Universidade Federal de Uberlândia
Curso de Licenciatura em Matemática

Estruturas Algébricas

Cícero Fernandes de Carvalho

2016

Professor, Cícero Fernandes de Carvalho
Estruturas Algébricas / Uberlândia, MG : UFU, 2015.

115 p.:il.

Licenciatura em Matemática.

1. Estruturas Algébricas

PRESIDENTE DA REPÚBLICA
Dilma Vana Rousseff

MINISTRO DA EDUCAÇÃO
Aloizio Mercadante

UNIVERSIDADE ABERTA DO BRASIL
DIRETORIA DE EDUCAÇÃO A DISTÂNCIA/CAPES
Jean Marc Georges Mutzig

UNIVERSIDADE FEDERAL DE UBERLÂNDIA - UFU
REITOR
Elmiro Santos Resende

VICE-REITOR
Eduardo Nunes Guimarães

CENTRO DE EDUCAÇÃO A DISTÂNCIA
DIRETORA E REPRESENTANTE UAB/UFU
Maria Teresa Menezes Freitas

SUPLENTE UAB/UFU
José Benedito de Almeida Júnior

FACULDADE DE MÁTEMÁTICA – FAMAT – UFU
DIRETOR
Luís Antonio Benedetti

COORDENADOR DO CURSO DE LICENCIATURA EM MATEMÁTICA – PARFOR
Rogério de Melo Costa Pinto

COORDENAÇÃO DE TUTORIA
Janser Moura Pereira

EQUIPE DO CENTRO DE EDUCAÇÃO A DISTÂNCIA DA UFU - CEaD/UFU

ASSESSORA DA DIRETORIA
Sarah Mendonça de Araújo

EQUIPE MULTIDISCIPLINAR
Alberto Dumont Alves Oliveira
Dirceu Nogueira de Sales Duarte Júnior
Gustavo Bruno do Vale
João Victor da Silva Alves
Otaviano Ferreira Guimarães

SETOR DE FORMAÇÃO CONTINUADA
Marisa Pinheiro Mourão

REVISORA
Paula Godoi Arbex

EQUIPE DE ESTAGIÁRIOS DO CEAD
E DO CURSO DE MATEMÁTICA

SUMÁRIO

INFORMAÇÕES

Prezado(a) aluno(a),

Ao longo deste guia impresso você encontrará alguns "ícones" que lhe ajudará a identificar as atividades.

Fique atento ao significado de cada um deles, isso facilitará a sua leitura e seus estudos.

Destacamos alguns termos no texto do Guia cujos sentidos serão importantes para sua compreensão. Para permitir sua iniciativa e pesquisa não criamos um glossário, mas se houver dificuldade interaja no *Fórum de Dúvidas*.

MÓDULO 1

Relações de equivalência e introdução a grupos

RELAÇÕES DE EQUIVALÊNCIA E INTRODUÇÃO A GRUPOS

1.1 Relações de equivalência

Uma construção bastante conhecida que se pode fazer a partir de dois conjuntos A e B é o ***produto cartesiano*** $A\times B$, que consiste de todos os pares ordenados (a,b) onde o primeiro elemento pertence a A e o segundo elemento pertence a B.

Exemplo 1.1.1 Sejam $A=\{1,2,3,4\}$ e $B=\{5,6\}$, temos que:

$A\times B=\{(1,5),(1,6),(2,5),(2,6),(3,5),(3,6),(4,5),(4,6)\}$,

$B\times A=\{(5,1),(5,2),(5,3),(5,4),(6,1),(6,2),(6,3),(6,4)\}$, e ainda

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

Definição 1.1.2 Uma ***relação*** de A em B é simplesmente um subconjunto não vazio do produto cartesiano $A\times B$.

Exemplos 1.1.3

i. O conjunto $R=\{(1,5),(2,6),(3,5),(4,5)\}\subset A\times B$ é uma relação de A em B.

ii. O conjunto $S=\{(5,4),(6,3),(6,4)\}\subset B\times A$ é uma relação de B em A (mas não de A em B pois $S\not\subset A\times B$).

iii. O conjunto $T=\{(5,5),(6,6)\}$ é uma relação de B em B.

Quando temos uma relação R de A em A dizemos simplesmente que R *é uma relação sobre* A. Assim é correto dizer que no exemplo 1.1.3 (iii) o conjunto T é uma relação sobre B.

I - ATIVIDADES – GUIA IMPRESSO

No espaço abaixo escreva uma relação de A em diferente do exemplo acima. Escreva também uma relação de B em A, e ainda um subconjunto de $A \times A$ que **não** seja uma relação sobre A.

Relações com propriedades especiais aparecem em toda a matemática, e de maneira tão frequente que muitas vezes nem percebemos. Por exemplo, a definição mais abrangente de função entre conjuntos é baseada no conceito de relação.

Definição 1.1.4 Uma ***função*** de um conjunto A num conjunto B é uma relação R de A em B que tem a seguinte propriedade: para cada elemento a em A existe exatamente um par ordenado em R que tem a como primeira entrada.

Exemplos 1.1.5

Sejam $A = \{1,2,3,4\}$ e $B = \{5,6\}$, temos que é uma função de A em B, pois é claramente uma relação de A em B e para cada elemento $a \in A$ existe um único elemento $b \in B$ tal que $(a,b) \in R$.

Quando os conjuntos envolvidos são infinitos não é possível listar os pares ordenados da função, e nesse caso temos que apelar para outras formas de indicar a escolha dos pares ordenados selecionados. Por exemplo, se $\Re$ é o conjunto dos números reais, então um exemplo de função sobre $\Re$ é $S = \{(a,b) \in \Re \times \Re \mid b = a^2\}$. Vemos que para cada

elemento $a \in \Re$ existe um único par ordenado em S que tem a como primeira entrada, a saber, o par (a, a^2). Já o conjunto $T = \{(a,b) \in \Re \times \Re \mid a = b^2\}$ apesar de ser uma relação sobre $\Re$ não é uma função sobre $\Re$ pois, por exemplo, $(4,2) \in T$ e $(4,-2) \in T$

Da mesma forma $U = \{(a,b) \in \Re \times \Re \mid a = b^3, a \neq 0\}$ não é uma função sobre $\Re$ pois não há em U nenhum par ordenado que tenha 0 como primeira entrada.

II- ATIVIDADES – GUIA IMPRESSO

Em cada item abaixo, verifique se T é uma função sobre $\Re$ e justifique sua resposta.

i) $T = \{(a,b) \in \Re \times \Re \mid b = a + 3\}$;

ii) $T = \{(a,b) \in \Re \times \Re \mid a = b^3, a \neq 0\} \cup \{(0,9)\}$;

iii) $T = \{(a,b) \in \Re \times \Re \mid a = 3b - 2\}$;

iv) $T = \{(a,b) \in \Re \times \Re \mid b = 5\}$;

v) $T = \{(a,b) \in \Re \times \Re \mid a > 0, b = 1/a\} \cup \{(a,b) \in \Re \times \Re \mid a < 0, b = -3/a\} \cup \{(0,0)\}$.

Observe que na definição de função apresentada acima não entra a palavra “regra” ou “lei de formação”. Essas expressões são por vezes utillizadas no ensino do conceito de função em cursos de nível anterior ao universitário, ou em cursos univesitários que não sejam o de matemática. Para matemáticos a definição acima é fundamental, pois em diversos lugares aparecem funções sobre $\Re$ que não têm “lei de formação”. Um exemplo é a famosa função de Weierstrass, um exemplo de função que é contínua mas não possui derivada em nenhum ponto (!). Ela é construída como um limite de funções. Prova-se que tal limite existe e define uma função, mas não é possível escrever uma “lei de formação” como as das funções nos exemplos e atividades acima. Se quiser saber mais sobre essa função, faça um procura na internet sobre “função de Weierstrass” ou consulte o primeiro artigo da revista da FAMAT-UFU, número 13, disponível em: *http://www.portal.famat.ufu.br/node/262* .

