UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Grupos e semigrupos

Gabriel Rodrigues da Silva

Dissertação de Mestrado do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)

ICMC USP SÃO CARLOS

Gabriel Rodrigues da Silva

Grupos e semigrupos

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Mestrado Profissional em Matemática em Rede Nacional. *EXEMPLAR DE DEFESA*

Área de Concentração: Mestrado Profissional em Matemática em Rede Nacional

Orientador: Prof. Dr. Hermano de Souza Ribeiro

USP – São Carlos
Janeiro de 2019

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

S586g

Silva, Gabriel Rodrigues da
Grupos e semigrupos / Gabriel Rodrigues da Silva; orientador Hermano de Souza Ribeiro. -- São Carlos, 2019.
165 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2019.

1. Grupos. 2. Semigrupos. I. Ribeiro, Hermano de Souza, orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

Gabriel Rodrigues da Silva

Groups and semigroups

Master dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP, in partial fulfillment of the requirements for the degree of Mathematics Professional Master's Program. *EXAMINATION BOARD PRESENTATION COPY*

Concentration Area: Professional Master Degree Program in Mathematics in National Network

Advisor: Prof. Dr. Hermano de Souza Ribeiro

USP – São Carlos
January 2019

Dedico esta dissertação à pessoa mais maravilhosa que já conheci em toda a minha vida: Cristina Rodrigues.

AGRADECIMENTOS

Em primeiro lugar, agradeço o professor Hermano pela oportunidade de ser seu orientando. Muito obrigado por toda a paciência e por todos os ensinamentos ao longo desses anos. Obrigado também à professora Karina por ter me ensinado a gostar de álgebra e por ter sido minha orietadora na graduação e minha amiga na vida.

Não posso deixar de agradecer os integrantes da minha família que sempre me deram suporte nas minhas escolhas e que sempre me deram oportunidades para trilhar meu caminho; em especial, obrigado à minha mãe por ser simplesmente a pessoa mais excepcional desse planeta.

Júlio, Jeffrey e Italo, os irmãos que a vida me deu, vocês são as pessoas mais companheiras que já conheci. O meu amor por vocês não pode ser medido aqui.

Angel, Rick, Rafa, Dio, Bazão, Pri, Tan, Mel e Nati, a eterna Máfia da Alice, muito obrigado pelos aprendizados na escola e pela amizade fora dela. Trabalhar com vocês foi fundamental pra me tornar o profissional que sou hoje e conviver com vocês é delicioso.

Mános, Rê e Patty, as melhores roomates que eu poderia ter, muito obrigado por serem quem são. Todo o tempo dividindo experiências foi maravilhoso. Sinto saudades todos os dias.

Toni, Jhonny, Pedro, Elvis, Varal, Dani e Bruno, grandes amigos que estiveram comigo durante boa parte da minha vida em São Carlos, muito obrigado pelos momentos icônicos que passamos juntos.

Mari, Marina, Lê, Ana, Bia e Vivi, obrigado pelos ensinamentos diários e pela parceria de sempre. A educação ganha muito com vocês dentro da sala de aula e espero continuar fazendo parte desse processo com vocês.

Gugs, Gui, Paulinha, Pak, Cris, Ti, Alface, Nico e todos os amigos do Vôlei Federal e do Vôlei CAASO, dividir a quadra e as medalhas com vocês foi engrandecedor.

Unidas no Vôlei, vocês fazem parte da melhor equipe de voleibol do mundo. Só tenho a agradecer pela oportunidade de ser o treinador de mulheres tão guerreiras.

Fer, obrigado pelo carinho e pelo cuidado de sempre. Você é meu bobão preferido.

Simone, muito obrigado pela ajuda milagrosa. Você é sensacional.

Finalmente, um obrigado especial a todos os mantenedores das escolas que acreditaram no meu trabalho e a todos os alunos maravilhosos que conheci nesse processo árduo e gratificante.

“Unless they paying your bills,
pay them bitches no mind.”
(RuPaul Charles)

RESUMO

SILVA, G. R. **Grupos e semigrupos**. 2019. 165 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2019.

Baseado no conjunto das funções parciais injetoras em um conjunto não vazio e no conjunto das funções booleanas de várias variáveis, a dissertação apresenta os conceitos de grupos e de semigrupos inversos, que são constituídos por elementos inversíveis. No caso de grupos, a definição de elemento inversível é a usual e, no caso de semigrupos inversos, a definição de elemento inversível é uma generalização do conceito usual de elemento inversível.

Palavras-chave: Grupo, Semigrupo, Semigrupo inverso.

ABSTRACT

SILVA, G. R. **Groups and semigroups**. 2019. 165 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2019.

Based on the set of injective partial functions in a non empty set and in the set of booleans functions with many variables, this paper shows the concepts of groups and inverse semigroups, which are both made of inversible elements. In groups, the definition of inversible element is the usual and, in inverse semigroups, the definition of inversible element is a generalization of the usual concept of inversible element.

Keywords: Groups, Semigroups, Inverse semigroups.

SUMÁRIO

CAPÍTULO

1

INTRODUÇÃO

O segundo capítulo desta dissertação aborda a teoria dos conjuntos, focando no conceito de relações binárias e, em particular, de funções. O capítulo exibe a construção da intersecção de todas as relações binárias de equivalência em um conjunto não vazio que contém uma relação binária dada e em conjuntos finitos mostra a construção da intersecção de todas as relações binárias transitivas que contém uma relação binária dada. Os números de Stirling de segunda espécie calculam o número de relações binárias de equivalência em um conjunto finito e usa um número pré fixado de classes de equivalência. O número de funções parciais e de funções totais em um conjunto finito também são calculados no capítulo. As funções totais em um conjunto finito, cujo domínio de definição é o conjunto em questão, são funções compostas de uma determinada função total fixada e de permutações dos elementos do conjunto, enquanto que as funções parciais, além de admitirem extensão a funções totais, também são funções compostas de uma determinada função parcial fixada e de permutações dos elementos do conjunto. Estas funções compostas são ilustradas através de vários exemplos.

O terceiro capítulo apresenta as funções booleanas de várias variáveis booleanas, bem como a associatividade, detalhada pelo teste Light de associatividade das principais operações binárias booleanas. As definições das operações binárias booleanas guardam grande analogia com as operações binárias internas da teoria dos conjuntos. A construção das formas conjuntiva e disjuntiva normais das funções booleanas é apresentada como o método de Quine-McCluskey para a determinação das formas mínimas de uma função booleana.

O quarto capítulo trata de grupos e semigrupos e é escrito com a intenção de fazer paralelismos entre a teoria de grupos e a teoria de semigrupos. O primeiro paralelismo é a definição de relações binárias de equivalência compatíveis à esquerda e à direita com a operação binária interna de semigrupo e a definição de relações de equivalências compatíveis à esquerda e à direita com a operação binária interna de grupo, determinadas pelos subgrupos normais

de um grupo. O segundo paralelismo são os três teoremas do isomorfismo e o teorema da correspondência para grupos e os três teoremas do isomorfismo e o teorema da correspondência para semigrupos. O terceiro paralelismo explorado é o teorema da estrutura de grupos cíclicos e o teorema da estrutura de subgrupos cíclicos. Finalmente, o último paralelismo alcançado é dado pelos vários teoremas de representação de Cayley válidos para grupos, semigrupos e semigrupos inversos.

Os semigrupos ditos inversos, objetos do último capítulo, em que o elemento inverso de semigrupo de um elemento do semigrupo, definido como generalização dos elementos inversos de um grupo, existe e é unicamente determinado para cada elemento. A unicidade do elemento inverso de semigrupo para cada elemento do semigrupo inverso é equivalente logicamente à comutatividade da operação binária interna de semigrupo no subconjunto dos elementos idempotentes do semigrupo. Além do mais, semigrupos inversos admitem uma relação de ordem motivada pela relação de ordem natural existente no conjunto das funções booleanas. Nem o semigrupo das funções totais e nem o semigrupo das funções parciais em um conjunto são exemplos de semigrupos inversos, mas o semigrupo das funções injetoras em um conjunto é um exemplo de semigrupos inversos e trivialmente o semigrupo das funções booleanas.

CAPÍTULO

2

TEORIA DOS CONJUNTOS

Seja U um conjunto não vazio. Um subconjunto não vazio A do conjunto U é um conjunto com a propriedade de que todo elemento de A é elemento de U. Por vacuidade, o conjunto $\emptyset$ é um subconjunto de U.

O conjunto das partes $\mathscr{P}(U)$ do conjunto U é o conjunto constituído por todos os subconjuntos do conjunto U.

A relação de inclusão $\subset$ de dois subconjuntos A e B do conjunto U, indicado por $A \subset B$, significa que todo elemento de A é elemento de B.

A relação de igualdade $=$ de dois subconjuntos A e B do conjunto U, indicado por $A = B$, significa que $A \subset B$ e $B \subset A$.

A união $A \cup B$ de dois subconjunto A e B do conjunto U é o conjunto constituído por todos os elementos pertencentes a pelo menos um dos subconjuntos A e B de U.

Propriedades 2.1.

Sejam A, B e C subconjuntos de um conjunto U. Então:

(i) (Lei da idempotência da união) $A \cup A = A$

(ii) (Lei comutativa da união) $A \cup B = B \cup A$

(iii) (Lei associativa da união) $A \cup (B \cup C) = (A \cup B) \cup C$

(iv) (Lei do vazio) $A \cup \emptyset = A$

(v) (Lei do universo) $A \cup U = U$

A intersecção $A \cap B$ de dois subconjuntos A e B do conjunto U é o conjunto constituído por todos os elementos pertencentes simultaneamente aos dois subconjuntos A e B de U.

Propriedades 2.2.

Sejam A, B e C subconjuntos de um conjunto U. Então:

(i) (Lei da idempotência da interseçcão) $A \cap A = A$

(ii) (Lei comutativa da interseçcão) $A \cap B = B \cap A$

(iii) (Lei associativa da interseçcão) $A \cap (B \cap C) = (A \cap B) \cap C$

(iv) (Lei do vazio) $A \cap \emptyset = \emptyset$

(v) (Lei do universo) $A \cap U = A$

Define-se a tabela de pertinência da união e da intersecção de dois subconjuntos A e B de um conjunto não vazio U, respectivamente, por:

A	B	$A \cup B$	$A \cap B$
1	1	1	1
1	0	1	0
0	1	1	0
0	0	0	0

O subconjunto complementar $\overline{A}$ de um subconjunto A do conjunto U é o conjunto constituído por todos os elementos de U que não são elementos de A. Sua tabela de pertinência é dada por:

A	$\overline{A}$
1	0
0	1

Propriedades 2.3 (Leis da absorção)**.**

Sejam A e B subconjuntos de um conjunto U. Então:

(i) $A \cup (A \cap B) = A$

(ii) $A \cap (A \cup B) = A$

(iii) $A \cup (\overline{A} \cap B) = A \cup B$

Demonstração.

A tabela abaixo auxilia na demonstração:

A	B	$A \cap B$	$A \cup (A \cap B)$	$A \cup B$	$A \cap (A \cup B)$	$\overline{A} \cap B$	$A \cup (\overline{A} \cap B)$
1	1	1	1	1	1	0	1
1	0	0	1	1	1	0	1
0	1	0	0	1	0	1	1
0	0	0	0	0	0	0	0

Como a primeira e a quarta colunas são iguais, está provado que $A = A \cup (A \cap B)$, assim como está provado que $A = A \cap (A \cup B)$, já que a primeira e a sexta coluna são iguais. Da mesma forma, como a quinta e a oitava coluna são iguais, está provado que $A \cup B = A \cup (\overline{A} \cap B)$. □

O conjunto diferença $A - B$ do conjunto A em relação ao conjunto B, ambos subconjuntos do conjunto U, é o conjunto constituído por todos os elementos de A que não são elementos de B.

O conjunto diferença simétrica $A \Delta B$ de dois subconjuntos A e B do conjunto U é definido como $A \Delta B = (A - B) \cup (B - A)$.

Define-se a tabela de pertinência da diferença e da diferença simétrica de dois subconjuntos A e B de um conjunto não vazio U por:

A	B	$A - B$	$B - A$	$A \Delta B$
1	1	0	0	0
1	0	1	0	1
0	1	0	1	1
0	0	0	0	0

Propriedades 2.4.

Sejam A, B e C subconjuntos de um conjunto U. Então:

(i) (Lei comutativa da diferença simétrica) $A \Delta B = B \Delta A$

(ii) (Lei associativa da diferença simétrica) $A \Delta (B \Delta C) = (A \Delta B) \Delta C$

(iii) (Lei do vazio) $A \Delta \emptyset = A$

(iv) (Lei do universo) $A \Delta U = \overline{A}$

Propriedades 2.5.

Sejam A e B subconjuntos de um conjunto U. Então:

(i) $A - B = A \cap \overline{B}$

(ii) $A - B = A - (A \cap B)$

(iii) $A \cup B = A \cup (B - A)$

(iv) $A \Delta B = (A \cup B) - (A \cap B)$

Propriedades 2.6.

Sejam A, B e C subconjuntos de um conjunto U. Então:

(i) $A \cap (B - C) = (A \cap B) - (A \cap C)$

(ii) $(A - C) \cup (B - C) = (A \cup B) - C$

(iii) $(A - C) \cap (B - C) = (A \cap B) - C$

(iv) se $A \subset B$, $B \subset C$, $A \cup B = C$ e $A \cap B = \emptyset$, então $A = C - B$

(v) valem as leis distributivas da união em relação a intersecção e da intersecção em relação a união:

a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Teorema 2.7 (Leis de Morgan)**.**

Sejam A e B subconjuntos de um conjunto U não vazio. Então:

(i) $\overline{A \cup B} = \overline{A} \cap \overline{B}$

(ii) $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Demonstração.

(i) A inclusão $\overline{A \cup B} \subset \overline{A} \cap \overline{B}$ é provada abaixo:

1. $x \in \overline{A \cup B}$
2. $x \notin A \cup B$
3. $x \notin A$ e $x \notin B$
4. $x \in \overline{A}$ e $x \in \overline{B}$
5. $x \in \overline{A} \cap \overline{B}$

Agora, a inclusão $\overline{A} \cap \overline{B} \subset \overline{A \cup B}$ é provada:

6. $x \in \overline{A} \cap \overline{B}$
7. $x \in \overline{A}$ e $x \in \overline{B}$

8. $x \notin A$ e $x \notin B$
9. $x \notin A \cup B$
10. $x \in \overline{A \cup B}$

Portanto, $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

(ii) A inclusão $\overline{A \cap B} \subset \overline{A} \cup \overline{B}$ é provada abaixo:

1. $x \in \overline{A \cap B}$
2. $x \notin A \cap B$

3a. $x \in A$ e $x \notin B$ sem perda de generalidade

3b. $x \notin A$ e $x \notin B$

4. admitindo (3a), $x \notin \overline{A}$ e $x \in \overline{B}$
5. $x \in \overline{A} \cup \overline{B}$
6. admitindo (3b), $x \in \overline{A}$ e $x \in \overline{B}$
7. $x \in \overline{A} \cup \overline{B}$

Em seguida, a inclusão $\overline{A} \cup \overline{B} \subset \overline{A \cap B}$ é provada:

8. $x \in \overline{A} \cup \overline{B}$

9a. $x \in \overline{A}$ e $x \notin \overline{B}$ sem perda de generalidade

9b. $x \in \overline{A}$ e $x \in \overline{B}$

10. admitindo (9a), $x \notin A$ e $x \in B$
11. $x \notin A \cap B$
12. $x \in \overline{A \cap B}$
13. admitindo (9b), $x \notin A$ e $x \notin B$
15. $x \notin A \cap B$
16. $x \in \overline{A \cap B}$

Portanto, $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

□

Teorema 2.8 (Leis de Morgan para a operação binária interna diferença de conjuntos)**.**

Sejam A, B e C subconjuntos de um conjunto U. Então:

(i) $(C - A) \cap (C - B) = C - (A \cup B)$

(ii) $(C-A)\cup(C-B)=C-(A\cap B)$

Demonstração.

(i) A inclusão $(C-A)\cap(C-B)\subset C-(A\cup B)$ é provada abaixo:

1. $x\in(C-A)\cap(C-B)$
2. $x\in(C-A)$ e $x\in(C-B)$
3. $x\in C$ e $x\neq A$
4. $x\in C$ e $x\neq B$
5. $x\in C$, $x\neq A$ e $x\neq B$
6. $x\in C$ e $x\neq A\cup B$
7. $x\in C-(A\cup B)$

Agora, a inclusão $C-(A\cup B)\subset(C-A)\cap(C-B)$ é provada:

8. $x\in C-(A\cup B)$
9. $x\in C$ e $x\neq A\cup B$
10. $x\in C$, $x\neq A$ e $x\neq B$
11. $x\in C$ e $x\neq B$
12. $x\in C$ e $x\neq A$
13. $x\in(C-A)$ e $x\in(C-B)$
14. $x\in(C-A)\cap(C-B)$

Portanto, $(C-A)\cap(C-B)=C-(A\cup B)$.

(ii) A inclusão $(C-A)\cup(C-B)\subset C-(A\cap B)$ é provada abaixo:

1. $x\in(C-A)\cup(C-B)$

2a. $x\in(C-A)$

2b. $x\in(C-B)$

3. admitindo (2a), $x\in C$ e $x\neq A$
4. $x\in C$ e $x\neq A\cap B$
5. $x\in C-(A\cap B)$
6. admitindo (2b), $x\in C$ e $x\neq B$
7. $x\in C$ e $x\neq A\cap B$

8. $x \in C - (A \cap B)$

Em seguida, a inclusão $C - (A \cup B) \subset (C - A) \cap (C - B)$ é provada:

9. $x \in C - (A \cap B)$
10. $x \in C$ e $x \neq A \cap B$
11a. $x \in C$, $x \in A$ e $x \neq B$
11b. $x \in C$, $x \neq A$ e $x \in B$
11c. $x \in C$, $x \neq A$ e $x \neq B$
12. admitindo (11a), $x \in C - B$
13. admitindo (11b), $x \in C - A$
14. admitindo (11c), $x \in C - A$ e $x \in C - B$
15. $x \in (C - A) \cup (C - B)$

Portanto, $C - (A \cup B) = (C - A) \cap (C - B)$.

□

Teorema 2.9 (Leis do cancelamento)**.**

Sejam A, B e C subconjuntos de um conjunto U. Então:

(i) se $A \cap C = B \cap C$ e se $A \cup C = B \cup C$, então $A = B$

(ii) se $A \cap C = B \cap C$ e se $A \cap \overline{C} = B \cap \overline{C}$, então $A = B$

(iii) se $A \cup C = B \cup C$ e se $A \cup \overline{C} = B \cup \overline{C}$, então $A = B$

Demonstração.

(i) A inclusão $A \subset B$ é provada abaixo:

1. $x \in A$
2a. $x \in C$
2b. $x \notin C$
3. admitindo (2a), como $x \in A$, então $x \in A \cap C$
4. como $A \cap C = B \cap C$ por hipótese, então $x \in B \cap C$
5. $x \in B$
6. nesse caso, $A \subset B$

7. admitindo (2b), como $x \in A$ e $x \in A \cup C$
8. como $A \cup C = B \cup C$ por hipótese, então $x \in B \cup C$
9. $x \in B$, pois $x \notin C$
10. nesse caso, $A \subset B$

Portanto, $A \subset B$ em ambos os casos ($x \in C$ ou $x \notin C$) e, pela simetria da proposição, $B \subset A$, o que implica que $A = B$.

(ii) A inclusão $A \subset B$ é provada abaixo:

1. $x \in A$

2a. $x \in C$

2b. $x \notin C$

3. admitindo (2a), como $x \in A$, então $x \in A \cap C$
4. como $A \cap C = B \cap C$ por hipótese, então $x \in B \cap C$
5. $x \in B$
6. nesse caso, $A \subset B$
7. admitindo (2b), $x \in \overline{C}$ e, como $x \in A$, então $x \in A \cap \overline{C}$
8. como $A \cap \overline{C} = B \cap \overline{C}$ por hipótese, então $x \in B \cap \overline{C}$
9. $x \in B$
10. nesse caso, $A \subset B$

Portanto, $A \subset B$ em ambos os casos ($x \in C$ ou $x \notin C$) e, pela simetria da proposição, $B \subset A$, o que implica que $A = B$.

(iii) A inclusão $A \subset B$ é provada abaixo:

1. $x \in A$

2a. $x \in C$

2b. $x \notin C$

3. admitindo (2a), $x \notin \overline{C}$
4. como $x \in A \cup \overline{C} = B \cup \overline{C}$ por hipótese, então $x \in B \cup \overline{C}$
5. $x \in B$, pois $x \notin \overline{C}$
6. nesse caso, $A \subset B$
7. admitindo (2b), como $x \in A$, então $x \in A \cup C$
8. como $A \cup C = B \cup C$ por hipótese, então $x \in B \cup C$

9. $x \in B$, pois $x \notin C$
10. nesse caso, $A \subset B$

Portanto, $A \subset B$ em ambos os casos ($x \in C$ ou $x \notin C$) e, pela simetria da proposição, $B \subset A$, o que implica que $A = B$.

□

O produto cartesiano $X \times Y$ de dois conjuntos X e Y é o conjunto formado por todos os pares ordenados (x,y) tais que $x \in X$ e $y \in Y$. Por vacuidade, $X \times \emptyset = \emptyset$ e $\emptyset \times X = \emptyset$.

Propriedades 2.10.

Sejam os conjuntos X, Y e Z. Então:

(i) $X \times (Y \cap Z) = (X \times Y) \cap (X \times Z)$

(ii) $X \times (Y \cup Z) = (X \times Y) \cup (X \times Z)$

2.1 Relações binárias

Uma relação binária R de um conjunto X em um conjunto Y é um subconjunto vazio ou não vazio R do produto cartesiano $X \times Y$. A notação xRy significa que $(x,y) \in R$.

O domínio de definição $D(R)$ de uma relação binária R de X em Y é o conjunto dos elementos $x \in X$ tais que existe $y \in Y$ com $(x,y) \in R$.

O conjunto imagem ou o conjunto de valores $Im(R)$ de uma relação binária R de X em Y é o conjunto dos elementos $y \in Y$ tais que existe $x \in X$ com $(x,y) \in R$.

A relação binária R^{-1} do conjunto Y no conjunto X é o subconjunto R^{-1} do produto cartesiano $Y \times X$ constituído pelos pares ordenados (y,x) com $y \in Y$ e $x \in X$ de modo que $(x,y) \in R$.

A relação de pertinência $\in$ é uma relação binária do conjunto X no conjunto $\mathscr{P}(X)$ cujos elementos são todos os subconjuntos de X.

A relação binária de inclusão $R_{\subset} = \{(A,B) : A,B \in \mathscr{P}(X) \text{ e } A \subset B\}$ é uma relação binária no conjunto das partes $\mathscr{P}(X)$ de um conjunto X. A notação $AR_{\subset}B$ significa que $(A,B) \in R_{\subset}$ e que $A \subset B$ para subconjuntos A e B de X.

Uma função f do conjunto X no conjunto Y é uma relação binária f de X em Y com as seguintes propriedades:

(i) Para cada $x \in X$ e $y_1, y_2 \in Y$, se $(x,y_1) \in f$ e $(x,y_2) \in f$, então $y_1 = y_2$.

(ii) Para cada $x \in D(f)$, o domínio de definição da relação binária f, $f(x)$ é o único elemento de Y tal que $(x, f(x)) \in f$.

2.1.1 Relações binárias e funções em um conjunto não vazio

Uma relação binária R em um conjunto X é um subconjunto vazio ou não vazio R do produto cartesiano $X \times X$.

Seja X um conjunto não vazio e seja $B(X)$ o conjunto de todas as relações binárias R no conjunto X, isto é, o conjunto de todos os subconjuntos R do produto cartesiano $X \times X$.

Definição 2.11.

Se S e R são relações binárias no conjunto não vazio X, a relação binária $R \circ S$ no conjunto X é definida por:

$$R \circ S = \{(x,y) \in X \times X : (\exists\, z \in X)((x,z) \in S)((z,y) \in R)\}.$$

Proposição 2.12 (Lei associativa da composição)**.**

Sejam R, S e T relações binárias em um conjunto não vazio X. Então,

$$(R \circ S) \circ T = R \circ (S \circ T).$$

Demonstração.

A inclusão $(R \circ S) \circ T \subset R \circ (S \circ T)$ é provada abaixo:

1. $(x,y) \in (R \circ S) \circ T$
2. $(\exists\, z \in X)((x,z) \in T$ e $(z,y) \in R \circ S)$
3. $(\exists\, w \in X)((z,w) \in S$ e $(w,y) \in R)$
4. $(x,w) \in S \circ T$, pois $(x,z) \in T$ e $(z,w) \in S$
5. $(x,y) \in R \circ (S \circ T)$, pois $(x,w) \in S \circ T$ e $(w,y) \in R$

Agora, a inclusão $R \circ (S \circ T) \subset (R \circ S) \circ T$ é provada:

6. $(x,y) \in R \circ (S \circ T)$
7. $(\exists\, z \in X)((x,z) \in S \circ T$ e $(z,y) \in R)$
8. $(\exists\, w \in X)((x,w) \in T$ e $(w,z) \in S)$
9. $(w,y) \in R \circ S$, pois $(w,z) \in S$ e $(z,y) \in R$

10. $(x,y) \in (R \circ S) \circ T$, pois $(x,w) \in T$ e $(w,y) \in R \circ S$

Portanto, $R \circ (S \circ T) = (R \circ S) \circ T$. □

Teorema 2.13.

Para relações binárias R, S, T em um conjunto não vazio X, se $R \subset S$, então:

(i) $R \circ T \subset S \circ T$

(ii) $T \circ R \subset T \circ S$

Demonstração.

(i) 1. $(x,y) \in R \circ T$

2. $(\exists\, z \in X)((x,z) \in T \text{ e } (z,y) \in R)$

3. $(z,y) \in S$, pois $R \subset S$

4. $(x,y) \in S \circ T$, pois $(x,z) \in T$ e $(z,y) \in S$

(ii) A prova é análoga à prova do item anterior.

□

Uma função f em um conjunto não vazio X é uma relação binária f em X com a seguinte propriedade: para x, y_1, $y_2 \in X$, se $(x,y_1) \in f$ e $(x,y_2) \in f$, então $y_1 = y_2$.

O único valor y para o qual $(x,y) \in f$ é indicado com o símbolo $f(x)$ e denominado o valor da função f no elemento x.

A operação binária interna de composição de relações binárias aplicada a funções f e g em um conjunto X resulta em uma relação binária $g \circ f$ em X que é uma função em X. De fato, para x, y_1, $y_2 \in X$, se $(x,y_1) \in g \circ f$, significa a existência de $z_1 \in X$ tal que

$$(x,z_1) \in f \text{ e } (z_1,y_1) \in g$$

e, se $(x,y_2) \in g \circ f$, significa a existência de $z_2 \in X$ tal que

$$(x,z_2) \in f \text{ e } (z_2,y_2) \in g,$$

mas, como f é função,

$$\text{se } (x,z_1) \in f \text{ e } (x,y_2) \in f, \text{ então } z_1 = z_2$$

e, como g é função,

$$\text{se } (z_1,y_1) \in g \text{ e } (z_2,y_2) \in g, \text{ então } y_1 = y_2.$$

Portanto,

$$\text{se } (x,y_1) \in g \circ f \text{ e } (x,y_2) \in g \circ f, \text{ então } y_1 = y_2.$$

Uma relação binária R em um conjunto não vazio X é uma relação binária

(i) reflexiva quando, e somente quando,

$$(\forall\, x \in X)((x,x) \in R).$$

(ii) simétrica quando, e somente quando,

$$(\forall\, x \in X)(\forall\, y \in X)((x,y) \in R \Leftrightarrow (y,x) \in R)$$

ou, equivalentemente, quando, e somente quando, $R = R^{-1}$.

(iii) transitiva quando, e somente quando,

$$(\forall\, x \in X)(\forall\, y \in X)(\forall\, z \in X)((x,y) \in R \text{ e } (y,z) \in R \Rightarrow (x,z) \in R)$$

ou, equivalentemente, quando, e somente quando, $R \circ R \subset R$, pois, se $(x,y) \in R$ e $(y,z) \in R$, então $(x,z) \in R \circ R$.

(iv) antisimétrica quando, e somente quando,

$$(\forall\, x \in X)(\forall\, y \in X)((x,y) \in R \text{ e } (y,x) \in R \Rightarrow x = y).$$

O fecho reflexivo R_r de uma relação binária R em um conjunto não vazio X é a relação binária em X definida por:

$$R_r = R \cup \{(x,x) : x \in X\}$$

e é igual a intersecção de todas as relações binária reflexivas em X que contém R. O fecho reflexivo de uma relação binária R é uma relação binária reflexiva.

O fecho simétrico R_s de uma relação binária R em um conjunto não vazio X é a relação binária em X definida por:

$$R_s = R \cup R^{-1}$$

e é igual a intersecção de todas as relações binárias simétricas em X que contém R. O fecho simétrico de uma relação binária R é uma relação binária simétrica.

Teorema 2.14.

Seja R uma relação binária reflexiva em um conjunto não vazio X. Então:

(i) $R \subset (R \circ R) \subset (R \circ R \circ R) \subset \ldots$.

(ii) O fecho transitivo R_t da relação binária reflexiva R, que é a intersecção de todas as relações binárias transitivas em X que contém R, é igual a

$$R_t = R \cup (R \circ R) \cup (R \circ R \circ R) \cup \ldots = \bigcup_{j=1}^{\infty} R^j,$$

em que, para cada número $n \in \mathbb{N} = \{1, 2, \ldots\}$, $R^n = R \circ R \circ \ldots \circ R$ (n vezes).

Demonstração.

A relação binária $R^\infty = \bigcup_{j=1}^{\infty} R^j$ é uma relação binária reflexiva no conjunto X, porque $\Delta_X \subset R$ e $R = R \circ \Delta_X \subset R \circ R$, sendo que $\Delta_X = \{(x,x) : x \in X\}$.

A relação binária R^∞ é uma relação binária transitiva no conjunto X. De fato, para elementos x, y, $z \in X$ tais que $(x,y) \in R^\infty$ e $(y,z) \in R^\infty$, então existem números naturais m, $n \in \{1, 2, \ldots\}$ de modo que $(x,y) \in R^m$ e $(y,z) \in R^n$, o que implica que $(x,z) \in R^{m+n} = R^n \circ R^m \subset R^\infty$.

Se T é uma relação binária transitiva no conjunto X tal que $R \subset T$, então

$$R^2 = R \circ R \subset T \circ T \subset T$$

e, em geral, para cada $n \in \{1, 2, \ldots\}$, $R^n \subset T$, o que resulta em $R^\infty \subset T$. □

Propriedades 2.15.

Uma relação binária reflexiva R definida em um conjunto não vazio X é tal que

$$R = \Delta_X \circ R \subset R \circ R.$$

Uma relação binária transitiva R definida em um conjunto não vazio X é tal que

$$R \circ R \subset R.$$

Uma relação binária reflexiva e transitiva R definida em um conjunto não vazio X é tal que

$$R \circ R = R.$$

Relações binárias de equivalência em um conjunto não vazio X são relações binárias em X as quais são simultaneamente reflexivas, simétricas e transitivas em X.

Relações binárias de ordem parcial em um conjunto não vazio X são relações binárias em X as quais são simultaneamente reflexivas, antissimétricas e transitivas em X.

Portanto, relações binárias de equivalência R em um conjunto X não vazio satisfazem $R \circ R = R$ (a condição de transitividade para relações binárias de equivalência R é que $R \circ R = R$),

ou seja, relações binárias de equivalência em X são elementos idempotentes em relação à operação binária interna de composição no conjunto $B(X)$ constituído por todas as relações binárias em X. Além disso, o domínio de definição e o conjunto de valores de uma relação binária de equivalência R em X são iguais a X pelo fato de que o domínio de definição $D(R)$ de R contém o domínio de definição $D(\Delta_X) = X$ da relação binária Δ_X, e o mesmo é válido para o conjunto de valores.

A classe de equivalência de um elemento x pertencente a um conjunto X não vazio segundo uma relação binária R de equivalência em X é indicada por Rx e é igual ao conjunto de todos os elementos $y \in X$ tais que $(x,y) \in R$. Além disso:

(i) $Ra = Rb$ quando, e somente quando, $(a,b) \in R$.

(ii) Se $(a,b) \notin R$, então $Ra \cap Rb = \emptyset$.

Uma família $\{A_y : y \in I\}$ de subconjuntos não vazios de um conjunto X não vazio constitui uma partição de X se, e somente se,

(i) $(\forall\, y \in I)(\forall\, k \in I)(A_j \cap A_k = \emptyset)$ ou $(A_j = A_k)$ e

(ii) $\bigcup\limits_{j \in I} A_j = X$.

O conjunto de todas as classes de equivalências de uma relação binária de equivalência em um conjunto X não vazio constitui uma partição do conjunto X e, reciprocamente, toda partição de um conjunto não vazio X origina uma relação binária de equivalência em X.

Seja F uma função de X em Y cujo domínio de definição $D(F)$ é igual a X e cujo conjunto de valores $R(F)$ é um subconjunto de Y. Então, $F^{-1} \circ F$ é uma relação binária de equivalência no conjunto não vazio X. De fato,

$$\begin{aligned} F^{-1} \circ F &= \{(x,y) \in X \times X : (\exists\, z \in X)((x,z) \in F \text{ e } (z,y) \in F^{-1})\} \\ &\quad \big[(z,y) \in F^{-1} \text{ significa que } (y,z) \in F \text{ ou } F(y) = z\big] \\ &= \{(x,y) \in X \times X : F(x) = F(y)\}, \end{aligned}$$

pois, de $F(x) = z$ e $F(y) = z$, segue que $F(x) = F(y)$ e a última igualdade evidencia que $F^{-1} \circ F$ é uma relação binária de equivalência em X.

A relação binária de equivalência $F^{-1} \circ F$ em X é denominada núcleo da função F de X em Y.

A função natural ou função quociente Π_R de X no conjunto quociente X/R (o conjunto das classes de equivalência da relação binária de equivalência R em X) é a função cujo domínio

de definição é $D(\Pi_R) = X$, cujo conjunto de valores é $R(\Pi_R) = X/R$ e que é definida por: para cada $x \in X$,

$$\Pi_R(x) = Rx.$$

O núcleo da função natural Π_R é a relação binária de equivalência R em X.

Teorema 2.16.

Seja R uma relação binária em um conjunto não vazio X, então R_{eq} que, por definição, é a relação binária de equivalência em X, intersecção de todas as relações binárias de equivalência que contém a relação binária R em X, é igual ao fecho transitivo da relação binária reflexiva e simétrica $R \cup R^{-1} \cup \Delta_X$ em X, isto é,

$$R_{eq} = \bigcup_{j=1}^{\infty} (R \cup R^{-1} \cup \Delta_X)^j,$$

em que $\Delta_X = \{(x,x) : x \in X\}$.

Demonstração.

A relação binária $R \cup R^{-1} \cup \Delta_X$ é uma relação binária reflexiva e simétrica em X.

Para cada número $n \in \mathbb{N} = \{1,2,\ldots\}$, a igualdade

$$\begin{aligned}(R \cup R^{-1} \cup \Delta_X)^n &= \{(R \cup R^{-1} \cup \Delta_X)^{-1}\}^n \\ &= \{(R \cup R^{-1} \cup \Delta_X)^n\}^{-1}\end{aligned}$$

mostra que, para cada número $n \in \mathbb{N} = \{1,2,\ldots\}$, $(R \cup R^{-1} \cup \Delta_X)^n$ é uma relação binária simétrica em X e, então, a relação binária $\bigcup_{j=1}^{\infty} (R \cup R^{-1} \cup \Delta_X)^j$ é uma relação binária simétrica em X. De fato, para elementos x, $y \in X$, tais que $(x,y) \in \bigcup_{j=1}^{\infty} (R \cup R^{-1} \cup \Delta_X)^j$, existe um número $n \in \mathbb{N} = \{1,2,\ldots\}$ tal que $(x,y) \in (R \cup R^{-1} \cup \Delta_X)^n$, que é uma relação binária simétrica em X e, portanto,

$$(y,x) \in (R \cup R^{-1} \cup \Delta_X)^n \subset \bigcup_{j=1}^{\infty} (R \cup R^{-1} \cup \Delta_X)^j.$$

A relação binária $\bigcup_{j=1}^{\infty} (R \cup R^{-1} \cup \Delta_X)^j$ é uma relação binária transitiva em X. De fato, para elementos x, y, $z \in X$, se (x,y) e (y,z) são elementos de $\bigcup_{j=1}^{\infty} (R \cup R^{-1} \cup \Delta_X)^j$, então existe números naturais m, $n \in \{1,2,\ldots\}$ tais que:

$$(x,y) \in (R \cup R^{-1} \cup \Delta_X)^m$$

$$(y,z) \in (R \cup R^{-1} \cup \Delta_X)^n$$

e, então,

$$(x,z) \in (R \cup R^{-1} \cup \Delta_X)^m \circ (R \cup R^{-1} \cup \Delta_X)^n = (R \cup R^{-1} \cup \Delta_X)^{m+n} \subset \bigcup_{j=1}^{\infty} (R \cup R^{-1} \cup \Delta_X)^j.$$

Logo, a relação binária $\bigcup_{j=1}^{\infty} (R \cup R^{-1} \cup \Delta_X)^j$ é reflexiva, simétrica e transitiva em X que contém a relação binária R, isto é, $\bigcup_{j=1}^{\infty} (R \cup R^{-1} \cup \Delta_X)^j$ é uma relação de equivalência em X que contém a relação binária R.

Seja E uma relação de equivalência em X tal que $R \subset E$. Então,

$$(R \cup R^{-1} \cup \Delta_X) \circ (R \cup R^{-1} \cup \Delta_X) \subset E \circ E = E$$

e, em geral, para cada número $n \in \mathbb{N} = \{1,2,\ldots\}$, $(R \cup R^{-1} \cup \Delta_X)^n \subset E$, o que mostra que $\bigcup_{j=1}^{\infty} (R \cup R^{-1} \cup \Delta_X)^j \subset E$. □

Teorema 2.17.

Sejam R uma relação binária em um conjunto não vazio X e R_{eq} a intersecção de todas as relações binárias de equivalência em X contendo R. Então,

$$(x,y) \in R_{eq}$$

se, e somente se, ou $x = y$ ou, para algum $n \in \mathbb{N} = \{1,2,\ldots\}$, existe uma sequência z_1, z_2, …, z_n de elementos de X tais que $x = z_1 \to z_2 \to \ldots \to z_n = y$, o que significa que, para cada $j \in \{1,2,\ldots,n\}$, ou $(z_j, z_{j+1}) \in R$ ou $(z_{j+1}, z_j) \in R$.

2.1.2 Relações binárias em um conjunto finito

Para cada número natural n, seja $X_n = \{1,2,\ldots,n\}$ com n elementos. A matriz M_R de uma relação binária R em X_n (que é um subconjunto do produto $X_n \times X_n$) é uma matriz quadrada de ordem n formada pelos dígitos 0 e 1 de modo que, se $(i,j) \in R$, então o elemento da matriz M_R situado na linha i e coluna j é igual ao dígito 1 e, se $(i,j) \notin R$, então o elemento da matriz M_R situado na linha i e coluna j é igual ao dígito 0.

A matriz M_R de uma relação binária reflexiva R no conjunto X_n apresenta todos os dígitos da diagonal principal iguais a 1 enquanto que a matriz M_R de uma relação binária simétrica R no conjunto X_n é uma matriz quadrada simétrica de ordem n: a sequência dos dígitos da primeira linha da matriz coincide com a sequência dos dígitos da primeira coluna e assim sucessivamente para as demais linhas e colunas.

O número natural 2^{n^2} é o número de matrizes quadradas de ordem n formada pelos dígitos 0 e 1 e é igual ao número de relações binárias em X_n devido à correspondência biunívoca existente entre matrizes quadradas de ordem n com dígitos 0 e 1 e relações binárias no conjunto X_n.

