primeira é impossível, concluimos que $a^2 + 3b^2 = 1$ ou $c^2 + 3d^2 = 1$. Aplicando agora o raciocínio usado anteriormente, obtemos que $a + b\sqrt{-3}$ é uma unidade ou $c + d\sqrt{-3}$ é uma unidade. Logo $1 + \sqrt{-3}$ é irredutível.

Divisibilidade

$1 + \sqrt{-3}$ **não é um elemento primo**:

O elemento $1 + \sqrt{-3}$ não é primo pois divide $4\,(= 2 \times 2)$, porque

$$4 = (1 + \sqrt{-3})(1 - \sqrt{-3}),$$

e não divide 2, uma vez que, se $1 + \sqrt{-3} \mid 2$, existiria $a + b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ tal que

$$2 = (1 + \sqrt{-3})(a + b\sqrt{-3}) = (a - 3b) + (b + a)\sqrt{-3},$$

ou seja, existiria $b \in \mathbb{Z}$ tal que

$$\begin{cases} 2 = a - 3b \\ 0 = b + a \end{cases}$$

i.e., existiria $b \in \mathbb{Z}$ tal que $2 = -4b$, o que não acontece.

Divisibilidade

Definição Dados $a, b \in D$, um elemento d de D diz-se um máximo divisor comum de a e b, e escreve-se d é mdc (a, b) se:

(i) $d \mid a$ e $d \mid b$ e

(ii) $(\forall c \in D) \quad c \mid a$ e $c \mid b \Longrightarrow c \mid d$.

Exemplo. No domínio de integridade dos números inteiros, 2 e -2 são $\text{mdc}(4, 6)$.

Observação. Num anel com identidade, existem sempre divisores comuns a quaisquer dois elementos. No entanto, dois elementos podem ter dois divisores comuns, digamos a e b, sem que $a \mid b$ ou $b \mid a$. Há, assim, anéis onde não existem máximos divisores comuns de pares de elementos dados. O seguinte exemplo ilustra esta situação.

Exemplo. $2 + 2\sqrt{-3},\ 8 \in \mathbb{Z}[\sqrt{-3}]$. Para além das unidades, os divisores comuns dos dois elementos são

$$2, -2, 1 + \sqrt{-3}, -1 - \sqrt{-3}.$$

No entanto, nenhum destes elementos é divisível por todos os outros (basta verificar que $2 \nmid 1 + \sqrt{-3}$ e $1 + \sqrt{-3} \nmid 2$, todos os outros casos se reduzem a este a menos de uma unidade). Assim, não existe máximo divisor comum destes dois elementos em $\mathbb{Z}[\sqrt{-3}]$.

Divisibilidade

Proposição Sejam d um mdc (a, b) e $d' \in D$. Então,

$$d' \text{ é } mdc(a, b) \Longleftrightarrow d' \in d\,\mathcal{U}_D.$$

Dem. Exercício

S existe mdc (a, b), ele é univocamente determinado a menos do produto por uma unidade. Assim, representando por $[a, b]$ o conjunto dos mdc (a, b) em D, se d é mdc(a, b), temos que

$$[a, b] = d\,\mathcal{U}_D.$$

Como a relação de associado é uma relação de equivalência, o conjunto $[a, b]$ pode ser visto como uma classe de equivalência. Temos assim, o seguinte resultado.

Corolário Sejam $a, b, c, e, d, d' \in D$ tais que $d \in [a, b]$, $d' \in [c, e]$ e d e d' são associados. Então, $[a, b] = [c, e]$.

Divisibilidade

Proposição Sejam $a, b, p \in D$. Então,

(i) se $a \mid b$, $a \in [a, b]$ e, portanto, $[a, b] = a\mathcal{U}_D$;

(ii) se p é irredutível, existe $\mathrm{mdc}(a, p)$ e

$$[a, p] = \mathcal{U}_D \qquad ou \qquad [a, p] = p\mathcal{U}_D.$$

Proposição Em D, sempre que as expressões fizerem sentido, são válidas as seguintes igualdades:

(i) $[ac, bc] = [a, b]c$;

(ii) $[[a, b], c] = [a, [b, c]]$.

Exemplo. No domínio de integridade $\mathbb{Z}[\sqrt{-3}]$, não existe $\mathrm{m.d.c.}(8, 2 + 2\sqrt{-3})$, mas, como $1 + \sqrt{-3} \mid 4$, existe $\mathrm{m.d.c.}(4, 1 + \sqrt{-3})$. Assim, **não faz sentido** dizer que

$$\mathrm{m.d.c.}(2 \times 4, (1 + \sqrt{-3}) \times 2] = [4, 1 + \sqrt{-3}] \times 2.$$

Proposição Sejam $a, b, c \in D$. Se existe mdc de qualquer par de elementos em D, então,

$$[a, b] = \mathcal{U}_D, \ \ [a, c] = \mathcal{U}_D \Longrightarrow [a, bc] = \mathcal{U}_D.$$

Num domínio de integridade, nem todo o elemento irredutível é primo. No entanto, se existir $\mathrm{m.d.c.}$ de dois quaisquer elementos do domínio, todo o elemento irredutível é primo.

Proposição Se $[a, b] \neq \emptyset$, para quaisquer $a, b \in D$, então, qualquer elemento irredutível é primo.

Demonstração Sejam $x \in D$ um elemento irredutível e $a, b \in D$ tais que $x \mid ab$. Se $x \nmid a$ e $x \nmid b$, teríamos $[x, a] = [x, b] = \mathcal{U}$ e, portanto,

$$[x, ab] = \mathcal{U}.$$

Como $x \mid ab$, temos

$$[x, ab] = x\mathcal{U}_D.$$

No entanto, $x\mathcal{U} \neq \mathcal{U}$, já que $x \notin \mathcal{U}$. A contradição veio de termos suposto que $x \nmid a$ e $x \nmid b$. Logo, $x \mid a$ ou $x \mid b$.

Estudamos de seguida algumas classes de domínios de integridade nas quais existe m.d.c. de quaisquer dois elementos.