Neste curso vamos utilizar um tipo especial de relação sobre um conjunto A chamada de relação de equivalência sobre A .

Definição 1.1.6 Seja A um conjunto não vazio. Dizemos que uma relação $R \subset A \times A$ é uma relação de equivalência sobre A se R satisfaz as seguintes condições:

i) $(a,a) \in R$ para todo $a \in A$;

ii) se $(a,b) \in R$ então $(b,a) \in R$; e

iii) se $(a,b) \in R$ e $(b,c) \in R$ então $(a,c) \in R$.

Assim uma relação de equivalência é uma relação reflexiva (porque tem a propriedade (i)), simétrica (porque tem a propriedade (ii)) e transitiva (porque tem a propriedade (iii)).

Exemplos 1.1.7 . Seja

a) Temos que $R = \{(1,1),(2,2),(3,3)\} \subset A \times A$ é uma relação de equivalência sobre A pois satisfaz (i), (ii) e (iii).

b) Temos que $R = \{(1,1),(2,2),(3,3),(1,2),(2,1)\} \subset A \times A$ é uma relação de equivalência sobre A pois satisfaz (i), (ii) e (iii).

c) Temos que $R = \{(1,1),(2,2),(1,2),(2,1)\} \subset A \times A$ não é uma relação de equivalência sobre A pois não satisfaz a condição (i).

d) Temos que $R = \{(1,1),(2,2),(1,2),(2,1),(3,1),(1,3)\} \subset A \times A$ não é uma relação de equivalência sobre A pois não satisfaz a condição (i).

e) Temos que $R = \{(1,1),(2,2),(3,3),(1,2)\} \subset A \times A$ não é uma relação de equivalência sobre A pois não satisfaz a condição (ii);

f) Temos que $R = \{(2,2),(3,3),(1,2),(2,1)\} \subset A \times A$ não é uma relação de equivalência sobre A pois não satisfaz a condição (iii) (já que $(1,2) \in R, (2,1) \in R$ mas $(1,1) \notin R$) - é claro que R também não satisfaz a condição (i).

g) Seja $\Re$ o conjunto dos números reais e considere a relação sobre $\Re$ definida por $R = \{(a,b) \in \Re \times \Re \mid b-a$ é um número inteiro . Vejamos que R é uma relação de equivalência sobre R . Iniciamos observando que para todo $a \in \Re$ vale que $(a,a) \in R$ pois $a-a$ é o inteiro 0, e portanto R satisfaz a condição (i). Por outro lado, se $(a,b) \in R$ então $b-a$ é um inteiro n logo $a-b$ é o inteiro $-n$ e portanto $(b,a) \in R$

Finalmente temos que se $(a,b) \in R$ e $(b,c) \in R$ então $b-a=n$ e $c-b=m$ com n e m inteiros, logo $c-a$ é um inteiro (pois $c-a=(c-b)+(b-a)=m+n$) e portanto $(a,c) \in R$. Isso completa a prova de que R é uma relação de equivalência sobre $\Re$. Entre os pares ordenados que estão em R temos $(0,0),(0,4),(3,0),(1,2),(3,1),$ $(5,3),(0.5,3.5),(\pi-2,\pi),(\sqrt{2}+3,\sqrt{2})$ e $(17/3,5/3)$.

h) Seja Z o conjunto dos números inteiros e considere a relação sobre Z definida por $R=\{(a,b) \in Z \times Z \mid b-a$ é um múltiplo inteiro de 5 $\}$ (onde $b-a$ é um múltiplo inteiro de 5 significa que $b-a=m.5$, com m um inteiro). Vejamos que R é uma relação de equivalência sobre Z. Para começar observe que se $a \in Z$ vale que $(a,a) \in R$ pois $a-a=0$ e $0=0.5$ é múltiplo inteiro de 5, assim R satisfaz a condição (i). Por outro lado, se $(a,b) \in R$ então $b-a$ é um múltiplo inteiro de 5, digamos $b-a=m.5$, com m um inteiro, logo $a-b=(-m).5$ e portanto $(b,a) \in R$ .Por último, se $(a,b) \in R$ e $(b,c) \in R$ então temos $b-a=n.5$ e $c-b=m.5$, com n e m números inteiros, logo $c-a=(c-b)+(b-a)=(m+n)5$ donde $(a,c) \in R.$ Isso prova que R de fato é uma relação de equivalência sobre Z. Denotando por $5Z$ o conjunto dos múltiplos inteiros de 5 então podemos reescrever R como $R=\{(a,b) \in Z \times Z \mid b-a \in 5Z\}$. Observe que o conjunto $5Z=\{...,-15,-10,-5,0,5,10,15,...\}$ coincide com o conjunto dos múltiplos inteiros de –5 de modo que o conjunto R não muda se o definimos como $R=\{(a,b) \in Z \times Z \mid b-a$ é um múltiplo inteiro de –5 $\}$. Entre os pares ordenados que estão em R temos $(0,5),(5,0),(1,6),(7,2),(3,8),(9,4),(1,-4),(-3,2),(113,28)$ etc.

Um conceito associado ao de relação de equivalência que é fundamental é o de classe de equivalência.

Definição 1.1.8. Seja A um conjunto e R uma relação de equivalência sobre A. Para cada elemento $a \in A$ definimos a classe de equivalência de a (notação: $\overline{a}$) como sendo o conjunto dos elementos de A que aparecem como entrada em pares ordenados de R que têm a como a outra entrada. Assim a classe de equivalência de $a \in A$ é o subconjunto de A definido por $\overline{a} = \{b \in A \mid (a,b) \in R\}$.

Depois de ler na definição acima que a classe de equivalência de $a \in A$ é "o conjunto dos elementos de A que aparecem como entrada em pares ordenados de R que têm a como a outra entrada" pode ser que você tenha esperado que, em símbolos, tivéssemos $\overline{a} = \{b \in A \mid (a,b) \in R$ ou $(b,a) \in R\}$. Isso não está errado, no entanto observe que como R é uma relação de equivalência se temos $(b,a) \in R$ então também temos $(a,b) \in R$ por isso para encontrar $\overline{a}$ basta procurar pelos elementos $b \in A$ tais que $(a,b) \in R$.

Em matemática, quando aparece algum conjunto numa definição devemos sempre pensar se tal conjunto pode ser ou não o conjunto vazio. Acima, vimos que a classe de equivalência de um elemento $a \in A$ é um determinado subconjunto $\overline{a} \subset A$. Será que esse conjunto pode ser vazio? Vamos parar e pensar ..... huummm..... Não! Não pode ser vazio pois como R é uma relação de equivalência sobre A temos que ter $(a,a) \in R$ e logo a é um dos elementos de A que aparecem como entrada em pares ordenados de R que têm a como a outra entrada. Assim $a \in \overline{a}$ e portanto $\overline{a}$ não é o conjunto vazio.

Destacamos o resultado observado acima no seguinte lema.

Lema 1.1.9. Seja A um conjunto e R uma relação de equivalência sobre A. Para cada elemento $a \in A$ temos que $a \in \overline{a}$.

Exemplos 1.1.10. Nos exemplos 1.1.7 temos que os itens (a), (b), (g) e (h) são exemplos de relações de equivalência. Vamos ver algumas classes de equivalências que surgem em cada caso.