O número de relações binárias reflexivas no conjunto X_n é 2^{n^2-n}, lembrando que os dígitos da diagonal principal da matriz correspondente são iguais a 1, enquanto que o número de relações binárias simétricas é

$$2^{\frac{n^2-n}{2}}.2^n = 2^{\frac{n^2+n}{2}},$$

lembrando que a matriz de uma relação binária simétrica é uma matriz simétrica.

O detalhe importante é que, para relações binárias R e S em X_n, a matriz $M_{R\circ S}$ da relação binária $R\circ S$, composta de R e S nesta ordem, é igual à matriz produto $M_S M_R$ (ordem invertida entre R e S) definida da seguinte maneira: o elemento (i,j) da matriz produto é igual a 1 sempre que existir $k \in \{1,2,\ldots,n\}$ tal que o elemento (i,k) da matriz M_S é 1 e o elemento (k,j) da matriz M_R é 1; e, em caso contrário, o elemento (i,j) da matriz produto é 0.

Exemplo 2.18.

Sejam as relações binárias R e S no conjunto $X_4 = \{1,2,3,4\}$ definidas, respectivamente, por:

$$R = \{(1,1),(2,1),(3,2),(3,3),(4,3)\}$$

$$S = \{(1,4),(2,3),(2,4),(3,3),(4,2)\}.$$

As matrizes M_R e M_S de R e S são, respectivamente, iguais a

$$M_R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ e } M_S = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

e a matriz $M_{R\circ S} = M_S M_R$ da relação binária composta $R\circ S$ é igual a

$$M_{R\circ S} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

De fato:

$$(1,3) \in R\circ S, \text{ pois } (1,4) \in S \text{ e } (4,3) \in R;$$

$$(2,2) \in R\circ S, \text{ pois } (2,3) \in S \text{ e } (3,2) \in R;$$

$(2,3) \in R \circ S$, pois $(2,3) \in S$ e $(3,3) \in R$ e também pois $(2,4) \in S$ e $(4,3) \in R$;

$(3,2) \in R \circ S$, pois $(3,3) \in S$ e $(3,2) \in R$;

$(3,3) \in R \circ S$, pois $(3,3) \in S$ e $(3,3) \in R$;

$(4,1) \in R \circ S$, pois $(4,2) \in S$ e $(2,1) \in R$.

A matriz M_{R_r} do fecho reflexivo da relação binária R é igual a

$$M_{R_r} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

e, como $M_{R_r} \neq M_R$, R não é uma relação binária reflexiva em X_n.

A matriz M_{R_s} do fecho simétrico da relação binária R é igual a

$$M_{R_s} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

e, como $M_{R_s} \neq M_R$, R não é uma relação binária simétrica em X_n.

Para o cálculo da matriz do fecho transitivo de uma relação binária R em um conjunto não vazio e finito X, é necessário o uso do algoritmo de Warshall descrito a seguir:

Seja R uma relação binária no conjunto não vazio $X_n = \{1,2,\ldots,n\}$ em que $n \in \mathbb{N} = \{1,2,\ldots\}$. O algoritmo de Warshall constrói as seguintes $n+1$ matrizes cujos coeficientes são 0 e 1:

$$W_0 = M_R, W_1, \ldots, W_n,$$

em que $W_0 = M_R$ é a matriz da relação binária R em X_n e W_n é a matriz da relação binária R_t, fecho transitivo da relação binária R, por razões óbvias pela seguinte descrição: para cada $k \in \{1,2,\ldots,n\}$, o dígito w_{ij}^k da matriz W_k, referente à linha i e à coluna j, é definido como 1 caso exista uma sequência de elementos

$$i, x_1, x_2, \ldots, x_{r-1}, j,$$

em que $i, j \in X_n$ e $x_1, x_2, \ldots, x_{r-1} \in \{1,2,\ldots,k\}$ de modo que

$$(i,x_1) \in R, (x_1,x_2) \in R, \ldots, (x_{r-1}, j) \in R$$

ou caso $w_{ij}^{k-1} = 1$; e o dígito w_{ij}^k é definido como 0 caso tal sequência de elementos não exista. Em outros termos,

$$w_{ij}^k = w_{ij}^{k-1} \vee (w_{ij}^k \wedge w_{ij}^k),$$

em que $\vee$ e $\wedge$ são, respectivamente, as operações binárias OR e AND no conjunto $\{0,1\}$.

O exemplo seguinte ilustra o algoritmo de Warshall.

Exemplo 2.19.

Seja R a relação binária em $X_4 = \{1,2,3,4\}$, cuja matriz M_R é dada por

$$M_R = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

o que significa que

$$R = \{(1,4),(2,1),(2,3),(3,1),(3,4),(4,3)\}.$$

Pelo algoritmo de Warshall,

$$W_1 = W_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

O dígito w_{24}^1 é igual a 1 devido à sequência $2,1,4$.

$$W_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

O dígito w_{41}^3 é igual a 1 devido à sequência $4,3,1$.

O dígito w_{44}^3 é igual a 1 devido à sequência $4,3,4$.

$$W_4 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

O dígito w_{11}^4 é igual a 1 devido à sequência $1,4,3,1$.

O dígito w_{13}^4 é igual a 1 devido à sequência $1,4,3$.

O dígito w_{33}^4 é igual a 1 devido à sequência $3,4,3$.

Em resumo, R_t, fecho transitivo de R, é igual a

$$R_t = \{(1,1),(1,3),(1,4),(2,1),(2,3),(2,4),(3,1),(3,3),(3,4),(4,1),(4,3),(4,4)\}.$$

Um segundo exemplo ilustrativo se encontra abaixo:

Exemplo 2.20.

Seja R a relação binária em $X_4 = \{1,2,3,4\}$, cuja matriz M_R é dada por

$$M_R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

o que significa que

$$R = \{(1,1),(2,1),(3,2),(3,3),(4,3)\}.$$

Pelo algoritmo de Warshall,

$$W_0 = W_1 = M_R$$

$$W_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

O dígito w_{31}^2 é igual a 1 devido à sequência $3,2,1$.

$$W_3 = W_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

O dígito w_{41}^3 é igual a 1 devido à sequência $4,3,2,1$.

O dígito w_{42}^3 é igual a 1 devido à sequência $4,3,2$.

Em resumo, R_t, fecho transitivo de R, é igual a

$$R_t = \{(1,1),(2,1),(3,1),(3,2),(3,3),(4,1),(4,2),(4,3)\}.$$

Teorema 2.21.

Para números n e k pertencentes a $\mathbb{N} = \{1,2,\ldots\}$, o número de relações binárias de equivalência no conjunto $X_n = \{1,2,\ldots,n\}$ com k classes de equivalência, que é igual ao número de partições do conjunto X_n consistindo de k subconjuntos não vazios e disjuntos dois a dois, é calculado pelo número de Stirling de segunda espécie $S(n,k)$ definido pela seguinte relação de recorrência:

$$S(n+1,k+1) = S(n,k) + (k+1)S(n,k+1)$$

sujeito às condições $S(n,1) = S(n,n) = 1$ e, quando $k \in \{n+1,n+2,\ldots\}$, $S(n,k) = 0$.

Demonstração.

O número de partições de $X_{n+1} = \{1,2,\ldots,n+1\}$, com $k+1$ subconjuntos não vazios e disjuntos dois a dois em que um dos subconjuntos da partição é o subconjunto unitário $\{n+1\}$, é igual a $S(n,k)$ e o número de partições de X_{n+1}, com $k+1$ subconjuntos não vazios e disjuntos dois a dois em que um dos subconjuntos da partição não é o subconjunto unitário $\{n+1\}$, é igual a $(k+1)S(n,k+1)$ por haver $k+1$ escolhas para o elemento $n+1$ pertencer a um dos subconjuntos da partição. □

Exemplo 2.22.

O conjunto $\{1,2\}$ tem uma partição constituída pelo conjunto $\{1,2\}$ e uma partição constituída pelos dois subconjuntos unitários $\{1\}$ e $\{2\}$, isto é,

$$\{1,2\} = \{1\} \cup \{2\}.$$

O conjunto $\{1,2,3\}$ tem uma partição constituída pelo conjunto $\{1,2,3\}$, uma partição constituída por três subconjuntos unitários $\{1\}$, $\{2\}$ e $\{3\}$ e três partições constituídas por dois subconjuntos: $\{1\}$ e $\{2,3\}$, $\{2\}$ e $\{1,3\}$ e $\{3\}$ e $\{1,2\}$, isto é,

$$\{1,2,3\} = \{1\} \cup \{2,3\} = \{2\} \cup \{1,3\} = \{3\} \cup \{1,2\} = \{1\} \cup \{2\} \cup \{3\}.$$

Os números de Stirling de segunda espécie são apresentados na seguinte tabela para n e k pertencentes a $\{1,2,3,4,5,6\}$:

	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$
$n=1$	1	0	0	0	0	0
$n=2$	1	1	0	0	0	0
$n=3$	1	3	1	0	0	0
$n=4$	1	7	6	1	0	0
$n=5$	1	15	25	10	1	0
$n=6$	1	31	90	65	15	0

Por exemplo, o número de relações binárias de equivalência no conjunto X_5 com quatro classes de equivalência é igual a 10 e o número de relações binárias de equivalência no conjunto X_6 com três classes de equivalência é igual a 90.

2.2 Funções parciais em um conjunto X

Uma função parcial f em um conjunto não vazio X é uma função f em X, cujo domínio de definição $D(f)$ é um subconjunto vazio ou não vazio do conjunto X e cuja imagem (ou conjunto de valores) $R(f)$ é um subconjunto de X. A função vazia é a relação binária em X cujo domínio de definição e cujo conjunto de valores coincidem com o conjunto vazio.

O conjunto $P(X)$ é o conjunto constituído pela totalidade das funções parciais em um conjunto não vazio X e a operação binária de composição de relações binárias em X, restrita ao conjunto $P(X)$ das funções parciais em X, é uma operação binária interna associativa no conjunto $P(X)$, desde que a relação binária $g \circ f$ em X, composta das funções parciais f e g em X, seja uma função parcial em X. De fato, se $f \in P(X)$ e se $g \in P(X)$, então $g \circ f \in P(X)$.

Demonstração.

1. $(x, y_1) \in g \circ f$ e $(x, y_2) \in g \circ f$, com x, y_1, $y_2 \in X$
2. $(\exists\, z_1 \in X)((x, z_1) \in f, (z_1, y_1) \in g)$
3. $(\exists\, z_2 \in X)((x, z_2) \in f, (z_2, y_2) \in g)$
4. $(x, z_1) \in f$ e $(x, z_2) \in f$
5. $z_1 = z_2$
6. $(z_1, y_1) \in g$ e $(z_1, y_2) = (z_2, y_2) \in g$
7. $y_1 = y_2$

□

Para cada subconjunto não vazio A do conjunto não vazio X, a função inclusão i_A é a função parcial em X, cujo domínio de definição $D(i_A)$ coincide com A e cujo conjunto de valores $R(i_A)$ coincide com A, e que é definida por:

$$\text{para } x \in A,\ i_A(x) = x.$$

Para subconjuntos não vazios A e B do conjunto não vazio X, a função composta $i_A \circ i_B$ das funções inclusão i_A e i_B é a função inclusão $i_{A \cap B}$ do subconjunto $A \cap B$, intersecção dos subconjuntos A e B de X, isto é,

$$i_A \circ i_B = i_B \circ i_A = i_{A \cap B},\ \text{quando } A \cap B \neq \emptyset.$$

Note que, para $A \cap B = \emptyset$, $i_A \circ i_B = i_B \circ i_A$ é a função vazia.

O conjunto $I(X)$ é o conjunto constituído pela totalidade das funções parciais f em um conjunto não vazio X que são funções injetoras, ou seja, para $x_1, x_2 \in X$,

$$\text{se } x_1, x_2 \in D(f) \text{ e } f(x_1) = f(x_2), \text{ então } x_1 = x_2,$$

desde que é válido que a função parcial, composta das funções parciais injetoras f e g em X, é uma função parcial injetora em X.

A operação binária interna de composição de relações binárias em um conjunto não vazio X, restrita ao conjunto $I(X)$ das funções injetoras, é uma operação binária interna associativa no conjunto $I(X)$. De fato, se $f \in I(X)$ e se $g \in I(X)$, então $g \circ f \in I(X)$.

Demonstração.

1. $(x_1, y) \in g \circ f$ e $(x_2, y) \in g \circ f$, com $x_1, x_2, y \in X$.
2. $(g \circ f)(x_1) = g\big[f(x_1)\big] = y = (g \circ f)(x_2) = g\big[f(x_2)\big]$.
3. $f(x_1) = f(x_2)$ pela injetividade da função g
4. $x_1 = x_2$ pela injetividade da função f

□

A operação monária de inversão em $I(X)$ associa, a cada função parcial injetora f de $I(X)$, a função inversa f^{-1} (que é a relação binária inversa f^{-1} da relação binária f em X), cujo domínio de definição $D(f^{-1})$ coincide com o conjunto de valores $R(f)$ de f e cujo conjunto de valores $R(f^{-1})$ coincide com o domínio de definição $D(f)$ de f.

A função composta $f \circ f^{-1}$ é a igual a função inclusão $i_{D(f)}$ e a função composta $f^{-1} \circ f$ é a igual a função inclusão $i_{R(f)}$, ou seja,

$$f \circ f^{-1} = i_{D(f)}$$

$$f^{-1} \circ f = i_{R(f)}.$$

Além disso,

$$f \circ f^{-1} \circ f = f$$

$$f^{-1} \circ f \circ f^{-1} = f^{-1}.$$

2.3 Funções totais em um conjunto X

Uma função total f em um conjunto não vazio X é uma função em X, cujo domínio de definição $D(f)$ coincide com o conjunto X e cujo conjunto de valores $R(f)$ é um subconjunto de X.

O conjunto $T(X)$ é o conjunto constituído pela totalidade das funções totais de X e a operação binária de composição de relações binárias em X, restrita ao conjunto das funções totais em X, é uma operação binária interna em $T(X)$ (isto é, se $f, g \in T(X)$, então $g \circ f \in T(X)$, pois o domínio de definição $D(g \circ f)$ de $g \circ f$ iguala o conjunto X) que possui a propriedade associativa em $T(X)$ (caso particular da associatividade da composição de relações binárias em X).

2.4 Funções parciais e totais de um conjunto X em um conjunto Y

Uma função parcial f do conjunto não vazio X no conjunto não vazio Y é uma função cujo domínio de definição $D(f)$ é um subconjunto não vazio do conjunto X e cujo conjunto de valores $R(f)$ é um subconjunto não vazio do conjunto Y.

Para cada subconjunto vazio ou não vazio $A \subset X$,

$$f(A) = \{f(x) : x \in A \cap D(f)\}$$

é um subconjunto vazio ou não vazio de Y, denominado conjunto imagem de A em Y pela função f.

Para cada subconjunto vazio ou não vazio $B \subset Y$,

$$f^{-1}(B) = \{x \in D(f) : f(x) \in B\}$$

é um subconjunto vazio ou não vazio de X, denominado conjunto imagem inversa de B pela função f.

Teorema 2.23.

Seja f uma função cujo domínio de definição $D(f)$ é um subconjunto não vazio de X e cujo conjunto de valores $R(f)$ é um subconjunto de Y.

As afirmações são equivalentes:

(i) A função f é uma função injetora no sentido de que sempre que $f(x_1) = f(x_2)$, com x_1, $x_2 \in D(f)$, então $x_1 = x_2$.

(ii) Existe uma função g cujo domínio de definição $D(g)$ é um subconjunto do conjunto Y e cujo conjunto de valores $R(f)$ é um subconjunto do conjunto X tal que

$$g \circ f = i_X,$$

em que i_X é a função identidade em X, ou seja, $i_X(x) = x$ para cada $x \in X$.

Demonstração.

(ii) $\Rightarrow$ (i) Admitindo (ii), sejam $x_1, x_2 \in D(f) \subset X$ tais que $f(x_1) = f(x_2)$. Então:

$$\begin{aligned} x_1 &= i_X(x_1) \\ &= (g \circ f)(x_1) \\ &= g\big[f(x_1)\big] \\ &= g\big[f(x_2)\big] \\ &= (g \circ f)(x_2) \\ &= i_X(x_2) \\ &= x_2. \end{aligned}$$

(i) $\Rightarrow$ (ii) Assumindo (i), a relação binária inversa f^{-1} da função f é, de fato, uma função cujo domínio de definição é $R(f)$ e cujo conjunto de valores está contido em X.

Se $x \in X$ e $x_1 = f^{-1}\big[f(x)\big]$, então:

$$(f(x), x_1) \in f^{-1}$$

$$(f(x), x) \in f^{-1},$$

o que implica $x = x_1$, que é equivalente a $f^{-1}\big[f(x)\big] = x$.

□

Seja g uma extensão qualquer da função f^{-1} ao conjunto Y. Então, se $x \in X$,

$$(g \circ f)(x) = g\big[f(x)\big] = f^{-1}\big[f(x)\big] = x = i_X(x).$$

A função g tal que $g \circ f = i_X$ é chamada retração da função f ou função inversa à esquerda da função f, que é equivalente a afirmar que $g \circ f$ é uma função injetora.

Corolário 2.24.

Seja f uma função cujo domínio de definição $D(f)$ é o conjunto X e cujo conjunto de valores $R(f)$ é um subconjunto de Y e seja g uma função cujo domínio de definição $D(g)$ é o conjunto Y e cujo conjunto de valores $R(g)$ é um subconjunto de Z. Então:

(i) Se f e g são funções injetoras, então $g \circ f$ é uma função injetora.

(ii) Se $g \circ f$ é uma função injetora, então f é uma função injetora.

Demonstração.

(i) Sejam h e k as funções inversas à esquerda de f e de g, respectivamente, isto é,

$$h \circ f = i_X$$

$$k \circ g = i_Y.$$

Então, $h \circ k$ é a função inversa à esquerda da função composta $g \circ f$, pois

$$\begin{aligned}(h \circ k) \circ (g \circ f) &= h \circ (k \circ g) \circ f \\ &= h \circ i_Y \circ f \\ &= h \circ f \\ &= i_X,\end{aligned}$$

o que é equivalente a afirmar que $g \circ f$ é uma função injetora.

(ii) Se h é a função inversa à esquerda da função composta $g \circ f$, então $h \circ g$ é a função inversa à esquerda da função f, pois

$$\begin{aligned}(h \circ g) \circ f &= h \circ (g \circ f) \\ &= i_X,\end{aligned}$$

o que é equivalente a afirmar que f é uma função injetora.

□

Teorema 2.25.

Seja f uma função cujo domínio de definição $D(f)$ é o conjunto X e cujo conjunto de valores $R(f)$ é um subconjunto de Y e seja g uma função cujo domínio de definição $D(g)$ é o conjunto Y e cujo conjunto de valores $R(g)$ é um subconjunto de X tal que $f \circ g = i_Y$. Então, $R(f) = Y$.

Demonstração.

Como $R(f) \subset Y$, basta mostrar que $Y \subset R(f)$. Para tanto, seja $y \in Y$. Então, $g(y) \in X$ e

$$y = i_Y(y) = (f \circ g)(y) = f\big[g(y)\big],$$

o que mostra que $y \in R(f)$. □

A função g com a propriedade de que $f \circ g = i_Y$ é chamada seção da função f ou função inversa à direita da função f.

Teorema 2.26.

Seja f uma função cujo domínio de definição $D(f)$ é o conjunto X e cujo conjunto de valores $R(f)$ é um subconjunto de Y e seja g uma função cujo domínio de definição $D(g)$ é o conjunto Y e cujo conjunto de valores $R(g)$ é um subconjunto de Z. Então:

(i) Se f e g são funções sobrejetoras, no sentido de que $R(f) = Y$ e $R(g) = Z$, então $g \circ f$ é uma função sobrejetora, ou seja, $R(g \circ f) = Z$.

(ii) Se $g \circ f$ é uma função sobrejetora, então g é uma função sobrejetora.

Teorema 2.27.

Seja f uma função cujo domínio de definição $D(f)$ é o conjunto X e cujo conjunto de valores $R(f)$ é um subconjunto de Y. Então, as afirmações seguintes são equivalentes:

(i) A função f é uma função injetora e sobrejetora.

(ii) Existem funções r e s cujos domínios de definição são iguais ao conjunto Y com valores no conjunto X com

$$r \circ f = i_X \text{ e } f \circ s = i_Y.$$

(iii) Existe uma função g cujo domínio de definição é o conjunto Y com valores em X tal que

$$g \circ f = i_X \text{ e } f \circ g = i_Y.$$

Assim, se f é uma função injetora e sobrejetora, então a função inversa f^{-1} de f é a única função que é simultaneamente função inversa à esquerda e à direita da função f.

Corolário 2.28.

Seja f uma função cujo domínio de definição $D(f)$ é o conjunto X e cujo conjunto de valores $R(f)$ é um subconjunto de Y e seja g uma função cujo domínio de definição $D(g)$ é o conjunto Y e cujo conjunto de valores $R(f)$ é um subconjunto de X tal que $g \circ f = i_X$. Então, f é uma função injetora e g é uma função sobrejetora.

Corolário 2.29.

Seja f uma função cujo domínio de definição $D(f)$ é o conjunto X e cujo conjunto de valores $R(f)$ é um subconjunto de Y. Então, a função retração da função f é sobrejetora e a função seção da função f é injetora.

Funções totais f do conjunto não vazio X no conjunto não vazio Y são funções cujo domínio de definição $D(f)$ é igual a X e cujo conjunto de valores $R(f)$ é um subconjunto de Y.

Uma função total f de X em Y induz uma função total indicada pela mesma letra f do conjunto das partes $\mathscr{P}(X)$ de X no conjunto das partes $\mathscr{P}(Y)$ de Y, definida por: para cada subconjunto vazio ou não vazio $A \subset X$, a função induzida por f associa ao conjunto A o conjunto $f(A)$ e induz uma função total f^{-1} do conjunto das partes $\mathscr{P}(Y)$ de Y no conjunto das partes $\mathscr{P}(X)$ de X, definida por: para cada subconjunto vazio ou não vazio $B \subset Y$, a função f^{-1} induzida por f associa ao conjunto B o conjunto $f^{-1}(B)$, com as seguintes propriedades de fácil verificação:

(i) Para A_1 e A_2 subconjuntos de X,

$$f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$$

$$f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2).$$

(ii) Para subconjuntos B_1 e B_2 de Y,

$$f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$$

$$f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$$

$$f^{-1}(B_1 - B_2) = f^{-1}(B_1) - f^{-1}(B_2).$$

(iii) Para cada subconjunto $A \subset X$,

$$A \subset f^{-1}\big[f(A)\big].$$

(iv) Para cada subconjunto $A \subset X$ e para cada subconjunto $B \subset Y$,

$$f\big[f^{-1}(B) \cap A\big] = B \cap f(A)$$

e, em particular,

$$f\big[f^{-1}(B)\big] = B \cap f(X).$$

2.5 O conjunto das funções parciais e o conjunto das funções totais em um conjunto finito

Para cada $n \in \mathbb{N} = \{1, 2, \ldots\}$, sejam $X_n = \{1, 2, \ldots, n\}$ e $P(X_n)$ o conjunto constituído pela totalidade das funções parciais f em X_n, isto é, funções f cujo domínio de definição $D(f)$ é um conjunto vazio ou não vazio de X_n e cujo conjunto de valores $R(f)$ é um subconjunto contido em X_n.

O número de funções parciais em $P(X_n)$ é igual a

$$(n+1)^n = 1 + \binom{n}{1}n + \binom{n}{2}n^2 + \ldots + \binom{n}{n}n^n,$$

pois

(i) a parcela 1 é correspondente à função vazio com domínio de definição igual ao conjunto vazio;

(ii) a parcela $\binom{n}{1}n$ é correspondente às funções parciais cujo domínio de definição é um conjunto unitário de X_n: existem $\binom{n}{1}$ subconjuntos unitários de X_n e, para funções parciais f, cujo domínio de definição é um conjunto unitário, há n possibilidades para a defingão do valor de f no elemento do conjunto unitário;

(iii) a parcela $\binom{n}{2}n^2$ é correspondente às funções parciais cujo domínio de definição é um subconjunto de dois elementos $\{i,j\} \subset X_n$: existem $\binom{n}{2}$ subconjuntos com dois elementos $\{i,j\}$ com n possibilidades para o valor de f em i e n possibilidades do valor de f em j;

e assim por diante.

No caso em que X é um conjunto finito com m elementos e em que Y é um conjunto finito com n elementos, o número de funções parciais de X em Y é igual a

$$1 + \binom{m}{1}n + \binom{m}{2}n^2 + \ldots + \binom{m}{m}n^m.$$

Para cada $n \in \mathbb{N} = \{1,2,\ldots\}$, sejam $X_n = \{1,2,\ldots,n\}$ e $T(X_n)$ o conjunto constituído pela totalidade das funções totais f em X_n. O número de funções f em $T(X_n)$ é igual a n^n, porque, para cada $j \in X_n$, existem n possibilidades para a definição do valor da função f em j.

No caso em que X é um conjunto finito com m elementos e em que Y é um conjunto finito com n elementos, o número de funções totais de X em Y é igual a n^m.

Exemplo 2.30.

O número de funções totais sobrejetoras do conjunto $X = \{1,2,3,4,5\}$ sobre o conjunto $Y = \{1,2,3\}$ é calculado pelo princípio da inclusão-exclusão: seja U o conjunto de todas as funções totais f, cujo domínio de definição $D(f)$ é X e cujo conjunto de valores $R(f)$ é um subconjunto de Y e sejam

$$A = \{f \in U : 1 \notin R(f)\}$$

$$B = \{f \in U : 2 \notin R(f)\}$$

$$C = \{f \in U : 3 \notin R(f)\}.$$

Assim, o número de funções totais f sobrejetoras de X sobre Y é igual a 150:

$$\begin{aligned}|\overline{A} \cap \overline{B} \cap \overline{C}| &= |U| - \big[|A| + |B| + |C|\big] + \big[|A \cap B| + |A \cap C| + |B \cap C|\big] - |A \cap B \cap C| \\ &= 3^5 - \binom{3}{1}2^5 + \binom{3}{2}1^5 - \binom{3}{3}0^5\end{aligned}$$

e o número de funções parciais f sobrejetoras, cujo domínio de definição $D(f)$ é um subconjunto de X e cujo conjunto de valores $R(f)$ é um subconjunto de Y, é igual a 390:

$$\binom{5}{3}3! + \binom{5}{4}\left[3^4 - \binom{3}{1}2^4 + \binom{3}{2}1^4 - \binom{3}{3}0^4\right] + \binom{5}{5}\left[3^5 - \binom{3}{1}2^5 + \binom{3}{2}1^5 - \binom{3}{3}0^5\right],$$

pois existem $\binom{5}{3}$ possibilidades para a escolha do domínio de definição da função com três elementos, $\binom{5}{4}$ possibilidades para a escolha do domínio de definição da função com quatro elementos e $\binom{5}{5}$ possibilidades para a escolha do domínio de definição da função com cinco elementos.

2.5.1 O conjunto das funções injetoras e sobrejetoras em um conjunto finito

Para cada $n \in \mathbb{N} = \{1,2,\ldots\}$, sejam $X_n = \{1,2,\ldots,n\}$ e S_n o conjunto constituído pela totalidade das funções totais injetoras em X_n, que é igual ao conjunto de todas as funções sobrejetoras em X_n e que é igual ao conjunto constituído pela totalidade das funções injetoras e sobrejetoras em X_n.

O número de funções f injetoras e sobrejetoras no conjunto X_n é igual a $n! = n(n-1)\ldots 1$, porque existem n possibilidades para a definição do valor da função f em 1, existem $n-1$ possibilidades para a definição do valor da função f em 2 e assim por diante.

As funções de comprimento um $(1) = (2) = \ldots = (n)$ são todas iguais à função identidade no conjunto X_n.

Dados $i, j \in \{1,2,\ldots,n\}$, com $i \neq j$, a função transposição $(i\ j)$ ou a função ciclo de comprimento dois é definida por:

$$i \to j,$$

$$j \to i,$$

$$x \to x, \text{ para } x \in \{1,2,\ldots,n\}, x \neq i, x \neq j.$$

O número de funções ciclo de comprimento dois em S_n é igual a $\dfrac{n(n-1)}{2}$, porque, para $i \neq j$, $i, j \in \{1,2,\ldots,n\}$, $(i\ j) = (j\ i)$.

Dados $i, j, k \in \{1, 2, \ldots, n\}$, com i, j e k distintos dois a dois, a função ciclo de comprimento três $(i\ j\ k)$ é dada por:

$$i \to j$$

$$j \to k$$

$$k \to i$$

$$x \to x, \text{ para } x \in \{1, 2, \ldots, n\}, x \neq i, x \neq j, x \neq k.$$

As fórmulas abaixo são de verificação imediata:

(i) Para i, $j \in \{1, 2, \ldots, n\}$,

$$(i\ j) = (1\ i) \circ (1\ j) \circ (1\ i).$$

(ii) Para $j \in \{2, \ldots, n\}$

$$(1\ j) = (1\ j-1) \circ (j-1\ j) \circ (1\ j-1).$$

Por exemplo,

$$(1\ 3) = (1\ 2) \circ (2\ 3) \circ (1\ 2).$$

$$\begin{aligned}(1\ 4) &= (1\ 3) \circ (3\ 4) \circ (1\ 3) \\ &= \big[(1\ 2) \circ (2\ 3) \circ (1\ 2)\big] \circ (3\ 4) \circ \big[(1\ 2) \circ (2\ 3) \circ (1\ 2)\big].\end{aligned}$$

O número de funções ciclo de comprimento três em S_n é igual a $\dfrac{n(n-1)(n-2)}{3}$, porque, para i, j, $k \in \{1, 2, \ldots, n\}$, $(i\ j\ k) = (k\ i\ j) = (j\ k\ i)$.

Analogamente, são definidas as funções ciclo de comprimento quatro até comprimento n.

Para uma função ciclo $(a_1\ a_2\ \ldots\ a_k)$ de comprimento maior ou igual a três, em que $\{a_1, a_2, \ldots, a_k\} \subset \{1, 2, \ldots, n\}$,

$$(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_k) \circ \ldots \circ (a_1\ a_3) \circ (a_1\ a_2),$$

ou seja, uma função ciclo de comprimento k maior ou igual a três é composta de $k-1$ funções transposição.

Toda permutação $f \in S_n$, o conjunto das funções injetoras e sobrejetoras, cujo domínio de definição $D(f)$ e cujo conjunto de valores $R(f)$ é igual a $\{1, 2, \ldots, n\}$, é função composta de um número finito de funções ciclo. Por exemplo, se a matriz de valores de $f \in S_9$ é

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 7 & 1 & 8 & 3 & 5 & 6 & 2 \end{pmatrix},$$

então $f = (1\ 4) \circ (2\ 9) \circ (3\ 7\ 5\ 8\ 6)$.

Para dar resposta à questão "Quantas permutações do conjunto das permutações S_9 são da forma $(i\ j\ k\ l) \circ (m\ n) \circ (o\ p) \circ (q)$, em que as funções ciclo são duas a duas disjuntas?", basta efetuar o seguinte cálculo:

(i) 9 possibilidades para i, 8 para j, 7 para k e 6 para l, totalizando $\frac{9 \cdot 8 \cdot 7 \cdot 6}{4}$ possibilidades para $(i\ j\ k\ l)$.

(ii) 5 possibilidades para m, 4 para n, 3 para o e 2 para p, totalizando $\frac{1}{2!} \cdot \frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2}{2}$ possibilidades para $(m\ n) \circ (o\ p)$.

(iii) restando uma possibilidade para (q).

Portanto, a resposta à questão formulada é $\frac{9 \cdot 8 \cdot 7 \cdot 6}{4} \cdot \frac{1}{2!} \cdot \frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2}{2} \cdot 1$.

A resposta para a questão "Quantas permutações do conjunto das permutações S_9 são da forma $(i\ j\ k) \circ (m\ n\ o) \circ (p\ q\ r)$, em que as funções ciclo são duas a duas disjuntas?"é $\frac{1}{3!} \cdot \frac{9 \cdot 8 \cdot 7}{3} \cdot \frac{6 \cdot 5 \cdot 4}{3} \cdot \frac{3 \cdot 2 \cdot 1}{3}$.

As fórmulas abaixo de verificação imediata são válidas:

(i)
$$(2\ 3) = (1\ 2\ \ldots\ n)^{-1} \circ (1\ 2) \circ (1\ 2\ \ldots\ n).$$

(ii) Para cada $j \in \{1, 2, \ldots, n-1\}$,
$$(j\ j+1) = (1\ 2\ \ldots\ n)^{1-j} \circ (1\ 2) \circ (1\ 2\ \ldots\ n)^{j-1}.$$

(iii) Para cada $j \in \{2, 3, \ldots, n-1\}$,
$$(1\ j+1) = (j\ j+1) \circ (j-1\ j) \circ \ldots \circ (2\ 3) \circ (1\ 2) \circ (2\ 3) \circ \ldots \circ (j-1\ j) \circ (j\ j+1).$$

(iv) Para cada $i \in \{1, 2, \ldots, n-1\}$ e para cada $j \in \{1, 2, \ldots, n-i\}$,
$$(i\ i+j) = (1\ 2\ \ldots\ n)^{-i+1} \circ (1\ j+1) \circ (1\ 2\ \ldots\ n)^{i-1}.$$

Toda permutação no conjunto S_n é função composta de um número finito de transposições.

O número de Stirling de primeira espécie $s(n,k)$ para cada número natural n e para cada número natural $k \in \{0, 1, \ldots, n\}$ calcula o número de permutações em S_n expressas como função composta de k funções ciclo duas a duas disjuntas. Os números de Stirling de primeira espécie são definidos pela seguinte relação de recorrência:

$$s(n+1, k+1) = s(n,k) + ns(n, k+1)$$

sujeita às condições $s(n,0) = 0$ e $s(n,n) = 1$. De fato, a parcela $s(n,k)$ é devida ao fato da função ciclo de comprimento um, cujo único elemento é $n+1$, ocorrer na permutação e a parcela $ns(n,k+1)$ é devida ao fato da função ciclo $(n+1)$ de comprimento um não ocorrer na permutação: há n possibilidades para inserir o elemento $n+1$ em cada uma das $k+1$ funções ciclo de S_n duas a duas disjuntas.

A tabela abaixo mostra valores dos números de Stirling de primeira espécie para $n \in \{1,2,3,4,5,6\}$ e $k \in \{0,1,2,3,4,5,6\}$:

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$
$n=1$	0	1	0	0	0	0	0
$n=2$	0	1	1	0	0	0	0
$n=3$	0	2	3	1	0	0	0
$n=4$	0	6	11	6	1	0	0
$n=5$	0	24	50	35	10	1	0
$n=6$	0	120	274	225	85	15	1

Dada uma relação binária do conjunto $X_n = \{1,2,\ldots,n\}$, em que n é um número natural, o subconjunto de S_n constituído pelas permutações $f \in S_n$ compatíveis com a relação binária R no sentido de que, para i, $j \in \{1,2,\ldots,n\}$, se $(i,j) \in R$, então $(f(i),f(j)) \in R$ é um subconjunto fechado em relação à operação binária de composição de funções.

Exemplo 2.31.

Seja R a relação binária em $X_4 = \{1,2,3,4\}$ dada por $R = \{(1,4),(2,4),(3,4)\}$. Então, as seguintes permutações $f \in S_4$ são compatíveis com a relação binária R:

$$(1\ 2\ 3) \circ (4)$$

$$(1\ 3\ 2) \circ (4)$$

$$(1) \circ (2\ 3) \circ (4)$$

$$(2) \circ (1\ 3) \circ (4)$$

$$(3) \circ (1\ 2) \circ (4)$$

$$(1) \circ (2) \circ (3) \circ (4).$$

Exemplo 2.32.

Seja R a relação binária em $X_4 = \{1,2,3,4\}$ dada por $R = \{(1,2),(1,3),(2,1),(2,3),(3,4)\}$. Então, as seguintes permutações $f \in S_4$ são compatíveis com a relação binária R:

$$(1) \circ (2) \circ (3) \circ (4)$$

$$(1\ 2) \circ (3) \circ (4).$$

2.6 O conjunto das funções totais em um conjunto finito

Para cada $n \in \mathbb{N} = \{1,2,\ldots\}$, seja $X_n = \{1,2,\ldots,n\}$ e seja $T(X_n)$ o conjunto de todas as funções totais f em X_n.

Seja $f_{12} \in T(X_n)$ definida por:

$$f_{12}(1) = 2$$

$$f_{12}(x) = x, \text{ para } x \in \{2,3,\ldots,n\}.$$

Para i, $j \in \{1,2,\ldots,n\}$, define-se f_{ij} por

$$f_{ij}(i) = j$$

$$f_{ij}(x) = x, \text{ para } x \in \{1,2,\ldots,n\} \text{ e } x \neq i.$$

As fórmulas abaixo são de fácil verificação:

(i) Para $i \in \{3,4,\ldots,n\}$,

$$f_{i2} = (1\ i) \circ f_{12} \circ (1\ i).$$

(ii) Para $j \in \{3,4,\ldots,n\}$,

$$f_{1j} = (2\ j) \circ f_{12} \circ (2\ j).$$

(iii) Para i, $j \in \{3,4,\ldots,n\}$ e $i \neq j$,

$$f_{ij} = (1\ i) \circ (2\ j) \circ f_{12} \circ (2\ j) \circ (1\ i).$$

(iv) Para i, $j \in \{3,4,\ldots,n\}$ e $i \neq j$,

$$f_{ji} = (i\ j) \circ f_{ij} \circ (i\ j).$$

Seja $f \in T(X_n)$, cujo número de elementos do conjunto de valores $R(f)$ é menor ou igual a $n-1$ (se o número de elementos do conjunto de valores $R(f)$ é igual a n, então f é uma permutação em X_n). Então, existem i, $j \in \{1,2,\ldots,n\}$, com $i \neq j$, tal que $f(i) = f(j)$ e, para $k \in X_n \setminus R(f)$, considere $f_{ik} \in T(X_n)$. Portanto,

$$f = \widehat{f} \circ f_{ij},$$

em que $\widehat{f}$ é definida por:

$$\widehat{f}(i) = k$$

$$\widehat{f}(x) = f(x) \text{ para } x \in \{1,2,\ldots,n\} \text{ e } x \neq i.$$

Exemplo 2.33.

Seja $f \in T(X_4)$ cuja matriz de valores é $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 1 & 2 \end{pmatrix}$.

Como $3 \notin R(f)$, seja $\widehat{f}$ dada pela matriz de valores $\widehat{f} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$.

Portanto, $f = \widehat{f} \circ f_{23}$, em que $\widehat{f}$ é uma permutação em X_4 e

$$f_{23} = (1\ 2) \circ (2\ 3) \circ f_{12} \circ (2\ 3) \circ (1\ 2).$$

Exemplo 2.34.

Seja $f \in T(X_4)$ cuja matriz de valores é $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 1 & 1 \end{pmatrix}$.

Como $2 \notin R(f)$, seja $\widehat{f}$ dada pela matriz de valores $\widehat{f} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 1 \end{pmatrix}$.

Então, $f = \widehat{f} \circ f_{23} = \widehat{f} \circ f_{24}$.

Como $3 \notin R(\widehat{f})$, seja $\widehat{\widehat{f}}$ dada pela matriz de valores $\widehat{\widehat{f}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$.

Portanto, $\widehat{f} = \widehat{\widehat{f}} \circ f_{43}$ e

$$f = \widehat{f} \circ f_{23} = \widehat{\widehat{f}} \circ f_{43} \circ f_{23},$$

em que $\widehat{\widehat{f}}$ é uma permutação em X_4, e

$$f_{23} = (1\ 2) \circ (2\ 3) \circ f_{12} \circ (2\ 3) \circ (1\ 2)$$

$$f_{43} = (1\ 4) \circ (2\ 3) \circ f_{12} \circ (2\ 3) \circ (1\ 4).$$

Exemplo 2.35.

Seja $f \in T(X_4)$ cuja matriz de valores é $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 3 & 3 & 3 \end{pmatrix}$.

Como $1 \notin R(f)$, seja $\widehat{f}$ dada pela matriz de valores $\widehat{f} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 3 & 3 \end{pmatrix}$.