No exemplo 1.1.7 (a) as classes de equivalência são as mais simples possíveis, a saber $\overline{1} = \{1\}$, $\overline{2} = \{2\}$ e $\overline{3} = \{3\}$. Observe que $A = \overline{1} \cup \overline{2} \cup \overline{3}$.

Vamos determinar $\overline{1}$ no exemplo 1.1.7 (b). Temos que os elementos de A que aparecem como entrada nos pares ordenados de R que têm 1 como a outra entrada são 1 (que aparece no par $(1,1)$) e 2 (que aparece nos pares $(1,2)$ e $(2,1)$), logo $\overline{1} = \{1,2\}$. Para determinar $\overline{2}$ observamos que os elementos de A que aparecem nos pares ordenados de R que têm 2 como a outra entrada são 2 (que aparece no par $(2,2)$) e 1 (que aparece nos pares $(1,2)$ e $(2,1)$) logo $\overline{2} = \{1,2\}$. De maneira análoga é fácil ver que $\overline{3} = \{3\}$. Assim temos que $\overline{1} = \overline{2}$ e $\overline{1} \cap \overline{3} = \varphi$, onde φ é o conjunto vazio; mais ainda vale que $A = \overline{1} \cup \overline{3}$ (ou seja, A é igual à união das distintas classes de equivalência, algo que aconteceu acima também).

No exemplo 1.1.7 (g) vamos começar investigando que conjunto é a classe do zero. Por definição temos que $\overline{0}$ é composto pelos números reais b tais que $(0,b) \in R$, e da definição de R nesse exemplo temos que $(0,b) \in R$ se e só se $b-0$ é um número inteiro. Assim a classe de zero é formada exatamente pelo conjunto dos números inteiros

Z, ou seja, $\overline{0} = Z \subset \Re$. E a classe do 1? Ela é composta pelos números reais b tais que $(1,b) \in R$, ou seja, $b-1$ é um inteiro. Mas se $b-1$ é um inteiro então b é um inteiro e se b é um inteiro então $b-1$ é um inteiro. Assim o conjunto dos números reais b tais que $b-1$ é um inteiro é exatamente o conjunto dos inteiros, e portanto as classes do 1 e do 0 coincidem. Pensando bem, se n é um inteiro então a classe de n é composta dos números reais b tais que $b-n$ é um inteiro, e raciocinando como acima vemos que isso acontece, e só acontece, quando b é inteiro. Assim, para qualquer inteiro n temos $\overline{n} = \overline{0} = Z$. Então vamos agora pensar na classe de um número real que não seja inteiro, por exemplo, $1/2$. A classe de $1/2$ é formada pelos números reais b tais que $b-1/2$ é um inteiro, e temos $b-1/2 = n$ se e só se $b = n+1/2$, onde n é um inteiro. Assim $1/2$, $3/2$ e $5/2$ estão em $\overline{1/2}$, bem como $-1/2$ e $-3/2$, pois $\overline{1/2} = \{n+1/2 \mid n \in Z\}$. Observe que $\overline{1/2} \cap \overline{0} = \varphi$.

No exemplo 1.1.7 (h) vamos começar novamente investigando que conjunto é a classe do zero. Por definição temos que $\overline{0}$ é composto pelos números inteiros b tais que $(0,b) \in R$, e da definição de R nesse exemplo temos que $(0,b) \in R$ se e só se $b-0$ é um múltiplo inteiro de 5. Assim a classe de 0 é o conjunto $\overline{0} = \{\ldots -15,-10,-5,0,5,10,15,\ldots\} = \{m.5 \mid m \in Z\}$. Já a classe de 1 é formada pelos inteiros b tais que se $b-1$ é um múltiplo inteiro de 5, ou seja $b-1 = m.5$ para algum m inteiro, ou seja, $b = m.5+1$ para algum m inteiro. Temos, portanto que

$\overline{1} = \{...-14,-9,-4,1,6,11,16,...\} = \{m.5+1 \mid m \in Z\}$.

Da mesma forma temos que $\overline{2} = \{...-13,-8,-3,2,7,12,17,...\} = \{m.5+2 \mid m \in Z\}$, $\overline{3} = \{...-12,-7,-2,3,8,13,18,...\} = \{m.5+3 \mid m \in Z\}$ e $\overline{4} = \{...-11,-6,-1,4,9,14,19,...\} = \{m.5+4 \mid m \in Z\}$. Observe que temos $Z = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}$: de fato, dado um número inteiro n, se fazemos a divisão usual dele por 5 vamos escrever $n = m.5+r$ onde $r = \{0,1,2,3,4\}$ e portanto n está em uma das classes $\overline{0}, \overline{1}, \overline{2}, \overline{3}$ ou $\overline{4}$. Observe também que quaisquer duas dessas classes **não** têm elementos em comum (nesse caso dizemos que a união $\overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}$ é uma *união disjunta* porque a interseção de quaisquer dois conjuntos que aparecem nessa união é o conjunto vazio).

Nos exemplos acima pudemos verificar, como esperávamos, que se R é uma relação de equivalência sobre A e $a \in A$ então $a \in \overline{a}$, mas obervamos também que, ao menos nesses exemplos, duas classes de equivalência ou coincidem (como $\overline{1}$ e $\overline{2}$, no exemplo (b), ou $\overline{0}$ e $\overline{1}$, no exemplo (c)) ou são disjuntas (ou seja, sua interseção é o conjunto vazio). Além disso, em vários exemplos foi possível verificar que o conjunto A pode ser escrito como a união de classes de equivalência. Esse é um fato geral, que não é difícil de ser provado.

Proposição 1.1.11 Seja R uma relação de equivalência sobre um conjunto A. Então vale que :

$$A = \bigcup_{a \in A} \overline{a}$$

Prova. Para cada $a \in A$ temos, pela definição de classe de equivalência, que $\overline{a} \subset A$, logo $\bigcup_{a \in A} \overline{a} \subset A$. Por outro para cada $a \in A$ temos $a \in \overline{a}$ logo $A = \bigcup_{a \in A} \{a\} \subset \bigcup_{a \in A} \overline{a}$, o que completa a prova. □

Utilizamos o símbolo □ para indicar o final de uma demonstração (os bons e velhos c.q.d. ou q.e.d. caíram de moda!). Assim fica claro a separação entre o texto de uma prova e o texto expositivo. Tal prática é comum em livros de matemática, sendo também utilizados os símbolos ■ ou ♦ com o mesmo objetivo.

O que fizemos acima é um "método" bastante utilizado de pesquisa, até mesmo em pesquisas de alto nível, que buscam resultados matemáticos ainda desconhecidos. O que se faz é estudar um grande número de exemplos de um mesmo objeto tentando detectar padrões que sejam indicadores de um resultado teórico mais geral. Isso mostra a importância de se fazer exemplos, especialmente em matérias onde os conceitos são "abstratos". E fazer exemplos também é muito importante para a compreensão de tais conceitos. Por isso, sugiro fortemente que em todas as matérias desse e demais cursos de matemática que você fizer, sempre faça ou procure nos livros o maior número de

exemplos que puder quando estiver estudando um conceito novo. Isso te ajudará a entendê-lo e talvez até a antecipar resultados que irá estudar.

No exemplo (b) acima vimos que $\overline{1} = \{1, 2\}$ e depois verificamos que $\overline{1} = \overline{2}$. No exemplo (c) vimos que $\overline{0} = Z$ e que para qualquer inteiro n vale $\overline{n} = \overline{0}$. Isso sugere que se R é uma relação de equivalência sobre um conjunto A e $b \in \overline{a}$ então $\overline{b} = \overline{a}$, e de fato isso é verdade!