Então, $f = \widehat{f} \circ f_{21} = \widehat{f} \circ f_{23} = \widehat{f} \circ f_{24}$.

Como $2 \notin R(\widehat{f})$, seja $\widehat{\widehat{f}}$ dada pela matriz de valores $\widehat{\widehat{f}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 3 & 2 \end{pmatrix}$.

Então, $\widehat{f} = \widehat{\widehat{f}} \circ f_{43} = \widehat{\widehat{f}} \circ f_{41}$.

Como $4 \notin R(\widehat{\widehat{f}})$, seja $\widehat{\widehat{\widehat{f}}}$ dada pela matriz de valores $\widehat{\widehat{f}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$.

Então, $\widehat{\widehat{f}} = \widehat{\widehat{\widehat{f}}} \circ f_{13}$.

Portanto,

$$\begin{aligned} f &= \widehat{f} \circ f_{21} \\ &= \widehat{\widehat{f}} \circ f_{43} \circ f_{21} \\ &= \widehat{\widehat{\widehat{f}}} \circ f_{13} \circ f_{43} \circ f_{21}, \end{aligned}$$

em que $\widehat{\widehat{\widehat{f}}}$ é uma permutação em X_4, e

$$f_{21} = (1\ 2) \circ (2\ 1) \circ f_{12} \circ (2\ 1) \circ (1\ 2)$$

$$f_{43} = (1\ 4) \circ (2\ 3) \circ f_{12} \circ (2\ 3) \circ (1\ 4)$$

$$f_{13} = (2\ 3) \circ f_{12} \circ (2\ 3).$$

Em vista dos exemplos acima, toda função total $f \in T(X_n)$ é expressa como função composta de um número finito de funções, todas elas pertencentes ao conjunto das transposições ou igual à função total f_{12}.

2.7 O conjunto das funções parciais em um conjunto finito

Para cada $n \in \mathbb{N} = \{1,2,\ldots\}$, seja $X_n = \{1,2,\ldots,n\}$ e seja $P(X_n)$ o conjunto de todas as funções parciais f em X_n, ou seja, funções cujo domínio de definição e cujo conjunto de valores são ambos subconjuntos de X_n.

Para cada subconjunto A de X_n, seja a função $f_A \in P(X_n)$ definida como uma inclusão $i_{X_n \setminus A}$ do subconjunto complementar $X_n \setminus A$. Por exemplo, $f_{\{1\}}$ tem como matriz de valores

$$\begin{pmatrix} 2 & 3 & \ldots & n \\ 2 & 3 & \ldots & n \end{pmatrix},$$

o que significa que

$$f_{\{1\}}(2) = 2$$

$$f_{\{1\}}(3) = 3$$

$$\ldots$$

$$f_{\{1\}}(n) = n$$

e que 1 não pertence ao domínio da função $f_{\{1\}}$.

A fórmula seguinte é de fácil verificação:

Para cada $i \in \{2,3,\ldots,n\}$,

$$f_{\{i\}} = (1\ i) \circ f_{\{1\}} \circ (1\ i).$$

A função, $\tilde{f}$ chamada completamento da função parcial f em X_n, é definida por:

$$\tilde{f}(x) = \begin{cases} f(x), & \text{se } x \in D(f) \\ x, & \text{se } x \in Y = X_n \setminus D(f) \end{cases}$$

e se relaciona com a função f pela fórmula

$$f = \tilde{f} \circ f_Y$$

em que, por exemplo, se $Y = \{1,2\}$, $f_Y = f_{\{1\}} \circ f_{\{2\}}$.

Exemplo 2.36.

Seja $f \in T(X_4)$ cuja matriz de valores é $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & - & 3 \end{pmatrix}$, o que significa que

$$f(1) = 2$$

$$f(2) = 1$$

$$3 \notin D(f)$$

$$f(4) = 3.$$

Seja $\tilde{f}$ dada pela matriz de valores $\tilde{f} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 3 & 4 \end{pmatrix}$.

Então, $f = \tilde{f} \circ f_Y$, com $Y = \{3\}$, ou seja, $f = \tilde{f} \circ f_{\{3\}}$, em que $\tilde{f}$ é uma função total em X_4 e $f_{\{3\}} = (1\ 3) \circ f_{\{1\}} \circ (1\ 3)$.

Exemplo 2.37.

Seja $f \in T(X_4)$ cuja matriz de valores é $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ - & 1 & 4 & - \end{pmatrix}$, o que significa que

$$1 \notin D(f)$$

$$f(2) = 1$$

$$f(3) = 4$$

$$4 \notin D(f).$$

Seja $\tilde{f}$ dada pela matriz de valores $\tilde{f} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 4 & 4 \end{pmatrix}$.

Então, $f = \tilde{f} \circ f_Y$, com $Y = \{1,4\}$, ou seja, $f = \tilde{f} \circ f_{\{1\}} \circ f_{\{4\}} = \tilde{f} \circ f_{\{4\}} \circ f_{\{1\}}$, em que $\tilde{f}$ é uma função total em X_4 e $f_{\{4\}} = (1\ 4) \circ f_{\{1\}} \circ (1\ 4)$.

Exemplo 2.38.

Seja $f \in T(X_4)$ cuja matriz de valores é $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ - & 3 & - & - \end{pmatrix}$, o que significa que

$$1 \notin D(f)$$

$$f(2) = 3$$

$$3 \notin D(f)$$

$$4 \notin D(f).$$

Seja $\tilde{f}$ dada pela matriz de valores $\tilde{f} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 3 & 4 \end{pmatrix}$.

Então, $f = \tilde{f} \circ f_Y$, com $Y = \{1,3,4\}$, ou seja, $f = \tilde{f} \circ f_{\{1\}} \circ f_{\{3\}} \circ f_{\{4\}}$, em que $\tilde{f}$ é uma função total em X_4, $f_{\{3\}} = (1\ 3) \circ f_{\{1\}} \circ (1\ 3)$ e $f_{\{4\}} = (1\ 4) \circ f_{\{1\}} \circ (1\ 4)$.

Em vista dos exemplos anteriores, toda função parcial f em $P(X_n)$ é função composta de um número finito de funções, todas elas pertencentes ao conjunto das transposições ou igual à f_{12} ou igual a $f_{\{1\}}$.

CAPÍTULO

3

OPERAÇÕES BINÁRIAS BOOLEANAS

Uma operação binária interna booleana no conjunto $\{0,1\}$ é uma função μ, cujo domínio de definição é o conjunto $\{0,1\} \times \{0,1\}$ constituído pelos quatro pares ordenados $(0,0),(0,1),(1,0)$ e $(1,1)$, com valores no conjunto $\{0,1\}$.

Existem dezesseis operações binárias internas booleanas $\mu_0, \mu_1, \ldots, \mu_{15}$ no conjunto $\{0,1\}$ constituído pelos dígitos 0 e 1 cujas tabelas de valores são:

x	y	$\mu_0(x,y)$	$\mu_1(x,y)$	$\mu_2(x,y)$	$\mu_3(x,y)$	...	$\mu_{15}(x,y)$
1	1	0	0	0	0		1
1	0	0	0	0	0		1
0	1	0	0	1	1		1
0	0	0	1	0	1		1

A numeração das operações binárias internas booleanas no conjunto $\{0,1\}$ é feita de acordo com a representação binária do índice da operação binária interna. Por exemplo, as tabelas de valores de μ_{11} e μ_{12} são

x	y	$\mu_{11}(x,y)$	$\mu_{12}(x,y)$
1	1	1	1
1	0	0	1
0	1	1	0
0	0	1	0

Isso acontece devido à representação binária do número 11 ser 1011, o que significa que $11 = 1.2^3 + 0.2^2 + 1.2^1 + 1.2^0$, e à representação binária do número 12 ser 1100, o que significa que $12 = 1.2^3 + 1.2^2 + 0.2^1 + 0.2^0$.

A operação binária interna booleana OR, indicada pelo símbolo $\vee$, é definida pela tabela de valores abaixo:

x	y	$x \vee y$
1	1	1
1	0	1
0	1	1
0	0	0

que é a tabela de valores da operação binária interna booleana μ_{14}: para x, $y \in \{0,1\}$, $\mu_{14}(x,y) = x \vee y$ (0 é o elemento neutro da operação binária interna booleana OR e 1 é o elemento zero da operação binária interna booleana OR, no sentido que $0 \vee 1 = 1$ e $1 \vee 1 = 1$).

A operação binária interna booleana AND, indicada pelo símbolo $\wedge$, é definida pela tabela de valores abaixo:

x	y	$x \wedge y$
1	1	1
1	0	0
0	1	0
0	0	0

que é a tabela de valores da operação binária interna booleana μ_8: para x, $y \in \{0,1\}$, $\mu_8(x,y) = x \wedge y$ (1 é o elemento neutro da operação binária interna booleana AND e 0 é o elemento zero da operação binária interna booleana AND, no sentido que $0 \wedge 1 = 0$ e $0 \wedge 0 = 0$).

A operação binária interna booleana XOR, indicada pelo símbolo $\oplus$, é definida pela tabela de valores abaixo:

x	y	$x \oplus y$
1	1	0
1	0	1
0	1	1
0	0	0

que é a tabela de valores da operação binária interna booleana μ_6: para x, $y \in \{0,1\}$, $\mu_6(x,y) = x \oplus y$ (0 é o elemento neutro da operação binária interna booleana XOR e não existe o elemento zero da operação binária interna booleana XOR, no sentido que $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$ e $1 \oplus 1 = 0$).

A dificuldade está em saber, das dezesseis operações binárias internas booleanas μ no conjunto $\{0,1\}$, quais tem a propriedade associativa, isto é, quais destas operações são tais que a igualdade

$$\mu\left[x, \mu(y,z)\right] = \mu\left[\mu(x,y), z\right]$$

é válida para os oito valores possíveis dos elementos x, y e z pertencentes a $\{0,1\}$.

O método exaustivo para o reconhecimento das operações binárias internas booleanas associativas μ no conjunto $\{0,1\}$ é a construção da tabela abaixo:

x	y	z	$\mu(x,y)$	$\mu(y,z)$	$\mu(x,\mu(y,z))$	$\mu(\mu(x,y),z)$
1	1	1	$\mu(1,1)$	$\mu(1,1)$	$\mu[1,\mu(1,1)]$	$\mu[\mu(1,1),1]$
1	1	0	$\mu(1,1)$	$\mu(1,0)$	$\mu[1,\mu(1,0)]$	$\mu[\mu(1,1),0]$
1	0	1	$\mu(1,0)$	$\mu(0,1)$	$\mu[1,\mu(0,1)]$	$\mu[\mu(1,0),1]$
1	0	0	$\mu(1,0)$	$\mu(0,0)$	$\mu[1,\mu(0,0)]$	$\mu[\mu(1,0),0]$
0	1	1	$\mu(0,1)$	$\mu(1,1)$	$\mu[0,\mu(1,1)]$	$\mu[\mu(0,1),1]$
0	1	0	$\mu(0,1)$	$\mu(1,0)$	$\mu[0,\mu(1,0)]$	$\mu[\mu(0,1),0]$
0	0	1	$\mu(0,0)$	$\mu(0,1)$	$\mu[0,\mu(0,1)]$	$\mu[\mu(0,0),1]$
0	0	0	$\mu(0,0)$	$\mu(0,0)$	$\mu[0,\mu(0,0)]$	$\mu[\mu(0,0),0]$

e a verificação dos valores apresentados nas últimas duas colunas: caso as duas últimas colunas apresentem os mesmos valores em cada linha, μ é associativa e, caso contrário, μ não é associativa.

3.1 Teste Light de associatividade de operações binárias internas em um conjunto finito

Seja X um conjunto finito com n elementos. Cada enumeração dos elementos de X define uma correspondência biunívoca entre os elementos de X e os índices 1, 2, ..., n da enumeração.

Operações binárias internas definidas no conjunto de índices $\{1,2,\ldots,n\}$ induzem operações binárias internas no conjunto X de n elementos.

Há $(n^2)^n$ operações binárias internas em $\{1,2,\ldots,n\}$, pois, para cada par ordenado (i,j), com $i, j \in \{1,2,\ldots,n\}$, existem n possíveis valores para o valor da operação binária interna em (i,j).

Definida uma operação binária interna μ em $\{1,2,\ldots,n\}$, a fim de demonstrar a associatividade de μ, é preciso calcular $\mu\big[i,\mu(j,k)\big]$ e $\mu\big[\mu(i,j),k\big]$, para cada $i, j, k \in \{1,2,\ldots,n\}$, e mostrar que estes dois valores são os mesmos. Para tal, o teste Light de associatividade propõe escrever, para cada $j \in \{1,2,\ldots,n\}$, duas tabelas.

A primeira tabela a ser construída é

	$\mu(j,1)$	$\mu(j,2)$	$\ldots$	$\mu(j,i)$	$\ldots$	$\mu(j,j)$	$\ldots$	$\mu(j,k)$	$\ldots$	$\mu(j,n)$
1										
2										
$\vdots$										
i								$\mu\left[i,\mu(j,k)\right]$		
$\vdots$										
j										
$\vdots$										
k										
$\vdots$										
n										

e registrar o valor $\mu\left[i,\mu(j,k)\right]$ na intersecção da linha i e da coluna k genéricas.

A segunda tabela a ser construída é

	1	2	$\ldots$	i	$\ldots$	j	$\ldots$	k	$\ldots$	n
$\mu(1,j)$										
$\mu(2,j)$										
$\vdots$										
$\mu(i,j)$								$\mu\left[\mu(i,j),k\right]$		
$\vdots$										
$\mu(j,j)$										
$\vdots$										
$\mu(k,j)$										
$\vdots$										
$\mu(n,j)$										

e registrar o valor $\mu\left[\mu(i,j),k\right]$ na intersecção da linha i e da coluna k genéricas.

Como, para cada índice $\{1,2,\ldots,n\}$, as duas tabelas construídas para o elemento j apresentam os mesmos valores, a associatividade da operação binária interna μ é provada.

Na hipótese de, para um particular índice $j \in \{1,2,\ldots,n\}$, as duas tabelas construídas para o elemento j não apresentarem os mesmos valores, a operação binária interna μ não é associativa em $\{1,2,\ldots,n\}$.

O teste Light de associatividade de uma operação binária interna μ em $\{1,2,\ldots,n\}$ é ilustrado pelos exemplos a seguir.

Exemplo 3.1.

Seja μ a operação binária interna em $\{1,2,3,4\}$ dada pela tabela de Cayley abaixo:

	1	**2**	**3**	**4**
1	1	2	3	4
2	2	1	3	4
3	3	4	3	4
4	4	3	3	4

Pelo teste Light de associatividade,

(i) as duas tabelas de Cayley construídas para o elemento 1 são:

	$\mu(1,1)=1$	$\mu(1,2)=2$	$\mu(1,3)=3$	$\mu(1,4)=4$
1	1	2	3	4
2	2	1	3	4
3	3	4	3	4
4	4	3	3	4

	1	2	3	4
$\mu(1,1)=1$	1	2	3	4
$\mu(2,1)=2$	2	1	3	4
$\mu(3,1)=3$	3	4	3	4
$\mu(4,1)=4$	4	3	3	4

(ii) as duas tabelas de Cayley construídas para o elemento 2 são:

	$\mu(2,1)=2$	$\mu(2,2)=1$	$\mu(2,3)=3$	$\mu(2,4)=4$
1	2	1	3	4
2	1	2	3	4
3	4	3	3	4
4	3	4	3	4

	1	2	3	4
$\mu(1,2)=2$	2	1	3	4
$\mu(2,2)=1$	1	2	3	4
$\mu(3,2)=3$	4	3	3	4
$\mu(4,2)=4$	3	4	3	4

(iii) as duas tabelas de Cayley construídas para o elemento 3 são:

	$\mu(3,1)=3$	$\mu(3,2)=4$	$\mu(3,3)=3$	$\mu(3,4)=4$
1	3	4	3	4
2	3	4	3	4
3	3	4	3	4
4	3	4	3	4

	1	2	3	4
$\mu(1,3)=3$	3	4	3	4
$\mu(2,3)=3$	3	4	3	4
$\mu(3,3)=3$	3	4	3	4
$\mu(4,3)=3$	3	4	3	4

(iv) as duas tabelas de Cayley construídas para o elemento 4 são:

	$\mu(4,1)=4$	$\mu(4,2)=3$	$\mu(4,3)=3$	$\mu(4,4)=4$
1	4	4	3	4
2	4	3	3	4
3	4	3	3	4
4	4	3	3	4

	1	2	3	4
$\mu(1,4)=4$	4	3	3	4
$\mu(2,4)=4$	4	3	3	4
$\mu(3,4)=4$	4	3	3	4
$\mu(4,4)=4$	4	3	3	4

Como as duas tabelas de Cayley construídas para o elemento 1, para o elemento 2, para o elemento 3 e para o elemento 4 apresentam os mesmos valores, μ é uma operação binária interna associativa em $\{1,2,3,4\}$.

Exemplo 3.2.

Seja μ a operação binária interna definida em $\{1,2,3\}$ pela tabela de Cayley:

	1	**2**	**3**
1	2	1	1
2	3	1	2
3	1	2	2

Pelo teste Light de associatividade, as duas tabelas de Cayley a serem construídas para o elemento 1 são:

	$\mu(1,1)=2$	$\mu(1,2)=1$	$\mu(1,3)=1$
1	1	2	2
2	1	3	3
3	2	1	1

	1	2	3
$\mu(1,1)=2$	3	1	2
$\mu(2,1)=3$	1	2	2
$\mu(3,1)=1$	2	1	1

e estas duas tabelas já demonstram a não associatividade da operação binária interna μ em $\{1,2,3\}$, pois:

$$\mu\big[1,\mu(1,1)\big] = 1 \neq 3 = \mu\big[\mu(1,1),1\big]$$
$$\mu\big[1,\mu(1,2)\big] = 2 \neq 1 = \mu\big[\mu(1,1),2\big]$$
$$\mu\big[2,\mu(1,2)\big] = 3 \neq 2 = \mu\big[\mu(2,1),2\big]$$
$$\mu\big[2,\mu(1,3)\big] = 3 \neq 2 = \mu\big[\mu(2,1),3\big].$$

O teste Light de associatividade determina, em particular, a associatividade de operações binárias internas booleanas μ no conjunto $\{0,1\}$ sempre que μ admite a existência do elemento neutro $e \in \{0,1\}$, ou seja, para cada $x \in \{0,1\}$,

$$\mu(x,e) = \mu(e,x) = x,$$

porque nos casos particulares

$$\begin{aligned} \text{em que } x = e, \text{ vem que } \mu\big[x,\mu(y,z)\big] &= \mu(y,z) \\ \mu\big[\mu(x,y),z\big] &= \mu(y,z), \end{aligned}$$

$$\begin{aligned} \text{em que } y = e, \text{ vem que } \mu\big[x,\mu(y,z)\big] &= \mu(x,z) \\ \mu\big[\mu(x,y),z\big] &= \mu(x,z), \end{aligned}$$

$$\begin{aligned} \text{em que } z = e, \text{ vem que } \mu\big[x,\mu(y,z)\big] &= \mu(x,y) \\ \mu\big[\mu(x,y),z\big] &= \mu(x,y), \end{aligned}$$

a igualdade descrita na definição de associatividade é sempre verificada.

As tabelas de Cayley necessárias para a verificação da associatividade da operação binária interna booleana OR são as tabelas abaixo construídas para o elemento 1, visto que o elemento 0 é elemento neutro desta operação:

$\vee$	$1\vee 0 = 1$	$1\vee 1 = 1$
0	1	1
1	1	1

$\vee$	0	1
$0\vee 1 = 1$	1	1
$1\vee 1 = 1$	1	1

Como as tabelas apresentam os mesmos valores, a operação binária interna booleana OR tem a propriedade associativa no conjunto $\{0,1\}$ e o valor

$$x \vee y \vee z = (x \vee y) \vee z = x \vee (y \vee z)$$

é bem definido para x, y, $z \in \{0,1\}$.

As tabelas de Cayley necessárias para a verificação da associatividade da operação binária interna booleana AND são as tabelas abaixo construídas para o elemento 0, visto que o elemento 1 é elemento neutro da operação:

$\wedge$	$0\wedge 0=0$	$0\wedge 1=0$
0	0	0
1	0	0

$\wedge$	0	1
$0\wedge 0=0$	0	0
$1\wedge 0=0$	0	0

Como as tabelas apresentam os mesmos valores, a operação binária interna booleana AND tem a propriedade associativa no conjunto $\{0,1\}$ e o valor

$$x\wedge y\wedge z=(x\wedge y)\wedge z=x\wedge(y\wedge z)$$

é bem definido para x, y, $z\in\{0,1\}$.

As tabelas de Cayley necessárias para a verificação da associatividade da operação binária interna booleana XOR são as tabelas abaixo construídas para o elemento 1, visto que o elemento 0 é elemento neutro da operação:

$\oplus$	$1\oplus 0=1$	$1\oplus 1=1$
0	1	0
1	0	1

$\oplus$	0	1
$0\oplus 1=1$	1	0
$1\oplus 1=0$	0	1

Como as tabelas apresentam os mesmos valores, a operação binária interna booleana XOR tem a propriedade associativa no conjunto $\{0,1\}$ e o valor

$$x\oplus y\oplus z=(x\oplus y)\oplus z=x\oplus(y\oplus z)$$

é bem definido para x, y, $z\in\{0,1\}$.

As operações internas binárias booleanas NOTOR $(\overline{\vee})$, NOTAND $(\overline{\wedge})$ e implicação $(\rightarrow)$ definidas por suas respectivas tabelas de Cayley

$(\overline{\vee})$	0	1
0	1	0
1	0	0

$(\overline{\wedge})$	0	1
0	1	1
1	1	0

$\rightarrow$	0	1
0	1	1
1	0	1

ou por suas respectivas tabelas de valores

x	y	$x\,\overline{\vee}\,y=\mu_1(x,y)$	$x\,\overline{\wedge}\,y=\mu_7(x,y)$	$x\rightarrow y=\mu_{11}(x,y)$
1	1	0	0	1
1	0	0	1	0
0	1	0	1	1
0	0	1	1	1

não tem a propriedade associativa e nem a propriedade de existência do elemento neutro, pois, pelo teste Light de associatividade, as duas tabelas de Cayley construídas para o elemento 0 não apresentam os mesmos valores para a operação NOTOR:

$\overline{\vee}$	$0\overline{\vee}0=1$	$0\overline{\vee}1=0$
0	0	1
1	0	0

$\overline{\vee}$	0	1
$0\overline{\vee}0=1$	0	0
$1\overline{\vee}0=0$	1	0

O mesmo vale para as duas tabelas de Cayley construídas para o elemento 1:

$\overline{\vee}$	$1\overline{\vee}0=0$	$1\overline{\vee}1=0$
0	1	1
1	0	0

$\overline{\vee}$	0	1
$0\overline{\vee}1=0$	1	0
$1\overline{\vee}1=0$	1	0

Portanto, conclui-se que:

$$0\overline{\vee}(0\overline{\vee}1)=1\neq 0=(0\overline{\vee}0)\overline{\vee}1$$

$$1\overline{\vee}(0\overline{\vee}0)=0\neq 1=(1\overline{\vee}0)\overline{\vee}0$$

$$0\overline{\vee}(1\overline{\vee}1)=1\neq 0=(0\overline{\vee}1)\overline{\vee}1$$

$$1\overline{\vee}(1\overline{\vee}0)=0\neq 1=(1\overline{\vee}1)\overline{\vee}0.$$

Analogamente, as duas tabelas de Cayley construídas para o elemento 0 não apresentam os mesmos valores para a operação NOTAND:

$\overline{\wedge}$	$0\overline{\wedge}0=1$	$0\overline{\wedge}1=0$
0	1	1
1	0	0

$\overline{\wedge}$	0	1
$0\overline{\wedge}0=1$	1	0
$1\overline{\wedge}0=1$	1	0

O mesmo vale para as duas tabelas de Cayley construídas para o elemento 1:

$\overline{\wedge}$	$1\overline{\wedge}0=1$	$1\overline{\wedge}1=0$
0	1	1
1	0	1

$\overline{\wedge}$	0	1
$0\overline{\wedge}1=1$	1	0
$1\overline{\wedge}1=0$	1	1

Portanto, conclui-se que:

$$0\overline{\wedge}(0\overline{\wedge}1)=1\neq 0=(0\overline{\wedge}0)\overline{\wedge}1$$

$$1\overline{\wedge}(0\overline{\wedge}0)=0\neq 1=(1\overline{\wedge}0)\overline{\wedge}0$$

$$0\overline{\wedge}(1\overline{\wedge}1)=1\neq 0=(0\overline{\wedge}1)\overline{\wedge}1$$

$$1 \overline{\wedge} (1 \overline{\wedge} 0) = 0 \neq 1 = (1 \overline{\wedge} 1) \overline{\wedge} 0.$$

Da mesma forma, as duas tabelas de Cayley construídas para o elemento 0 não apresentam os mesmos valores para a operação implicação:

$\rightarrow$	$0 \rightarrow 0 = 1$	$0 \rightarrow 1 = 1$
0	1	1
1	1	1

$\rightarrow$	0	1
$0 \rightarrow 0 = 1$	0	1
$1 \rightarrow 0 = 0$	1	1

O mesmo vale para as duas tabelas de Cayley construídas para o elemento 1:

$\rightarrow$	$1 \rightarrow 0 = 0$	$1 \rightarrow 1 = 1$
0	1	1
1	0	1

$\rightarrow$	0	1
$0 \rightarrow 1 = 1$	0	1
$1 \rightarrow 1 = 1$	0	1

Portanto, conclui-se que:

$$0 \rightarrow (0 \rightarrow 0) = 1 \neq 0 = (0 \rightarrow 0) \rightarrow 0$$

$$0 \rightarrow (1 \rightarrow 0) = 1 \neq 0 = (0 \rightarrow 1) \rightarrow 0$$

$$1 \rightarrow (1 \rightarrow 0) = 0 \neq 1 = (1 \rightarrow 1) \rightarrow 0.$$

3.2 Funções booleanas de uma variável

As quatro $(4 = 2^2 = 2^{2^1})$ funções booleanas de uma variável são dadas pelas tabelas de valores abaixo:

x	$f_0(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$
1	0	0	1	1
0	0	1	0	1

A numeração das funções booleanas de uma variável é dada de acordo com a representação binária do índice. Por exemplo, $f_2(1) = 1$, $f_2(0) = 0$ e $10 = 1.2^1 + 0.2^0 = 2$ é a representação binária do índice 2.

A função booleana f_1 de uma variável é a conhecida operação monária de inversão no conjunto $\{0,1\}$: $f_1(0) = \overline{0} = 1$ e $f_1(1) = \overline{1} = 0$, ou seja, $f_1(x) = \overline{x}$, para $x \in \{0,1\}$.

A função booleana f_2 de uma variável é a função identidade em $\{0,1\}$: $f_2(0) = 0$ e $f_2(1) = 1$, isto é, $f_2(x) = x$, para $x \in \{0,1\}$.

A função booleana f_3 de uma variável tem por fórmula $f_3(x) = x \vee \overline{x}$, para $x \in \{0,1\}$, enquanto que a função booleana f_0 de uma variável tem por fórmula $f_0(x) = x \wedge \overline{x}$, para $x \in \{0,1\}$.

3.3 Funções booleanas de duas variáveis

As dezesseis $(16 = 2^4 = 2^{2^2})$ funções booleanas de duas variáveis são definidas pelas tabelas de valores abaixo:

x	y	$f_0(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	...	$f_{15}(x)$
1	1	0	0	0	0		1
1	0	0	0	0	0		1
0	1	0	0	1	1		1
0	0	0	1	0	1		1

e as funções booleanas de duas variáveis e operações binárias internas booleanas são sinônimos.

As operações binárias internas booleanas no conjunto $\{0,1\}$ induzem operações binárias internas no conjunto das funções booleanas de duas variáveis: as operações binárias internas OR $(\vee)$, AND $(\wedge)$ e XOR $(\oplus)$ são definidas para funções booleanas de duas variáveis, ou seja, se f e g são funções booleanas de duas variáveis, $f \vee g$, $f \wedge g$ e $f \oplus g$ são funções booleanas definidas por

$$(f \vee g)(x,y) = f(x,y) \vee g(x,y)$$

$$(f \wedge g)(x,y) = f(x,y) \wedge g(x,y)$$

$$(f \oplus g)(x,y) = f(x,y) \oplus g(x,y)$$

e, em geral, se μ é uma operação binária interna booleana no conjunto $\{0,1\}$, então, com abuso de notação, para funções booleanas f e g, a função booleana $\mu(f,g)$ é definida por:

$$\big[\mu(f,g)\big](x,y) = \mu\big[f(x,y), g(x,y)\big], \text{para } x, y \in \{0,1\}.$$

Além disso, para x, $y \in \{0,1\}$,

$$f_1(x,y) = \overline{x} \wedge \overline{y}$$

$$f_2(x,y) = \overline{x} \wedge y$$

$$f_3(x,y) = (\overline{x} \wedge \overline{y}) \vee (\overline{x} \wedge y)$$

$$\ldots$$

$$f_{12}(x,y) = (x \wedge \overline{y}) \vee (x \wedge y)$$

$$\ldots$$

$$f_{15}(x,y) = \overline{x} \wedge \overline{y} \vee (\overline{x} \wedge y) \vee (x \wedge \overline{y}) \vee (x \wedge y).$$

As funções booleanas f_0, f_1, ..., f_{15} de duas variáveis também podem ser definidas por mapas de Karnaugh.

O mapa de Karnaugh, formado por 2^n células, sendo n o número de variáveis, é uma tabela montada para a minimização de funções booleanas e permitem a simplificação de funções de duas, três, quatro ou mais variáveis.

Definição 3.3.

Duas células são adjacentes entre si quando apenas uma de suas variáveis muda de valor. Por exemplo, as células $xy = 00$ e $xy = 01$ são adjacentes, pois apenas y muda de valor. Já as células $xy = 01$ e $xy = 10$ não são adjacentes, pois x e y mudam de valor.

Definição 3.4.

Enlace é o agrupamento de células adjacentes, com valores iguais, do qual se pode extrair diretamente uma expressão booleana simplificada, já que a variável que muda de valor desaparece.

Se o valor considerado no mapa de Karnaugh for igual a 1, cada enlace é dado pela operação AND entre as variáveis que não mudam de valor e a operação entre os enlaces é dada pela operação OR. Esta é a chamada forma disjuntiva normal da função booleana.

Se o valor considerado no mapa de Karnaugh for igual a 0, cada enlace é dado pela operação OR entre as variáveis que não mudam de valor e a operação entre os enlaces é dada pela operação AND. Esta é a chamada forma conjuntiva normal da função booleana.

Exemplo 3.5.

Em um primeiro exemplo, seja f a função booleana de duas variáveis definida por: $f(x,y) = (x \wedge \overline{y}) \vee (\overline{x} \wedge y)$, para x, $y \in \{0,1\}$. Dessa forma, o mapa de Karnaugh de f é dado abaixo:

	y	$\overline{y}$
x	0	1
$\overline{x}$	1	0

Agora, em um segundo exemplo, seja g a função booleana de duas variáveis definida pelo mapa de Karnaugh abaixo:

	y	$\overline{y}$
x	1	1
$\overline{x}$	1	0

Assim, a função booleana g pode ser escrita, para $x, y \in \{0,1\}$, como:

$$\begin{aligned} g(x,y) &= (x \wedge y) \vee (x \wedge \overline{y}) \vee (\overline{x} \wedge y) \\ &= \left[x \wedge (y \vee \overline{y})\right] \vee (\overline{x} \wedge y) \\ &= x \vee (\overline{x} \wedge y) \end{aligned}$$

ou como:

$$\begin{aligned} g(x,y) &= (x \wedge y) \vee (\overline{x} \wedge y) \vee (x \wedge \overline{y}) \\ &= \left[y \wedge (x \vee \overline{x})\right] \vee (x \wedge \overline{y}) \\ &= y \vee (x \wedge \overline{y}). \end{aligned}$$

Exemplo 3.6.

A tabela de valores e o mapa de Karnaugh da função booleana f_6, respectivamente representados por

x	y	$f_6(x,y)$
1	1	0
1	0	1
0	1	1
0	0	0

	$\overline{y}$	y
$\overline{x}$	0	1
x	1	0

indicam que a função booleana f_6 é dada pela sua forma disjuntiva normal

$$f_6(x,y) = (\overline{x} \wedge y) \vee (x \wedge \overline{y}), \text{para } x, y \in \{0,1\}$$

e pela sua forma conjuntiva normal

$$f_6(x,y) = (x \vee y) \wedge (\overline{x} \vee \overline{y}), \text{para } x, y \in \{0,1\}.$$

Da mesma forma, a tabela de valores e o mapa de Karnaugh da função booleana f_9, respectivamente representados por

x	y	$f_9(x,y)$
1	1	1
1	0	0
0	1	0
0	0	1

	$\overline{y}$	y
$\overline{x}$	1	0
x	0	1

indicam que a função booleana f_9 é dada pela sua forma disjuntiva normal

$$f_9(x,y) = (\overline{x} \wedge \overline{y}) \vee (x \wedge y), \text{para } x, y \in \{0,1\}$$

e pela sua forma conjuntiva normal

$$f_9(x,y) = (x \vee \overline{y}) \wedge (\overline{x} \vee y), \text{para } x, y \in \{0,1\}.$$

Por simplicidade de notação, a operação binária OR pode ser indicada pela operação binária booleana de adição $+$ e a operação binária AND, por sua vez, pode ser indicada pela operação binária booleana de multiplicação, ou seja, para $x, y \in \{0,1\}$:

$$x + y = x \vee y$$

$$xy = x \wedge y.$$

Exemplo 3.7.

A tabela de valores e o mapa de Karnaugh da função booleana f_7, respectivamente representados por

x	y	$f_7(x,y)$
1	1	0
1	0	1
0	1	1
0	0	1

	$\overline{y}$	y
$\overline{x}$	1	1
x	1	0

indicam que a função booleana f_7 é dada pela sua forma disjuntiva normal

$$f_7(x,y) = \overline{x}\overline{y} + \overline{x}y + x\overline{y}, \text{para } x, y \in \{0,1\},$$

e pela sua forma conjuntiva normal

$$f_7(x,y) = x + y, \text{para } x, y \in \{0,1\}.$$

De maneira similar, a tabela de valores e o mapa de Karnaugh da função booleana f_{12}, respectivamente representados por

x	y	$f_{12}(x,y)$
1	1	1
1	0	1
0	1	0
0	0	0

	$\overline{y}$	y
$\overline{x}$	0	0
x	1	1

indicam que a função booleana f_{12} é dada pela sua forma disjuntiva normal

$$f_{12}(x,y) = x\overline{y} + xy, \text{para } x, y \in \{0,1\},$$

e pela sua forma conjuntiva normal

$$f_{12}(x,y) = (\overline{x}+\overline{y})(\overline{x}+y), \text{para } x, y \in \{0,1\}.$$

De maneira análoga, são definidas as funções soma $f+g = f \vee g$, produto $fg = f \wedge g$ e a função $f \oplus g$ quando f e g são funções booleanas de três ou mais variáveis.

As funções booleanas de duas variáveis f_1, f_2, f_4 e f_8, respectivamente iguais a μ_1, μ_2, μ_4 e μ_8, são particularmente importantes, pois suas tabelas de valores apresentam um único valor igual a um.

Além disso, para cada $x, y \in \{0,1\}$,

$$p_1(x,y) = \overline{x} \wedge \overline{y} = \overline{xy}$$

$$p_2(x,y) = \overline{x} \wedge y = \overline{x}y$$

$$p_4(x,y) = x \wedge \overline{y} = x\overline{y}$$

$$p_8(x,y) = x \wedge y = xy$$

e suas tabelas de valores são

x	y	$\overline{xy}$	$\overline{x}y$	$x\overline{y}$	xy
1	1	0	0	0	1
1	0	0	0	1	0
0	1	0	1	0	0
0	0	1	0	0	0

Cada função booleana de duas variáveis é soma das funções booleanas p_1, p_2, p_4 e p_8 com coeficientes em $\{0,1\}$, como se observa no exemplo a seguir.

Exemplo 3.8.

As funções μ_{11} e μ_{12} são escritas da seguinte forma:

$$\begin{aligned}\mu_{11} &= 1.p_8(x,y) + 0.p_4(x,y) + 1.p_2(x,y) + 1.p_1(x,y)\\ &= xy + \overline{x}y + \overline{xy}.\end{aligned}$$

$$\begin{aligned}\mu_{12} &= 1.p_8(x,y) + 1.p_4(x,y) + 0.p_2(x,y) + 0.p_1(x,y)\\ &= xy + x\overline{y}.\end{aligned}$$

Por um processo dual, definem-se as funções booleanas de duas variáveis cujas tabelas de valores apresentam um único valor igual a zero. Dessa forma, para cada $x, y \in \{0,1\}$,

$$s_1(x,y) = x \vee y = x + y$$

$$s_2(x,y) = x \vee \overline{y} = x + \overline{y}$$

$$s_4(x,y) = \overline{x} \vee y = \overline{x} + y$$

$$s_8(x,y) = \overline{x} \vee \overline{y} = \overline{x} + \overline{y}$$

e suas tabelas de valores são

x	y	$x+y$	$x+\overline{y}$	$\overline{x}+y$	$\overline{x}+\overline{y}$
1	1	1	1	1	0
1	0	1	1	0	1
0	1	1	0	1	1
0	0	0	1	1	1

De acordo com as tabelas anteriores:

$$s_1(x,y) = \overline{p_1(x,y)}$$

$$s_2(x,y) = \overline{p_2(x,y)}$$

$$s_4(x,y) = \overline{p_4(x,y)}$$

$$s_8(x,y) = \overline{p_8(x,y)}.$$

Assim, utilizando o exemplo anterior:

$$\begin{aligned}
\mu_{11}(x,y) &= 1.p_8(x,y) + 0.p_4(x,y) + 1.p_2(x,y) + 1.p_1(x,y) \\
\overline{\mu_{11}(x,y)} &= \overline{1.p_8(x,y) + 0.p_4(x,y) + 1.p_2(x,y) + 1.p_1(x,y)} \\
&= \overline{p_8(x,y)}.\overline{p_2(x,y)}.\overline{p_1(x,y)} \\
&= s_8(x,y).s_2(x,y).s_1(x,y) \\
&= (\overline{x}+\overline{y}).(x+\overline{y}).(x+y).
\end{aligned}$$

$$\begin{aligned}
\mu_{12}(x,y) &= 1.p_8(x,y) + 1.p_4(x,y) + 0.p_2(x,y) + 0.p_1(x,y) \\
\overline{\mu_{12}(x,y)} &= \overline{1.p_8(x,y) + 1.p_4(x,y) + 0.p_2(x,y) + 0.p_1(x,y)} \\
&= \overline{p_8(x,y)}.\overline{p_4(x,y)} \\
&= s_8(x,y).s_4(x,y) \\
&= (\overline{x}+\overline{y}).(\overline{x}+y).
\end{aligned}$$

Portanto:

$$\begin{aligned}
\overline{\mu_{11}(x,y)} &= \mu_4(x,y) \\
\mu_{11}(x,y) &= \overline{\mu_4(x,y)} \\
&= s_4(x,y) \\
&= \overline{x}+y.
\end{aligned}$$

$$\begin{aligned}\overline{\mu_{12}(x,y)} &= \mu_2(x,y)+\mu_1(x,y)\\ \mu_{12}(x,y) &= \overline{\mu_2(x,y)+\mu_1(x,y)}\\ &= \overline{\mu_2(x,y)}.\overline{\mu_1(x,y)}\\ &= s_2(x,y).s_1(x,y)\\ &= (x+\overline{y}).(x+y).\end{aligned}$$

3.4 Funções booleanas de três variáveis

As duzentas e cinquenta e seis $(256 = 2^8 = 2^{2^3})$ funções booleanas de três variáveis são preferencialmente definidas por mapas de Karnaugh.

Exemplo 3.9.