Proposição 1.1.12 Seja R uma relação de equivalência sobre um conjunto A e sejam a e b elementos de A. Se $b \in \overline{a}$ (ou equivalentemente, se $(a,b) \in R$) então $\overline{b} = \overline{a}$.

Prova. Como $\overline{b}$ e $\overline{a}$ são conjuntos vamos provar que $\overline{b} = \overline{a}$ provando que $\overline{b} \subset \overline{a}$ e $\overline{a} \subset \overline{b}$. A hipótese é que $b \in \overline{a}$ e sabemos da Definição 1.1.8 que isso é equivalente a $(a,b) \in R$. Por outro lado como R é uma relação de equivalência temos que $(a,b) \in R$ se e só se $(b,a) \in R$; assim podemos usar à vontade, por hipótese, que $b \in \overline{a}$ ou $(a,b) \in R$ ou $(b,a) \in R$.

Para mostrar que $\overline{b} \subset \overline{a}$, seja $c \in \overline{b}$. Então, por definição de classe de equivalência, temos que $(b,c) \in R$. Como, por hipótese, vale $(a,b) \in R$ temos da propridade (iii) da definição de relação de equivalência (Def. 1.1.6) que $(a,c) \in R$, logo novamente pela definição de classe de equivalência temos $c \in \overline{a}$. Isso prova que $\overline{b} \subset \overline{a}$.

Para mostrar que $\overline{a} \subset \overline{b}$, seja $c \in \overline{a}$. Então, por definição de classe de equivalência, temos que $(a,c) \in R$. Por hipótese vale $(b,a) \in R$, e de $(b,a) \in R$ e $(a,c) \in R$ temos (de

novo por (iii) na Def. 1.1.6) que $(b,c) \in R$, logo $c \in \overline{b}$. Isso prova que $\overline{a} \subset \overline{b}$, e portanto $\overline{b} = \overline{a}$. □

Observamos também nos Exemplos 1.1.10 que classes de equivalência podem ser disjuntas, e não encontramos exemplos onde a interseção de duas classes fosse um subconjunto próprio das duas. Por outro lado, dados a e b em A, e $R \subset A \times A$ uma relação de equivalência sobre A, é claro que ou $(a,b) \in R$ ou $(a,b) \notin R$. Se $(a,b) \in R$ o resultado acima mostra que $\overline{b} = \overline{a}$, logo se $(a,b) \notin R$ a análise acima indica que devemos ter as classes $\overline{a}$ e $\overline{b}$ disjuntas, e de fato isso acontece.

Proposição 1.1.13 Seja R uma relação de equivalência sobre um conjunto A e sejam a e b elementos de A. Se $(a,b) \notin R$ (ou equivalentemente, se $b \notin \overline{a}$) então $\overline{b} \cap \overline{a} = \varphi$.

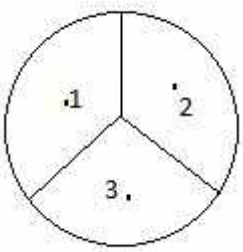
Prova. Faremos uma prova "por absurdo", ou seja, vamos mostrar que não se pode ter ao mesmo tempo a hipótese e o contrário do que queremos mostrar (ou seja, o contrário da tese), assim sempre que tivermos a hipótese teremos que ter a tese. A hipótese é que $(a,b) \notin R$ e a tese é que $\overline{b} \cap \overline{a} = \varphi$, logo o contrário da tese é que $\overline{b} \cap \overline{a} \neq \varphi$. Assim vamos supor juntamente com a hipótese que exista um elemento $c \in \overline{b} \cap \overline{a}$. Como $c \in \overline{b}$ temos pela definição de classe de equivalência que $(b,c) \in R$ e como $c \in \overline{a}$ temos que $(a,c) \in R$. Da propriedade (ii) na definição de relação de equivalência temos que como $(b,c) \in R$ também vale que $(c,b) \in R$. De $(a,c) \in R$ e $(c,b) \in R$ (mais a propriedade (iii) na definição de relação de equivalência) temos que $(a,b) \in R$ em contradição lógica

com a hipótese $(a,b) \notin R$. Isso prova que sempre que tivermos $(a,b) \notin R$ também temos que ter $\overline{b} \cap \overline{a} = \varphi$. □

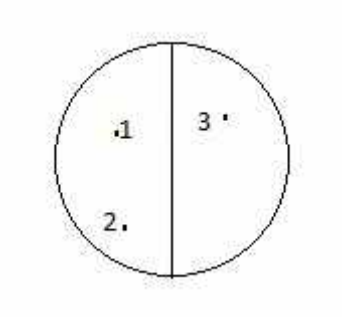
As proposições 1.1.12 e 1.1.13 acima mostram que duas classes de equivalência $\overline{a}$ e $\overline{b}$ ou coincidem ou são disjuntas, coincidindo quando $(a,b) \in R$ e sendo disjuntas quando $(a,b) \notin R$. Por outro lado, na proposição 1.1.11 vimos que A é a união das classes de equivalência de R. Daí concluímos que as distintas classes de equivalência determinadas por R formam uma *partição* de A (quando um conjunto A é a união de uma coleção de conjuntos disjuntos, dizemos que essa coleção de conjuntos formam uma *partição* de A).

Exemplos 1.1.14. Nos exemplos abaixo, que fazem referência a exemplos que já tratamos anteriormente, vamos imaginar que os pontos de A estão num círculo. Queremos ver como as classes de equivalência de R, em cada exemplo, dividem A em conjuntos disjuntos.

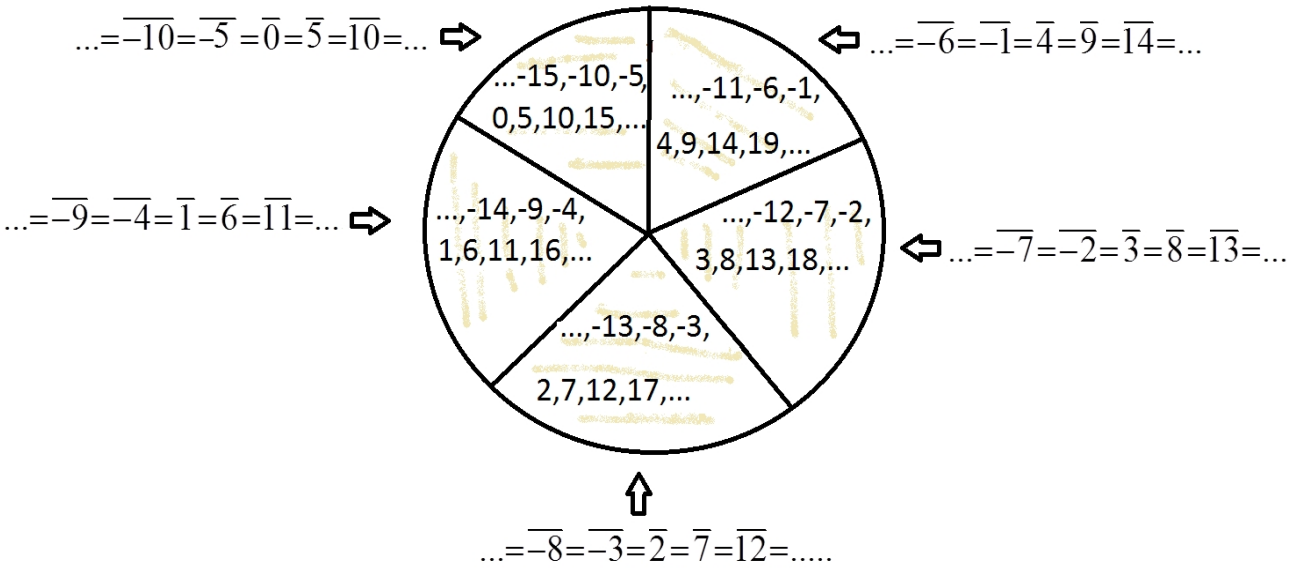
a) Nos Exemplos 1.1.7(a) e 1.1.10(a) temos que $A = \{1,2,3\}$ e $R = \{(1,1),(2,2),(3,3)\} \subset A \times A$ de modo que $\overline{1} = \{1\}$, $\overline{2} = \{2\}$ e $\overline{3} = \{3\}$. Assim A é a união de três classes de equivalência distintas:



b) Nos Exemplos 1.1.7 (b) e 1.1.10 (b) temos que $A=\{1,2,3\}$ e $R=\{(1,1),(2,2),(3,3),(1,2),(2,1)\}\subset A\times A$ de modo que A é a união de duas classes de equivalência distintas, a saber $\overline{1}=\overline{2}=\{1,2\}$ e $\overline{3}=\{3\}$:



c) Nos exemplos 1.1.7 (h) e 1.1.10 (d) temos uma relação de equivalência sobre o conjunto Z dos inteiros dada por $R=\{(a,b)\in Z\times Z\,|\,b-a$ é um múltiplo inteiro de 5 $\}$ e vimos que $Z=\overline{0}\cup\overline{1}\cup\overline{2}\cup\overline{3}\cup\overline{4}$. Como $\overline{1}=\{\ldots-14,-9,-4,1,6,11,16,\ldots\}=\{m.5+1\,|\,m\in Z\}$ temos da Proposição 1.1.12 que para todo $m\in Z$ vale $\overline{m.5+1}=\overline{1}$ (pois $m.5+1\in\overline{1}$), da mesma forma $\overline{m.5+2}=\overline{2}$, $\overline{m.5+3}=\overline{3}$, $\overline{m.5+4}=\overline{4}$ e $\overline{m.5}=\overline{0}$. Isso mostra que as distintas classes de equivalência são exatamente $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$ e $\overline{4}$, e temos



d) Nos Exemplos acima vimos que a relação de equivalência dividiu o conjunto sobre o qual ela está definida em um número finito de subconjuntos, que são as distintas classes de equivalência – de fato, podemos pensar que o conjunto foi "fatiado" como uma pizza em um número finito de pedaços, sendo que cada pedaço contém uma das distintas classes de equivalência. Já nos exemplos 1.1.7 (g) e 1.1.10 (c) essa idéia continua válida, só que teremos agora um número infinito de pedaços de pizza. De fato, as distintas classes de equivalência são exatamente aquelas da forma $\overline{a}$, onde a é um número real tal que $0 \le a < 1$. Vejamos que as classes desses números são distintas, lembrando que a relação R é definida sobre o conjunto $\Re$ dos reais por $R = \{(a,b) \in \Re \times \Re \mid b-a$ é um número inteiro$\}$. Assim, se $a,b \in [0,1)$ então não temos $(a,b) \in R$ (pois $b-a$ não é um inteiro) logo pela Proposição 1.1.13 temos $\overline{b} \cap \overline{a} = \varphi$, e em particular $\overline{b} \neq \overline{a}$. Não vamos provar formalmente que essas são todas as classes, mas observe, por exemplo que se $\pi = 3,14159265...$ então $\overline{\pi} = \overline{0,14159265...}$ pela Proposição 1.1.12, já que $(\pi,\ 0,14159265...) \in R$ pois $\pi - 0,14159265... = 3 \in Z$. Por outro lado $\overline{-\pi} = \overline{(1-0,14159265...)} = \overline{0,85840734...}$ já que $-\pi - 0,85840734... = -\pi - (1-0,14159265...) = -3,14159265... - 1 + 0,14159265... = -4 \in Z$. Dessa forma pode-se mostrar que dado um número real a existe um único $b \in [0,1)$ tal que $\overline{a} = \overline{b}$.

As propriedades de classe de equivalência enunciadas nas poposições 1.1.12 e 1.1.13 são fundamentais e devem ser bem entendidas. Isso porque nas aplicações de relações de equivalência, como veremos, o objetivo sempre é trabalhar com as classes de equivalências como os novos objetos de estudo. Assim, passa-se do estudo do conjunto A sobre o qual está definida a relação de equivalência R, para o estudo do *conjunto*

quociente de A *por* R que é o conjunto $\{\overline{a} \mid a \in A\}$ das classes de equivalência determinadas por R. Como visto acima, os conceitos de relação de equivalência e classe de equivalência são simples (certo?) mas devemos ficar atentos às aplicações, pois em cada caso as notações para a relação de equivalência e classes de equivalência podem não ser iguais às vistas acima. Nesse livro mostraremos, em cada aplicação, como entender as relações de equivalências que aparecerão segundo a teoria apresentada acima.

1.2 Introdução à estrutura de grupos

Nessa segunda parte do Módulo 1 veremos os conceitos básicos sobre a estrutura conhecida como grupo. No Módulo 2, utilizando entre outros conhecimentos resultados sobre relações de equivalência, aprofundaremos o estudo de grupos.

O estudo de grupos foi motivado por observações como as seguintes:

1) A soma de dois inteiros é um inteiro, a soma é associativa, existe um inteiro – o zero – que quando somado a qualquer outro o resultado é esse qualquer outro, e dado um inteiro existe outro que somado a ele dá como resultado o zero;

2) A soma de duas matrizes (digamos 2x2 e com entradas reais) é uma matriz, a soma é associativa, existe uma matriz – a matriz nula – que quando somada a qualquer outra o resultado é essa qualquer outra, e dada uma matriz existe outra que somada a ela dá como resultado a matriz nula;

3) A soma de dois polinômios (digamos que eles tenham coeficientes reais) é um polinômio, a soma é associativa, existe um polinômio – o polinômio nulo – que quando somado a qualquer outro o resultado é esse qualquer outro, e dado um polinômio existe outro que somado a ele dá como resultado o polinômio nulo.

Definição 1.2.1. Dizemos que um conjunto não vazio G é um grupo se existe uma operação sobre G, que será denotada por $.$, de modo que sejam satisfeitas as seguintes condições:

a) a operação é associativa, ou seja, para todos a, b e c em G vale que $(a.b).c = a.(b.c)$;

b) existe um elemento em G, que será denotado por e, tal que $e.a = a.e = a$ para todo a em G;

c) para cada elemento a em G existe um elemento que será denotado por a^{-1} tal que $a.a^{-1} = a^{-1}.a = e$.

É muito importante observar que $.$, e e a^{-1} são *notações* que designam uma operação e elementos com determinadas propriedades no grupo, e não é verdade, de modo geral, que $.$ é a multiplicação usual de números, e a^{-1} é o inverso multiplicativo de um número a. No primeiro exemplo abaixo essa coincidência vai ocorrer, mas os demais exemplos vão mostar que nem sempre é assim.

Esse e muitos outros exemplos deram origem à seguinte definição:

Exemplos 1.2.2 Para dar exemplo de um grupo é preciso, segundo a definição acima, especificar um conjunto e uma operação sobre os elementos desse conjunto.