Seja f a função booleana de três variáveis definida pelo mapa de Karnaugh abaixo:

	yz	$y\overline{z}$	$\overline{y}z$	$\overline{yz}$
x	1	0	1	0
$\overline{x}$	0	0	1	1

Assim, a função f pode ser escrita como:

$$\begin{aligned}f(x,y,z) &= xyz+x\overline{y}z+\overline{xy}z+\overline{xyz}\\ &= xyz+\overline{y}z(x+\overline{x})+\overline{xyz}\\ &= xyz+\overline{y}z+\overline{xyz}.\end{aligned}$$

O exemplo a seguir ilustra o procedimento realizado para encontrar o índice de uma função booleana de três variáveis.

Exemplo 3.10.

Seja f uma função booleana de três variáveis, cujo mapa de Karnaugh é

	$\overline{xy}$	$\overline{x}y$	xy	$x\overline{y}$
$\overline{z}$	1	0	1	0
z	0	0	0	1

e tem como forma disjuntiva normal

$$f(x,y,z) = \overline{xyz}+xy\overline{z}+x\overline{y}z, \text{para } x, y, z \in \{0,1\}$$

e como forma conjuntiva normal

$$f(x,y,z) = (\overline{x}+\overline{y}+z)(\overline{x}+y+\overline{z})(\overline{x}+y+z)(x+y+z)(x+\overline{y}+\overline{z}), \text{para } x, y, z \in \{0,1\}.$$

A tabela de valores da função booleana f é

x	y	z	$f(x,y,z)$
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	1

e seu índice de numeração é

$$\begin{aligned} 01001001 &= 0.2^7 + 1.2^6 + 0.2^5 + 0.2^4 + 1.2^3 + 0.2^2 + 0.2^1 + 1.2^0 \\ &= 64 + 8 + 1 \\ &= 73. \end{aligned}$$

Portanto, a função booleana f de três variáveis dada pelo mapa de Karnaugh acima é a função booleana de três variáveis de número 73.

As funções booleanas de três variáveis, analogamente como nos casos de funções booleanas de uma e de duas variáveis, são soma de funções elementares (com um único valor igual a 1 em sua tabela de valores) e são produto de funções elementares (com um único valor igual a 0 em sua tabela de valores).

Exemplo 3.11.

Seja μ_{123} a função booleana de três variáveis, cuja tabela de valores é dada por:

x	y	z	$\mu_{123}(x,y,z)$
1	1	1	0
1	1	0	1
1	0	1	1
1	0	0	1
0	1	1	1
0	1	0	0
0	0	1	1
0	0	0	1

uma vez que $123 = 0.2^7 + 1.2^6 + 1.2^5 + 1.2^4 + 1.2^3 + 0.2^2 + 1.2^1 + 1.2^0$.

Então, μ_{123} é escrita como:

$$\begin{aligned} \mu_{123}(x,y,z) = 0.\mu_{128}(x,y,z) + 1.\mu_{64}(x,y,z) + 1.\mu_{32}(x,y,z) + 1.\mu_{16}(x,y,z) \\ + 1.\mu_8(x,y,z) + 0.\mu_4(x,y,z) + 1.\mu_2(x,y,z) + 1.\mu_1(x,y,z). \end{aligned}$$

Da mesma maneira,

$$\begin{aligned}\overline{\mu_{123}(x,y,z)} &= 1.\mu_{128}(x,y,z) + 1.\mu_4(x,y,z)\\ &= s_{128}(x,y,z).s_4(x,y,z)\\ &= (\overline{x}+\overline{y}+\overline{z}).(x+\overline{y}+z).\end{aligned}$$

3.5 Funções booleanas de quatro variáveis

As sessenta e cinco mil, quinhentos e trinta e seis $(65.536 = 2^{16} = 2^{2^4})$ funções booleanas de quatro variáveis são preferencialmente definidas por mapas de Karnaugh.

Exemplo 3.12.

Seja f a função booleana de quatro variáveis definida pelo mapa de Karnaugh abaixo:

	yz	$y\overline{z}$	$\overline{y}z$	$\overline{yz}$
wx	0	0	0	0
$w\overline{x}$	1	0	0	1
$\overline{w}x$	1	0	0	1
$\overline{wx}$	0	0	0	0

Assim, a função f pode ser escrita como:

$$\begin{aligned}f(w,x,y,z) &= w\overline{x}yz + \overline{w}xyz + w\overline{xyz} + \overline{w}x\overline{yz}\\ &= yz(w\overline{x}+\overline{w}x) + \overline{yz}(w\overline{x}+\overline{w}x)\\ &= (w\overline{x}+\overline{w}x)(yz+\overline{yz})\end{aligned}$$

O exemplo a seguir ilustra o procedimento realizado para encontrar o índice de uma função booleana de quatro variáveis.

Exemplo 3.13.

Seja f uma função booleana de quatro variáveis, cujo o mapa de Karnaugh é

	$\overline{yz}$	$\overline{y}z$	yz	$y\overline{z}$
$\overline{wx}$	1	0	1	0
$\overline{w}x$	0	1	1	0
wx	1	0	0	0
$w\overline{x}$	0	0	0	0

e tem como forma disjuntiva normal

$$f(w,x,y,z) = \overline{wxyz} + \overline{w}x\overline{yz} + \overline{w}xyz + \overline{w}xy\overline{z} + wx\overline{yz}, \text{para } w, x, y, z \in \{0,1\}$$

e como forma conjuntiva normal

$$\begin{aligned} f(w,x,y,z) = {} & (\overline{w}+\overline{x}+\overline{y}+z)(\overline{w}+\overline{x}+y+\overline{z})(\overline{w}+x+\overline{y}+\overline{z})(\overline{w}+x+y+\overline{z}) \\ & (w+x+\overline{y}+z)(w+x+y+z)(w+x+y+\overline{z})(w+\overline{x}+\overline{y}+\overline{z}) \\ & (w+\overline{x}+\overline{y}+z)(w+\overline{x}+y+z)(w+\overline{x}+y+\overline{z}), \text{para } w, x, y, z \in \{0,1\}. \end{aligned}$$

O índice de numeração da função dada é obtido da seguinte forma: a tabela de valores de f apresenta $f(w,x,y,z) = 1$ nas linhas

w	x	y	z	$f(w,x,y,z)$
0	0	0	0	1
0	0	1	1	1
0	1	0	1	1
0	1	1	1	1
1	1	0	0	1

cujos números relacionados são

Representação binária	*Representação decimal* α	2 *elevado à potência* α
0000	0	2^0
0011	3	2^3
0101	5	2^5
0111	7	2^7
1100	12	2^{12}

e o índice da função f é dada por

$$\begin{aligned} 2^0+2^3+2^5+2^7+2^{12} &= 1+8+32+128+4.096 \\ &= 4.265. \end{aligned}$$

Portanto, a função booleana f de quatro variáveis dada pelo mapa de Karnaugh acima é a função de número 4.265.

As operações binárias booleanas de adição $+$ (ou OR), de produto $\cdot$ (ou AND) e a operação binária $\oplus$ (ou XOR) no conjunto $\{0,1\}$ que possuem as propriedades associativa, comutativa e de existência do elemento neutro implicam que as operações binárias internas OR, AND e XOR definidas no conjunto de todas as funções booleanas de n variáveis herdam as propriedades associativa, comutativa e de existência do elemento neutro.

A operação binária interna de implicação $(\rightarrow)$ também é definida para funções booleanas de n variáveis: se f e g são funções booleanas de n variáveis, então $f \rightarrow g$ é a função booleana

de n variáveis tal que:

$$(f \to g)(x_1, x_2, \ldots, x_n) = \begin{cases} 0, & \text{quando } f(x_1, x_2, \ldots, x_n) = 1 \text{ e } g(x_1, x_2, \ldots, x_n) = 0 \\ 1, & \text{nos demais casos} \end{cases}$$

O conjunto das funções booleanas de n variáveis admite uma relação de ordem parcial, definida da seguinte maneira: para f e g funções booleanas de n variáveis, $f \leq g$ se, e somente se, para cada n-upla $(i_1, i_2, \ldots, i_n)$ formada pelos dígitos 0 e 1,

$$f(i_1, i_2, \ldots, i_n) \leq g(i_1, i_2, \ldots, i_n),$$

ou, equivalentemente, quando $f(i_1, i_2, \ldots, i_n) = 1$, implica que $g(i_1, i_2, \ldots, i_n) = 1$.

Em outras palavras, $f = f \wedge g$, em que $g \wedge g = g$.

3.6 O método de Quine-McCluskey para obtenção da forma mínima de uma função booleana

As formas mínimas para a função booleana f de três variáveis, definida pelo mapa de Karnaugh

	$\overline{z}$	z
$\overline{xy}$	1	0
$\overline{x}y$	1	1
xy	0	0
$x\overline{y}$	1	1

	0	1
00	1	0
01	1	1
11	0	0
10	1	1

são $f(x,y,z) = \overline{xz} + \overline{x}y + x\overline{y}$ e $f(x,y,z) = \overline{yz} + \overline{x}y + x\overline{y}$.

De fato, a função f apresenta valores iguais a 1 nas células 000, 010, 011, 100 e 101, que são representações binárias, respectivamente, dos números 0, 2, 3, 4 e 5, o que evidencia que o índice de numeração da função f é

$$\begin{aligned} 2^0 + 2^2 + 2^3 + 2^4 + 2^5 &= 1 + 4 + 8 + 16 + 32 \\ &= 61. \end{aligned}$$

De acordo com o índice encontrado, pode-se escrever:

$$\begin{aligned} f_{61}(x,y,z) &= \overline{xyz} + \overline{x}y\overline{z} + \overline{x}yz + x\overline{yz} + x\overline{y}z \\ &= (\overline{xyz} + \overline{x}y\overline{z}) + (\overline{x}y\overline{z} + \overline{x}yz) + (x\overline{yz} + x\overline{y}z) \\ &= \overline{xz}(\overline{y} + y) + \overline{x}y(\overline{z} + z) + x\overline{y}(\overline{z} + z) \\ &= \overline{xz}1 + \overline{x}y1 + x\overline{y}1 \\ &= \overline{xz} + \overline{x}y + x\overline{y} \end{aligned}$$

ou

$$\begin{aligned} f_{61}(x,y,z) &= \overline{xyz}+\bar{x}y\bar{z}+\bar{x}yz+x\overline{yz}+x\bar{y}z \\ &= (\overline{xyz}+x\overline{yz})+(\bar{x}y\bar{z}+\bar{x}yz)+(x\overline{yz}+x\bar{y}z) \\ &= \overline{yz}(\bar{x}+x)+\bar{x}y(\bar{z}+z)+x\bar{y}(\bar{z}+z) \\ &= \overline{yz}1+\bar{x}y1+x\bar{y}1 \\ &= \overline{yz}+\bar{x}y+x\bar{y}. \end{aligned}$$

A forma mínima da função booleana f_{61} de três variáveis obtida pelo método de Quine-McCluskey é obtida pelo processo abaixo:

1. Organizar as células de acordo com a quantidade de dígitos 1:

$$\left.\begin{matrix}000\end{matrix}\right\}\text{célula com zero dígitos 1}$$

$$\left.\begin{matrix}010\\100\end{matrix}\right\}\text{células com um dígito 1}$$

$$\left.\begin{matrix}011\\101\end{matrix}\right\}\text{células com dois dígitos 1}$$

2. Agrupar os elementos de campos adjacentes que difiram em um único dígito:

$$\begin{matrix}000\\010\end{matrix}\text{ é substituído por } 0-0$$

$$\begin{matrix}000\\100\end{matrix}\text{ é substituído por } -00$$

$$\begin{matrix}010\\011\end{matrix}\text{ é substituído por } 01-$$

$$\begin{matrix}100\\101\end{matrix}\text{ é substituído por } 10-$$

3. Escrever uma tabela da seguinte forma:

	0 0 0	0 1 0	1 0 0	0 1 1	1 0 1
$0-0$	✓	✓			
-00	✓		✓		
$01-$		✓		✓	
$10-$			✓		✓

Esta primeira tabela fornece o núcleo da fórmula mínima $\bar{x}y+x\bar{y}$.

4. Escrever outra tabela da seguinte forma:

	0 0 0
$0-0$	✓
-00	✓

Esta tabela mostra que faltam os monômios $\overline{xz}$ ou $\overline{yz}$ e, assim,

$$f_{61}(x,y,z) = \bar{x}y + x\bar{y} + \overline{xz} = \bar{x}y + x\bar{y} + \overline{yz}.$$

CAPÍTULO

4

GRUPOS E SEMIGRUPOS

Uma operação binária interna μ em um conjunto não vazio X é uma função μ cujo domínio de definição é igual ao produto cartesiano $X \times X$ e cujo conjunto de valores é um subconjunto de X.

A lei do fechamento abaixo da operação binária interna μ em um conjunto não vazio X é outra maneira de expressar que o domínio de definição de μ é $X \times X$ e que o conjunto de valores de μ é um subconjunto de X:

$$(\forall\, x_1 \in X)(\forall\, x_2 \in X)(\mu(x_1, x_2) \in X).$$

A propriedade associativa de uma operação binária interna μ em um conjunto não vazio X significa que

$$(\forall\, x \in X)(\forall\, y \in X)(\forall\, z \in X)\left(\mu\left[x, \mu(y,z)\right] = \mu\left[\mu(x,y), z\right]\right).$$

A propriedade comutativa de uma operação binária interna μ em um conjunto não vazio X significa que

$$(\forall\, x_1 \in X)(\forall\, x_2 \in X)(\mu(x_1, x_2) = \mu(x_2, x_1)).$$

A propriedade de existência do elemento neutro (necessariamente único) para uma operação binária interna μ em um conjunto não vazio X significa a existência de um elemento $e \in X$ tal que

$$(\forall\, x \in X)(\mu(e,x) = \mu(x,e) = x).$$

A unicidade do elemento neutro de uma operação binária interna μ é provada a seguir: caso existam $e_1 \in X$ e $e_2 \in X$ com a propriedade acima, $\mu(e_1, e_2) = e_1$ já que e_2 é elemento neutro para μ e $\mu(e_1, e_2) = e_2$ já que e_1 também é elemento neutro para μ, o que mostra que $e_1 = e_2$.

As operações binárias internas de união, intersecção, diferença e diferença simétrica são exemplos de operações binárias internas no conjunto das partes $\mathscr{P}(X)$ de um conjunto X.

As operações binárias internas de união, intersecção e diferença simétrica são operações binárias internas associativas, comutativas e tem a propriedade de existência do elemento neutro no conjunto das partes $\mathscr{P}(X)$ de um conjunto não vazio X, ou seja, para $A, B, C \in \mathscr{P}(X)$, valem as igualdades abaixo:

$$A \cup (B \cup C) = (A \cup B) \cup C$$
$$A \cap (B \cap C) = (A \cap B) \cap C$$
$$A \Delta (B \cup C) = (A \Delta B) \cup C$$
$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$
$$A \Delta B = B \Delta A$$
$$A \cup \emptyset = A$$
$$A \cap X = A$$
$$A \Delta \emptyset = A$$

Por outro lado, a operação binária interna de diferença no conjunto das partes $\mathscr{P}(X)$ de um conjunto não vazio não é associativa, pois a igualdade

$$(A - B) - C = A - (B - C)$$

ou

$$\begin{aligned}(A \cap \overline{B}) \cap \overline{C} &= A \cap (\overline{B} \cap \overline{C}) \\ &= A \cap (\overline{B} \cup C) \\ &= (A \cap \overline{B}) \cup (A \cap C)\end{aligned}$$

não é válida para $A, B, C \in \mathscr{P}(X)$: por exemplo, quando $C = X$, o primeiro membro é o conjunto vazio $\emptyset$, enquanto que o segundo membro é $(A \cap \overline{B}) \cup A = A$ que, em geral, é um conjunto não vazio. Quando $B = X$, o primeiro membro é o conjunto vazio $\emptyset$ e o segundo membro é $A \cap C$ que, em geral, é um conjunto não vazio.

Definição 4.1.

Um grupoide (S, μ) é um par ordenado em que S é um conjunto não vazio e μ é uma operação binária em S.

Os elementos idempotentes do grupoide (S, μ) são os elementos x do conjunto S com a propriedade $\mu(x, x) = x$.

Exemplo 4.2.

O conjunto das partes $\mathscr{P}(X)$ de um conjunto não vazio X com a operação binária interna da diferença é um grupoide.

Definição 4.3.

Um semigrupo (S,μ) é um par ordenado em que S é um conjunto não vazio e μ é uma operação binária associativa em X, ou seja,

$$(\forall\, x \in S)(\forall\, y \in S)(\forall\, z \in S)\left(\mu\left[x,\mu(y,z)\right] = \mu\left[\mu(x,y),z\right]\right).$$

Exemplo 4.4.

O conjunto das partes $\mathscr{P}(X)$ de um conjunto não vazio X com a operação binária interna de união é um semigrupo e todos os elementos são idempotentes.

O conjunto das partes $\mathscr{P}(X)$ de um conjunto não vazio X com a operação binária interna de intersecção é um semigrupo e todos os elementos são idempotentes.

O conjunto das partes $\mathscr{P}(X)$ de um conjunto não vazio X com a operação binária interna de diferença simétrica é um semigrupo e todos os elementos são idempotentes.

Definição 4.5.

Dados os semigrupos (S,μ) e (T,ν), o semigrupo produto cartesiano dos semigrupos dados é o par ordenado $(S\times T,\mu\times\nu)$, em que a operação binária interna $\mu\times\nu$ é definida no conjunto $S\times T$ por: para $(s_1,t_1)\in S\times T$ e $(s_2,t_2)\in S\times T$,

$$(\mu\times\nu)\left[(s_1,t_1),(s_2,t_2)\right] = (\mu(s_1,s_2),\nu(t_1,t_2)),$$

que é claramente uma operação binária interna associativa no produto cartesiano $S\times T$.

Definição 4.6.

Um monoide (S,μ) é um semigrupo (S,μ) em que existe um elemento $e\in S$, denominado elemento neutro em relação a μ, com a propriedade

$$(\forall\, x \in S)(\mu(e,x) = \mu(x,e) = x).$$

Caso exista, o elemento neutro em relação a operação binária μ é único. De fato, caso existam e_1, $e_2\in S$ com as propriedades

$$(\forall\, x \in S)(\mu(e_1,x) = \mu(x,e_1) = x)$$

$$(\forall\, x \in S)(\mu(e_2,x) = \mu(x,e_2) = x),$$

então

$$e_2 = \mu(e_1,e_2) = e_1.$$

Exemplo 4.7.

O conjunto das partes $\mathscr{P}(X)$ de um conjunto não vazio X com a operação binária interna da união é um monoide, cujo elemento neutro é $\emptyset$.

O conjunto das partes $\mathscr{P}(X)$ de um conjunto não vazio X com a operação binária interna da intersecção é um monoide, cujo elemento neutro é X.

O conjunto das partes $\mathscr{P}(X)$ de um conjunto não vazio X com a operação binária interna da diferença simétrica é um monoide, cujo elemento neutro é $\emptyset$.

Exemplo 4.8.

Para cada número $n \in \mathbb{N} = \{1,2,\ldots\}$, o semigrupo $(T(X_n), \circ)$, em que $T(X_n)$ é o conjunto das funções totais em $X_n = \{1,2,\ldots,n\}$, com a operação binária interna da composição é um monoide, cujo elemento neutro é a função identidade.

Exemplo 4.9.

Para cada número $n \in \mathbb{N} = \{1,2,\ldots\}$, o semigrupo $(P(X_n), \circ)$, em que $P(X_n)$ é o conjunto das funções parciais em $X_n = \{1,2,\ldots,n\}$, com a operação binária interna da composição é um monoide, cujo elemento neutro é a função identidade.

Exemplo 4.10.

O conjunto das funções booleanas de n variáveis com a operação binária interna OR é um monoide, cujo elemento neutro é a função booleana constante igual a 0.

O conjunto das funções booleanas de n variáveis com a operação binária interna AND é um monoide, cujo elemento neutro é a função booleana constante igual a 1.

Exemplo 4.11.

Para cada número $m \in \mathbb{N} = \{1,2,\ldots\}$, o conjunto $\mathbb{Z}_m = \{0,1,\ldots,m-1\}$ com a operação binária interna de multiplicação $\mod m$ é definido como o monoide multiplicativo comutativo $(\mathbb{Z}_m, \cdot)$, cujo elemento neutro é 1, em que, para i, $j \in \{0,1,\ldots,m-1\}$, o produto $ij \mod m$ é o resto da divisão do produto usual dos fatores i e j pelo número natural m.

Exemplo 4.12.

O conjunto dos números naturais $\mathbb{N} = \{1,2,\ldots\}$ admite várias estruturas de semigrupos comutativos. Por exemplo:

(i) $(\mathbb{N}, +)$ é um semigrupo aditivo comutativo e a operação binária interna em $\mathbb{N}$ é a operação de adição.

(ii) $(\mathbb{N}, \cdot)$ é um monoide multiplicativo com elemento neutro 1 e a operação binária interna em $\mathbb{N}$ é a operação de multiplicação.

(iii) $(\mathbb{N}, \wedge)$ é um semigrupo comutativo em que todos os elementos são idempotentes e a operação binária interna em $\mathbb{N}$ é a operação definida por: $a \wedge b = \min(a,b)$, para $a, b \in \mathbb{N}$.

(iv) $(\mathbb{N}, \vee)$ é um semigrupo comutativo em que todos os elementos são idempotentes e a operação binária interna em $\mathbb{N}$ é a operação definida por: $a \vee b = \max(a,b)$, para $a, b \in \mathbb{N}$.

(v) $(\mathbb{N}, (\,))$ é um semigrupo comutativo em que todos os elementos são idempotentes e a operação binária interna em $\mathbb{N}$ é a operação definida por: $(a,b) = \text{mdc}(a,b)$, o máximo divisor comum entre a e b, para $a, b \in \mathbb{N}$.

(vi) $(\mathbb{N}, [\,])$ é um semigrupo comutativo em que todos os elementos são idempotentes e a operação binária interna em $\mathbb{N}$ é a operação definida por: $\left[a,b\right] = \text{mmc}(a,b)$, o mínimo múltiplo comum entre a e b para $a, b \in \mathbb{N}$.

(vii) $(\mathbb{N}, \uparrow)$ é um grupoide e a operação binária interna em $\mathbb{N}$ é a operação de potenciação. Por exemplo, $(2 \uparrow 3) \uparrow 4 \neq 2 \uparrow (3 \uparrow 4)$.

(viii) $(\mathbb{N}^0, +)$, em que $\mathbb{N}^0 = \{0, 1, \ldots\}$, é um monoide comutativo com elemento neutro igual a 0 e a operação binária interna em $\mathbb{N}^0$ é a operação de adição.

(ix) $(\mathbb{N}^0, \cdot)$, em que $\mathbb{N}^0 = \{0, 1, \ldots\}$, é um monoide comutativo com elemento neutro igual a 1 e elemento zero igual a 0 e a operação binária interna em $\mathbb{N}^0$ é a operação de multiplicação.

Exemplo 4.13.

Seja o conjunto dos números inteiros $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$. Então:

(i) $(\mathbb{Z}, \cdot)$ é um monoide multiplicativo comutativo com elemento neutro igual a 1 e a operação binária interna em $\mathbb{Z}$ é a operação de multiplicação.

(ii) $(\mathbb{Z}, \wedge)$ é um semigrupo comutativo em que todos os elementos são idempotentes e a operação binária interna $\wedge$ é dada, para $a, b \in \mathbb{Z}$, por

$$\begin{aligned} a \wedge b &= \min(a,b) \\ &= \frac{a+b-|a-b|}{2}, \end{aligned}$$

sendo que $|x|$ indica o módulo de x e é dado por

$$|x| = \begin{cases} x, & \text{se } x \in \mathbb{Z} \text{ e } x \geq 0 \\ -x, & \text{se } x \in \mathbb{Z} \text{ e } x < 0 \end{cases}.$$

(iii) $(\mathbb{Z}, \vee)$ é um semigrupo comutativo em que todos os elementos são idempotentes e a operação binária interna $\vee$ dada, para $a, b \in \mathbb{Z}$, por

$$\begin{aligned} a \vee b &= \max(a,b) \\ &= \frac{a+b+|a-b|}{2}, \end{aligned}$$

sendo que $|x|$ indica o módulo de x.

Exemplo 4.14. Seja $(\mathbb{Z},\mu)$ um monoide multiplicativo comutativo em que $\mathbb{Z}=\{\ldots,-2,-1,0,1,2,\ldots\}$ e μ é a operação binária interna definida por: $\mu(x,y)=x+y-xy$. Então, 0 é o elemento neutro para a operação binária interna μ, pois $\mu(x,0)=\mu(0,x)=x$.

Para $x\neq 1$,

$$\begin{aligned} x+y-xy&=0\\ x+y(1-x)&=0\\ y&=-\frac{x}{1-x}\\ y&=\frac{x}{x-1}. \end{aligned}$$

Portanto, para $x\neq 1$, o elemento inverso de x é igual a $\dfrac{x}{x-1}$. De fato,

$$\begin{aligned} \mu\left(x,\frac{x}{x-1}\right)&=x+\frac{x}{x-1}-x\left(\frac{x}{x-1}\right)\\ &=\frac{x^2-x+x-x^2}{x-1}\\ &=0. \end{aligned}$$

O número inteiro 1 não tem inverso em relação à operação binária interna μ.

Seja (S,μ) um semigrupo que não contém em S o elemento neutro para a operação binária interna μ. Considerando um elemento $1\notin S$ e definindo a operação binária interna $\overline{\mu}_1$ em $S^1=S\cup\{1\}$ por

$$\overline{\mu}_1(1,1)=1$$

$$\overline{\mu}_1(1,s)=\overline{\mu}_1(s,1)=s,\ \text{para cada } s\in S$$

$$\overline{\mu}_1(s,t)=\mu(s,t),\ \text{para cada } s,t\in S,$$

conclui-se que $(S^1,\overline{\mu}_1)$ é um monoide com elemento neutro igual a 1, pois $\overline{\mu}_1$ é uma operação binária interna associativa em S^1.

Por definição, o monoide $(S^1,\overline{\mu}_1)$ é denominado monoide associado ao semigrupo (S,μ).

Caso o conjunto S não contenha o elemento zero, considerando um elemento $0\notin S$ e definindo a operação binária interna $\overline{\mu}_0$ em $S^0=S\cup\{0\}$ por

$$\overline{\mu}_0(0,0)=0$$

$$\overline{\mu}_0(0,s)=\overline{\mu}_0(s,0)=0,\ \text{para cada } s\in S$$

$$\overline{\mu}_0(s,t)=\mu(s,t),\ \text{para cada } s,t\in S,$$

conclui-se que $(S^0, \overline{\mu}_0)$ é um semigrupo com elemento zero igual a 0.

Seja (S, μ) um semigrupo. Um elemento zero à esquerda do semigrupo é um elemento θ com a propriedade: $\mu(\theta, s) = \theta$, para cada $s \in S$, enquanto que um elemento zero à direita do semigrupo é um elemento θ com a propriedade: $\mu(s, \theta) = \theta$, para cada $s \in S$.

Um semigrupo (S, μ) em que a operação binária interna associativa μ em S é definida por:

$$\mu(s,t) = s, \text{ para } s, t \in S$$

é um semigrupo em que todo elemento é um elemento zero à esquerda.

Um semigrupo (S, μ) em que a operação binária interna associativa μ em S é definida por:

$$\mu(s,t) = t, \text{ para } s, t \in S$$

é um semigrupo em que todo elemento é um elemento zero à direita.

Um número real a qualquer é elemento zero do semigrupo, cujo conjunto é o intervalo fechado $\left[a, b\right]$ de números reais dados entre os números a e b, com $a < b$, e cuja operação binária interna associativa em $\left[a, b\right]$ é definida como o mínimo entre dois valores $s, t \in \left[a, b\right]$.

A operação binária interna μ de um semigrupo (S, μ) induz a seguinte operação binária interna $\mu_{\mathscr{P}}$ no conjunto das partes $\mathscr{P}(S)$ do conjunto não vazio S:

$$\text{para } A, B \subset \mathscr{P}(S), A \neq \emptyset, B \neq \emptyset, \mu_{\mathscr{P}}(A,B) = \{\mu(a,b) : a \in A \text{ e } b \in B\}$$

e, se A ou B é o conjunto vazio, então

$$\mu_{\mathscr{P}}(A,B) = \emptyset.$$

A operação binária interna $\mu_{\mathscr{P}}$ em $\mathscr{P}(S)$ é uma operação associativa em $\mathscr{P}(S)$, cujo elemento zero é o conjunto vazio.

Definição 4.15.

Um subconjunto não vazio T de um conjunto não vazio S, em que (S, μ) é um semigrupo, é um subsemigrupo de (S, μ) se, e somente se, o conjunto T é fechado em relação à operação binária interna μ, isto é, se t_1 e $t_2 \in T$, então $\mu(t_1, t_2) \in T$.

Exemplo 4.16.

O conjunto dos números naturais ímpares $\{1, 3, \ldots\}$ e o conjunto dos números naturais pares $\{2, 4, \ldots\}$ são fechados em relação à operação binária interna de multiplicação. Assim, $(\{1, 3, \ldots\}, \cdot\}$ e $(\{2, 4, \ldots\}, \cdot\}$ são subsemigrupos do semigrupo multiplicativo $(\mathbb{N}, \cdot)$.

Exemplo 4.17.

Seja (S,μ) um semigrupo comutativo. Então, o subconjunto $E(S)$ dos elementos idempotentes do semigrupo (S,μ) é tal que $(E(S),\mu)$ é um subsemigrupo de (S,μ).

Definição 4.18.

Seja (S,μ) um semigrupo. O subsemigrupo gerado por um subconjunto A não vazio do conjunto S é definido como a intersecção de todos os subsemigrupos do semigrupo (S,μ) que contém o conjunto A. Os elementos de A são denominados geradores do subsemigrupo gerado pelo conjunto A.

Definição 4.19.

Seja (M,μ) um monoide. O submonoide gerado por um subconjunto A não vazio do conjunto S é definido como a intersecção de todos os submonoides do monoide (M,μ) que contém o conjunto A. Os elementos de A são denominados geradores do submonoide gerado pelo conjunto A.

Exemplo 4.20.

Para cada número $n \in \mathbb{N} = \{1,2,\ldots\}$, o semigrupo $(T(X_n),\circ)$, em que $T(X_n)$ é o conjunto das funções totais em $X_n = \{1,2,\ldots,n\}$, com a operação binária interna da composição, é um monoide gerado pela união do conjunto de todas as transposições de X_n com o conjunto unitário constituído pela função total f_{12}.

Exemplo 4.21.

Para cada número $n \in \mathbb{N} = \{1,2,\ldots\}$, o semigrupo $(P(X_n),\circ)$, em que $P(X_n)$ é o conjunto das funções parciais em $X_n = \{1,2,\ldots,n\}$, com a operação binária interna da composição, é um monoide gerado pela união do conjunto de todas as transposições de X_n com o conjunto constituído de dois elementos: a função total f_{12} e a função parcial $f_{\{1\}}$.

Definição 4.22.

Um subconjunto não vazio A do conjunto não vazio S, em que (S,μ) é um semigrupo, é um ideal à esquerda do semigrupo quando, e somente quando,

$$\{\mu(s,a) : s \in S, a \in A\} \subset A,$$

ou seja, para $s \in S$ e $a \in A$, $\mu(s,a) \in A$ enquanto que um subconjunto não vazio A de S é um ideal à direita do semigrupo (S,μ) quando, e somente quando,

$$\{\mu(a,s) : a \in A, s \in S\} \subset A,$$

ou seja, para $s \in S$ e $a \in A$, $\mu(a,s) \in A$.

Ideais à esquerda e à direita simultaneamente são chamados simplesmente ideais do semigrupo.

Exemplo 4.23.

O subsemigrupo dos números naturais pares $(\{2,4,\ldots\},\cdot)$ do semigrupo multiplicativo $(\mathbb{N},\cdot)$ é um ideal. O subsemigrupo dos números naturais $(\{3,6,\ldots\},\cdot)$ do semigrupo multiplicativo $(\mathbb{N},\cdot)$ é um ideal. O subsemigrupo dos números naturais $(\{4,8,\ldots\},\cdot)$ do semigrupo multiplicativo $(\mathbb{N},\cdot)$ é um ideal. E, assim, sucessivamente.

Em contrapartida, o subsemigrupo dos números naturais ímpares $(\{1,3,\ldots\},\cdot)$ do semigrupo multiplicativo $(\mathbb{N},\cdot)$ não é um ideal.

Seja I um ideal próprio do semigrupo (S,μ), ou seja, $I \neq S$ e $I \neq \{0\}$, caso 0 seja o elemento zero do semigrupo. O ideal I do semigrupo induz a seguinte partição no conjunto S:

$$I \cup \bigcup_{s \in S/I} \{s\},$$

a qual induz a relação de equivalência R_I, cujas classes de equivalência são os subconjuntos da partição induzida pelo ideal I.

O conjunto quociente S/R_I admite a seguinte operação binária interna μ_I:

$$\text{se } s_1, s_2 \in S/I, \mu_I(\{s_1\},\{s_2\}) = \mu(s_1,s_2),$$

$$\text{se } s \in S/I, \mu_I(I,\{s\}) = \mu_I(\{s\},I) = I,$$

$$\mu_I(I,I) = I.$$

O semigrupo quociente $(S/I,\mu_I)$ é o conjunto quociente S/R_I com a operação binária interna evidentemente associativa μ_I e I é o elemento zero do semigrupo quociente. Além de relação de equivalência, R_I é uma congruência no semigrupo (S,μ) denominada congruência de Rees determinada pelo ideal I de S. Uma congruência em um semigrupo (S,μ) é uma relação de equivalência no conjunto S compatível à esquerda e à direita com a operação binária interna μ do semigrupo.

Definição 4.24.

Dados os semigrupos (S,μ) e (S',ν), um homomorfismo de semigrupo h do semigrupo (S,μ) no semigrupo (S',ν) é uma função, cujo domínio de definição $D(h)$ é S e cujo conjunto de valores $R(h)$ é um subconjunto de S' com a propriedade: se $s_1, s_2 \in S$,

$$h\big[\mu(s_1,s_2)\big] = \nu\big[h(s_1),h(s_2)\big].$$

Quando o homomorfismo de semigrupo h do semigrupo (S,μ) no semigrupo (S',ν) for uma função injetora, h é denominado monomorfismo de semigrupo do semigrupo (S,μ) no semigrupo (S',ν).

Quando o homomorfismo de semigrupo h do semigrupo (S,μ) no semigrupo (S',ν) for uma função sobrejetora, h é chamado epimorfismo de semigrupo do semigrupo (S,μ) no semigrupo (S',ν).

Um isomorfismo de semigrupo é, simultaneamente, um monomorfismo e um epimorfismo de semigrupo.

Definição 4.25.

Seja (S,μ) um semigrupo. O conjunto $HomS$ é definido como o conjunto de todos os homomorfismos de semigrupo do semigrupo (S,μ) no semigrupo (S,μ).

Propriedade 4.26.

O par ordenado $(HomS,\circ)$ é um monoide com a operação binária interna $\circ$ de composição de funções.

Propriedades 4.27.

Dado um homomorfismo de semigrupo h do semigrupo (S,μ) no semigrupo (S',ν), o conjunto de valores $(h(S),\nu)$ é um subsemigrupo de (S',ν). Além disso, se e é um elemento idempotente de S, no sentido de que $\mu(e,e)=e$, então $h(e)$ é um elemento idempotente de S'.

Se (T,μ) é um subsemigrupo de (S,μ), então $(h(T),\nu)$ é um subsemigrupo de (S',ν) e se (T',ν) é um subsemigrupo de (S',ν), então $(h^{-1}(T'),\mu)$ é um subsemigrupo de (S,μ).

Se h é um epimorfismo de semigrupo de S em S' e se I é um ideal de S, então $h(I)$ é um ideal de S' e, além disso, a imagem por h do elemento zero de S, quando existir, é o elemento zero de S' e a imagem do elemento neutro de S, quando existir, é o elemento neutro de S'.

Definição 4.28.

Sejam (M,μ) e (M',ν) monoides, ou seja, semigrupos com elementos neutros e e e', respectivamente. Um homomorfismo de monoide h do monoide (M,μ) no monide (M',ν) é um homomorfismo de semigrupo com a propriedade adicional de que $h(e)=e'$.

Teorema 4.29.

Seja $(P(X),\circ)$ o semigrupo constituído por todas as funções parciais f, cujo domínio de definição $D(f)$ e cujo conjunto de valores $R(f)$ são ambos subconjuntos de X. Sejam $0\notin X$, $Y=X\cup\{0\}$ e $\tilde{f}$, cujo domínio de definição é Y e cujo conjunto de valores é um subconjunto de

Y, definida por:

$$\tilde{f}(y) = \begin{cases} f(y), & \text{se } y \in D(f) \\ 0, & \text{se } y \in Y \setminus D(f) \end{cases}$$

Então, h, cujo domínio de definição é $P(X)$ e cujo domínio de valores é um subconjunto de $T(Y)$, o conjunto das funções totais de Y, definida por: para $f \in P(X)$, $h(f) = \tilde{f}$ é um monomorfismo de semigrupo do semigrupo $(P(X), \circ)$ no semigrupo $(T(Y), \circ)$.

Em consequência, se X é um conjunto de n elementos, então o número de funções parciais em X é igual a $(n+1)^n$.

Definição 4.30.

Um grupo (G, μ) é um monoide com a propriedade de que, para cada $x \in G$, existe um elemento $y \in G$ tal que

$$\mu(x,y) = \mu(y,x) = e.$$

Para cada $x \in G$, o elemento $y \in G$ com a propriedade acima é único: de fato, caso existam $y_1, y_2 \in G$,

$$e = \mu(x,y_1) = \mu(x,y_2) = \mu(y_1,x) = \mu(y_2,x),$$

então:

$$\begin{aligned} y_1 &= \mu(e,y_1) \\ &= \mu\big[\mu(y_2,x),y_1\big] \\ &= \mu\big[y_2,\mu(x,y_1)\big] \\ &= \mu(y_2,e) \\ &= y_2. \end{aligned}$$

Para cada $x \in G$, o elemento $y \in G$ é chamado de elemento inverso de x (denotado por x^{-1}) e é o único elemento de G com a propriedade

$$\mu(x,x^{-1}) = \mu(x^{-1},x) = e.$$

Além disso, $(x^{-1})^{-1} = x$.

Propriedade 4.31.

Para x e y elementos de um grupo (G, μ), o elemento inverso $\mu(x,y)^{-1}$ de $\mu(x,y)$ é igual a $\mu(y^{-1},x^{-1})$.

Exemplo 4.32.

Seja $(\mathbb{Z}, \mu_1)$ um grupo aditivo comutativo em que $\mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$ e μ_1 é a operação binária interna definida por: $\mu_1(x,y) = x+y-1$. Então, 1 é o elemento neutro para a

operação binária interna μ_1. Seja μ_2 a operação binária interna definida por: $\mu_2(x,y) = x+y-2$. Então, 2 é o elemento neutro para a operação binária interna μ_2. Analogamente, para cada número inteiro a, seja μ_a a operação binária interna definida por: $\mu_a(x,y) = x+y-a$. Então, a é o elemento neutro para a operação binária interna μ_a. O elemento inverso do elemento a com relação à operação binária interna μ_a é o número inteiro $2a-x$, pois $x+(2a-x)-a = a$.

Exemplo 4.33.

O conjunto das funções booleanas de n variáveis com a operação binária interna XOR é um grupo, cujo elemento neutro é a função booleana constante igual a 0 e a função inversa de uma função booleana é a própria função booleana.

Exemplo 4.34.

O conjunto das partes $\mathscr{P}(X)$ de um conjunto não vazio X com a operação binária interna da diferença simétrica é um grupo, cujo elemento neutro é $\emptyset$ e cujo elemento inverso de um subconjunto $A \subset X$ é o próprio subconjunto A.

Teorema 4.35 (Lei do cancelamento para grupos)**.**

Seja (G,μ) um grupo com elemento neutro e e sejam x, y, $z \in G$. Então:

(i) Se $\mu(x,z) = \mu(y,z)$, então $x = y$.