1) Como um primeiro exemplo, vamos tomar o conjunto dos números reais diferentes de zero, normalmente denotado por $\Re^*$, e a operação vai ser a multiplicação usual (de

modo que nesse primeiro exemplo, o símbolo $.$ que aparece na definição de grupo de fato vai simbolizar multiplicação). Sabemos que a multiplicação de números reais é associativa, de modo que a condição (a) está satisfeita. Sabemos que existe um elemento, que no caso vai ser o número real 1, que de fato tem a propriedade de que $1 . a = a . 1 = a$ para todo $a \in \Re$, de modo que (b) também fica satisfeita se tomamos o elemento e como sendo o número 1. E dado um número real a se tomamos seu inverso multiplicativo a^{-1} é claro que vale $a . a^{-1} = a^{-1} . a = 1$. Assim $\Re^*$ é um grupo com a operação de multiplicação usual.

2) Como segundo exemplo, tome o conjunto dos números inteiros Z e a operação como sendo a soma usual de inteiros, ou seja, na definição de grupos agora temos $G = Z$ e $.$ agora é a soma usual. Nesse caso, a condição expressa no item (a) da definição 1.2.1, que é $(a . b) . c = a . (b . c)$ para todos a, b e c em G nesse exemplo se traduz como $(a + b) + c = a + (b + c)$ para todos a, b e c em Z o que de fato é verdade, de modo que a condição (a) está satisfeita nesse exemplo. Para verificar a condição (b) devemos ter um elemento no grupo, que na definição é simbolizado por e, tal que valha $e . a = a . e = a$ para todo a em G, e como a operação $.$ nesse exemplo é a soma usual, vemos que o elemento que procuramos é o número 0 já que $0 + a = a + 0 = a$. Assim, nesse exemplo, o número 0 é o elemento que na definição 1.2.1 é simbolizado por e (e a soma usual é a operação representada por $.$ naquela definição). Usando essa "tradução" dos símbolos na definição para o nosso exemplo, procuramos agora, dado um a em Z,

um elemento b em Z tal que $a+b=b+a=0$, e é claro que podemos tomar $b=-a$, ou seja, o elemento que na definição 1.2.1 é representado por a^{-1} nesse exemplo específico é o inverso aditivo $-a$. Isso mostra que Z é um grupo com a operação de soma usual.

3) Vamos agora tomar para G o conjunto M das matrizes 2×2 com entradas reais, e para a operação . tomamos a soma usual de matrizes. Dadas matrizes a, b e c em M é fácil verificar que a soma é associativa, ou seja, $(a+b)+c=a+(b+c)$, logo a condição (a) da definição 1.2.1 é satisfeita. Para a condição (b) temos que encontrar uma matriz e tal que $e+a=a+e=a$ para todo a em M e portanto basta tomar e como sendo a matriz nula (assim o símbolo e que aparece na definição de grupo nesse exemplo é a matriz nula 0). Por último, dada uma matriz $a=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ se tomamos a matriz $-a=\begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$ temos que $a+(-a)=(-a)+a=0$ (lembrando que 0 aqui significa a matriz nula) e portanto a condição (c) também é satisfeita (e vemos que o elemento a^{-1} da definição nesse exemplo é a matriz $-a$).

4) Como último exemplo veremos um grupo "abstrato". Nesse caso tomaremos para o conjunto G o conjunto $G=\{\alpha,\beta\}$ onde α e β são elementos que se combinam segundo a tabela abaixo:

.	α	β
α	$\alpha\,.\,\alpha=\alpha$	$\alpha\,.\,\beta=\beta$
β	$\beta\,.\,\alpha=\beta$	$\beta\,.\,\beta=\alpha$

Para mostrar G com a operação . satisfaz à condição (a) temos que considerar todas as possibilidades de combinação de dois elementos em três posições. Deixamos a maioria das verificações para o leitor, fazendo apenas algumas:

$(\alpha \,.\, \beta) \,.\, \alpha = \beta \,.\, \alpha = \beta$ e $\alpha \,.\, (\beta \,.\, \alpha) = \alpha \,.\, \beta = \beta$ logo $(\alpha \,.\, \beta) \,.\, \alpha = \alpha \,.\, (\beta \,.\, \alpha)$; $(\beta \,.\, \beta) \,.\, \alpha = \alpha \,.\, \alpha = \alpha$ e $\beta \,.\, (\beta \,.\, \alpha) = \beta \,.\, \beta = \alpha$ logo $(\beta \,.\, \beta) \,.\, \alpha = \beta \,.\, (\beta \,.\, \alpha)$; etc. Olhando a tabela vemos que $\alpha \,.\, \alpha = \alpha$ e $\alpha \,.\, \beta = \beta \,.\, \alpha = \beta$ logo o elemento α é o que na definição de grupo é simbolizado por e, e temos que a condição (b) está satisfeita. Finalmente falta verificar se para cada elemento existe um outro que multiplicado pelo primeiro tem como resultado o elemento α (pois vimos acima que o elemento α serve como o elemento e da definição de grupo) e da tabela temos que $\alpha \,.\, \alpha = \alpha$ e $\beta \,.\, \beta = \alpha$. Assim $\alpha^{-1} = \alpha$, $\beta^{-1} = \beta$ e temos que a condição (c) também está satisfeita.

O conjunto dos inteiros com a operação usual de produto de inteiros **não** é um grupo. Pense e verá que as condições (a) e (b) são satisfeitas – e, na (b), quem é o elemento que faz o papel do elemento e? – mas a condição (c) não é satisfeita.

No exemplo (4) acima escrevemos que "o elemento α serve como o elemento e" na definição de grupo. Se observamos a condição (b) daquela definição vemos que ela postula a existência de um elemento e com a propriedade de que $e \,.\, a = a \,.\, e = a$ para todo a em G, e em princípio seria possível encontrar um exemplo de grupo no qual diversos elementos tivessem a propriedade que caracteriza e. O próximo resultado

mostra que isso não pode acontecer, e assim, quando encontrarmos num grupo um elemento que "serve como e" podemos estar certos de que não existe outro que tenha a mesma propriedade.

Proposição 1.2.3. Num grupo o elemento denotado por e é único.

Prova. De fato, suponha que num grupo G temos dois elementos, digamos e e f, satisfazendo a condição (b) da definição de grupo, ou seja, $e.a = a.e = a$ e $f.a = a.f = a$ para todo a em G. Em particular temos $e.f = f$ pois e satisfaz (b), e também $e.f = e$ pois f satisfaz (b), assim $e = e.f = f$ o que prova a unicidade.

□

Devido à unicidade acima, dado um gupo G o (único) elemento e que satisfaz a condição $e.a = a.e = a$ para todo a em G é chamado de *elemento neutro de* G ou de *elemento neutro da operação de* G.

Da mesma forma, a condição (c) pede que para cada elemento a em G exista um elemento a^{-1} em G tal que $a.a^{-1} = a^{-1}.a = e$, então podemos nos perguntar se pode haver em algum grupo G algum elemento a tal que $a.b = b.a = e$ e $a.c = c.a = e$ para distintos elementos b e c de G. O próximo resultado mostra que isso não acontece.

Proposição 1.2.4. Seja G um grupo e a um elemento de G. Existe um único elemento b em G tal que $a.b = b.a = e$, onde e é o elemento neutro de G.

Prova. Sejam b e c elementos de G tais que $a.b=b.a=e$ e $a.c=c.a=e$. Então $b=b.e=b.(a.c)=(b.a).c=e.c=c$, o que mostra a unicidade de b. □

Assim, o elemento a^{-1} cuja existência é garantida pela condição (c) da definição de grupo é único e é chamado de *inverso* do elemento a do grupo G.

Proposição 1.2.5. Seja G um grupo, e a e b elementos de G. Temos que $(a^{-1})^{-1}=a$ e $(a.b)^{-1}=b^{-1}.a^{-1}$.

Prova. Como $a^{-1}.a=a.a^{-1}=e$ temos, de (c) na Definição 1.2.1 que a é um inverso (e logo, o inverso) de a^{-1}. Da mesma forma, de $(a.b).(b^{-1}.a^{-1})=(a.b.b^{-1}).a^{-1}=(a.e).a^{-1}=a.a^{-1}=e$ e $(b^{-1}.a^{-1}).(a.b)=(b^{-1}.a^{-1}.a).b=(b^{-1}.e).b=e$ temos do item (c) da Definição 1.2.1 que $b^{-1}.a^{-1}$ é um (e logo o) inverso de $a.b$. □

Obervamos que de modo geral, dados a e b elementos de um grupo G, os elementos $a.b$ e $b.a$ podem ser diferentes.

Exemplo 1.2.6. Vamos tomar para G o conjunto M das matrizes 2×2 com entradas reais e determinante diferente de zero, e a operação de G será o produto usual das matrizes. Lembramos que se $a=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ é uma matriz 2×2 seu determinante é o número real $\det(a)=a_{11}a_{22}-a_{12}a_{21}$. É claro que a matriz identidade $e=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ tem determinante não nulo ($\det(e)=1$), logo e está em G e é fácil verificar que vale

$e \,.\, a = a \,.\, e = a$ para todo a em G. Mais ainda, se $\det(a)$ não é zero então tomando a^{-1} como sendo a matriz dada por $a^{-1} = \begin{pmatrix} \dfrac{a_{22}}{a_{11}\,a_{22} - a_{12}\,a_{21}} & \dfrac{-a_{12}}{a_{11}\,a_{22} - a_{12}\,a_{21}} \\ \dfrac{-a_{21}}{a_{11}\,a_{22} - a_{12}\,a_{21}} & \dfrac{a_{11}}{a_{11}\,a_{22} - a_{12}\,a_{21}} \end{pmatrix}$ é fácil verificar que vale $a \,.\, a^{-1} = a^{-1} \,.\, a = e$. Além disso, sabemos que o produto de matrizes é associativo e portanto concluímos que G é de fato um grupo. Sejam agora $a = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ e $b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, temos que $a.b = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$ e $b.a = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$, logo $a \,.\, b \neq b \,.\, a$.

Definição 1.2.7. Um grupo G onde vale $a \,.\, b = b \,.\, a$ para todos a e em G é dito grupo comutativo ou abeliano.

O adjetivo *abeliano* é uma homenagem a Niels Henrik Abel (1802 – 1829), matemático norueguês cujo trabalho contribuiu (juntamente com os de outros matemáticos) para o aparecimento da teoria de grupos.da matemática.

III - LEITURA COMPLEMENTAR

No endereço *http://www.ime.usp.br/~leo/imatica/historia/grupoabst.html* você encontra algumas considerações sobre o aparecimento da definição de grupo na história da matemática. E no endereço *http://www.bienasbm.ufba.br/M18.pdf* se encontra um arquivo com notas bem detalhadas sobre a história da álgebra abstrata.

MÓDULO 2

Introdução à teoria de grupos

INTRODUÇÃO À TEORIA DE GRUPOS

Nesse módulo estudaremos subconjuntos de grupos que também são grupos (subgrupos) e veremos que um subgrupo pode ser usado para definir uma relação de equivalência sobre o grupo que o contém. Em um determinado caso especial, que estudaremos, pode ser dada uma estrutura de grupo ao conjunto das classes de equivalência dessa relação.

2.1 Subgrupos

Definição 2.1.1 . Seja G um grupo e seja H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G (notação: $H < G$) se H é um grupo com a mesma operação de G.

Exemplos 2.1.2.

1) É fácil verificar que o conjunto dos números reais $\Re$ com a operação de soma usual é um grupo (faça isso como exercício!). Temos que o conjunto dos inteiros Z é subconjunto de $\Re$ e também é fácil verificar que Z é um grupo com essa operação, logo Z é subgrupo de $\Re$, e podemos escrever $Z < \Re$.

2) Vimos no exemplo 1.2.2 (1) que o conjunto dos números reais diferentes de zero, denotado por $\Re^*$, é um grupo com a operação de multiplicação usual. O conjunto dos números inteiros não nulos, que denotaremos por $Z \setminus \{0\}$ é um subconjunto de $\Re^*$, no entanto *não* é um subgrupo de $\Re^*$ pois dado um inteiro não nulo a, diferente de 1 e -1 seu inverso multiplicativo a^{-1} não é um inteiro (e logo não está em $Z \setminus \{0\}$). O próximo resultado nos dá uma outra maneira, além de usar a definição acima, de verificar se um

subconjunto não vazio H de G é um subgrupo de G.

Proposição 2.1.3. Um subconjunto não vazio H de G é um subgrupo de G se e só se valem as seguintes condições:

i) para todos elementos a e b de H temos que $a.b \in H$;

ii) para todo $a \in H$ temos que $a^{-1} \in H$.

Prova. Se $H < G$ então pela definição H é um grupo com a operação $.$ (a mesma definida em G) e portanto valem (i) e (ii). Suponha agora que H é um subconjunto não vazio de G e que valem as condições (i) e (ii). Precisamos mostrar que H é um grupo com a mesma operação de G, ou seja, precisamos mostrar que para H valem as condições (a), (b) e (c) da Definição 1.2.1. Para verificar (a) temos que mostrar que para todos a, b e c em H vale que $(a.b).c = a.(b.c)$, mas isso é verdade pois como $H \subset G$ temos que a, b e c estão em G e como G é grupo sua operação é associativa, ou seja, vale $(a.b).c = a.(b.c)$. Para mostrar o item (b) observamos que H não é vazio, logo existe $a \in H$, e do item (ii) de nossa hipótese temos então que $a^{-1} \in H$. Aplicando agora o item (i) aos elementos a e a^{-1} de H temos que $a.a^{-1} \in H$, mas a e a^{-1} são elementos do grupo G e logo $a.a^{-1} = e$, onde e é o elemento neutro de G. Assim e também está em H e temos que a condição (b) da Definição 1.2.1 está satisfeita. Finalmente o item (c) da Definição 1.2.1 é uma consequência direta do item (ii) de nossa hipótese, e concluímos que H é um grupo com a mesma operação de G, ou seja, H é

um subgrupo de G. □

Corolário 2.1.4. Seja G um grupo e H um subgrupo de G. Então o elemento neutro e de G também está em H e é o elemento neutro de H.

Prova. Temos que H é não vazio e tomando $a \in H$ da Proposição acima vem que $a^{-1} \in H$ e $a.a^{-1} = e \in H$. Assim o elemento neutro de G está em H e como o elemento neutro em um grupo é único temos que e é o elemento neutro de H. □

Exemplos 2.1.5.

1) Se G é um grupo então é claro da definição de subgrupo que G é um subgrupo de G. Seja e o elemento neutro de G e seja $H = \{e\}$. Da Proposição acima temos que H é um subgrupo de G pois $e.e = e$ (e logo vale a condição (i)) e $e^{-1} = e$ (e logo vale a condição (ii)). Os subgrupos $\{e\}$ e G são chamados de subgrupos *triviais* de G.

2) Seja $5\mathbb{Z} = \{m5 \mid m \in \mathbb{Z}\}$ o subconjunto dos números inteiros $\mathbb{Z}$ formado pelos múltiplos de 5. Sabemos que $\mathbb{Z}$ é um grupo com a operação de soma usual e $5\mathbb{Z}$ é um subgrupo de $\mathbb{Z}$: de fato, a soma de dois múltiplos de 5 é um múltiplo de 5 (e logo vale a condição (i)) e dado $m5 \in 5\mathbb{Z}$ temos que $(-m)5 \in 5\mathbb{Z}$ (e logo vale a condição (ii)). De modo geral, dado um número inteiro $n \in \mathbb{Z}$ temos que o conjunto dos múltiplos inteiros de n, usualmente denotado por $n\mathbb{Z}$, é um subgrupo de $\mathbb{Z}$ (isso se mostra de maneira análoga à que fizemos acima para $5\mathbb{Z}$).