(ii) Se $\mu(z,x) = \mu(z,y)$, então $x = y$.

Demonstração.

(i) De $\mu(x,z) = \mu(y,z)$, vem que
$$\begin{aligned} x &= \mu\left[\mu(x,z), z^{-1}\right] \\ &= \mu\left[\mu(y,z), z^{-1}\right] \\ &= \mu\left[y, \mu(z, z^{-1})\right] \\ &= \mu(y,e) \\ &= y. \end{aligned}$$

(ii) De $\mu(z,x) = \mu(z,y)$, vem que
$$\begin{aligned} x &= \mu\left[z^{-1}, \mu(z,x)\right] \\ &= \mu\left[z^{-1}, \mu(z,y)\right] \\ &= \mu\left[\mu(z^{-1}, z), y)\right] \\ &= \mu(e,y) \\ &= y. \end{aligned}$$

□

Exemplo 4.36.

Para cada número $m \in \mathbb{N} = \{1, 2, \ldots\}$, o conjunto $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ com a operação binária interna de adição $\mod m$ é definido como o grupo aditivo comutativo $(\mathbb{Z}_m, +)$, cujo elemento neutro é 0, em que, para $i,\ j \in \{0, 1, \ldots, m-1\}$, a soma $i + j \mod m$ é o resto da divisão da soma usual das parcelas i e j pelo número natural m.

Teorema 4.37.

Seja (M, μ) um monoide com elemento neutro e e seja o conjunto $U(M)$ o subconjunto de M constituído por todos os elementos inversíveis de M. Então, o par ordenado $(U(M), \mu)$ é um grupo.

Definição 4.38.

Um homomorfismo de grupo h do grupo (G, μ) no grupo (G', ν) é simplesmente um homomorfismo de semigrupo h do semigrupo subjacente (G, μ) no semigrupo subjacente (G', ν).

Teorema 4.39.

Seja h um monomorfismo de grupo do grupo (G, μ) com elemento neutro e no grupo (G', ν) com elemento neutro e'. Então, o núcleo $N(h)$ de h, definido por

$$N(h) = \{x \in G : h(e) = e'\},$$

é o conjunto unitário constituído pelo elemento e e, reciprocamente, se $N(h) = e$, então h é um monomorfismo de grupo do grupo (G, μ) com elemento neutro e no grupo (G', ν) com elemento neutro e'.

Propriedades 4.40.

O par ordenado $(HomG, \circ)$ é um monoide com a operação binária interna $\circ$ de composição de funções, em que $HomG$ é o conjunto de todos os homomorfismos de grupo do grupo (G, μ) no grupo (G, μ).

O par ordenado $(AutG, \circ)$ é um grupo com a operação binária interna $\circ$ de composição de funções, em que $AutG$ é o conjunto de todos os isomorfismos de grupo do grupo (G, μ) no grupo (G, μ), lembrando que $AutG = U\big[HomG\big]$.

Definição 4.41.

Seja H um subconjunto não vazio de um conjunto não vazio G, em que (G, μ) é um grupo com elemento neutro e. Então, (H, μ) é um subgrupo de (G, μ) se, e somente se,

(i) $e \in H$.

(ii) se $x, y \in H$, então $\mu(x, y) \in H$.

(iii) para cada $x \in H$, o elemento inverso x^{-1} de x pertence a H.

Teorema 4.42.

Seja H um subconjunto não vazio de um conjunto G, em que (G,μ) é um grupo. Uma condição necessária e suficiente para que (H,μ) seja um subgrupo de (G,μ) é que, para cada x, $y \in H$,

$$\mu(x,y^{-1}) \in H.$$

Definição 4.43.

Seja (G,μ) um grupo. O centro $Z(G)$ é o conjunto de todos os elementos z do conjunto G com a propriedade: para cada $x \in G$, $\mu(x,z) = \mu(z,x)$.

Definição 4.44.

Seja (G,μ) um grupo. Para cada elemento $a \in G$, o centralizador $C_G(a)$ é o conjunto de todos os elementos x do conjunto G tal que $\mu(a,x) = \mu(x,a)$. A intersecção de todos os conjuntos centralizadores dos elementos do conjunto G é igual ao centro $Z(G)$ de G.

Propriedade 4.45.

$(Z(G),\mu)$ é um subgrupo de (G,μ).

Demonstração.

Para z_1 e z_2 em $Z(G)$ e para $x \in G$,

$$\begin{aligned}\mu\left[z_1,\mu(z_2,x)\right] &= \mu\left[z_1,\mu(x,z_2)\right]\\ &= \mu\left[\mu(z_1,x),z_2\right]\\ &= \mu\left[\mu(x,z_1),z_2\right]\\ &= \mu\left[x,\mu(z_1,z_2)\right].\end{aligned}$$

Para $z \in Z(G)$ e $x \in G$,

$$\begin{aligned}\mu(z^{-1},x) &= \left[\mu(x^{-1},z)\right]^{-1}\\ &= \left[\mu(z,x^{-1})\right]^{-1}\\ &= \mu(x,z^{-1}).\end{aligned}$$

□

Propriedade 4.46.

Seja (G,μ) um grupo. Para cada elemento $a \in G$, $(C_G(a),\mu)$ é um subgrupo do grupo (G,μ).

Demonstração.

Sejam x e y elementos do conjunto centralizador do elemento a, então $\mu(x,a) = \mu(a,x)$ e $\mu(y,a) = \mu(a,y)$. Para provar que $\mu(x,y^{-1}) \in C_G(a)$,

$$\begin{aligned}
\mu\left[\mu(x^{-1},y),a\right] &= \mu\left[x^{-1},\mu(y,a)\right] \\
&= \mu\left[x^{-1},\mu(a,y)\right] \\
&= \mu\left[\mu(x^{-1},a),y\right] \\
&= \mu\left[\mu(a,x^{-1}),y\right] \\
&= \mu\left[a,\mu(x^{-1},y)\right],
\end{aligned}$$

desde que, de $\mu(x,a) = \mu(a,x)$, segue que

$$\mu(x^{-1},a) = \mu(a,x^{-1}),$$

pois $a = \mu\left[x^{-1},\mu(a,x)\right]$ e

$$\mu(a,x^{-1}) = \mu\left[\mu(x^{-1},a),\mu(x,x^{-1})\right] = \mu\left[\mu(x^{-1},a),e\right] = \mu(x^{-1},a),$$

em que e é o elemento neutro do grupo (G,μ). □

Propriedade 4.47.

A intersecção de uma família de subgrupos de um grupo (G,μ) é um subgrupo deste grupo (G,μ).

Definição 4.48.

Seja A um subconjunto não vazio de um conjunto G, em que (G,μ) é um grupo. O subgrupo gerado pelo conjunto A é definido como a intersecção de todos os subgrupos do grupo que contém o conjunto A e é indicado pelo símbolo $< A >$. Em particular, $< a >$ indica o subgrupo gerado por um único elemento $a \in G$.

Propriedades 4.49.

Dados dois grupos (G,μ) e (G',ν) e um homomorfismo de grupo h do grupo (G,μ) no grupo (G',ν), então:

(i) O elemento neutro e de (G,μ) é aplicado por h no elemento neutro e' de (G',ν).

(ii) Para cada $x \in G$, o valor da função h no elemento inverso x^{-1} de x é igual ao elemento inverso $h(x)^{-1}$ de $h(x)$, isto é $h(x^{-1}) = \left[h(x)\right]^{-1}$.

(iii) Se (H,μ) é um subgrupo do grupo (G,μ), então $(h(H),\nu)$ é um subgrupo do grupo (G',ν). Em particular, $(h(G),\mu)$ é um subgrupo de (G',ν).

(iv) Se (H', ν) é um subgrupo do grupo (G', ν), então $(h^{-1}(H'), \mu)$ é um subgrupo do grupo (G, μ). Em particular, $(h^{-1}(\{e\}), \mu)$ é um subgrupo de (G, μ).

Seja (H, μ) um subgrupo de um grupo (G, μ). Então, o subgrupo (H, μ) induz duas relações binárias de equivalência no conjunto G: a relação binária de equivalência R_H^+ e R_H^-, denominadas relações de equivalências módulo H à direita e módulo H à esquerda, respectivamente, definidas por:

$$R_H^+ = \{(x,y) \in G \times G : \mu(x, y^{-1}) \in H\}$$

$$R_H^- = \{(x,y) \in G \times G : \mu(x^{-1}, y) \in H\}.$$

De fato, R_H^+ e R_H^- são relações binárias de equivalência no conjunto G por apresentar as propriedades reflexiva, simétrica e transitiva:

(i) (Reflexiva) Para cada $x \in G$, $(x,x) \in R_H^+$ e $(x,x) \in R_H^-$, pois $\mu(x, x^{-1}) = \mu(x^{-1}, x) = 1 \in H$.

(ii) (Simétrica) Para os elementos x, y no conjunto G, se $(x,y) \in R_H^+$, então $(y,x) \in R_H^+$ (ou se $(x,y) \in R_H^-$, então $(y,x) \in R_H^-$):

De $(x,y) \in R_H^+$, vem que $\mu(x, y^{-1}) \in H$ e $\mu(y, x^{-1}) = \mu(x, y^{-1})^{-1} \in H$ e $(y,x) \in R_H^+$. A demonstração da propriedade simétrica para R_H^- é análoga.

(iii) (Transitiva) Para os elementos x, y e z no conjunto G, se $(x,y) \in R_H^+$ e se $(y,z) \in R_H^+$, então $(x,z) \in R_H^+$ (ou se $(x,y) \in R_H^-$ e se $(y,z) \in R_H^-$, então $(x,z) \in R_H^-$):

De $(x,y) \in R_H^+$ e de $(y,z) \in R_H^+$, $\mu(x, y^{-1}) \in H$ e $\mu(y, z^{-1}) \in H$; assim, $\mu(x, z^{-1}) = \mu\left[\mu(x, y^{-1}), \mu(y, z^{-1})\right] \in H$ e $(x,z) \in R_H^+$. A demonstração da propriedade transitiva para R_H^- é análoga.

A classe de equivalência, segundo R_H^+, do elemento $x \in G$ é o conjunto $\{\mu(h,x) : h \in H\}$ e, analogamente, a classe de equivalência, segundo R_H^-, do elemento $x \in G$ é o conjunto $\{\mu(x,h) : h \in H\}$.

De fato, para cada elemento $y \in G$ com $(x,y) \in R_H^+$, $\mu(x, y^{-1}) \in H$, ou seja, existe um elemento $h \in H$ tal que $\mu(x, y^{-1}) = h$ e, em consequência, $\mu(y, x^{-1}) = h^{-1}$ e $y = \mu(h^{-1}, x)$, com $h^{-1} \in H$. A inclusão reversa é trivial.

A classe lateral à direita módulo H do elemento $x \in G$ é definida como a classe de equivalência de $x \in G$ segundo R_H^+, enquanto que a classe lateral à direita módulo H do elemento $x \in G$ é definida como a classe de equivalência de $x \in G$ segundo R_H^-.

A função que associa, à classe lateral à direita módulo H do elemento $x \in G$, a classe lateral à esquerda do elemento inverso, é uma função total injetora e sobrejetora do conjunto das classes laterais à direita módulo H sobre o conjunto das classes laterais à esquerda módulo H.

A função que associa, a cada elemento h do conjunto H, o elemento $\mu(h,x)$, pertencente à classe lateral à direita módulo H do elemento $x \in G$ fixado, é uma função total injetora e sobrejetora do conjunto H sobre a classe lateral à direita módulo H de um elemento $x \in G$ fixado.

Em um grupo (G,μ) com um número finito de elementos, seja (H,μ) um subgrupo de (G,μ). O número de classes laterais à direita módulo H (que é igual ao número de classes laterais à esquerda módulo H) é denominado o índice do subgrupo (H,μ) no grupo (G,μ) e é indicado pelo símbolo $\big[G:H\big]$. O número de elementos de cada classe lateral à esquerda e à direita módulo H são iguais ao número de elementos de H, lembrando que o conjunto das classes laterais à direita módulo H, assim como o conjunto das classes laterais à esquerda módulo H, constituem uma partição do conjunto G.

Teorema 4.50 (Teorema de Lagrange)**.**

Seja (H,μ) um subgrupo de um grupo (G,μ) em que o número $|G|$ de elementos de G é finito. Então,

$$|G| = \big[G:H\big]|H|,$$

em que $|H|$ é o número de elementos do conjunto H, isto é, o número $|H|$ de elementos do conjunto H divide o número $|G|$ de elementos do conjunto G.

Em particular, a ordem de um elemento $a \in G$, que é definida como o número de elementos do subgrupo gerado por a, em que (G,μ) é um grupo com um número finito de elementos, divide o número $|G|$ de elementos do grupo G.

Para quais subgrupos (N,μ) de um grupo (G,μ), a relação binária de equivalência R_N^+ definida no conjunto G é compatível à esquerda e à direita com a operação binária interna μ do grupo? Isto é, para quais subgrupos (N,μ) de um grupo (G,μ) é válido que, se $(x,y) \in R_N^+$, então:

$$(\mu(z,x),\mu(z,y)) \in R_N^+$$

$$(\mu(x,z),\mu(y,z)) \in R_N^+,$$

em que x, y e z são elementos do conjunto G, ou seja, se $\mu(x,y^{-1}) \in N$, então, para cada $z \in G$,

$$\begin{aligned}\mu\big[\mu(z,x),\mu(z,y)^{-1}\big] &= \mu\big[\mu(z,x),\mu(y^{-1},z^{-1})\big] \\ &= \mu\Big[z,\mu\big[\mu(x,y^{-1}),z^{-1}\big]\Big] \in N,\end{aligned}$$

e se $\mu(x,y^{-1}) \in N$, então, para cada $z \in G$,

$$\begin{aligned}\mu\big[\mu(x,z),\mu(y,z)^{-1}\big] &= \mu\big[\mu(x,z),\mu(z^{-1},y^{-1})\big] \\ &= \mu(x,y^{-1}) \in N?\end{aligned}$$

As considerações agora feitas sugerem a definição de subgrupo normal de um grupo.

Definição 4.51.

Um subgrupo (N,μ) de um grupo (G,μ) é um subgrupo normal em G quando, e somente quando, para cada $x \in G$ e para cada $n \in N$,

$$\mu\left[x,\mu(n,x^{-1})\right] \in N$$

ou, equivalentemente, para cada $x \in G$ e para cada $n \in N$,

$$\mu\left[x^{-1},\mu(n,x)\right] \in N.$$

Propriedade 4.52.

As relações binárias de equivalência R_N^+ e R_N^- no conjunto G induzidas pelo subgrupo normal (N,μ) em (G,μ) são iguais e a relação binária de equivalência módulo N é indicada por R_N, ou seja, $R_N = R_N^+ = R_N^-$.

Demonstração.

De fato, para elementos x e y no conjunto G, se $(x,y) \in R_N^+$, então $\mu(x,y^{-1}) \in N$ e, em consequência,

$$\mu\left[x^{-1},\mu\left[\mu(x,y^{-1}),x\right]\right] = \mu(x^{-1},y) \in N,$$

pelo fato de N ser um subgrupo normal em G, o que prova que $(x,y) \in R_N^-$ e que $R_N^+ \subset R_N^-$. A demonstração da inclusão reversa é análoga. □

Além disso, a relação binária de equivalência R_N no conjunto G é compatível à esquerda e à direita com a operação binária interna μ do grupo (G,μ).

De fato, para os elementos x, y e z no conjunto G, tal que $(x,y) \in R_N$, vem que

$$(\mu(z,x),\mu(z,y)) \in R_N$$

$$(\mu(x,z),\mu(y,z)) \in R_N,$$

pois

$$\begin{aligned}\mu\left[\mu(z,x),\mu(z,y)^{-1}\right] &= \mu\left[\mu(z,x),\mu(y^{-1},z^{-1})\right] \\ &= \mu\left[\mu\left[z,\mu(x,y^{-1})\right],z^{-1}\right] \in N,\end{aligned}$$

desde que $\mu(x,y^{-1}) \in N$ e (N,μ) é um subgrupo normal em (G,μ) e se $\mu(x,y^{-1}) \in N$, então, para cada $z \in G$,

$$\begin{aligned}\mu\left[\mu(x,z),\mu(y,z)^{-1}\right] &= \mu\left[\mu(x,z),\mu(z^{-1},y^{-1})\right] \\ &= \mu(x,y^{-1}) \in N.\end{aligned}$$

Reciprocamente, seja R uma relação binária de equivalência no conjunto G compatível à esquerda e à direita com a operação binária interna μ do grupo (G,μ). Então, a classe de equivalência N do elemento neutro e do grupo é tal que (N,μ) é subgrupo normal de (G,μ).

De fato, para os elementos $x \in G$ e $n \in N$, como $(n,e) \in R$,

$$(\mu(x,n),\mu(x,e)) = (\mu(x,n),x) \in R$$

$$\left(\mu\left[\mu\left(x,n\right),x^{-1}\right],\mu(x,x^{-1})\right) = \left(\mu\left[x,\mu(n,x^{-1})\right],e\right) \in R,$$

o que é equivalente a afirmar que $\mu\left[x,\mu(n,x^{-1})\right] \in N$, a classe de equivalência do elemento neutro e segundo R.

Exemplo 4.53.

Seja (G,μ) um grupo. A relação binária R_c de conjugação no conjunto G é definida como: para elementos x e y no conjunto G, $(x,y) \in R_c$ se, e somente se, existe um elemento $z \in G$ tal que $y = \mu\left[z,\mu(x,z^{-1})\right]$ é uma relação binária de equivalência no conjunto G.

Teorema 4.54.

Seja (G,μ) um grupo. Então, $(Z(G),\mu)$ é um subgrupo normal do grupo (G,μ).

Demonstração.

Para cada elemento $x \in G$ e, para cada elemento $z \in Z(G)$,

$$\mu\left[x,\mu(z,x^{-1})\right] = \mu\left[x,\mu(x^{-1},z)\right] = \mu\left[\mu(x,x^{-1}),z\right] = z \in Z(G).$$

□

Propriedade 4.55.

Os subgrupos triviais de um grupo (G,μ) com elemento neutro e são $(\{e\},\mu)$ e o próprio (G,μ); além disso, os subgrupos triviais são subgrupos normais no grupo (G,μ).

Propriedade 4.56.

Em um grupo (G,μ) comutativo, todos os subgrupos de (G,μ) são subgrupos normais.

Exemplo 4.57.

Seja $(X_4,\cdot)$ o grupo de Klein, multiplicativo e comutativo, em que $X_4 = \{1,2,3,4\}$, e a operação binária interna é dada pela tabela de Cayley abaixo:

	1	**2**	**3**	**4**
1	1	2	3	4
2	2	1	4	3
3	3	4	3	4
4	4	3	4	3

Os subgrupos normais não triviais no grupo de Klein são $(\{1,2\},\cdot)$, $(\{1,3\},\cdot)$ e $(\{1,4\},\cdot)$ que definem, respectivamente, três relações binárias de equivalência compatíveis à esquerda e à

direita com a operação binária interna do grupo, cujas classes de equivalência são $\{1,2\}\cup\{3,4\}$, $\{1,3\}\cup\{2,4\}$ e $\{1,4\}\cup\{2,3\}$.

Alguns autores apresentam o grupo de Klein como o conjunto das quatro matrizes abaixo com a operação binária interna de multiplicação usual para matrizes:

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$$

Teorema 4.58.

Seja h um homomorfismo de grupo do grupo (G,μ) no grupo (G',ν) com elemento neutro e'. Então:

(i) Para cada subgrupo normal (N',ν) no grupo (G',ν), $(h^{-1}(N'),\mu)$ é subgrupo normal no grupo (G,μ) e, em particular, $(h^{-1}(e'),\mu)$ é um subgrupo normal no grupo (G,μ).

(ii) Se h é um epimorfismo de grupo do grupo (G,μ) sobre o grupo (G',ν), então, para cada subgrupo normal (N,μ) no grupo (G,μ), $(h(N),\nu)$ é um subgrupo normal no grupo (G',ν).

Em resumo, com a notação multiplicativa da operação binária interna μ de um grupo (G,μ), isto é, denotando $\mu(x,y)=x*y$ para elementos x e y do conjunto G,

(i) a afirmação de que $(H,*)$ é um subgrupo do grupo $(G,*)$ é equivalente à afirmação de que, para elementos x e y em H, $x*y^{-1}\in H$ ou, equivalentemente, $y*x^{-1}=(x*y^{-1})^{-1}\in H$.

(ii) a afirmação de que $(N,*)$ é um subgrupo normal do grupo $(G,*)$ é equivalente à afirmação de que, para cada $x\in G$ e para cada $n\in N$, $x*n*x^{-1}\in N$ ou, equivalentemente, $x^{-1}*n*x\in N$ e, além disso, a classe lateral à direita módulo N de um elemento $a\in G$, indicada por $Na=\{n*a:n\in N\}$, coincide com a classe lateral à esquerda módulo N, indicada por $aN=\{a*n:n\in N\}$.

Com a notação aditiva da operação binária interna μ de um grupo (G,μ), isto é, denotando $\mu(x,y)=x+y$ para elementos x e y do conjunto G,

(i) a afirmação de que $(H,+)$ é um subgrupo do grupo $(G,+)$ é equivalente à afirmação de que, para elementos x e y em H, $x+(-y)\in H$ ou, equivalentemente, $(-x)+y\in H$, em que $-x$ é a notação para o elemento inverso aditivo de x.

(ii) a afirmação de que $(N,+)$ é um subgrupo normal do grupo $(G,+)$ é equivalente à afirmação de que, para cada $x\in G$ e para cada $n\in N$, $(-x)+(n+x)\in N$ ou, equivalentemente, $(x+n)+(-x)\in N$ e, além disso, a classe lateral à direita módulo N de um elemento $a\in G$,

indicada por $Na = \{n + a : n \in N\}$, coincide com a classe lateral à esquerda módulo N, indicada por $aN = \{a + n : n \in N\}$.

Teorema 4.59.

Seja $(N, *)$ um subgrupo do grupo $(G, *)$ tal que o índice de N em G é igual a dois. Então, $(N, *)$ é um subgrupo normal no grupo $(G, *)$.

Demonstração.

As duas classes de equivalência módulo N à direita são N e Na, com $a \notin N$ e as duas classes de equivalência módulo N à esquerda são N e aN, com $a \notin N$. Então, $Na = aN$ e $(N, *)$ é subgrupo normal no grupo $(G, *)$. □

Teorema 4.60.

Seja $(N, *)$ um subgrupo normal no grupo $(G, *)$ e seja G/N o conjunto de todas as classes laterais à direita módulo N, que é igual ao conjunto de todas as classes laterais à esquerda módulo N. Então, G/N com a operação binária interna $*$ é definida por: para elementos x e y em G,

$$xN * yN = (x * y)N.$$

O conjunto G/N é o conjunto quociente G/R_N, desde que R_N é uma relação binária de equivalência no conjunto G.

Demonstração.

Para elementos x, x', y e y' pertencentes ao conjunto G, se $xN = x'N$ e se $yN = y'N$, então, de $(x, x') \in R_N$ e de $(y, y') \in R_N$, segue que $(x * y, x' * y') \in R_N$ e que $(x * y)N = (x' * y')N$.

O elemento neutro em G/N é o próprio conjunto N, enquanto que, para cada $x \in G$, o elemento inverso $(xN)^{-1}$ de xN é $x^{-1}N$. □

Definição 4.61.

Seja h um homomorfismo de grupo do grupo $(G, *)$ no grupo $(G', \diamond)$. O núcleo $N(h)$ de h é definido como a imagem inversa do elemento neutro do grupo $(G', \diamond)$, ou seja,

$$N(h) = \{x \in G : h(x) = e'\},$$

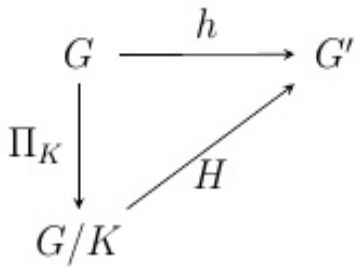
em que e' é o elemento neutro do grupo $(G', \diamond)$.

Teorema 4.62 (Primeiro teorema do isomorfismo para grupos)**.**

Seja h um homomorfismo de grupo do grupo $(G, *)$ no grupo $(G', \diamond)$ em que e e e' são os elementos nutros dos grupos $(G, *)$ e $(G', \diamond)$ respectivamente. Então:

(i) O núcleo $N(h)$ de h é um subgrupo normal do grupo $(G,*)$.

(ii) Se $(K,*)$ é um subgrupo normal no grupo $(G,*)$ tal que K está contido no núcleo $N(h)$ de h, então existe um monomorfismo de grupo H do grupo quociente $(G/K,*_K)$ no grupo $(G',\diamond)$ tal que o diagrama abaixo é comutativo:



ou seja, $h = H \circ \Pi_K$ e, além disso, H é um isomorfismo de grupo do grupo quociente $(G/K,*_K)$ no subgrupo $(h(G),\diamond)$ do grupo $(G,\diamond)$.

Demonstração.

A função H associa, a cada classe lateral Kx de K em G, o elemento $h(x)$ do conjunto G' e esta função é bem definida, pois é independente da escolha do representante x da classe lateral Kx. De fato, para x, $x' \in G$ tal que $Kx = Kx'$ ou, equivalentemente, $x' * x^{-1} \in K$ e $h(x' * x^{-1}) = h(x') * h(x^{-1}) = h(x') * h(x)^{-1} = e'$, isto é, $h(x) = h(x')$. Portanto, $H(Kx) = h(x) = H(Kx') = h(x')$.

A verificação de que H é um monomorfismo de grupo é imediata. □

Definição 4.63.

Seja $(G,*)$ um grupo. Para cada $x \in G$, seja o homomorfismo de grupo f_x do grupo $(G,*)$ no grupo $(G,*)$, definido por: para cada $y \in G$, $f_x(y) = x * (y * x^{-1})$. Então, para cada $x \in G$, f_x é um isomorfismo de grupo do grupo $(G,*)$ no grupo $(G,*)$ denominado automorfismo interno do grupo G.

Exemplo 4.64.

Seja $(G,*)$ um grupo. O conjunto InG é o conjunto de todos os automorfismos internos do grupo $(G,*)$. O conjunto InG com a operação binária interna de composição é um subgrupo do grupo dos automorfismos $(AutG,\circ)$ do grupo $(G,*)$.

Exemplo 4.65.

Seja $(G,*)$ um grupo e seja h a função que associa a cada elemento $x \in G$ o automorfismo interno f_x do grupo $(G,*)$. Então, h é um epimorfismo de grupo do grupo $(G,*)$ no grupo

$(In(G),\circ)$, cujo núcleo $N(h)$ é igual ao conjunto centralizador $Z(G)$ de G. Pelo primeiro teorema do isomorfismo para grupos, o grupo quociente $(G/Z(G),*_{Z(G)})$ é isomorfo ao grupo $(In(G),\circ)$.

Teorema 4.66 (Segundo teorema do isomorfismo para grupos)**.**

Sejam $(S,*)$ e $(T,*)$ subgrupos do grupo $(G,*)$ em que $(T,*)$ é um subgrupo normal em $(G,*)$. Então:

(i) $(S\cap T,*)$ é um subgrupo normal em $(T,*)$.

(ii) O subgrupo gerado pela união $S\cup T$ dos subconjuntos S e T coincide com

$$ST = TS = \{s*t : s\in S \text{ e } t\in T\}.$$

(iii) Existe um isomorfismo de grupo H do grupo quociente $(S/S\cap T,*_{S\cap T})$ no grupo quociente $(ST/T,*_T)$.

Demonstração.

Por hipótese, $(T,*)$ é um subgrupo normal em $(G,*)$. Se s_1, $s_2\in T$ e t_1, $t_2\in T$,

$$s_1*t_1\in ST$$

$$s_2*t_2\in ST$$

$$\begin{aligned}(s_1*t_1)*(s_2*t_2)^{-1} &= (s_1*t_1)*(t_2^{-1}*s_2^{-1})\\ &= s_1*(t_1*t_2^{-1})*s_2^{-1}\\ &= s_1*t_3*s_2^{-1},\text{ em que } t_3 = t_1*t_2^{-1}\in T\\ &= s_1*s_2^{-1}*t_4,\text{ em que } t_4 = s_2*t_3*s_2^{-1}\in T\\ &= s_3*t_4,\text{ em que } s_3 = s_1*s_2^{-1}\in S.\end{aligned}$$

Seja Π_T o homomorfismo natural de grupo do grupo $(G,*)$ no grupo quociente $(G/T,*_T)$ e seja i_S o homomorfismo inclusão do grupo S no grupo G. Se $h=\Pi_T\circ i_S$, então, para $s\in S$,

$$(\Pi_T\circ i_S) = \Pi_T\left[i_S(s)\right] = \Pi_T(s) = Ts.$$

O núcleo do homomorfismo de grupo h do grupo $(S,*)$ no grupo imagem por h é $S\cap T$ e o grupo imagem por h é constituído por todas as classes laterais de T cujos representantes pertencem a S que são precisamente as classes laterais de T cujos representantes pertencem a ST. □

Corolário 4.67.

Sejam $(S,*)$ e $(T,*)$ subgrupos de um grupo $(G,*)$, o qual possui um número finito de elementos, sendo que $(T,*)$ é um subgrupo normal em $(G,*)$. Então, é válida a seguinte fórmula:

$$|S||T| = |S\cap T||S\cup T| = |S\cap T||ST|.$$

Exemplo 4.68.

Seja o grupo aditivo comutativo $(\mathbb{Z},+)$. A intersecção dos subgrupos cíclicos $3\mathbb{Z}\cap 4\mathbb{Z}$ é igual a $12\mathbb{Z}$ e a soma $3\mathbb{Z}+4\mathbb{Z}$ é igual a $\mathbb{Z}$, o que significa que todo número inteiro é soma de um múltiplo de 3 com um múltiplo de 4, pois o máximo divisor comum entre 3 e 4 é igual a 1 e, portanto, existem números inteiros r e s tais que $1 = 3r+4s$. Então, existe um isomorfismo de grupo do grupo quociente aditivo $3\mathbb{Z}/12\mathbb{Z}$ no grupo quociente $\mathbb{Z}/4\mathbb{Z} = (3\mathbb{Z}+4\mathbb{Z})/4\mathbb{Z}$.

Teorema 4.69 (Terceiro teorema do isomorfismo para grupos)**.**

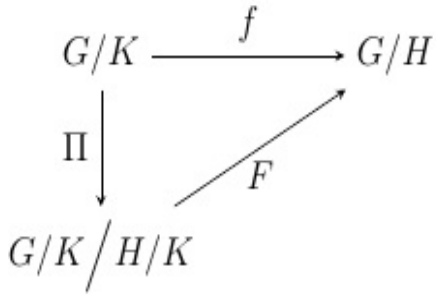
Sejam $(H,*)$ e $(K,*)$ subgrupos normais no grupo $(G,*)$ tal que $K \subset H$. Então:

(i) O grupo quociente $(H/K,*)$ é um subgrupo normal no grupo quociente $(G/K,*_K)$.

(ii) $G/K\Big/H/K \simeq G/H$, o que significa que existe um isomorfismo de grupo F do grupo quociente $\left(G/K\Big/H/K,*_{H/K}\right)$ no grupo quociente $(G/H,*_H)$.

Demonstração.

O primeiro teorema do isomorfismo aplicado ao homomorfismo de grupo f do grupo quociente $(G/K,*)$ no grupo quociente, definido por: para $x \in G$, $f(kx) = Hx$, prova a existência de um isomorfismo de grupo F do grupo quociente $\left(G/K\Big/H/K,*_{H/K}\right)$ no grupo quociente $(G/H,*)$ de modo que o diagrama abaixo é comutativo:



lembrando que o núcleo de f é H/K e que f é um epimorfismo de grupo do grupo quociente $(G/K,*_K)$ no grupo quociente $(G/H,*_H)$. □

Teorema 4.70.

Seja $(K,*)$ um subgrupo do grupo $(G,*)$ e seja h um homomorfismo de grupo do grupo $(G,*)$ no grupo $(G',\diamond)$, sendo $N(h)$ o núcleo de h. Então, para cada $x \in h^{-1}\left[h(K)\right]$, existem elementos $y \in K$ e $z \in N(h)$ tal que $x = y*z$ e, reciprocamente, se $y \in K$ e $z \in N(h)$ então $y*z \in h^{-1}\left[h(K)\right]$.

Demonstração.

Seja $x \in h^{-1}\big[h(K)\big]$. Então, existe $y \in K$ tal que $h(x) = h(y)$ ou $h(x * y^{-1}) = e'$, em que e' é o elemento neutro do grupo $(G', \diamond)$. Portanto, $x = (x * y^{-1}) * y$, com $x * y^{-1} \in N(h)$ e $y \in K$. Reciprocamente, seja $y \in K$ e $z \in N(h)$ tal que $x = y * z$. Então, $h(x) = h(y) \in h(K)$ e, portanto, $x \in h^{-1}\big[h(K)\big]$. □

Corolário 4.71.

Seja $(K, *)$ um subgrupo do grupo $(G, *)$ e seja h um homomorfismo de grupo do grupo $(G, *)$ no grupo $(G', \diamond)$ tal que $K = h^{-1}\big[h(K)\big]$. Então, $N(h) \subset K$.

Teorema 4.72.

Seja $(K, *)$ um subgrupo do grupo $(G, *)$ e seja h um homomorfismo de grupo do grupo $(G, *)$ no grupo $(G', \diamond)$ tal que o núcleo $N(h)$ de h está contido em K. Então, $K = h^{-1}\big[h(K)\big]$.

Demonstração.

Para cada subconjunto A do conjunto $A \subset h^{-1}\big[h(A)\big]$. Para demonstrar a inclusão reversa, seja $x \in h^{-1}\big[h(K)\big]$. Então, $h(x) \in h(K)$ e existe $y \in K$ tal que $h(x) = h(y)$ ou $x * y^{-1} \in N(h) \subset K$, isto é, existe $z \in K$ tal que $z = x * y^{-1}$ e $x = z * y \in K$. □

Teorema 4.73.

Seja $(N, *)$ um subgrupo normal no grupo $(G, *)$ e seja h um homomorfismo de grupo do grupo $(G, *)$ no grupo $(G', \diamond)$ tal que o núcleo $N(h)$ de h está contido em N. Então, existe um isomorfismo de grupo do grupo quociente $(G/N, *_N)$ no grupo quociente $(h(G)/h(N), *_{h(N)})$.

Demonstração.

Seja $\tilde{h}$ o homomorfismo de grupo que associa, a cada elemento $x \in G$, a classe lateral de $h(x)$ segundo a congruência $R_{h(N)}$ e o núcleo de $\tilde{h}$ coincide com o conjunto $h^{-1}\big[h(N)\big]$, que é igual a N. □

Teorema 4.74 (Teorema da correspondência para grupos)**.**

Seja $(K, *)$ um subgrupo normal no grupo $(G, *)$ e seja Π_K o epimorfismo natural do grupo $(G, *)$ sobre o grupo quociente $(G/K, *_K)$. Então, Π_K estabelece uma correspondência biunívoca entre o conjunto de todos os subgrupos de $(G, *)$ que contém K e o conjunto de todos os subgrupos do grupo quociente $(G/K, *_K)$.

Teorema 4.75.

Seja $(H, +)$ um subgrupo do grupo aditivo $(\mathbb{Z}, +)$. Então, ou $H = \{0\}$ ou existe um número $m \in \mathbb{N} = \{1, 2, \ldots\}$ tal que $H = m\mathbb{Z}$, sendo m o menor número natural pertencente a H.

Demonstração.

Seja $(H,+)$ um subgrupo do grupo aditivo $(\mathbb{Z},+)$. Então, ou $H=\{0\}$ ou H contém um número natural e seja m o menor número natural pertencente a H. É trivial a inclusão

$$m\mathbb{Z}=\{\ldots,-2m,-m,0,m,2m,\ldots\}\subset H.$$

Para a inclusão reversa, seja um elemento $h\in H$ e, assim, existem números inteiros q e r tais que $r\in\{0,1,\ldots,m-1\}$ e $h=mq+r$ pelo algoritmo da divisão ou $r=h-qm\in H$ pela inclusão anterior. Pela minimalidade de m, $r=0$ e $h=qm$, o que prova que

$$H\subset\{\ldots,-2m,-m,0,m,2m,\ldots\}=m\mathbb{Z}.$$

Para cada número $m\in\mathbb{N}=\{1,2,\ldots\}$,

$$m\mathbb{Z}=-m\mathbb{Z}$$

e o grupo aditivo $(m\mathbb{Z},+)$ tem apenas dois geradores, a saber m e $-m$. □

Em resumo, os subgrupos aditivos do grupo aditivo comutativo $(\mathbb{Z},+)$ são:

$0\mathbb{Z}=\{0\}$

$1\mathbb{Z}=-1\mathbb{Z}=\mathbb{Z}$

$2\mathbb{Z}=-2\mathbb{Z}=\{\ldots,-4,-2,0,2,4,\ldots\}$

$3\mathbb{Z}=-3\mathbb{Z}=\{\ldots,-6,-3,0,3,6,\ldots\}$

E assim sucessivamente.

Para cada número $m\in\{1,2,\ldots\}$, $(m\mathbb{Z},+)$ é um subgrupo normal em $(\mathbb{Z},+)$ e a relação de equivalência módulo $m\mathbb{Z}$ à esquerda e à direita coincidem com a relação binária de equivalência R_m definida por: para os números inteiros a e b, $(a,b)\in R_m$ quando, e somente quando, os restos da divisão de a e b por m são iguais, ou seja, quando, e somente quando, $b-a\in m\mathbb{Z}$.

Para os números naturais $m,n\in\mathbb{N}\{1,2,\ldots\}$, $m\mathbb{Z}\cap n\mathbb{N}=\text{mmc}(m,n)\mathbb{Z}$, em que mmc é o mínimo múltiplo comum entre os números naturais m e n.

Teorema 4.76 (Teorema da estrutura dos grupos cíclicos)**.**

(i) Seja $(G,*)$ um grupo cíclico infinito gerado por um elemento $a\in G$. Então, $(G,*)$ é isomorfo ao grupo aditivo $(\mathbb{Z},+)$.

(ii) Seja $(G,*)$ um grupo cíclico finito com m elementos gerado por um elemento $a\in G$. Então, $(G,*)$ é isomorfo ao grupo aditivo $(m\mathbb{Z},+)$.

Demonstração.

Seja F a função que associa a cada número $n \in \mathbb{N} = \{1,2,\ldots\}$, o elemento $a^n = a * a * \ldots * a$ (n vezes) e $a^{-n} = a^{-1} * a^{-1} * \ldots * a^{-1}$ caso n é um número natural e associa ao número zero o elemento $a^0 = e$, em que e é o elemento neutro do grupo $(G,*)$. Então, F é um epimorfismo de grupo do grupo aditivo $(\mathbb{Z},+)$ no grupo cíclico $(G,+)$ gerado pelo elemento a.

Caso o núcleo do epimorfismo F é $\{0\}$, então F é um isomorfismo de grupo do grupo $(\mathbb{Z},+)$ no grupo $(G,*)$.

Caso o núcleo do epimorfismo F é $m\mathbb{Z}$ para algum número natural m, m é o menor número natural tal que $a^m = e$.

Para os inteiros r, $s \in \mathbb{Z}$, as afirmações são equivalentes:

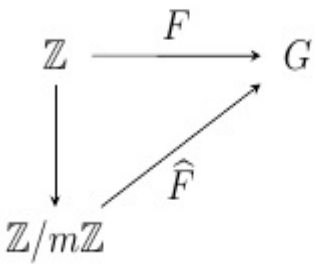
(i) $a^r = a^s$.

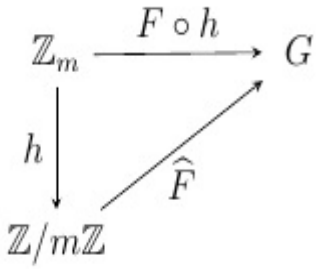
(ii) $a^{r-s} = e$.

(iii) $r - s \in m\mathbb{Z}$.

(iv) m divide $r - s$.

Pelo primeiro teorema do isomorfismo de grupos, a função $\widehat{F}$ é um isomorfismo de grupo do grupo quociente aditivo $(\mathbb{Z}/m\mathbb{Z},+)$ sobre o grupo $(G,*)$, lembrando que a função h, que associa, a cada elemento $n \in \{0,1,\ldots,m-1\}$, a classe lateral $n + m\mathbb{Z}$ à esquerda e à direita módulo $m\mathbb{Z}$, é um isomorfismo de grupo do grupo aditivo $(\mathbb{Z}_m,+)$ no grupo quociente aditivo $(\mathbb{Z}/m\mathbb{Z},+)$ e, assim, $\widehat{F} \circ h$ é um isomorfismo de grupo do grupo aditivo $(\mathbb{Z}_m,+)$ no grupo cíclico $(G,*)$ gerado pelo elemento a. Os diagramas abaixo ilustram tais fatos:





□

Definição 4.77.

Seja $(G,*)$ um grupo. A ordem do grupo $(G,*)$ é definida como infinita quando o conjunto G tem um número infinito de elementos.

Quando o conjunto G é finito, a ordem do grupo $(G,*)$ é definida como o número de elementos $|G|$ do conjunto G.

A ordem de um elemento $a \in G$, indicada por $\text{ord}(a)$, em que $(G,*)$ é um grupo, é definida como a ordem do subgrupo cíclico gerado por a.

Teorema 4.78.

Seja $(G,*)$ um grupo com elemento neutro e e seja x um elemento de ordem finita n, em que $n \in \mathbb{N} = \{1,2,\ldots\}$.

Para cada número $k \in \mathbb{N} = \{1,2,\ldots\}$, a ordem do elemento $x^k = x.x.\ldots.x$ (k vezes) na notação multiplicativa é igual a $\dfrac{n}{d}$, em que $d = \text{mdc}(n,k)$ é o máximo divisor comum entre os números naturais n e k.

Para cada número $k \in \mathbb{N} = \{1,2,\ldots\}$, a ordem do elemento $kx = x+x+\ldots+x$ (k vezes) na notação aditiva é igual a $\dfrac{n}{d}$, em que $d = \text{mdc}(n,k)$ é o máximo divisor comum entre os números naturais n e k.

Demonstração.

Seja d o máximo divisor comum entre os números naturais n e k. Por definição, se a ordem de x é n, então n é o menor número natural tal que $x^n = e$. Se a ordem de x^k é m, então m é o menor número inteiro tal que $(x^k)^m = e$.

Como $(x^k)^{\frac{n}{d}} = (x^n)^{\frac{k}{d}} = e$, então m é um divisor natural do número natural $\dfrac{n}{d}$. Assim, existem números inteiros r e s tais que $d = rk + sn$, enquanto que $1 = r\dfrac{k}{d} + s\dfrac{n}{d}$ indica que $\dfrac{k}{d}$ e $\dfrac{n}{d}$ não tem fatores primos em comum.

Resta mostrar que $\dfrac{n}{d}$ é um divisor natural de m. Como $(x^k)^m = (x^m)^k = e$, então n é um divisor natural de km, isto é, existe um número natural q tal que $km = qn$ e, dividindo ambos os membros da igualdade por m, vem que $\dfrac{k}{d}m = q\dfrac{n}{d}$, ou seja, $\dfrac{n}{d}$ divide o produto $m\dfrac{k}{d}$ e não tem fatores primos em comum com $\dfrac{k}{d}$. Assim, $\dfrac{n}{d}$ divide m.

Portanto, $m = \dfrac{n}{d}$. □

Exemplo 4.79.

Seja o grupo aditivo $(\mathbb{Z}_{10},+)$, em que $\mathbb{Z}_{10} = \{0,1,2,3,4,5,6,7,8,9\}$. Então:

$$\text{ord}(1) = \frac{10}{\text{mdc}(1,10)} = 10$$

$$\text{ord}(2) = \frac{10}{\text{mdc}(2,10)} = 5$$

$$\text{ord}(3) = \frac{10}{\text{mdc}(3,10)} = 10$$

$$\text{ord}(4) = \frac{10}{\text{mdc}(4,10)} = 5$$

$$\text{ord}(5) = \frac{10}{\text{mdc}(5,10)} = 2$$

$$\text{ord}(6) = \frac{10}{\text{mdc}(6,10)} = 5$$

$$\text{ord}(7) = \frac{10}{\text{mdc}(7,10)} = 10$$

$$\text{ord}(8) = \frac{10}{\text{mdc}(8,10)} = 5$$

$$\text{ord}(9) = \frac{10}{\text{mdc}(9,10)} = 10$$

Exemplo 4.80.

Seja o grupo multiplicativo $(U(\mathbb{Z}_{21}),\cdot)$ dos elementos inversíveis do monoide multiplicativo $(\mathbb{Z}_{21},\cdot)$, sendo $U(\mathbb{Z}_{21}) = \{1,2,4,5,8,10,11,13,16,17,19,20\}$. Então:

$$\text{ord}(2) = \text{ord}(2^1) = \frac{6}{\text{mdc}(1,6)} = 6$$

$$\text{ord}(4) = \text{ord}(2^2) = \text{ord}(5^2) = \frac{6}{\text{mdc}(2,6)} = 3$$

$$\text{ord}(5) = \text{ord}(5^1) = \frac{6}{\text{mdc}(1,6)} = 6$$

$$\text{ord}(8) = \text{ord}(2^3) = \frac{6}{\text{mdc}(3,6)} = 2$$

$$\text{ord}(11) = \text{ord}(2^5) = \frac{6}{\text{mdc}(5,6)} = 6$$

$$\text{ord}(16) = \text{ord}(2^4) = \text{ord}(5^4) = \frac{6}{\text{mdc}(4,6)} = 3$$

$$\text{ord}(17) = \text{ord}(5^5) = \frac{6}{\text{mdc}(5,6)} = 6$$

$$\text{ord}(20) = \text{ord}(5^3) = \frac{6}{\text{mdc}(3,6)} = 2$$

Teorema 4.81.

Seja $(G,*)$ um grupo, com elemento neutro e e seja a um elemento de G. Então:

(i) Ou o elemento a tem ordem infinita e os elementos da sequência infinita

$$a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, \ldots$$

são dois a dois distintos.

(ii) Ou existem números inteiros r e s tais que $a^r = a^s$ e o elemento a tem ordem finita m, de modo que

a) $m \in \mathbb{N} = \{1,2,\ldots\}$ é o menor número natural tal que $a^m = e$.

b) Para cada número inteiro $z \in \mathbb{Z}$, $a^k = e$ se, e somente se, m divide k.

c) Para números inteiros r, $s \in \mathbb{Z}$, $a^r = a^s$ se, e somente se, m divide $r-s$.

d) O subgrupo cícliclo $(< a >, *)$ gerado pelo elemento $a \in G$ é tal que o conjunto $< a >$ é constituído pelos elementos $a, a^2, \ldots, a^m = e$.

e) para cada número inteiro $k \in \mathbb{Z}$, tal que k divide m, a ordem $|a^k|$ do elemento a^k é igual a m/k.

Teorema 4.82.

Seja $(G,*)$ um grupo cíclico gerado pelo elemento $a \in G$. Então:

(i) Se $(H,*)$ é um subgrupo do grupo $(G,*)$, então $(H,*)$ é um grupo cíclico.

(ii) Se $(H,*)$ é um subgrupo não trivial do grupo cíclico $(G,*)$ e se $m \in \mathbb{N} = \{1,2,\ldots\}$ é o menor número natural tal que $a^m \in H$, então o grupo $(H,*)$ é um grupo cíclico gerado pelo elemento a^m.

(iii) Se $(G,*)$ é um grupo cíclico finito gerado pelo elemento a e se h é um homomorfismo de grupo do grupo $(G,*)$ no grupo $(G',\diamond)$, então o subgrupo $(h(G),\diamond)$ do grupo $(G',\diamond)$ é um grupo cíclico finito gerado pelo elemento $h(a)$; além disso, a ordem $|h(a)|$ do elemento $h(a)$ divide a ordem $|a|$ do elemento a, desde que $h(a)^m = h(a^m) = h(e) = e'$, em que e' é o elemento neutro do grupo $(G',\diamond)$.

Definição 4.83.

O grupo dos automorfismos do grupo $(G,*)$ é o grupo $(AutG,\circ)$, em que o conjunto $AutG$ é constituído por todos os isomorfismos de grupo do grupo $(G,*)$ no grupo $(G,*)$, com a operação binária interna $\circ$ de composição de funções. O isomorfismo identidade é o elemento neutro do grupo $(AutG,\circ)$.

Teorema 4.84.

Seja $(G,*)$ um grupo cíclico gerado pelo elemento $a \in G$. Então:

(i) Se o número de elementos do conjunto G é infinito, a e a^{-1} são os únicos geradores de G, isto é, $G =< a >=< a^{-1} >$ e $AutG$ é constituído por dois isomorfismos de grupo: o isomorfismo identidade que associa ao elemento a o próprio elemento a e o isomorfismo de grupo que associa ao elemento a o elemento inverso a^{-1} de a.

(ii) Se o conjunto G tem um número finito de elementos, então a^k é um elemento gerador do grupo, isto é, $G =< a^k >$ se, e somente se, o máximo divisor comum dos números k e m é igual a 1.

Propriedade 4.85.

Seja $(S,*)$ um semigrupo em que os ideais principais à esquerda e à direita gerado por cada elemento a pertencente ao semigrupo são coincidentes com o conjunto S, ou seja, para cada $a \in S$, $a*S = S = S*a$. Então, $(S,*)$ é um grupo.

A relação binária à esquerda L de um semigrupo $(S,*)$ é o conjunto

$$L = \{(a,b) \in S \times S : \{a\} \cup (S*a) = \{b\} \cup (S*b)\}$$

enquanto que a relação binária à direita R de um semigrupo $(S,*)$ é o conjunto

$$R = \{(a,b) \in S \times S : \{a\} \cup (a*S) = \{b\} \cup (b*S)\}.$$

É fácil ver que L e R são relações binárias de equivalência no semigrupo.

Exemplo 4.86.

Seja (S,μ) o semigrupo comutativo em que $S = \{1,2,3,4\}$ e cuja tabela de Cayley para a operação binária interna μ é dada abaixo:

	1	**2**	**3**	**4**
1	1	2	3	4
2	2	1	3	4
3	3	4	3	4
4	4	3	3	4

A relação binária à esquerda L e a relação binária à direita R são iguais e as classes de equivalência, segundo L e segundo R, são: $\{1\}$, $\{2\}$ e $\{3,4\}$.

Propriedades 4.87.

Sejam a e b elementos distintos de um semigrupo $(S,*)$. Então:

(i) $(a,b) \in L$ quando, e somente quando, existirem $s, t \in S$ tais que $s*a = b$ e $t*b = a$.

(ii) $(a,b) \in R$ quando, e somente quando, existirem $s, t \in S$ tais que $a*s = b$ e $b*t = a$.

(iii) Se $(a,b) \in L$ e se $c \in S$, então $(a*c, b*c) \in L$.

(iv) Se $(a,b) \in R$ e se $c \in S$, então $(c*a, c*b) \in R$.

Demonstração.

(i) 1. $a, b \in S, a \neq b, (a,b) \in L$

2. $\{a\} \cup (S*a) = \{b\} \cup (S*b)$

3. $b \in (S*a) = \{s*a : s \in S\}$

4. $\exists\, s \in S : b = s*a$

(ii) 1. $a, b, c \in S, a \neq b, (a,b) \in L$

2. por (i), $\exists\, s, t \in S : s*a = b$ e $t*b = a$

3. $s*(a*c) = b*c$ e $t*(b*c) = a*c$

4. $(a*c, b*c) \in L$

□

Como todo semigrupo $(S,*)$ está contido em um monoide $(M,*)$ com elemento neutro 1, lembrando que a operação binária interna em M quando restrita a $S \subset M$ é a operação binária interna do semigrupo, as propriedades das relações binárias à esquerda L e à direita R são apresentadas a seguir.

Propriedades 4.88.

Sejam a e b elementos de um monoide $(M,*)$ com elemento neutro 1. Então:

(i) $(a,b) \in L$ quando, e somente quando, existirem $s, t \in M$ tais que $s*a = b$ e $t*b = a$.

(ii) $(a,b) \in R$ quando, e somente quando, existirem $s, t \in M$ tais que $a*s = b$ e $b*t = a$.

Demonstração.

(i) 1. $a, b \in M$ e $(a,b) \in L$

2. $M*a = M*b$

3. $b \in M*a = \{s*a : s \in M\}$

4. $\exists\, s \in M : b = s*a$

e, reciprocamente,

5. caso existam $s, t \in M$ tais que $s*a = b$ e $t*b = a$

6. $b \in M*a$ e $a \in M*b$

7. se $m \in M$, então $m*a \in M*a$

8. $m*a = (m*t)*b \in M*b$

9. $M*a \subset M*b$

10. analogamente, $M*b \subset M*a$
11. $M*a = M*b$ e $(a,b) \in L$

□

As propriedades (i) e (ii) acima são semelhantes às relações de divisibilidade entre os elementos de um monoide e é importante notar que se e e f são elementos idempotentes do monoide e se $(e,f) \in L$, isto é, existirem $s, t \in M$ tais que $s*e = f$ e $t*f = e$, então

$$e*f = e*(f*f) = (t*f)*(f*f) = t*f = e,$$

enquanto que se e e f são elementos idempotentes do monoide e se $(e,f) \in R$, isto é, existirem s, $t \in M$ tais que $e*s = f$ e $f*t = e$, então

$$e*f = (e*e)*f = (e*e)*(e*s) = e*s = f.$$

Como consequência, se a, b, $c \in M$ e se $(a,b) \in L$, então $(a*c, b*c) \in L$, enquanto que se $(a,b) \in R$, então $(c*a, c*b) \in R$.

Propriedade 4.89.

As relações binárias à esquerda L e à direita R em um monoide $(M,*)$ são tais que

$$R \circ L = L \circ R.$$

Demonstração.

A inclusão $R \circ L \subset L \circ R$ é provada abaixo:

1. $(a,b) \in R \circ L$
2. $(\exists\, c \in M)(((a,c) \in L)((c,b) \in R))$
3. $(\exists\, x, y, u, v \in M)((x*a = c)(y*c = a)(c*u = b)(b*v = c))$
4. $d = y*c*u$
5. $a*u = y*c*u = d$
6. $d*v = y*c*u*v = y*b*v = y*c = a$
7. $y*b = y*c*u = d$
8. $x*d = x*y*c*u = x*a*u = c*u = b$
9. $(a,d) \in R$ e $(d,b) \in L$

10. $(a,b) \in L \circ R$

A prova da inclusão reversa $L \circ R \subset R \circ L$ é análoga.

Portanto, $L \circ R = R \circ L$. □

A relação binária total T em um monoide $(M,*)$ com elemento neutro 1 é definida como

$$T = \{(a,b) \in M \times M : M * a * M = M * b * M\},$$

em que

$$M * a * M = \{s * a * t : s \in M \text{ e } t \in M\}$$

$$M * b * M = \{s * b * t : s \in M \text{ e } t \in M\}.$$

Se $(a,b) \in T$, como $b \in M * a * M$, existem x, $y \in M$ tais que

$$x * a * y = b$$

e, como $a \in M * b * M$, existem u, $v \in M$ tais que

$$u * b * v = a.$$

Então, $(a,b) \in T$ é equivalente à existência de x, y, u, $v \in M$ tais que

$$x * a * y = b$$

$$u * b * v = a.$$

Como é imediato que $L \subset T$ (já que $(a,b) \in L$, existem s, $t \in M$ tais que $s * a = t$ e $t * b = a$, isto é, $s * a * 1 = t$ e $t * b * 1 = a$, que é equivalente a $(a,b) \in T$) e que $R \subset T$, então a intersecção D de todas as relações binárias de equivalência em M contendo as relações binárias à esquerda L e à direita R também é uma relação binária de equivalência contida na relação binária de equivalência T.

Teorema 4.90 (Teorema da representação de Cayley para semigrupos)**.**

Seja $(S,*)$ um semigrupo e seja o monoide canônico $M = S \cup \{1\}$ com elemento neutro 1 associado ao semigrupo. Então, existe uma função canônica ϕ de S em $T(M)$, o conjunto das funções totais em M, tal que ϕ é um homomorfismo injetor entre o semigrupo $(S,*)$ e o semigrupo $(T(M),\circ)$, em que $\circ$ é a operação binária interna de composição em $T(M)$.

Demonstração.

Para cada $s \in S$, seja a função translação à direita T_s por s em M:

$$(\forall\, x \in M)(T_s(x) = s * x).$$

A função canônica ϕ de S em $T(M)$ é definida por: $\phi(s) = T_s$. A função ϕ assim definida é uma função injetora de S em $T(M)$, pois, se $\phi(s_1) = T_{s_1} = \phi(s_2) = T_{s_2}$, então, para cada $x \in M$,

$$T_{s_1}(x) = s_1 * x = T_{s_2}(x) = s_2 * x$$

e, em particular,

$$s_1 * 1 = s_1 = s_2 * 1 = s_2.$$

A função ϕ é um homomorfismo de semigrupos entre o semigrupo $(S, *)$ e o semigrupo $(T(M), \circ)$, pois, se s_1, $s_2 \in S$, então:

$$\phi(s_1 * s_2) = T_{s_1 * s_2}$$

$$\phi(s_1) = T_{s_1}$$

$$\phi(s_2) = T_{s_2}$$

e, para cada $x \in M$:

$$\begin{aligned}(T_{s_1} \circ T_{s_2})(x) &= T_{s_1}\left[T_{s_2}(x)\right] \\ &= T_{s_1}(s_2 * x) \\ &= s_1 * (s_2 * x) \\ &= (s_1 * s_2) * x \\ &= T_{s_1 * s_2}(x)\end{aligned}$$

ou, em outros termos, para s_1, $s_2 \in S$,

$$\phi(s_1) \circ \phi(s_2) = \phi(s_1 * s_2).$$

□

Exemplo 4.91.

Seja $(S, *)$ o semigrupo comutativo em que $S = \{1, 2, 3, 4\}$ e a tabela de Cayley para a operação binária interna $*$ é a seguinte:

	1	**2**	**3**	**4**
1	1	2	3	4
2	2	1	3	4
3	3	4	3	4
4	4	3	3	4

Seja f a função cujo domínio de definição é S e cujo conjunto de valores está contido no conjunto $T(X)$ em que $X = \{1, 2\}$ constituído por todas as funções totais em X definida por:

$$f(1) = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

$$f(2) = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

$$f(3) = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

$$f(4) = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

e seja g a função cujo domínio de definição é S e cujo conjunto de valores está contido no conjunto $T(S)$, o conjunto de todas as funções totais em S, definida por:

$$g(1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$g(2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$g(3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 3 & 3 & 3 \end{pmatrix}$$

$$g(4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 4 & 4 & 4 \end{pmatrix}$$

Então, f é um monomorfismo de monoide do monoide $(S, *)$ no monoide $(T(X_2), \circ)$ com a operação binária interna de composição e g é um monomorfismo de monoide do monoide $(S, *)$ no monoide $(T(X_4), \circ)$ com a operação binária interna de composição.

Para definir tais monomorfismos de monoides, é necessário levar os elementos idempotentes 3 e 4 do conjunto S em funções constantes, que são elementos idempotentes no semigrupo das funções.

Teorema 4.92 (Teorema da representação de Cayley para grupos)**.**

Seja $(G, *)$ um grupo. Então, existe um monomorfismo de grupo entre o grupo $(G, *)$ e o grupo $(S_G, \circ)$, em que S_G é o conjunto de todas as funções injetoras e sobrejetoras cujo domínio de definição e cujo domínio de valores são iguais a G com a operação binária interna da composição.

Demonstração.

Para cada elemento $x \in G$, seja a função translação T_x cujo domínio de definição é G definida, para cada $y \in G$, por

$$T_x(y) = x * y.$$

Pela lei do cancelamento para grupos, T_x é uma função injetora no conjunto G e, além disso, T_x é uma função sobrejetora sobre G, pois, dado $z \in G$,

$$\begin{aligned} T_x(x^{-1} * z) &= x * (x^{-1} * z) \\ &= (x * x^{-1}) * z \\ &= z. \end{aligned}$$

Para elementos $x_1, x_2 \in G$,

$$T_{x_1} \circ T_{x_2} = T_{x_1 * x_2},$$

pois, para cada $y \in G$,

$$\begin{aligned} (T_{x_1} \circ T_{x_2})(y) &= T_{x_1}\left[T_{x_2}(y)\right] \\ &= T_{x_1}(x_2 * y) \\ &= x_1 * (x_2 * y) \\ &= (x_1 * x_2) * y \\ &= T_{x_1 * x_2}(y) \end{aligned}$$

Seja h a função que associa a cada elemento $x \in G$ a função injetora e sobrejetora T_x, ou seja $h(x) = T_x$. Então, para elementos $x_1, x_2 \in G$,

$$\begin{aligned} h(x_1 * x_2) &= T_{x_1 * x_2} \\ &= T_{x_1} \circ T_{x_2} \\ &= h(x_1) \circ h(x_2), \end{aligned}$$

o que demonstra que h é um homomorfismo de grupo do grupo $(G, *)$ no grupo $(S_G, \circ)$.

Para demonstrar que h é um monomorfismo de grupo, seja $x \in G$ tal que T_x é a função identidade, ou seja, para cada $y \in G$, $T_x(y) = x * y = y$.

De $x * y = y$, vem $(x * y) * y^{-1} = y * y^{-1} = e$, que é equivalente a $x = e$, em que e é o elemento neutro do grupo $(G, *)$. □

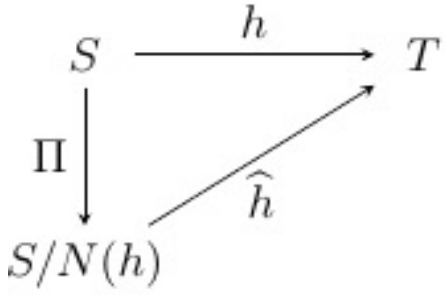
Teorema 4.93 (Primeiro teorema do isomorfismo para semigrupos)**.**

Seja $(S, *)$ um semigrupo e seja R uma congruência em S, no sentido de que R é um relação binária de equivalência no conjunto S compatível à esquerda e à direita com a operação binária interna $*$ do semigrupo. Então:

(i) $(S/R, *_R)$ é um semigrupo.

(ii) A aplicação natural Π_R é um homomorfismo de semigrupos do semigrupo $(S, *)$ no semigrupo $(S/R, *_R)$.

(iii) Se é h um homomorfismo de semigrupos do semigrupo (S,u) no semigrupo (T,v), então o núcleo de h indicado por $N(h) = h^{-1} \circ h$ é uma congruência em S e existe um homomorfismo de semigrupos $\widehat{h}$ do semigrupo $(S/N(h), *_{N(h)})$ no semigrupo $(T,*)$, cujo conjunto de valores em T coincide com o conjunto de valores de h em T e é tal que o diagrama abaixo é comutativo:



em que, para cada $s \in S$, $\Pi(s) = N(h)s$ e $\widehat{h}(N(h)s) = h(s)$.

Demonstração.

Sejam Rx, Ry e Rz, respectivamente, as classes de equivalência dos elementos x, y e z pertencentes a S. Então:

$$Rx *_R Ry = R(x*y)$$

$$Ry *_R Rz = R(y*z)$$

$$\begin{aligned}(Rx *_R Ry) *_R Rz &= R(x*y) *_R Rz \\ &= R\big[(x*y)*z\big] \\ &= R\big[x*(y*z)\big] \\ &= Rx *_R R(y*z) \\ &= Rx *_R (Ry *_R Rz),\end{aligned}$$

o que prova a associatividade da operação binária interna $*_R$ no conjunto quociente S/R.

A aplicação natural Π_R é um epimorfismo de semigrupo do semigrupo $(S,*)$ no semigrupo $(S/R, *_R)$, pois, dados x, $y \in S$,

$$\begin{aligned}\Pi_R(x) *_R \Pi_R(y) &= Rx *_R Ry \\ &= R(x*y) \\ &= \Pi_R(x*y).\end{aligned}$$

□

Exemplo 4.94.

A tabela de Cayley do semigrupo multiplicativo comutativo $(\mathbb{Z}_6, \cdot)$ é a seguinte:

	0	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Então, $I = \{0,2,4\}$ é um ideal do semigrupo $(\mathbb{Z}_6, \cdot)$ e o semigrupo quociente $(\mathbb{Z}_6/I, \cdot_I)$ apresenta a seguinte tabela de Cayley:

	$\{0,2,4\}$	$\{1\}$	$\{3\}$	$\{5\}$
$\{0,2,4\}$	$\{0,2,4\}$	$\{0,2,4\}$	$\{0,2,4\}$	$\{0,2,4\}$
$\{1\}$	$\{0,2,4\}$	$\{1\}$	$\{3\}$	$\{5\}$
$\{3\}$	$\{0,2,4\}$	$\{3\}$	$\{3\}$	$\{3\}$
$\{5\}$	$\{0,2,4\}$	$\{5\}$	$\{3\}$	$\{1\}$

Analogamente, $J = \{0,3\}$ também é um ideal do semigrupo $(\mathbb{Z}_6, \cdot)$ e o semigrupo quociente $(\mathbb{Z}_6/J, \mu_J)$ apresenta a seguinte tabela de Cayley:

	$\{0,3\}$	$\{1\}$	$\{2\}$	$\{4\}$	$\{5\}$
$\{0,3\}$	$\{0,3\}$	$\{0,3\}$	$\{0,3\}$	$\{0,3\}$	$\{0,3\}$
$\{1\}$	$\{0,3\}$	$\{1\}$	$\{2\}$	$\{4\}$	$\{5\}$
$\{2\}$	$\{0,3\}$	$\{2\}$	$\{4\}$	$\{2\}$	$\{4\}$
$\{4\}$	$\{0,3\}$	$\{4\}$	$\{2\}$	$\{4\}$	$\{2\}$
$\{5\}$	$\{0,3\}$	$\{5\}$	$\{4\}$	$\{2\}$	$\{1\}$

Exemplo 4.95.

Seja $(\mathbb{Z}_4, \cdot)$ um monoide multiplicativo comutativo. Então, $I = \{0,2\}$ é um ideal do monoide $(\mathbb{Z}_4, \cdot)$ e o semigrupo quociente $(\mathbb{Z}_4/I, \cdot_I)$ apresenta a seguinte tabela de Cayley:

	$\{0,2\}$	$\{1\}$	$\{3\}$
$\{0,2\}$	$\{0,2\}$	$\{0,2\}$	$\{0,2\}$
$\{1\}$	$\{0,2\}$	$\{1\}$	$\{3\}$
$\{3\}$	$\{0,2\}$	$\{3\}$	$\{1\}$

e tem elemento neutro igual a $\{1\}$. Portanto, $(\mathbb{Z}_4/I, \cdot_I)$ é um monoide.

Exemplo 4.96.

Seja $(S,*)$ o semigrupo comutativo em que $S=\{1,2,3,4\}$ e cuja tabela de Cayley para a operação binária interna $*$ é dada abaixo:

	1	**2**	**3**	**4**
1	1	2	3	4
2	2	1	4	3
3	3	4	3	4
4	4	3	4	3

Então, $\{3,4\}$ é um ideal do semigrupo $(S,*)$ e o semigrupo quociente $(S/I,*_I)$ apresenta a seguinte tabela de Cayley:

	$\{3,4\}$	$\{1\}$	$\{2\}$
$\{3,4\}$	$\{3,4\}$	$\{3,4\}$	$\{3,4\}$
$\{1\}$	$\{3,4\}$	$\{1\}$	$\{2\}$
$\{2\}$	$\{3,4\}$	$\{2\}$	$\{1\}$

Teorema 4.97.

Sejam $(S,*)$ um semigrupo e R uma congruência definida em S. Então:

(i) $(S/R,*_R)$ é um semigrupo.

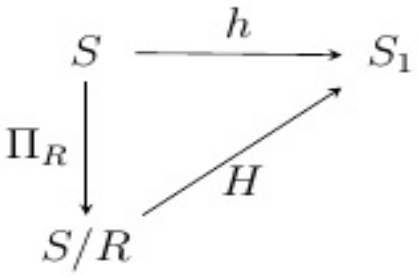
(ii) A função natural Π_R, cujo domínio de definição é S e cujo conjunto de valores coincide com S/R, é um epimorfismo de semigrupo do semigrupo $(S,*)$ no semigrupo $(S/R,*_R)$.

Teorema 4.98.

Seja $(S_1,*_1)$ um semigrupo e seja h um homomorfismo de semigrupo do semigrupo $(S,*)$ no semigrupo $(S_1,*_1)$. Então:

(i) O núcleo $N(h)$ de h, dado por $N(h)=\{(s,t)\in S\times S : h(s)=h(t)\}$, é uma congruência em S.

(ii) Se R é uma congruência em S, contido no núcleo de h, então existe um monomorfismo de semigrupo H do semigrupo quociente $(S/R,*_R)$ no semigrupo $(S_1,*_1)$ de modo que o conjunto de valores de H coincide com o conjunto de valores de h e o diagrama abaixo é comutativo:



ou seja, $h = H \circ \Pi_R$, em que Π_R é o epimorfismo natural de semigrupo do semigrupo $(S, *)$ no semigrupo quociente $(S/R, *_R)$.

Demonstração.

(i) A prova deste item é de verificação imediata.

(ii) A função H, cujo domínio de definição é S/R e cujo conjunto de valores é um subconjunto do conjunto S_1, é definida como:

$$\text{para } x \in S, H(Rx) = h(x)$$

e H é uma função bem definida em vista de que, se $x_1, x_2 \in S$ e $Rx_1 = Rx_2$, então $(x_1, x_2) \in R \subset N(h)$ por hipótese, o que significa que $h(x_1) = h(x_2)$.

A função H é um homomorfismo de semigrupo do semigrupo $(S/R, *_R)$ no semigrupo $(S_1, *_1)$, pois, se x, $y \in S$, então:

$$\begin{aligned} H(Rx *_R Ry) &= H\left[R(x * y)\right] \\ &= h(x * y) \\ &= h(x) *_1 h(y), \end{aligned}$$

tendo em vista que h é um homomorfismo de semigrupo do semigrupo $(S, *)$ no semigrupo $(S_1, *_1)$.

A função H é um monomorfismo de semigrupo do semigrupo $(S/R, *_R)$ no semigrupo $(S_1, *_1)$, pois, se x, $y \in S$ e

$$\begin{gathered} H(Rx) = H(Ry) \\ h(x) = h(y) \\ (x, y) \in R \subset N(h) \\ Rx = Ry. \end{gathered}$$

□

Corolário 4.99.

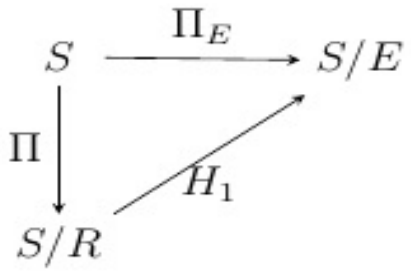
Sejam R e E congruências definidas no semigrupo $(S, *)$ tal que $R \subset E$. Então, o conjunto quociente de congruências

$$E/R = \{(Rx, Ry) \in S/R \times S/R : (x, y) \in E\} \subset S/R \times S/R$$

é uma congruência no semigrupo quociente $(S/R, *_R)$ e existe um isomorfismo de semigrupo H do semigrupo $\left(S/R \Big/ E/R, *_{E/R}\right)$ no semigrupo $(S/R, *_R)$.

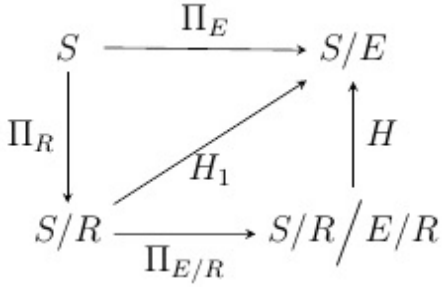
Demonstração.

Pelo teorema anterior, existe um homomorfismo de semigrupo H_1 do semigrupo $(S/R, *_R)$ no semigrupo $(S/E, *_E)$ de modo que o diagrama é comutativo:



ou seja, para $x \in S$, $H(Rx) = Ex$.

Analogamente, existe um homomorfismo de semigrupo H do semigrupo quociente $\Big(S/R\Big/E/R, *_{E/R}\Big)$ no semigrupo $(S/E, *_E)$ de modo que o diagrama abaixo é comutativo:



ou seja, para $x \in S$,

$$H\big[(E/R)Rx\big] = Ex,$$

em que Ex é a classe de equivalência de x segundo E e $(E/R)Rx$ é a classe de equivalência do elemento $Rx \in S/R$ segundo E/R.

Pelo teorema anterior, H é um monomorfismo de semigrupo, cujo conjunto de valores coincide com S/E, que é o conjunto de valores de Π_E, logo H é um isomorfismo de semigrupo.

□

Teorema 4.100.

Dada uma relação binária R no conjunto não vazio S, em que $(S, *)$ é um semigrupo, a intersecção de todas as relações binárias compatíveis à esquerda e à direita que contém R com a operação binária interna $*$ é a seguinte relação binária compatível à esquerda e à direita com a operação binária interna:

$$R^C = \{(x*(a*y), (x*(b*y)) : x, y \in M \text{ e } (a,b) \in R\},$$

em que $(M, \overline{*})$ é o monoide canônico associado ao semigrupo $(S, *)$.

Demonstração.

Além da relação binária R^C conter a relação binária R em S (basta escolher $x = y = 1$ o elemento neutro de M), na definição de R^C, R^C é uma congruência em S, pois, se x, y, z, a e b são elementos de S, com $(a,b) \in R$ e com $(x*(a*y),(x*(b*y)) \in R^C$, segue que

$$z*\big[x*(a*y)\big] = z*\big[x*(b*y)\big]$$

ou

$$(z*x)*(a*y) = (z*x)*(b*y),$$

o que mostra que R^C é relação binária compatível à esquerda com a operação binária interna $*$.

A prova de que R^C é relação binária compatível à direita com a operação binária interna $*$ é análoga. □

Dada uma congruência E em S contendo R, é fácil ver que $R^C \subset E$, ou seja, R^C é a intersecção de todas as congruências em S que contém a relação binária R.

Propriedades 4.101.

Dadas R_1 e R_2 relações binárias no conjunto não vazio S, em que $(S,*)$ é um semigrupo. Então:

(i) $R_1 \subset R_2 \Rightarrow R_1^C \subset R_2^C$

(ii) $(R_1^{-1})^C = (R_1^C)^{-1}$

(iii) $(R_1 \cup R_2)^C = R_1^C \cup R_2^C$

Proposição 4.102.

Dada uma relação binária R em um conjunto não vazio S, em que $(S,*)$ é um semigrupo, a intersecção de todas as congruências em S que contém R é a intersecção de todas as relações de equivalência que contém R^C (que é a intersecção de todas as relação binárias compatíveis à esquerda e à direita com a operação binária interna μ que contém R).

Demonstração.

A relação binária $(R^C)_{eq}$ é uma relação binária de equivalência que contém a relação binária R^C em S e que contém a relação binária R em S por R estar contida em R^C.

Para mostrar que $(R^C)_{eq}$ é uma congruência em S, isto é, para mostrar que $(R^C)_{eq}$ é compatível à esquerda e à direita com a operação binária interna $*$, considere a relação binária E definida por:

$$E = R^C \cup (R^{-1})^C \cup \Delta_S^C = (R \cup R^{-1} \cup \Delta_S)^C, \text{ pois } \Delta_S^C = \Delta_S,$$

compatível à esquerda e à direita com a operação binária interna $*$, e, para cada $n \in \mathbb{N} = \{1,2,\ldots\}$,

$$En = E \circ E \circ E \ \ (n \text{ vezes})$$

também é compatível à esquerda e à direita com a operação binária interna $*$; assim, se $(s,t) \in (R^C)^e$, existe um número natural n tal que $(s,t) \in En$ e, para cada $x \in S$,

$$(x*s, x*t) \in En \subset (R^C)_{eq}$$

$$(s*x, t*x) \in En \subset (R^C)_{eq},$$

o que mostra que $(R^C)_{eq}$ é uma congruência em S.

A fim de provar que $(R^C)_{eq}$ é a intesecção de todas as congruências de S que contém R, seja C uma congruência em S. $R^C \subset C^C = C$, o que mostra que C é uma relação de equivalência contendo R^C e, por definição, $(R^C)_{eq} \subset C$. □

Exemplo 4.103.

Seja $(S,*)$ o semigrupo comutativo, em que $S = \{1,2,3,4\}$, cuja tabela de Cayley para a operação binária interna $*$ é dada abaixo:

	1	**2**	**3**	**4**
1	1	2	3	4
2	2	1	4	3
3	3	4	3	4
4	4	3	4	3

Para a determinação das relações binárias de equivalência R compatíveis à esquerda e à direita com a operação binária interna do semigrupo que contém o elemento $(1,2)$:

Se $(1,2) \in R$, então:

$$(1*2, 2*2) = (2,1) \in R$$

$$(1*3, 2*3) = (3,4) \in R$$

$$(1*4, 2*4) = (4,3) \in R.$$

Se $(2,1) \in R$, então:

$$(2*2, 1*2) = (1,2) \in R$$

$$(2*3, 1*3) = (4,3) \in R$$

$$(2*4, 1*4) = (3,4) \in R.$$

Se $(3,4) \in R$, então:

$$(3*2, 4*2) = (4,3) \in R$$

$$(3*3,4*3) = (3,4) \in R$$

$$(3*4,4*4) = (4,3) \in R.$$

Portanto, a relação binária de equivalência R compatível à esquerda e à direita com a operação binária interna do semigrupo tem como matriz

$$M_R = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} = M_{R\circ R}.$$

Logo, $R \circ R = R$ e R é a relação binária de equivalência compatível à esquerda e à direita com a operação binária interna do semigrupo procurada.

Uma descrição alternativa de $(R^C)_{eq}$ é dada pela proposição seguinte:

Proposição 4.104.

Seja R uma relação binária no conjunto não vazio S, em que $(S,*)$ é um semigrupo. Então, $(x,y) \in (R^C)_{eq}$, com x, $y \in S$ e $x \neq y$, se, e somente se, existe um número natural n e elementos x_1, $x_2,\ldots,x_n \in S$ de modo que existe uma sequência de R-transições elementares conectando x a y:

$$x = x_1 \to x_2 \to \ldots \to x_n = y.$$

Uma R-transição elementar conectando $s \in S$ a $t \in S$ acontece quando

$$s = u*(a*v)$$

$$t = u*(b*v),$$

de forma que u, $v \in S \cup \{1\}$, sendo 1 o elemento neutro do monoide canônico M associado a S, com $(a,b) \in R$ ou com $(b,a) \in R$.

Se R é uma relação binária compatível à esquerda e à direita com a operação binária interna $*$, então, dados c, s, $t \in S$, com $(s,t) \in R$, temos $(c*s,c*t) \in R$ e $(s*c,t*c) \in R$ e o mesmo é válido para uma relação binária

$$R_n = R \circ R \circ \ldots \circ R \ \ (n \text{ vezes}),$$

com $n \in \mathbb{N} = \{1,2,\ldots\}$, pois, se $(s,t) \in R_n$, existe uma sequência finita $x_1,x_2,\ldots,x_{n-1} \in S$ de modo que

$$(s,x_1),(x_1,x_2),\ldots,(x_{n-1},t) \in R,$$

o que implica, por hipótese, que

$$(c*s,c*x_1),(c*x_1,c*x_2),\ldots,(c*x_{n-1},c*t)\in R,$$

$$(s*c,x_1*c),(x_1*c,x_2*c),\ldots,(x_{n-1}*c,t*c)\in R$$

e que $(c*s,c*t)\in R_n$ e que $(s*c,t*c)\in R_n$.

Dada uma relação binária R em S,

$$R^C=\{(x*a*y,x*b*y):x,y\in S\cup\{1\}\text{ e }(a,b)\in R\}$$

é a intesecção de todas as relações binárias que contém a relação binária e são compatíveis à esquerda e à direita com a operação binária interna do semigrupo, pois, se $(x*a*y,x*b*y)\in R^C$, então, para cada $c\in S$,

$$(c*(x*a*y),c*(x*b*y))\in R^C.$$

Dada uma relação binária de equivalência E no conjunto não vazio S, em que $(S,*)$ é um semigrupo, a relação binária

$$E^b=\{(s,t)\in S\times S:\forall\, x,y\in S\cup\{1\},(x*a*y,x*b*y)\in E\}$$

é a união de todas as congruências em S que estão contidas na relação binária de equivalência E.

Demonstração.

(i) $E^b\subset E$:

$(s,t)\in E^b\Rightarrow(s,t)=(1*s*1,1*t*1)\in E$

(ii) E^b é uma relação binária de equivalência em S

(iii) E^b é uma relação binária em S compatível à esquerda e à direita com a operação binária interna $*$ de S:

1. $(s,t)\in E^b$
2. $c\in S$
3. $(x*c*s*y,x*c*t*y)\in E$ para todos os valores de x e y pertencentes a $S\cup\{1\}$
4. $(c*s,c*t)\in E^b$ e, analogamente, $(s*c,t*c)\in E^b$

(iv) Se C é uma congruência em S contida em E, então $C\subset E^b$:

1. $s,t\in S$ e $(s,t)\in C$
2. $\forall\, x,y\in S\cup\{1\},(x*a*y,x*b*y)\in C\subset E$

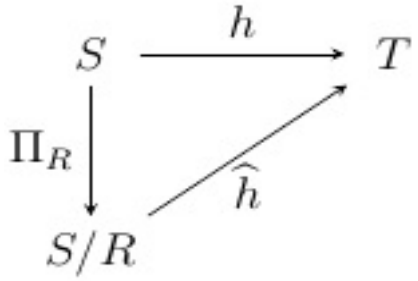
3. $(s,t) \in E^b$

□

Para cada subconjunto não vazio A do conjunto não vazio S em que $(S,*)$ é um semigrupo, a relação de equivalência Π_A associada a A é a relação de equivalência em S induzida pela partição $S = A \cup \overline{A}$, sendo $\overline{A}$ é o subconjunto complementar de A em S e

$$\Pi_A^b = \{(s,t) \in S \times S : \forall\, x,y \in S \cup \{1\}, x*s*y \in A \Leftrightarrow x*t*y \in A\}.$$

Seja $(S,*)$ um semigrupo e seja R uma congruência em S. Seja h um homomorfismo de semigrupos entre os semigrupos $(S,*)$ e $(T,\diamond)$ tal que $R \subset N(h)$. Então, existe um único monomorfismo de semigrupos $\widehat{h}$ de S/R em T, cujo conjunto de valores de $\widehat{h}$ em T coincide com o conjunto de valores de h em T e é tal que o diagrama abaixo é comutativo:

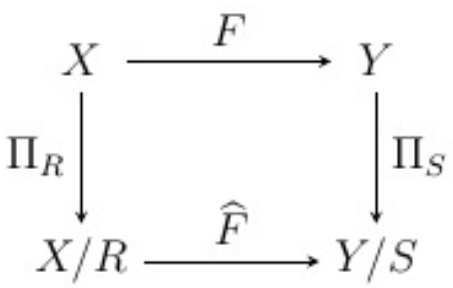


em que Π_R é a aplicação natural de S em S/R.

Teorema 4.105.

Sejam R e S relações binárias de equivalência, respectivamente nos conjuntos X e Y, ambos não vazios, e seja F uma função total de X em Y, isto é, o domínio de definição $D(F)$ de F é igual a X e o conjunto de valores de F é um subconjunto de Y compatível com as relações binárias de equivalência R e S no sentido de que, se $(x,y) \in R$, então $(F(x),F(y)) \in S$.

Então, existe uma única função total $\widehat{F}$ do conjunto quociente X/R no conjunto quociente Y/S, cujo domínio de definição $D(\widehat{F})$ é igual a X/R e cujo conjunto de valores de $\widehat{F}$ é um subconjunto de Y de modo que o diagrama abaixo é comutativo:



ou seja,

$$\widehat{F} \circ \Pi_R = \Pi_S \circ F.$$

Para cada $x \in X$, Rx é a classe de equivalência de x segundo a relação de equivalência R em x

$$\widehat{F}(Rx) = SF(x),$$

em que $SF(x)$ é a classe de equivalência de $F(x)$ segundo a relação de equivalência S em Y.

A função $\widehat{F}$ está bem definida, pois, se, para $x_1, x_2 \in X$, $Rx_1 = Rx_2$, isto é, $(x_1, x_2) \in R$, então $(F(x_1), F(x_2)) \in S$ pela compatibilidade de F em relação a R e S e as classes de equivalência de $F(x_1)$ e de $F(x_2)$ segundo S são iguais.

Definição 4.106.

Seja $(S, *)$ um semigrupo. Uma relação binária R no conjunto não vazio S é

(i) compatível à esquerda com a operação binária interna de S se, e somente se,

$$(\forall\, r \in S)(\forall\, s \in S)(\forall\, t \in S)((r,s) \in R \Rightarrow (t*r, t*s) \in R).$$

(ii) compatível à direita com a operação binária interna de S se, e somente se,

$$(r,s) \in R \Rightarrow (r*t, s*t) \in R.$$

(iii) compatível com a operação binária interna de S se, e somente se,

$$(\forall\, s \in S)(\forall\, t \in S)(\forall\, u \in S)(\forall\, v \in S)((s,t) \in R \text{ e } (u,v) \in R \Rightarrow (s*u, t*v) \in R).$$

(iv) uma congruência quando, e somente quando, R é uma relação de equivalência no conjunto S compatível à esquerda e à direita com a operação binária interna do semigrupo.

Teorema 4.107.

Sejam R_1 e R_2 congruências em relação à operação binária interna $*$ de um semigrupo $(S, *)$ de modo que $R_1 \subset R_2$. Então,

$$R_2/R_1 = \{(R_1x, R_1y) \in S/R_1 \times S/R_1 : (x,y) \in R_2\}$$

é uma congruência em relação à operação binária interna natural $*$ de S/R_1 e existe um isomorfismo h de semigrupo entre o semigrupo $(S/R_2, *_{R_2})$ e o semigrupo $\left(S/R_1 \Big/ R_2/R_1, *_{R_2/R_1}\right)$ dotados de suas respectivas operações binárias internas naturais.

Teorema 4.108.

Seja $(G, *)$ um grupo e sejam R_1 e R_2 duas congruências no grupo. Então,

$$R_1 \circ R_2 = R_2 \circ R_1.$$

Demonstração.

Sejam os elementos x e y do conjunto G de modo que $(x,y) \in R_1 \circ R_2$. Então, existe $z \in G$ tal que $(x,z) \in R_2$ e $(z,y) \in R_1$.

De $(z,y) \in R_1$, vem que $(z*z^{-1}*x, y*z^{-1}*x) = (x, y*z^{-1}*x) \in R_1$.

De $(x,z) \in R_2$, vem que $(y*z^{-1}*x, y*z^{-1}*z) = (y*z^{-1}*x, y) \in R_2$.

Portanto, $(x,y) \in R_2 \circ R_1$ e a demonstração da inclusão reversa é análoga. □

Teorema 4.109.

Seja R uma relação binária no conjunto S em que $(S,*)$ é um semigrupo. Então, se M é o monoide $M = S \cup \{1\}$ com elemento neutro 1 cuja operação binária interna restrita à $S \times S$ e à operação binária interna de S, a relação binária R^C no conjunto S, definida por:

$$R^C = \{(x*a*y, x*b*y) : x,y \in M \text{ e } (a,b) \in R\},$$

é a intersecção de todas as relações binárias no conjunto S que contém R e que são compatíveis à esquerda e à direita com a operação binária interna do semigrupo.

Demonstração.

A relação binária R em S está contida em R^C: se a, $b \in S$ e $(a,b) \in R$, então $(1*a*1, 1*b*1) = (a,b) \in R^C$.

Para mostrar que R^C é uma relação binária em S compatível à esquerda com a operação binária interna de S, sejam u, $v \in S$ tais que $(u,v) \in R^C$ e seja $w \in S$. Então, existem x, $y \in M$ tais que $u = x*a*y$ e $v = x*b*y$, com a, $b \in S$ e $(a,b) \in R$. De

$$w*u = w*(x*a*y) = (w*x)*a*y$$

$$w*v = w*(x*b*y) = (w*x)*b*y,$$

segue que $(w*u, w*v) \in R^C$.

A demonstração da compatibilidade à direita da relação binária R^C em relação à operação binária interna do semigrupo é análoga.

Seja R_1 uma relação binária em S compatível à esquerda e à direita com a operação binária interna do semigrupo que contém R. Assim, se x, $y \in M$ e se a, $b \in S$, com $(a,b) \in R \subset R_1$, então $(x*a*y, x*b*y) \in R_1$, o que evidencia que $R^C \subset R_1$. □

Teorema 4.110.

Sejam R_1 e R_2 relações binárias no conjunto não vazio S em que $(S,*)$ é um semigrupo. Então:

(i) Se $R_1 \subset R_2$, então $R_1^C \subset R_2^C$.

(ii) $(R_1^{-1})^C = (R_1^C)^{-1}$.

(iii) $(R_1 \cup R_2)^C = R_1^C \cup R_2^C$.

Teorema 4.111.

A relação binária de congruência $R^{\#}$ gerada por uma relação binária R em um conjunto não vazio S em que $(S,*)$ é um semigrupo é a intersecção de todas as relações binárias de congruência em S que contém R e, além disso,

$$R^{\#} = (R^C)_{eq}$$

em que $(R^C)_{eq}$ é a relação de equivalência em S gerada pela relação binária R^C em S, ou seja, se a, $b \in S$ e $(a,b) \in R^{\#}$ ou $a = b$ ou, para algum $n \in \mathbb{N} = \{1,2,\ldots\}$, existe uma sequência de elementos z_1, z_2, …, z_n de S tal que

$$a = z_1 \to z_2 \to \ldots \to z_n = b,$$

em que, para cada $j \in \{1,2,\ldots,n-1\}$, ou $(z_j, z_{j+1}) \in R$ ou $(z_{j+1}, z_j) \in R$.

Teorema 4.112.

Seja R uma relação de equivalência em um conjunto não vazio S em que $(S,*)$ é um semigrupo. A relação binária de congruêncua

$$R^b = \{(a,b) \in S \times S : \forall\, x,y \in M, (x*a*y, x*b*y) \in R\}$$

é a união de todas as relações binárias de congruência em S contidas na relação binária de congruência R.

Demonstração.

Sejam a, b, $c \in S$. Se $(a,b) \in R^b$, então $(x*c*a*y, x*c*b*y) \in R$ para todas as escolhas possíveis de x, $y \in M = S \cup \{1\}$, o que mostra que $(c*a, c*b) \in R^b$ e, analogamente, que $(a*c, b*c) \in R^b$.

Além disso, $R^b \subset R$, pois, se $(a,b) \in R^b$, então $(1*a*1, 1*b*1) = (a,b) \in R$. □

Seja $(S,*)$ um semigrupo. Uma relação binária R no conjunto não vazio S é

(i) compatível à esquerda com a operação binária interna de S se, e somente se,

$$(\forall\, r \in S)(\forall\, s \in S)(\forall\, t \in S)((r,s) \in R \Rightarrow (t*r, t*s) \in R).$$

(ii) compatível à direita com a operação binária interna de S se, e somente se,

$$(r,s) \in R \Rightarrow (r*t, s*t) \in R.$$

(iii) compatível com a operação binária interna de S se, e somente se,

$$(\forall\, s \in S)(\forall\, t \in S)(\forall\, u \in S)(\forall\, v \in S)((s,t) \in R \text{ e } (u,v) \in R \Rightarrow (s*u, t*v) \in R).$$

Seja R uma congruência em um semigrupo $(S,*)$, ou seja, R é uma relação binária de equivalência em S compatível com a operação binária interna de S, então existe uma operação binária interna natural no conjunto S/R de todas as classes de equivalência de R em S, a qual será indicada pelo mesmo símbolo $*$ (um abuso de linguagem, a saber, $(\forall\, a \in S)(\forall\, b \in S)(Ra * Rb = R(a*b))$) e esta operação binária interna em S/R está bem definida, pois, para a_1, a_2, b_1, $b_2 \in S$, se $Ra_1 = Ra_2$ e se $Rb_1 = Rb_2$, então $(a_1, a_2) \in R$ e $(b_1, b_2) \in R$ e, consequentemente, pela compatibilidade de R,

$$(a_1 * b_1, a_2 * b_2) \in R,$$

o que é equivalente afirmar que

$$R(a_1 * b_1) = R(a_2 * b_2).$$

Além disso, a operação binária interna natural em S/R é uma operação binária interna associativa em S/R.

Teorema 4.113 (Teorema da correspondência para semigrupos)**.**

Seja I um ideal próprio do semigrupo (S,μ), seja $\mathfrak{I}$ o conjunto de todos os ideais de S que contém I e seja $\mathfrak{J}$ o conjunto de todos os ideais do semigrupo quociente $(S/I, \mu_I)$. Então, a aplicação α cujo domínio de definição é $\mathfrak{I}$ e cujo conjunto de valores é $\mathfrak{J}$ definida por: se $J \in \mathfrak{I}$, então $\alpha(J) = J/I$ é uma correspondência biunívoca entre o conjunto $\mathfrak{I}$ e o conjunto $\mathfrak{J}$ que preserva a inclusão:

$$\text{se } J_1, J_2 \in \mathfrak{I}, \text{ com } J_1 \subset J_2, \text{ então } \alpha(J_1) \subset \alpha(J_2).$$

Teorema 4.114 (Segundo teorema do isomorfismo para semigrupos)**.**

Sejam I e J ideais do semigrupo $(S,*)$ tal que $I \subset J$. Então, os semigrupos quocientes $(S/J, *_J)$ e $\left(S/I \Big/ J/I, (*_I)_{J/I}\right)$ são isomorfos.

Teorema 4.115 (Terceiro teorema do isomorfismo para semigrupos)**.**

Sejam I e J ideais do semigrupo $(S,*)$. Então:

(i) $I \cap J$ e $I \cup J$ são ideais do semigrupo $(S,*)$ desde que

$$\emptyset \neq I * J = \{i * j : i \in I \text{ e } j \in J\} \subset I \cap J.$$

(ii) Os semigrupos quocientes $(I \cup J/J, *_J)$ e $(I/I \cap J, *_{I \cap J})$ são isomorfos.

Teorema 4.116 (Teorema da estrutura dos semigrupos cíclicos)**.**

Seja a um elemento de um semigrupo $(S, *)$. Então:

(i) Ou todas as potências de a são elementos distintos e o subsemigrupo (a) gerado pelo elemento a é isomorfo ao semigrupo $(\mathbb{N}, +)$, em que $\mathbb{N}$ é o conjunto dos números naturais com a operação binária interna de adição

(ii) Ou existem números naturais m (denominado o índice do elemento a) e r (denominado o período do elemento a) com as seguintes propriedades:

1. $a^m = a^{m+r}$
2. se $a^{m+u} = a^{m+v}$, então $u \equiv v \mod r$, ou seja, os restos da divisão dos números naturais u e v pelo número natural r são iguais e, reciprocamente, se $u \equiv v \mod r$, então $a^{m+u} = a^{m+v}$
3. $(a) = \{a, a^2, \ldots, a^{m+r-1}\}$
4. o núcleo K_a do elemento a é $K_a = \{a^m, a^{m+1}, \ldots, a^{m+r-1}\}$ e tem a propriedade de que $(K_a, *)$ é um grupo cíclico contido em (a)

Demonstração.

(i) Para cada número $n \in \mathbb{N} = \{1, 2, \ldots\}$, seja a função h que associa a cada número natural n o elemento $a^n \in S$. A função h é um isomorfismo de semigrupo do semigrupo aditivo $(\mathbb{N}, +)$ no semigrupo cíclico $(< a >, \cdot)$ gerado pelo elemento $a \in S$.

(ii) Seja a um elemento do semigrupo $(S, *)$ tal que o conjunto

$$\{n \in \mathbb{N} = \{1, 2, \ldots\} : \exists\, m \in \mathbb{N}, m \neq n, a^m = a^n\}$$

é um subconjunto não vazio de $\mathbb{N}$, o qual admite um elemento mínimo m denominado índice do elemento a do semigrupo.

O subconjunto de números naturais $\{n \in \mathbb{N} : a^{m+n} = a^m\}$ é um subconjunto não vazio que admite um elemento mínimo r denominado período do elemento a do semigrupo.

Seja a um elemento do semigrupo $(S, *)$ com índice m e período r. Assim,

$$a^m = a^{m+r}$$

$$a^m = a^{m+r} = a^m a^r = a^{m+r} a^r = a^{m+2r}$$

$$a^m = a^{m+2r} = a^m a^{2r} = a^{m+r} a^{2r} = a^{m+3r}$$

e assim por diante. Ou seja, para cada $q \in \mathbb{N} = \{1,2,\ldots\}$,

$$a^m = a^{m+qr}.$$

Em face da minimalidade do índice m e do período r do elemento a,

$$a, a^2, \ldots, a^m, a^{m+1}, \ldots, a^{m+r-1}$$

são elementos distintos dois a dois do semigrupo.

Para cada número $n \in \mathbb{N} = \{1,2,\ldots\}$, com $n > m$, pelo algoritmo da divisão de Euclides aplicado a $n-m$, existem números q e s tais que $n = m+qr$, em que $q \in \{0,1,\ldots\}$, $s \in \{0,1,\ldots,r-1\}$ e

$$a^n = a^{m+qr}a^s = a^m a^s = a^{m+s},$$

o que mostra que o subsemigrupo cíclico (a) gerado pelo elemento a do semigrupo é finito e é igual a

$$(a) = \{a, a^2, \ldots, a^{m+r-1}\}.$$

A ordem do elemento a do semigrupo é, por definição, o número de elementos do subsemigrupo cíclico (a) gerado por a e é igual a soma do índice de a com o período de a menos um.

O núcleo K_a do elemento a do semigrupo é, por definição,

$$K_a = \{a^m, a^{m+r}, \ldots, a^{m+r-1}\}$$

e $(K_a, *)$ é um grupo cíclico de ordem r gerado pelo elemento a^{m+t} em que $t \in \{0,1,\ldots,r-1\}$ e $m+t = 1 \mod r$, ou seja, a divisão de $m+t$ pelo período r do elemento a é igual a 1.

A escolha do número z tal que $z \in \{0,1,\ldots,r-1\}$ e $m+z = 0 \mod r$ produz o elemento a^{m+z}, que é um elemento idempotente do semigrupo e, portanto, o elemento neutro de K_a.

□

Exemplo 4.117.

Seja f a função total em $T(X_3)$ cuja matriz de valores é dada por:

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

$$f^2 = f \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 3 \end{pmatrix}$$

$$f^3 = f \circ f \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 2 \end{pmatrix}.$$

Conclusão: o índice da função f no semigrupo $(T(X_3),\circ)$ é igual a 1 e o período da função f é igual a 2.

Se $K_f = \{f, f\circ f\}$, então $(K_f,\circ)$ é um grupo cíclico gerado pelo elemento f.

Exemplo 4.118.

Seja f a função total em $T(X_3)$ cuja matriz de valores é dada por:

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

$$f^2 = f\circ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 3 \end{pmatrix}$$

$$f^3 = f\circ f\circ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 3 \end{pmatrix}.$$

Conclusão: o índice da função f no semigrupo $(T(X_3),\circ)$ é igual a 2 e o período da função f é igual a 1.

Se $K_f = \{f\circ f\}$, então $(K_f,\circ)$ é um grupo cíclico gerado pelo elemento $f\circ f$.

Exemplo 4.119.

Seja $X_7 = \{1,2,3,4,5,6,7\}$ e seja f a função parcial em X_7, ou seja, $f \in P(X_7)$ definida por:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 2 & - & 5 & - & 1 \end{pmatrix}.$$

Então:

$$f^2 = f\circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 3 & - & 5 & - & 2 \end{pmatrix}$$

$$f^3 = f\circ f\circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 2 & - & 5 & - & 3 \end{pmatrix}$$

$$f^4 = f\circ f\circ f\circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 3 & - & 5 & - & 2 \end{pmatrix}$$

$$f^5 = f\circ f\circ f\circ f\circ f = f^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 2 & - & 5 & - & 3 \end{pmatrix}.$$

O índice de f é igual a 3 e o período de f é igual a 2 e, em consequência, o núcleo K_f de f é o conjunto $\{f^3, f^4\}$, cuja tabela de Cayley associada é dada abaixo:

	f^3	f^4
f^3	f^4	f^4
f^4	f^3	f^3

Assim, nota-se que f^6 é o elemento neutro em K_f para o operação binária interna de composição e que $(K_f, \circ)$ é um grupo cíclico com elemento gerador f^4, pois

$$(f^4)^2 = f^5 \text{ e } (f^4)^3 = f^6.$$

Exemplo 4.120.

Seja $X_7 = \{1,2,3,4,5,6,7\}$ e seja f a função parcial em X_7, ou seja, $f \in P(X_7)$ definida por:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 5 & 7 & 2 & - & 3 \end{pmatrix}.$$

Então:

$$f^2 = f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 2 & 3 & 1 & - & 5 \end{pmatrix}$$

$$f^3 = f \circ f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 1 & 5 & 4 & - & 2 \end{pmatrix}$$

$$f^4 = f \circ f \circ f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 4 & 2 & 7 & - & 1 \end{pmatrix}$$

$$f^5 = f \circ f \circ f \circ f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 1 & 3 & - & 4 \end{pmatrix}$$

$$f^6 = f \circ f \circ f \circ f \circ f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & - & 7 \end{pmatrix}$$

$$f^7 = f \circ f \circ f \circ f \circ f \circ f \circ f = f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 5 & 7 & 2 & - & 3 \end{pmatrix}.$$

O índice de f é igual a 1 e o período de f é igual a 6 e, em consequência, o núcleo K_f de f é o conjunto $\{f^4, f^5, f^6\}$, cuja tabela de Cayley associada é dada abaixo:

	f^4	f^5	f^6
f^4	f^5	f^6	f^4
f^5	f^6	f^4	f^5
f^6	f^4	f^5	f^6

Assim, nota-se que f^6 é o elemento neutro em K_f para o operação binária interna de composição e que $(K_f, \circ)$ é um grupo cíclico com elemento gerador f^4, pois

$$(f^4)^2 = f^5 \text{ e } (f^4)^3 = f^6.$$

Exemplo 4.121.

Seja $X_7 = \{1,2,3,4,5,6,7\}$ e seja f a função parcial em X_7, ou seja, $f \in P(X_7)$ definida por:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 5 \end{pmatrix}.$$

Então:

$$f^2 = f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 5 & 6 \end{pmatrix}$$

$$f^3 = f \circ f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 5 & 6 & 7 \end{pmatrix}$$

$$f^4 = f \circ f \circ f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 7 & 5 & 6 & 7 & 5 \end{pmatrix}$$

$$f^5 = f \circ f \circ f \circ f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 5 & 6 & 7 & 5 & 6 \end{pmatrix}$$

$$f^6 = f \circ f \circ f \circ f \circ f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 6 & 7 & 5 & 6 & 7 \end{pmatrix}$$

$$f^7 = f \circ f \circ f \circ f \circ f \circ f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 7 & 5 & 6 & 7 & 5 \end{pmatrix}.$$

Como $f^4 = f^7$, o índice de f é igual a 4 e o período de f é igual a 3 e, em consequência, o núcleo K_f de f é o conjunto $\{f^4, f^5, f^6\}$, cuja tabela de Cayley associada é dada abaixo:

	f^4	f^5	f^6
f^4	f^5	f^6	f^4
f^5	f^6	f^4	f^5
f^6	f^4	f^5	f^6

Assim, nota-se que f^6 é o elemento neutro em K_f para o operação binária interna de composição e que $(K_f, \circ)$ é um grupo cíclico com elemento gerador f^4, pois

$$(f^4)^2 = f^5 \text{ e } (f^4)^3 = f^6.$$

Para cada par ordenado (m,r) de números naturais, existe um semigrupo $(S,*)$ que apresenta um elemento a cujos índice e período são, respectivamente, iguais a m e a r dados. Para tanto, seja S o semigrupo de todas as funções totais no conjunto $X = \{1,2,\ldots,m+r\}$ com a operação binária interna de composição e seja f a função total definida por:

$$f = \begin{pmatrix} 1 & 2 & 3 & \ldots & m & m+1 & m+2 & \ldots & m+r-1 & m+r \\ 2 & 3 & 4 & \ldots & m+1 & m+2 & m+3 & \ldots & m+r & m+1 \end{pmatrix}.$$

Então, o índice de f é igual a m e o período de f é igual a r dados.

Para cada par de números naturais (m,r), o semigrupo cíclico cujo gerador é o elemento a com índice m e período r é designado como $M(m,r)$ e é evidente que $M(1,r)$ é um grupo cíclico de ordem r.

Teorema 4.122.

Em um semigrupo periódico $(S,*)$, no sentido de que todos os elementos de S tem ordem finita, todo elemento a apresenta uma potência a^n, o qual é um elemento idempotente do semigrupo.

Em todo semigrupo periódico e, em particular, em todo semigrupo finito existe pelo menos um elemento idempotente.

Demonstração.

Se $a \in S$, em que $(S,*)$ é um semigrupo periódico, então $< a >$ é um conjunto finito e alguma potência de a é o elemento neutro do grupo cíclico $(K_a,*)$ e é, portanto, um elemento idempotente do semigrupo $(S,*)$. □

A hipótese de periodicidade do semigrupo é essencial: o semigrupo $(\mathbb{N},+)$ não possui elementos idempotentes no sentido de que, para cada $n \in \mathbb{N} = \{1,2,\ldots\}$, $n+n \neq n$.

Exemplo 4.123.

Seja o monoide multiplicativo comutativo $(\mathbb{Z}_{10},\cdot)$, em que $\mathbb{Z}_{10} = \{0,1,2,3,4,5,6,7,8,9\}$. Os elementos idempotentes do monoide $(\mathbb{Z}_{10},\cdot)$ são 0, 1, 5 e 6. O conjunto $U(\mathbb{Z}_{10})$ dos elementos inversíveis do monoide é igual a $\{1,3,7,9\}$ e $(U(\mathbb{Z}_{10}),\cdot)$ é um grupo multiplicativo comutativo.

Os cálculos dos períodos e dos índices dos elementos de $\mathbb{Z}_{10}$ são dados abaixo:

$< 1 >= \{1\}$ e o elemento 1 tem período 1 e índice 1.

$< 2 >= \{2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 6, 2^5 = 2, \ldots\} = \{2,4,8,6\}$ e o elemento 2 tem período 4 e índice 1.

$< 3 >= \{3^1 = 3, 3^2 = 9, 3^3 = 7, 3^4 = 1, 3^5 = 3, \ldots\} = \{3,9,7,1\}$ e o elemento 3 tem período 4 e índice 1.

$< 4 >= \{4^1 = 4, 4^2 = 6, 4^3 = 4, \ldots\} = \{4,6\}$ e o elemento 4 tem período 2 e índice 1.

$< 5 >= \{5\}$ e o elemento 5 tem período 1 e índice 1.

$< 6 >= \{6\}$ e o elemento 6 tem período 1 e índice 1.

$< 7 >= \{7^1 = 7, 7^2 = 9, 7^3 = 3, 7^4 = 1, 7^5 = 7, \ldots\} = \{7,9,3,1\}$ e o elemento 7 tem período 4 e índice 1.

$< 8 >= \{8^1 = 8, 8^2 = 4, 8^3 = 2, 8^4 = 6, 8^5 = 8, \ldots\} = \{8,4,2,6\}$ e o elemento 8 tem período 4 e índice 1.

$< 9 >= \{9^1 = 9, 9^2 = 1, 9^3 = 9, \ldots\} = \{9,1\}$ e o elemento 9 tem período 2 e índice 1.

Exemplo 4.124 (O semigrupo de Baer-Levi)**.**

O semigrupo conhecido como semigrupo de Baer-Levi é o exemplo clássico de um semigrupo que não possui elementos idempotentes e é definido como um subsemigrupo do semigrupo $(T(X), \circ)$, em que $T(X)$ é o conjunto de todas as funções totais cujo domínio de definição é o conjunto X e cujo conjunto de valores é um subconjunto de X com a operação binária interna de composição, da seguinte maneira:

Seja $\mathbb{N} = \{1,2,\ldots\}$ e seja S o conjunto de todas as funções totais f em $\mathbb{N}$, ou seja, f é uma função cujo domínio de definição $D(f)$ é $\mathbb{N}$ e cujo conjunto de valores $R(f)$ está contido em $\mathbb{N}$ com a propriedade adicional de que f é uma função injetora e que o complementar de $R(f)$ em $\mathbb{N}$ é um conjunto infinito. Por exemplo, para cada $n \in \mathbb{N}$, se $f(n) = 2n$, então $f \in S$ ou, se, para cada $n \in \mathbb{N}$, $g(n) = 2n-1$, então $g \in S$.

Assim, para cada $f \in S$, existe uma correspondência biunívoca entre os elementos do complementar do conjunto $R(f)$ em $\mathbb{N}$ e os elementos do complementar do conjunto $R(f \circ f)$ em $R(f)$, o qual é dada por: se $y = f(x)$ para algum $x \in \mathbb{N}$ e se $y \notin R(f \circ f)$, então, para cada $x \in \mathbb{N} \setminus f(\mathbb{N})$ associa-se o elemento $f(x)$, o qual é um elemento de $R(f)$, mas não é um elemento de $R(f \circ f)$, então, ao elemento $y \in R(f) \setminus R(f \circ f)$ é associado o elemento $x = f^{-1}(y) \in X \setminus R(f)$.

Lembrando que f é uma função injetora e que, se $x \in R(f)$, então $x = f(z)$ para algum $z \in \mathbb{N}$ e $(f \circ f)(z) = f\big[f(z)\big] = f(x) = y$, o que é contrário à hipótese de que $y \notin R(f \circ f)$.

Caso houvesse algum elemento h idempotente em S em relação a operação interna de composição, $h \circ h = h$, enquanto que $R(h \circ h) = R(h)$ e o complementar do conjunto $R(h \circ h)$ em $R(h)$ é o conjunto não vazio em correspondência biunívoca com o complementar do conjunto $R(h)$ em $\mathbb{N}$ que, por definição, é um subconjunto infinito de $\mathbb{N}$.

4.1 Grupos finitos

4.1.1 O grupo das permutações e o subgrupo das permutações pares

Uma permutação par é a permutação expressa como composta de um número par de transposições.

Teorema 4.125.

Para cada número natural $n \in \{2,3,\ldots\}$, o conjunto de todas as permutações dos números 1, 2, …, n, com a operação binária interna de composição de funções é um grupo $(S_n, \circ)$ não

comutativo gerado pelo conjunto formado pelas $n-1$ transposições:

(i) $(1\ 2), (1\ 3), \ldots, (1\ n)$

(ii) $(1\ 2), (2\ 3), \ldots, ((n-1)\ n)$

Além disso, o grupo $(S_n, \circ)$ é gerado pelo conjunto formado

(iii) pela transposição $(1\ 2)$ e pela função ciclo $(1\ 2\ \ldots\ n)$ de comprimento n.

(iv) pela transposição $(1\ 2)$ e pela função ciclo $(2\ 3\ \ldots\ n)$ de comprimento $n-1$

Para cada número natural $n \in \{3,4,\ldots\}$, o conjunto de todas as permutações pares dos números 1, 2, ..., n, com a operação binária interna de composição de funções é um grupo $(A_n, \circ)$ não comutativo gerado pela totalidade das funções ciclo de comprimento três e gerado pela totalidade das funções ciclo de comprimento três da forma $(i\ j\ k)$ com $k \in \{1,2,\ldots\}$ e $k \neq \{i,j\} \subset \{1,2,\ldots\}$. Além disso, $(A_n, \circ)$ é um subgrupo normal em $(S_n, \circ)$.

Demonstração.

O grupo das permutações $(S_n, \circ)$ é gerado pelo subconjunto constituído de todas as transposições.

Como, para números naturais $i,\ j \in \{1,2,\ldots,n\}$,

$$(i\ j) = (1\ i) \circ (1\ j) \circ (1\ i),$$

o grupo das permutações $(S_n, \circ)$ é gerado pelo subconjunto constituído pelas $n-1$ transposições: $(1\ 2)$, $(1\ 3)$, ..., $(1\ n)$.

Como, para $j \in \{2,3,\ldots,n\}$,

$$(1\ j) = (1\ j-1) \circ (j-1\ j) \circ (1\ j-1),$$

vem que

$$(1\ 3) = (1\ 2) \circ (2\ 3) \circ (1\ 2)$$

$$(1\ 4) = (1\ 3) \circ (3\ 4) \circ (1\ 3)$$

e assim por diante até

$$(1\ n) = (1\ n-1) \circ (n-1\ n) \circ (1\ n-1),$$

então o grupo das permutações $(S_n, \circ)$ é gerado pelo subconjunto constituído pelas $n-1$ transposições: $(1\ 2)$, $(2\ 3)$, ..., $(n-1\ n)$.

Como

$$(2\ 3) = (1\ 2\ \ldots\ n) \circ (1\ 2) \circ (1\ 2\ \ldots\ n)^{-1}$$

$$(3\ 4) = (1\ 2\ \ldots\ n) \circ (2\ 3) \circ (1\ 2\ \ldots\ n)^{-1}$$

e assim por diante até

$$(n-1\ n) = (1\ 2\ \ldots\ n) \circ (n-2\ n-1) \circ (1\ 2\ \ldots\ n)^{-1},$$

então o grupo das permutações $(S_n, \circ)$ é gerado pelo subconjunto constituído pela transposições $(1\ 2)$ e pela função ciclo $(1\ 2\ \ldots\ n)$ de comprimento n.

Como

$$(1\ 3) = (2\ 3\ \ldots\ n) \circ (1\ 2) \circ (2\ 3\ \ldots\ n)^{-1}$$

$$(1\ 4) = (2\ 3\ \ldots\ n) \circ (1\ 3) \circ (2\ 3\ \ldots\ n)^{-1}$$

e assim por diante até

$$(1\ n) = (2\ 3\ \ldots\ n) \circ (1\ n-1) \circ (2\ 3\ \ldots\ n)^{-1},$$

então o grupo das permutações $(S_n, \circ)$ é gerado pelo subconjunto constituído pela transposições $(1\ 2)$ e pela função ciclo $(2\ 3\ \ldots\ n)$ de comprimento $n-1$.

A demonstração de que $(A_n, \circ)$ é um subgrupo normal em $(S_n, \circ)$ é trivial, pois, para cada $f \in S_n$ e para cada $g \in A_n$,

$$f \circ g \circ f^{-1} \in A_n$$

devido a ser função composta de um número par de transposições: g é uma função composta de um número par de transposições e as transposições presentes em f e em f^{-1} ocorrem um número par de vezes.

Outra demonstração de que $(A_n, \circ)$ é um subgrupo normal em $(S_n, \circ)$ segue do fato de que $(A_n, \circ)$ tem índice dois em $(S_n, \circ)$: o número de permutações pares em A_n é a metade do número de permutações em S_n.

Para $n \in \{4, 5, \ldots\}$, as permutações pares pertencentes a A_n são funções compostas de um número par de transposições: duas transposições consecutivas são da forma

$$(i\ j) \circ (k\ l) = (i\ k\ j) \circ (i\ k\ l)$$

ou da forma

$$(i\ j) \circ (i\ k) = (i\ k\ j),$$

em que i, j, k e l são números dois a dois distintos de $\{1, 2, \ldots\}$.

A demonstração de que $(A_n, \circ)$ é gerado pela totalidade das funções ciclo de comprimento três está completa.

A demonstração de que $(A_n, \circ)$ é gerado pela totalidade das funções ciclo de comprimento três da forma $(i\ j\ k)$ com $k \in \{1,2,\ldots\}$ e $k \neq \{i,j\} \subset \{1,2,\ldots\}$ é feita a seguir, para $n \in \{4,5,\ldots\}$ desde que, no caso $n = 3$,

$$S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

e $A_3 = \{(1), (2\ 3\ 1), (3\ 2\ 1)\}$ é gerado pela função ciclo (231) de comprimento três ou pela função ciclo $(2\ 3\ 1)^{-1} = (3\ 2\ 1)$.

A prova é consequência das fórmulas abaixo: para $\{i,j,k,l,r,s\} \subset \{1,2,\ldots\}$,

(i) $(i\ k\ j) = (i\ j\ k) \circ (i\ j\ k)$

(ii) $(i\ k\ l) = (i\ j\ l) \circ (i\ j\ k) \circ (i\ j\ k)$

(iii) $(j\ k\ l) = (i\ j\ l) \circ (i\ j\ l) \circ (i\ j\ k)$

(iv) $(l\ r\ s) = (i\ j\ l) \circ (i\ j\ l) \circ (i\ j\ s) \circ (i\ j\ r) \circ (i\ j\ r) \circ (i\ j\ l)$

□

O resultado seguinte será utilizado na prova do Teorema da simplicidade do grupo $(A_n, \circ)$.

Lema 4.126.

Para cada número natural $n \in \{3,4,\ldots\}$, se $(N, \circ)$ é um subgrupo normal em $(A_n, \circ)$ e se uma função ciclo de comprimento três pertence a N, então $N = A_n$.

Demonstração.

Seja a função ciclo $(i\ j\ k)$ de comprimento três pertence a N com $\{i,j,k\} \subset \{1,2,\ldots,n\}$. Para cada $l \in \{1,2,\ldots,n\}$, $l \neq \{i,j,k\}$,

$$\begin{aligned}(i\ j\ l) &= (i\ j) \circ (k\ l) \circ (i\ j\ k) \circ (i\ j\ k) \circ (k\ l) \circ (i\ j) \\ &= \left[(i\ j) \circ (k\ l)\right] \circ (i\ j\ k) \circ \left[(i\ j) \circ (k\ l)\right]^{-1}\end{aligned}$$

pertence a N pelo fato de $(N, \circ)$ ser subgrupo normal em $(A_n, \circ)$. □

Teorema 4.127 (Teorema da simplicidade do grupo $(A_n, \circ)$)**.**

Para cada número $n \in \mathbb{N} = \{1,2,\ldots\}$, $n \neq 4$, $(A_n, \circ)$ é um grupo simples no sentido de que os únicos subgrupos normais em $(A_n, \circ)$ são os subgrupos triviais $(\{1\}, \circ)$ e $(A_n, \circ)$.

Demonstração.

Seja $(N, \circ)$ um subgrupo normal em $(A_n, \circ)$ para $n \in \{5,6,\ldots\}$. A demonstração de que $N = A_n$ segue dos seguintes casos:

(i) N contém uma função ciclo de comprimento três e, pelo lema anterior, $N = A_n$.

(ii) N contém uma permutação par f, em cuja decomposição em ciclos disjuntos ocorre uma função ciclo de comprimento $r \geq 4$, ou seja, $f = (i_1\ i_2 \ldots\ i_r) \circ g$, com $\{i_1, i_2, \ldots, i_r\} \subset \{1, 2, \ldots, n\}$. Se $h = (i_1\ i_2\ i_3)$, então $f^{-1} \circ (h \circ f \circ h^{-1}) = (i_1\ i_3\ i_r) \in N$ pelo fato de $(N, \circ)$ ser subgrupo normal em $(A_n, \circ)$ e, portanto, pelo lema anterior, $N = A_n$.

(iii) N contém uma permutação par f, em cuja decomposição em ciclos disjuntos ocorrem pelo menos duas funções ciclo de comprimento três consecutivas (sem perda de generalidade), ou seja, $f = (i_1\ i_2\ i_3) \circ (i_4\ i_5\ i_6)$, com $\{i_1, i_2, i_3, i_4, i_5, i_6\} \subset \{1, 2, \ldots, n\}$. Se $h = (i_1\ i_2\ i_4)$, então $f^{-1} \circ (h \circ f \circ h^{-1}) = (i_1\ i_4\ i_2\ i_6\ i_3) \in N$ pelo fato de $(N, \circ)$ ser subgrupo normal em $(A_n, \circ)$ e, pelo caso (ii), $N = A_n$.

(iv) N contém uma permutação par f, em cuja decomposição em ciclos disjuntos ocorrem uma função ciclo de comprimento três e as demais funções ciclo são transposições, ou seja, $f = (i_1\ i_2\ i_3) \circ g$, com $\{i_1, i_2, i_3\} \subset \{1, 2, \ldots, n\}$, em que g é uma função composta apenas de um número finito de transposições. Então:

a) $g \circ g = (1)$

b) $f \circ f = N$

c) $$\begin{aligned} f \circ f &= (i_1\ i_2\ i_3) \circ g \circ (i_1\ i_2\ i_3) \circ g \\ &= (i_1\ i_2\ i_3) \circ (i_1\ i_2\ i_3) \circ g \circ g \\ &= (i_1\ i_2\ i_3) \circ (i_1\ i_2\ i_3) \\ &= (i_1\ i_3\ i_2) \end{aligned}$$

e, pelo lema anterior, $N = A_n$.

(v) N contém uma permutação par f, em cuja decomposição em ciclos disjuntos ocorrem um número par finito de transposições, ou seja, $f = (i_1\ i_2) \circ (i_3\ i_4) \circ g$, com $\{i_1, i_2, i_3, i_4\} \subset \{1, 2, \ldots, n\}$, em que g é uma função composta apenas de um número finito de transposições. Se $h = (i_1\ i_2\ i_3)$, então $f^{-1} \circ (h \circ f \circ h^{-1}) = (i_1\ i_3) \circ (i_2\ i_4) \in N$ pelo fato de $(N, \circ)$ ser subgrupo normal em $(A_n, \circ)$ e, desde que $n \geq 5$, existe um $j \in \{1, 2, \ldots, n\}$ tal que $j \notin \{i_1, i_2, i_3, i_4\}$. De $(i_1\ i_3\ j) \in A_n$ e de $(i_1\ i_3) \circ (i_2\ i_4) \in N$, segue que

$$(i_1\ i_3) \circ (i_2\ i_4) \circ \left[(i_1\ i_3\ j)\right] \circ (i_1\ i_3) \circ (i_2\ i_4) \circ \left[(i_1 i_3 j)\right]^{-1} = (i_1\ i_3\ j) \in N$$

pelo fato de $(N, \circ)$ ser subgrupo normal em $(A_n, \circ)$ e, portanto, pelo lema anterior, $N = A_n$.

Para $n = 1$, $A_1 = S_1 = \{(1)\}$.

Para $n = 2$, $A_2 = \{(1)\}$ e $S_2 = \{(1), (2)\}$.

Para $n=3$, $A_3=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$ é um grupo cíclico simples de ordem três gerado por $(1\ 2\ 3)$ ou por $(1\ 2\ 3)^{-1}=(1\ 3\ 2)$.

Para $n=4$, $N=\{(1),(1\ 2)\circ(3\ 4),(1\ 3)\circ(2\ 4),(1\ 4)\circ(2\ 3)\}$ é um subgrupo normal em $(S_4,\circ)$ e em $(A_4,\circ)$, pois, para cada $f\in S_4$, para cada $\{i,j\}\in\{1,2,3,4,\}$ e para cada $\{k,l\}\in\{1,2,3,4,\}$,

$$f\circ(i\ j)\circ(k\ l)\circ f^{-1}=((f(i)\ f(j))\circ((f(k)\ f(l)).$$

□

4.1.2 O grupo das simetrias de um polígono regular

Para cada número natural $n\in\{3,4,\ldots\}$, $(D_n,\circ)$ é o grupo não comutativo, com a operação binária interna de composição de funções, gerado pela função ciclo de comprimento n

$$f=(1\ 2\ \ldots\ n)$$

e pela permutação g idempotente

$$g=\begin{pmatrix}1 & 2 & 3 & 4 & \ldots & j & \ldots & n-1 & n\\ 1 & n & n-1 & n-2 & \ldots & n+2-j & \ldots & 3 & 2\end{pmatrix}.$$

A propriedade de que $g\circ f=f^{-1}\circ g$ é de verificação imediata.

4.1.3 O grupo multiplicativo dos quatérnios $(Q_8,\cdot)$

O grupo multiplicativo $(Q_8,\cdot)$ é o par ordenado em que

$$Q_8=\{1,-1,i,-i,j,-j,k,-k\}$$

e, observando as letras $ijkijk$ em ordem alfabética, a operação binária interna de multiplicação é definida por:

$$ij=k=-ji$$

$$jk=i=-kj$$

$$ik=-j=ki$$

$$-1=ii=(-i)(-i)=jj=(-j)(-j)=kk=(-k)(-k)$$

$$-1i=-i$$

$$-1j=-j$$

$$-1k=-k$$

$$(-1)(-1)=1$$

e 1 é o elemento neutro da operação binária interna de multiplicação.

4.1.4 O grupo dos elementos inversíveis $(GL(2,\mathbb{Q}),\cdot)$ do monoide multiplicativo $(M(2,\mathbb{Q}),\cdot)$

O grupo multiplicativo $(GL(2,\mathbb{Q}),\cdot)$ constituído de todas as matrizes quadradas de ordem dois com coeficientes racionais e determinante não nulo é o grupo dos elementos inversíveis em relação à multiplicação de matrizes quadradas de ordem dois do monoide não comutativo $(M(2,\mathbb{Q}),\cdot)$ constituído de todas as matrizes quadradas de ordem dois com a operação binária interna de multiplicação de matrizes.

A matriz inversa A^{-1} de uma matriz $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ com $ad-bc\neq 0$ é calculado pela fórmula

$$A^{-1}=(ad-bc)^{-1}=\frac{1}{ad-bc}=\begin{pmatrix} d & -b \\ -c & d \end{pmatrix}.$$

As matrizes quadradas de ordem dois com determinante não nulo $A=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ e $B=\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ pertencentes ao grupo multiplicativo não comutativo $(GL(2,\mathbb{Q}),\cdot)$ com a operação binária interna de multiplicação de matrizes tem ordem finita 4 e ordem finita 3, respectivamente, ou seja, $A^4=B^3=I=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ e a matriz produto AB tem ordem infinita, pois, para cada número $n\in\mathbb{N}=\{1,2,\ldots\}$,

$$(AB)^n=\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

O grupo aditivo produto cartesiano dos grupos aditivos $(\mathbb{Z}_2,+)$ e $(\mathbb{Z},+)$ tem elementos de ordem infinita como, por exemplo, $(0,1)$, $(0,-1)$, $(1,1)$ e $(1,-1)$, enquanto que $(1,0)=(1,1)+(0,-1)$, soma de dois elementos de ordem infinita, tem ordem 2: $(1,0)+(1,0)=(0,0)$.

O subgrupo multiplicativo do grupo multiplicativo $(GL(2,\mathbb{C}),\cdot)$ gerado pelas matrizes quadradas de ordem dois com coeficientes complexos

$$A=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad\qquad B=\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

em que $A^4=B^4=I=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ e a fórmula $BA=A^3B=A^{-1}B$ é de verificação imediata. Tal subgrupo multiplicativo é denominado grupo dos quatérnios por alguns autores por ser isomorfo ao grupo dos quatérnios $(Q_8,\cdot)$.

O subgrupo multiplicativo do grupo multiplicativo $(GL(2,\mathbb{C}),\cdot)$ gerado pelas matrizes $M=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$ e $N=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ não é isomorfo ao grupo dos quatérnios $(Q_8,\cdot)$, mas é isomorfo ao grupo das simetrias $(D_4,\circ)$ do quadrado.

CAPÍTULO

5

SEMIGRUPOS INVERSOS

Neste capítulo, a operação binária interna em semigrupos será indicada com a notação multiplicativa usual, isto é, se μ é a operação binária interna do semigrupo, então, para elementos s e t do semigrupo, $\mu(s,t) = st$.

Definição 5.1.

Um semigrupo $(S,\cdot)$ é um semigrupo idempotente quando todos os elementos de S são elementos itempotentes no sentido de que: $s \in S$ é um elemento idempotente de S quando, e somente quando, $ss = s$.

Definição 5.2.

Um semigrupo $(S,\cdot)$ é um semigrupo regular quando todos os elementos de S são elementos regulares no sentido de que: $s \in S$ é um elemento regular de S quando, e somente quando, existe $t \in S$ de modo que $s(ts) = (st)s = s$.

Se s e t são elementos de um semigrupo tais que $sts = s$, então:

$$\begin{aligned}(tst)s(tst) &= t(sts)tst \\ &= tstst \\ &= t(sts)t \\ &= tst.\end{aligned}$$

Definição 5.3.

Um semigrupo $(S,\cdot)$ é um semigrupo inverso quando todos os elementos de S são elementos inversíveis de S no sentido de que: $s \in S$ é um elemento inversível de S quando, e somente quando, existe um único elemento $t \in S$ tal que $sts = s$ e $tst = t$.

O elemento t com as propriedades $sts = s$ e $tst = t$ recebe o nome de elemento inverso de semigrupo do elemento s e é denotado por s^{-1}.

Teorema 5.4.

Um semigrupo $(S, \cdot)$ é um semigrupo inverso se, e somente se,

(i) para cada elemento $s \in S$, existe um elemento $t \in S$ tal que

$$sts = s$$

$$tst = t;$$

(ii) a operação binária interna $\cdot$ do semigrupo $(S, \cdot)$ é uma operação binária interna comutativa no conjunto $E(S)$ de todos os n elementos idempotentes de S.

Demonstração.

Pode-se observar que, para cada elemento $s \in S$, a existência e a unicidade de um elemento $b \in S$ tal que $sts = s$ e $tst = t$ é equivalente à propriedade de que a operação binária interna $\cdot$ é comutativa no conjunto $E(S)$ dos elementos idempotentes de seu grupo.

Para um elemento $s \in S$, admite-se que existam elementos t, $v \in S$ com as propriedades abaixo:

$$sts = s = svs$$

$$tst = t$$

$$vsv = v$$

Assim,

$$(st)(st) = (sts)t = st$$

$$(ts)(ts) = (tst)s = ts$$

$$(sv)(sv) = (svs)v = sv$$

$$(vs)(vs) = (vsv)s = vs.$$

Como $st, ts \in E(S)$, vem que $sv, vs \in E(S)$ e, por hipótese,

$$(ts)(vs) = (vs)(ts)$$

$$(sv)(tv) = (tv)(sv)$$

$$(st)(sv) = (sv)(st),$$

então

$$\begin{aligned} t &= tst \\ &= t(svs)t \\ &= (ts)(vs)t \\ &= (vs)(ts)t \\ &= v(sts)t \\ &= vst \\ &= (vsv)st \\ &= v(sv)(st) \\ &= v(st)(sv) \\ &= v(sts)v \\ &= vsv \\ &= v. \end{aligned}$$

□

Propriedade 5.5.

O elemento inverso de grupo s^{-1} do elemento s pertencente a um grupo é igual ao elemento inverso de semigrupo na estrutura de semigrupo subjacente à estrutura de grupo.

Exemplo 5.6.

Os elementos do monoide não comutativo $(T(X_2), \circ)$ das funções totais definidas em $X_2 = \{1,2,\}$ são: a função f_1 constante igual a 1, a função f_2 constante igual a 2, a função identidade $(1) = (2)$ e a função transposição $(1\ 2)$.

Para a determinação dos elementos inversíveis de um semigrupo de uma função f pertencente ao monoide $(T(X_2), \circ)$ é preciso definir uma função total g em X_2 com as propriedades $f \circ g \circ f = f$ e $g \circ f \circ g = g$.

Quando f é a função identidade em X_2 das equações $(1) \circ g \circ (1) = (1)$ e $g \circ (1) \circ g = g$, segue que g é a função identidade. Portanto, o elemento inversível de semigrupo da função identidade é a própria função identidade.

No caso de f_1, a função constante igual a 1 em X_2, das equações $f_1 \circ g \circ f_1 = f_1$ e $g \circ f_1 \circ g = g$, ou seja, de

$$(f_1 \circ g \circ f_1)(1) = f_1(1) = 1$$

$$(f_1 \circ g \circ f_1)(2) = f_1(2) = 1$$

$$(g \circ f_1 \circ g)(1) = g(1)$$

$$(g \circ f_1 \circ g)(2) = g(2),$$

vem que

$$f_1\big[g(1)\big] = 1$$
$$f_1\big[g(1)\big] = 1$$
$$g(1) = g(1)$$
$$g(1) = g(2).$$

Portanto, as funções constantes f_1 e f_2 são elementos inversíveis de semigrupo da função f_1.

No caso de f_2, a função constante igual a 2 em X_2, das equações $f_2 \circ g \circ f_2 = f_2$ e $g \circ f_2 \circ g = g$, ou seja, de

$$(f_2 \circ g \circ f_2)(1) = f_2(1) = 2$$
$$(f_2 \circ g \circ f_2)(2) = f_2(2) = 2$$
$$(g \circ f_2 \circ g)(1) = g(1)$$
$$(g \circ f_2 \circ g)(2) = g(2),$$

vem que

$$f_2\big[g(2)\big] = 2$$
$$f_1\big[g(2)\big] = 2$$
$$g(2) = g(1)$$
$$g(2) = g(2).$$

Portanto, as funções constantes f_1 e f_2 são elementos inversíveis de semigrupo da função f_2.

No caso da função transposição $(1\ 2)$, das equações $(1\ 2) \circ g \circ (1\ 2) = (1\ 2)$ e $g \circ (1\ 2) \circ g = g$, segue que $g(1) = 2$ e $g(2) = 1$. Portanto, o elemento inversível de semigrupo da função transposição $(1\ 2)$ é a própria função transposição $(1\ 2)$.

Exemplo 5.7.

Seja f a função total pertencente a $T(X_4)$ cuja matriz de valores é dada por:

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

Para a determinação do elemento inverso de semigrupo da função f, é necessário definir uma função total g satisfazendo $f \circ g \circ f = f$ e $g \circ f \circ g = g$, ou seja:

$$f\Big[g\big[f(1)\big]\Big] = f\big[g(4)\big] = 4 = f(1)$$

$$f\Big[g\big[f(2)\big]\Big] = f\big[g(4)\big] = 4 = f(2)$$
$$f\Big[g\big[f(3)\big]\Big] = f\big[g(3)\big] = 3 = f(3)$$
$$f\Big[g\big[f(4)\big]\Big] = f\big[g(4)\big] = 1 = f(4).$$

Como $g(4) = 1$, $g(4) = 2$ e $g(4) = 4$, f não tem elemento inverso de semigrupo.

Exemplo 5.8.

Seja f a função total pertencente a $T(X_4)$ cuja matriz de valores é dada por:

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

Para a determinação do elemento inverso de semigrupo da função f, é necessário definir uma função total g satisfazendo $f \circ g \circ f = f$ e $g \circ f \circ g = g$, ou seja:

$$f\Big[g\big[f(1)\big]\Big] = f\big[g(1)\big] = 1$$
$$f\Big[g\big[f(2)\big]\Big] = f\big[g(4)\big] = 4$$
$$f\Big[g\big[f(3)\big]\Big] = f\big[g(4)\big] = 4$$
$$f\Big[g\big[f(4)\big]\Big] = f\big[g(2)\big] = 2.$$

Dessa forma, conclui-se que $g(1) = 1$, que $g(2) = 4$, que o valor de $g(4)$ é igual a 2 ou igual a 3 e que o valor de $g(3)$ pode ser igual a 1, 2, 3 ou 4. Escolhendo $g(3) = 1$, sem perda de generalidade, escreve-se a função total g como:

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 1 & 2 \text{ ou } 3 \end{pmatrix}.$$

Agora, resta analisar os dois casos abaixo:

(i) Se $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 1 & 2 \end{pmatrix}$, a igualdade $g \circ f \circ g = g$ é satisfeita.

(ii) Se $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 1 & 3 \end{pmatrix}$, a igualdade $g \circ f \circ g = g$ é satisfeita.

Portanto, a função f possui dois elementos inversos de semigrupo. A unicidade do elemento inverso de semigrupo é válida em semigrupos comutativos, como será estudado posteriormente.

Exemplo 5.9.

Sendo $\mathbb{Z}_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$, para calcular os elementos inversos de semigrupo do semigrupo $(\mathbb{Z}_{12}, \cdot)$, em que a operação binária interna $\cdot$ é a operação de multiplicação usual, basta tomar elementos $s, t \in \mathbb{Z}_{12}$ e calcular os produtos sts e tst. Como a operação de multiplicação é comutativa, vem que $sts = sst = s^2t$ e que $tst = tts = t^2s$. Se $s^2t = s$ e se $t^2s = t$, então t é o elemento inverso do elemento s do semigrupo $(\mathbb{Z}_{12}, \cdot)$. Assim, tomando $s = 3$, encontra-se a seguinte tabela:

s	s^2	t	s^2t
3	9	0	0
3	9	1	9
3	9	2	6
3	9	3	3
3	9	4	0
3	9	5	9
3	9	6	6
3	9	7	3
3	9	8	0
3	9	9	9
3	9	10	6
3	9	11	3

Os possíveis candidatos para inverso do elemento $s = 3$ são $t = 3$, $t = 7$ e $t = 11$. Como $7 \cdot 3 \cdot 7 = 3 \neq 7$ e como $11 \cdot 3 \cdot 11 = 3 \neq 11$, fica claro que $t = 3$ é o elemento inverso de semigrupo do elemento $s = 3$. De fato, $3 \cdot 3 \cdot 3 = 3$.

Da mesma forma, tomando $s = 8$, encontra-se a seguinte tabela:

s	s^2	t	s^2t
8	4	0	0
8	4	1	4
8	4	2	8
8	4	3	0
8	4	4	4
8	4	5	8
8	4	6	0
8	4	7	4
8	4	8	8
8	4	9	0
8	4	10	4
8	4	11	8

Analisando os possíveis candidatos e procedendo como anteriormente, $t = 8$ é o elemento inverso de semigrupo do elemento $s = 8$.

De maneira análoga, tomando $s = 6$, encontra-se a seguinte tabela:

s	s^2	t	s^2t
6	0	0	0
6	0	1	0
6	0	2	0
6	0	3	0
6	0	4	0
6	0	5	0
6	0	6	0
6	0	7	0
6	0	8	0
6	0	9	0
6	0	10	0
6	0	11	0

Como $6^2 \cdot t = 0 \neq 6$ para todos os valores de $t \in \mathbb{Z}_{12}$, então conclui-se que $s = 6$ não tem inverso de semigrupo.

Da mesma forma, pode-se concluir também que $s = 2$ e que $s = 10$ não têm inverso de semigrupo, pois, de acordo com as tabelas abaixo:

s	s^2	t	s^2t
2	4	0	0
2	4	1	4
2	4	2	8
2	4	3	0
2	4	4	4
2	4	5	8
2	4	6	0
2	4	7	4
2	4	8	8
2	4	9	0
2	4	10	4
2	4	11	8

s	s^2	t	s^2t
10	4	0	0
10	4	1	4
10	4	2	8
10	4	3	0
10	4	4	4
10	4	5	8
10	4	6	0
10	4	7	4
10	4	8	8
10	4	9	0
10	4	10	4
10	4	11	8

$2^2 \cdot t \neq 2$ e $10^2 \cdot t \neq 10$ para todos os valores de $t \in \mathbb{Z}_{12}$.

É evidente que todo elemento inversível de S é um elemento regular de S; em contrapartida, não é tão evidente que todo elemento regular de S é um elemento inversível de S, haja vista que, se $s \in S$ é um elemento regular de S, existe $t \in S$ tal que $sts = s$ e $tst = s'$ é tal que

$$ss's = s(tst)s = (sts)ts = sts = s$$

$$s'ss' = (tst)s(tst) = t(sts)tst = tstst = t(sts)t = tst = s'.$$

Exemplo 5.10.

Sejam X e Y conjuntos não vazios. A operação binária interna $*$ no produto cartesiano $X \times Y$ é definida na notação multiplicativa por: para $(x_1, y_1) \in X \times Y$ e $(x_2, y_2) \in X \times Y$,

$$(x_1, y_1)(x_2, y_2) = (x_1, y_2),$$

que é claramente associativa no produto cartesiano $X \times Y$.

Para $(x, y) \in X \times Y$,

$$(x,y)^2 = (x,y)(x,y) = (x,y)$$

$$(x,y)^3 = ((x,y)(x,y))(x,y) = (x,y)(x,y) = (x,y)$$

$$(x,y)^4 = (x,y)^2 = (x,y)$$

e, finalmente,

$$(x,y) = (x,y)(x,y)^2(x,y).$$

Além disso, para (x_1, y_1), (x_2, y_2) e $(x_3, y_3) \in X \times Y$,

$$(x_1,y_1)(x_2,y_2)(x_3,y_3) = (x_1,y_1)(x_2,y_3) = (x_1,y_3) = (x_1,y_1)(x_3,y_3).$$

Em particular, $(x_1, y_1)(x_2, y_2)(x_1, y_1) = (x_1, y_1)$.

Dessa forma, pode-se concluir que o semigrupo constituído do produto cartesiano $X \times Y$ com a operação binária interna acima definida é um semigrupo idempotente e é um semigrupo regular, mas não é um semigrupo inverso, pois o elemento inverso de semigrupo para cada elemento não é único.

Mas, em geral, $(x_1, y_2) = (x_1, y_1)(x_2, y_2) \neq (x_2, y_2)(x_1, y_1) = (x_2, y_1)$, ou seja, a operação binária interna do semigrupo não é comutativa nos elementos do semigrupo que são elementos idempotentes.

Propriedades 5.11.

Seja $(S, \cdot)$ um semigrupo inverso. Então:

(i) Para cada $s \in S$, $s^{-1}s$ e ss^{-1} são elementos idempotentes do semigrupo e

$$s(s^{-1}s) = s = (ss^{-1})s.$$

Demonstração.

1. $s \in S$

2. $(s^{-1}s)^2 = (s^{-1}s)(s^{-1}s)$
$= s^{-1}(ss^{-1}s)$
$= s^{-1}s$
3. $(ss^{-1})^2 = (ss^{-1})(ss^{-1})$
$= (s^{-1}ss^{-1})$
$= ss^{-1}$

□

(ii) $(s^{-1})^{-1} = s$ pela unicidade do elemento inverso.

(iii) Para cada elemento idempotente $e \in S$ e, para cada $s \in S$, $s^{-1}es$ é um elemento idempotente de S.

Demonstração.

1. $e \in S$
2. $e^2 = ee = e$
3. $s \in S$
4. $(s^{-1}es)^2 = (s^{-1}es)(s^{-1}es)$
$= (s^{-1}e)(ss^{-1})(es)$
$= (s^{-1}e)(ss^{-1})(se)$
$= (s^{-1}e)(ss^{-1}s)e$
$= (s^{-1}e)se$
$= (s^{-1}e)es$
$= (s^{-1}ee)s$
$= (s^{-1}e^2)s$
$= s^{-1}es$

□

(iv) Se e é um elemento idempotente do semigrupo, $e^{-1} = e$ pela unicidade do elemento inverso.

(v) Para cada elemento idempotente e do semigrupo e, para cada $s \in S$, existe um elemento idempotente e_1 do semigrupo tal que $es = se_1$.

Demonstração.

1. $s \in S$
2. $e \in S$, $e^2 = ee = e$
3. $e_1 = s^{-1}es$
4. $e_1^2 = e_1e_1 = e_1$
5. $se_1 = s(s^{-1}es)$
   $= (ss^{-1})es$
   $= e(ss^{-1})s$
   $= e(ss^{-1}s)$
   $= es$

□

(vi) Para cada elemento idempotente e do semigrupo e, para cada $s \in S$, existe um elemento idempotente e_2 do semigrupo tal que $se = e_2s$.

Demonstração.

1. $s \in S$
2. $e \in S$, $e^2 = ee = e$
3. $e_2 = ses^{-1}$
4. $e_2^2 = e_2e_2 = e_2$
5. $e_2s = (ses^{-1})s$
   $= se(s^{-1}s)$
   $= s(s^{-1}s)e$
   $= (ss^{-1}s)e$
   $= se$

□

(vii) Para cada elemento $a \in S$,

$$aS = \{as : s \in S\} = aa^{-1}S$$

e aa^{-1} é o único elemento idempotente gerador do conjunto aS.

Demonstração.

1. $a \in S$

2. $aS = (aa^{-1}a)S$
   $= (aa^{-1})aS \subset aa^{-1}S \subset aS$
   $= aa^{-1}S$
3. $e \in S$, $e^2 = ee = e$
4. $aS = eS$
5. $aa^{-1}S = eS$
6. $(\exists\, s_1 \in S)(aa^{-1}s_1 = es_2)$
7. $(\exists\, s \in S)(aa^{-1} = es)$
8. $(\exists\, t \in S)(e = aa^{-1}t)$
9. $eaa^{-1} = (aa^{-1}t)aa^{-1}$
10. $aa^{-1}e = aa^{-1}taa^{-1} = aa^{-1}$
11. $aa^{-1}e = ese = e$
12. $eaa^{-1} = aa^{-1}e = aa^{-1} = e$

□

(viii) Para cada elemento $a \in S$,

$$Sa = \{sa : s \in S\} = Sa^{-1}a.$$

(ix) Para elementos idempotentes e_1 e e_2 do semigrupo, tem-se:

$$e_1S \cap e_2S = e_1e_2S$$

$$Se_1 \cap Se_2 = Se_1e_2$$

Demonstração.

1. $a \in e_1S \cap e_2S$
2. $(\exists\, s_1 \in S)(\exists\, s_2 \in S)(a = e_1s_1 = e_2s_2)$

□

Propriedade 5.12.

Grupos são semigrupos inversos, cujo único elemento idempotente é o elemento neutro do grupo.

Demonstração.

1. e é o único elemento idempotente do semigrupo
2. $s \in S$
3. ss^{-1} e $s^{-1}s$ são elementos idempotentes do semigrupo
4. $ss^{-1} = s^{-1}s = e$ pela unicidade do elemento idempotente

□

5.1 Relação de ordem

A relação de ordem parcial natural $R_{\leq}$ em um semigrupo inverso $(S,\cdot)$ é definida como

$$R_{\leq} = \{(s,t) \in S \times S : \exists\, e \in E(S) : s = te\}.$$

(i) $R_{\leq}$ é reflexiva:

$(s,s) \in R_{\leq}$

$s = ss^{-1}s = (ss^{-1})s$ e $ss^{-1} \in E(S)$.

(ii) $R_{\leq}$ é transitiva:

$(s,t) \in R_{\leq} : \exists\, e_1 \in S : s = te_1$

$(t,u) \in R_{\leq} : \exists\, e_2 \in S : t = e_2u = ue_3$

$s = te_1 = e_2ue_1 = e_1e_3u$ pela comutatividade parcial e

(iii) $R_{\leq}$ é antisimétrica:

$(s,t) \in R_{\leq} : \exists\, e_1 \in E(S) : s = te_1$

$(t,s) \in R_{\leq} : \exists\, e_2 \in E(S) : t = se_2$

$s = te_1 = se_2e_1$.

Teorema 5.13.

Seja $R_{\leq}$ a relação de ordem parcial natural em um semigrupo inverso $(S,\cdot)$. Então, são equivalentes as afirmações:

(i) $(s,t) \in R_{\leq}$

(ii) $\exists\, e \in E(S) : s = et$

(iii) $(s^{-1},t^{-1}) \in R_{\leq}$

(iv) $s = ss^{-1}t$

(v) $s = ts^{-1}s$

Demonstração.

(i) $\Rightarrow$ (ii) é verificada pela comutatividade parcial

(ii) $\Rightarrow$ (iii)
1. $(\exists\, e \in E(S))(s = et)$
2. $s^{-1} = (et)^{-1} = t^{-1}e^{-1} = t^{-1}e$
3. $(s^{-1}, t^{-1}) \in R_{\leq}$

(iii) $\Rightarrow$ (iv)
1. $(s^{-1}, t^{-1}) \in R_{\leq}$
2. $(\exists\, e \in E(S))(s^{-1} = t^{-1}e)$
3. $s = et$
4. $es = e(et) = e^2t = et = s$
5. $ess^{-1} = ss^{-1}$
6. $s = et$
7. $s = ss^{-1}t$

(iv) $\Rightarrow$ (v)
1. $s = ss^{-1}t$
2. $s = te$
3. $se = (te)e = te^2 = te = s$
4. $s^{-1}se = s^{-1}s$
5. $s = ts^{-1}s$

(v) $\Rightarrow$ (i)
1. $(s,t) \in R_{\leq}$
2. $(t,s) \in R_{\leq}$
3. $s = ts^{-1}s$
4. $t = st^{-1}t$
5. $s = st^{-1}ts^{-1}s = s(t^{-1}t)(s^{-1}s) = s(s^{-1}s)(t^{-1}t) = st^{-1}t = t.$

□

Propriedades 5.14.

Seja $(S, \cdot)$ um semigrupo inverso. Então:

(i) Se $e_1 \in E(S)$ e $e_2 \in E(S)$, $(e_1, e_2) \in R_{\leq} \Leftrightarrow e_1 = e_1e_2 = e_2e_1$.

Demonstração.

1. $(e_1, e_2) \in R_{\leq}$
2. $(\exists\, t \in E(S))(e_1 = e_2 t)$
3. $e_2 e_1 = e_2(e_2 t) = e_2 t = e_1$
4. $e_1 e_2 = e_2 e_1 = e_1$

□

(ii) Se $(s,t) \in R_{\leq}$ e $(u,v) \in R_{\leq}$, então $(su, tv) \in R_{\leq}$.

(iii) Se $(s,t) \in R_{\leq}$, então $(s^{-1}s, t^{-1}t) \in R_{\leq}$ e $(ss^{-1}, tt^{-1}) \in R_{\leq}$.

Definição 5.15.

A relação de compatibilidade à esquerda R_l em um semigrupo inverso $(S, \cdot)$ é definida como

$$R_l = \{(s,t) \in S \times S : st^{-1} \in E(S)\}.$$

A relação de compatibilidade à direita R_r em um semigrupo inverso $(S, \cdot)$ é definida como

$$R_r = \{(s,t) \in S \times S : s^{-1}t \in E(S)\}.$$

A relação de compatibilidade em um semigrupo inverso $(S, \cdot)$ é definida como a intersecção das relações de compatibilidade à esquerda e à direita.

Teorema 5.16 (Teorema da representação de Cayley de semigrupos inversos)**.**

Seja $(S, \cdot)$ um semigrupo inverso em relação à operação binária interna $\cdot$ do semigrupo. Então, existe um conjunto não vazio X e um monomorfismo de semigrupo F, cujo domínio de definição é igual a S e cujo conjunto de valores é um subconjunto do monoide inverso $(I(X), \circ)$ constituído pela totalidade das funções f injetoras, cujo domínio de definição é um subconjunto não vazio de X e cujo conjunto de valores está contido em X tal que

$$(\forall\, x \in S)(\forall\, y \in S)(x \leq y \Rightarrow F(x) \subset F(y))$$

Demonstração.

Para cada elemento a de S, seja a função f_a, cujo domínio de definição é o subconjunto $a^{-1}aS = \{a^{-1}as : s \in S\}$ e cujo conjunto de valores é o subconjunto $aa^{-1}S = \{aa^{-1}s : s \in S\}$, definida por: para $x \in a^{-1}aS$,

$$f_a(x) = ax.$$

Como $x \in a^{-1}aS$, existe $s \in S$ tal que $x = a^{-1}as$ e, então,

$$f_a(x) = a(a^{-1}as) = aa^{-1}(as) \in aa^{-1}S.$$

Para cada elemento a de S, a função f_a^{-1}, cujo domínio de definição é o conjunto $(a^{-1})^{-1}a^{-1}S = aa^{-1}S$ e cujo conjunto de valores é o subconjunto $a^{-1}aS$, dada por: para $x \in aa^{-1}S$,

$$f_{a^{-1}}(x) = a^{-1}x,$$

é tal que:

(i) $f_{a^{-1}} \circ f_a$ é a restrição da função identidade ao conjunto $a^{-1}aS$.

De fato, se $x \in a^{-1}aS$, existe $s \in S$ tal que $x = a^{-1}as$ e

$$\begin{aligned}(f_{a^{-1}} \circ f_a)(x) &= f_{a^{-1}}\left[f_a(x)\right] \\ &= f_{a^{-1}}(ax) \\ &= a^{-1}(ax) \\ &= a^{-1}aa^{-1}as \\ &= a^{-1}(aa^{-1}a)s \\ &= a^{-1}as \\ &= x.\end{aligned}$$

(ii) Analogamente, $f_a \circ f_{a^{-1}}$ é a restrição da função identidade ao conjunto $aa^{-1}S$.

Assim, para cada elemento a de S, f_a é uma função injetora e é portanto um elemento do monoide inverso $(I(S), \circ)$ constituído pela totalidade das funções f injetoras cujo domínio de definição é um subconjunto não vazio de S e cujo conjunto de valores está contido em S.

Seja a função F, cujo domínio de definição é S e cujo conjunto de valores está contido em $I(S)$, dada por: para cada $a \in S$,

$$F(a) = f_a.$$

O objetivo é mostrar que F é um homomorfismo de semigrupo do semigrupo S no semigrupo $(I(S), \circ)$, ou seja,

$$(\forall\, a \in S)(\forall\, b \in S)(F(a) \circ F(b) = F(ab)) \text{ ou } f_a \circ f_b = f_{ab}.$$

O domínio de definição de f_{ab} é o conjunto $(ab)^{-1}(ab)S = b^{-1}a^{-1}abS$, que é igual a intersecção do domínio de definição $a^{-1}aS$ de f_a com o conjunto de valores $bb^{-1}S$ de f_b, isto é,

$$(a^{-1}aS) \cap (bb^{-1}S) = (ab)^{-1}(ab)S$$

e esta intersecção é o domínio de definição de f_{ab} e, além disso, para $x \in (ab)^{-1}(ab)S$,

$$\begin{aligned} f_{ab}(x) &= (ab)x \\ &= a(bx) \\ &= f_a(bx) \\ &= (f_a \circ f_b)(x) \end{aligned}$$

ou, em outros termos,

$$f_{ab} = f_a \circ f_b \text{ ou } F(ab) = F(a) \circ F(b),$$

o que demonstra que F é um homomorfismo de semigrupo do semigrupo S no semigrupo $(I(S), \circ)$. Resta mostrar que, se a e b são elementos de S, com $a \leq b$, então $F(a) \subset F(b)$, ou seja, $f_a \subset f_b$.

Se a e b são elementos de S, com $a \leq b$, então $a^{-1}a \leq b^{-1}b$ e $a^{-1}aS \subset b^{-1}bS$.

Para $x \in a^{-1}aS$, domínio de definição de f_a, segue que $x \in b^{-1}bS$, domínio de definição de f_b, e que existe $s \in S$ tal que, se $x = a^{-1}as$,

$$\begin{aligned} f_b(x) &= bx \\ &= b(a^{-1}as) \\ &= b(a^{-1}aa^{-1}as) \\ &= b(a^{-1}a(a^{-1}as)) \\ &= b(a^{-1}ax) \\ &= (ba^{-1}a)x \\ &= ax, \end{aligned}$$

lembrando que, se $a \leq b$, então $a = ba^{-1}a = f_a(x)$, o que comprova que $f_a \subset f_b$.

Se $f_a \subset f_b$ para elementos a e b de S, então, por definição,

$$a^{-1}aS \subset b^{-1}bS$$

$$a^{-1} \in a^{-1}aS,$$

visto que $a^{-1} = a^{-1}aa^{-1}$; por hipótese,

$$f_b(a^{-1}) = f_a(a^{-1}) \text{ ou}$$

$$ba^{-1} = aa^{-1}$$

$$ba^{-1}a = aa^{-1}a = a,$$

o que significa que $a \leq b$, lembrando que $a^{-1}a$ é um elemento idempotente de S.

O homomorfismo de semigrupo F do semigrupo $(S, \cdot)$ no semigrupo $(I(X), \circ)$ é, então, um monomorfismo de semigrupo, pois F é uma função injetora: para a e b elementos de S, se $F(a) = f_a = F(b) = f_b$, então, de $f_a \subset f_b$, segue que $a \leq b$ e, de $f_b \subset f_a$, vem que $b \leq a$. □

5.2 Método das divisões sucessivas

O método das divisões sucessivas de Euclides para o cálculo do máximo divisor comum de dois números naturais baseado na propriedade de que, dados dois números naturais $a, b \in \mathbb{N} = \{1, 2, \ldots\}$,

$$\text{mdc}(a, b) = \text{mdc}(q, r),$$

em que, q e r são respectivamente o quociente e o resto da divisão euclidiana de a por b, isto é, $a = bq + r$ e $r \in \{0, 1, \ldots, b-1\}$ exprimde o máximo divisor comum de a e b como

$$d = ra + sb,$$

com r, $s \in \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. Este método é utilizado para o cálculo do inverso multiplicativo dos elementos de $(U(\mathbb{Z}_m), \cdot)$, grupo multiplicativo dos elementos inversíveis do monoide multiplicativo $(\mathbb{Z}_m, \cdot)$.

O seguinte exemplo ilustra o método citado:

Exemplo 5.17.

Para o cálculo de 17^{-1}, inverso multiplicativo de 17 em $U(\mathbb{Z}_{100})$, o método das divisões sucessivas de Euclides é o seguinte:

100	17
$\underbrace{15}_{resto}$	$\underbrace{5}_{quociente}$

17	15
$\underbrace{2}_{resto}$	$\underbrace{1}_{quociente}$

15	2
$\underbrace{1}_{resto}$	$\underbrace{7}_{quociente}$

e o número 1, que é o máximo divisor comum entre 17 e 100, é expresso como:

$$\begin{aligned} 1 &= 15 - 7.2 \\ &= 15 - 7.(17 - 15) \\ &= 8.15 - 7.17 \\ &= 8(100 - 5.17) - 7.17 \\ &= 8.100 - 47.17, \end{aligned}$$

o que mostra que

$$17.(-47) \equiv 1 \mod 100$$

e que

$$17.(53) \equiv 1 \mod 100.$$

Portanto, o elemento inverso 17^{-1} de 17 no monoide multiplicativo $(\mathbb{Z}_{100}, \cdot)$ é igual a 53. De fato, $17.(53) = 901 = 9.(100) + 1$.

Para o cálculo do elemento inverso 17^{-1} de 17 no monoide multiplicativo $(\mathbb{Z}_{1000}, \cdot)$, o método das divisões sucessivas de Euclides é o seguinte:

1000	17
$\underbrace{14}_{resto}$	$\underbrace{58}_{quociente}$

17	14
$\underbrace{3}_{resto}$	$\underbrace{1}_{quociente}$

14	3
$\underbrace{2}_{resto}$	$\underbrace{4}_{quociente}$

3	2
$\underbrace{1}_{resto}$	$\underbrace{1}_{quociente}$

e o número 1, que é o máximo divisor comum entre 17 e 1000, é expresso como:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (14 - 4.3) \\ &= 5.3 - 14 \\ &= 5(17 - 14) - 14 \\ &= 5.17 - 6.14 \\ &= 5.17 - 6(1000 - 58.17) \\ &= -6.1000 + 353.17, \end{aligned}$$

o que mostra que

$$17.(353) \equiv 1 \mod 1000.$$

Portanto, o elemento inverso 17^{-1} de 17 no monoide multiplicativo $(\mathbb{Z}_{1000}, \cdot)$ é igual a 353. De fato, $17.(353) = 6001 = 6.(1000) + 1$.

REFERÊNCIAS

HOWIE, J. M. **Fundamentals of semigroups theory**. Clarendon Press, 2003. Nenhuma citação no texto.

HUNGERFORD, T. W. **Algebra**. Springer-Verlag, 1974. Nenhuma citação no texto.

LAWSON, M. V. **Inverse semigroups: the theroy of partial symmetries**. World Scientific, 1998. Nenhuma citação no texto.

LIDL, R.; PILZ, G. **Applied abstract algebra**. Springer-Verlag, 1984. Nenhuma citação no texto.

ROTMAN, J. J. **The theory of groups: an introduction**. Allyn and Bacon, Inc, 1965. Nenhuma citação no texto.


ICMC
USP
SÃO CARLOS