O segundo exemplo acima ilustra uma maneira comum de se produzir subgrupos de um

grupo G. A idéia é tomar um elemento $a \in G$ e operá-lo com ele mesmo repetidamente, fazer o mesmo com $a^{-1} \in G$ e ainda tomar o elemento neutro $e \in G$. Para formalizar essa idéia vamos denotar $a.a$ por a^2, $a.a.a$ por a^3, etc.; vamos também denotar $a^{-1}.a^{-1}$ por a^{-2}, $a^{-1}.a^{-1}.a^{-1}$ por a^{-3}, etc.; e convencionamos que $a^0 = e$. Com essas notações é fácil verificar que, dados quaisquer inteiros n e m, vale a propriedade $a^n.a^m = a^{n+m}$. Assim o subconjunto de G dado por

$$\langle a \rangle = \{a^n \in G \mid n \in Z\}$$

é um subgrupo de G: de fato, dados a^n e a^m em $\langle a \rangle$ temos $a^n.a^m = a^{n+m} \in \langle a \rangle$ (o que mostra o item (i) da Proposição 2.1.3, e dado a^n em $\langle a \rangle$ é claro que $a^{-n} \in \langle a \rangle$ (o que mostra o item (ii) da Proposição 2.1.3). Esse subgrupo é chamado o *subgrupo gerado por* $a \in G$.

Definição 2.1.6. Seja G um grupo e seja H um subgrupo de G. Se H é da forma $H = \langle a \rangle$ para algum $a \in G$ então dizemos que H é um subgrupo *cíclico* de G.

Exemplos 2.1.7.

1) Seja Z o grupo dos números inteiros com a operação de soma usual. Temos que o elemento neutro de Z é o zero e o inverso de $5 \in Z$, para a operação de soma, é -5. Assim para formar o subgrupo de Z gerado por 5 tomamos os inteiros 5, $5+5$, $5+5+5$ etc. , e também -5, $-5+(-5)$, $-5+(-5)+(-5)$, etc. e ainda o zero. Nesse caso temos $\langle 5 \rangle = \{m5 \in G \mid m \in Z\}$, e voltamos ao exemplo 2.1.5 (2) que havia originado a idéia de subgrupos cíclicos.

2) Observe que Z é um grupo cíclico, pois é gerado pelo 1 (ou pelo -1). De fato $Z = \langle 1 \rangle = \{m1 \in G \mid m \in Z\}$ e também vale $Z = \langle -1 \rangle = \{n(-1) \in G \mid n \in Z\}$.

3) Já vimos que o conjunto $\Re^*$ dos números reais diferentes de zero forma um grupo com a operação de produto usual de números reais. Nesse caso o elemento neutro de $\Re^*$ é o número 1. O subgrupo cíclico de $\Re^*$ gerado por $2 \in \Re^*$ consiste então das potências do tipo 2^n, com $n = 1,2,3,...$, das potências do tipo $\left(\frac{1}{2}\right)^n = 2^{-n}$, com $n = 1,2,3,...$ e do número 1, ou seja, $\langle 2 \rangle = \{2^m \in \Re^* \mid m \in Z\}$.

Uma importante categoria de grupos é a formada pelos *grupos finitos*, ou seja, grupos formados por um número finito de elementos. O próximo resultado lista importantes propriedades de grupos finitos e seus subgrupos. No que se segue, denotaremos o número de elementos de um conjunto finito T por $|T|$ (lembrando que, em matemática, quando dizemos "o número de elementos de um conjunto" queremos dizer o número de elementos *distintos* do conjunto).

Proposição 2.1.8. Seja G um grupo finito.

1) Seja $a \in G$, seja T um subconjunto de G, seja aT o conjunto $aT = \{a.t \mid t \in T\}$ e seja Ta o conjunto $Ta = \{t.a \mid t \in T\}$. Então $|aT| = |T| = |Ta|$ (ou seja, T, aT e Ta têm o mesmo número de elementos).

2) Seja $a \in G$, temos que $aG = G = Ga$.

3) Um subconjunto não vazio H de G é um subgrupo de G se e só se para todos elementos a e b de H temos que $a.b \in H$

Prova. 1) Seja $n = |T|$, então $T = \{t_1, ..., t_n\}$, onde $t_1, ..., t_n$ são distintos elementos de G, e $aT = \{at_1, ..., at_n\}$. É claro que o número de elementos distintos de aT é no máximo n, e só seria menor se tivéssemos $at_i = at_j$ com $i \neq j$, mas isso não acontece pois se $at_i = at_j$ então multiplicando à esquerda ambos os lados da igualdade por a^{-1} temos $a^{-1}.at_i = a^{-1}.at_j$, logo $t_i = t_j$ e portanto $i = j$. Assim $|aT| = n = |T|$. De maneira análoga se prova que $|Ta| = n = |T|$ (faça como exercício!).

2) Temos $aG = \{a.g \mid g \in G\}$ e como G é um grupo é claro que $aG \subset G$. Por outro lado, do item (1) acima temos que aG e G têm o mesmo número de elementos logo vale $aG = G$. Da mesma forma concluímos que $Ga = G$ (faça como exercício!).

3) Se H é um subgrupo de G então é claro que para todos elementos a e b de H temos $a.b \in H$. Para provar a recíproca, supomos que H seja um subconjunto de G com a propriedade de que dados elementos a e b de H vale que $a.b \in H$. Então, segundo a Proposição 2.1.3, para mostrar que H é subgrupo de G basta provar que dado a em H temos que a^{-1} também está em H. Seja então a em H e considere o subconjunto aH; pela hipótese temos que $aH \subset H$, e pelo item (1) temos que $|aH| = |H|$, logo devemos ter $aH = H$, ou seja, $\{a.b \mid b \in H\} = H$. Assim, como $a \in H$, para algum elemento b em H devemos ter $a.b = a$ e multiplicando à esquerda ambos os lados da igualdade por a^{-1} temos $b = e$. Assim descobrimos que $e \in H$ e

usando novamente que $a\,H = H$ vemos que para algum $c \in H$ devemos ter $a.c = e$; multiplicando novamente à esquerda ambos os lados dessa igualdade por a^{-1} temos $c = a^{-1}$, e assim chegamos a $a^{-1} \in H$. □

Exemplo 2.1.9. Vamos dar agora um exemplo que será muito útil no que se segue. Seja $A = \{1,2,3\}$ e seja G o conjunto das bijeções de A em A. Temos, por exemplo, que a função $\varphi : A \to A$ dada por $\varphi(1) = 2$, $\varphi(2) = 1$ e $\varphi(3) = 3$ está em G (pois é uma bijeção), bem como a função $\psi : A \to A$ dada por $\psi(1) = 2$, $\psi(2) = 3$ e $\psi(3) = 1$. Observe que a cada bijeção corresponde uma permutação da sequência $(1,2,3)$: por exemplo, φ corresponde à permutação que passa de $(1,2,3)$ para $(2,1,3)$, enquanto ψ corresponde à permutação que passa de $(1,2,3)$ para $(2,3,1)$; e inversamente, a cada permutação temos uma bijeção correspondente. Do estudo de permutações sabemos que existem 6 permutações possíveis para a sequência $(1,2,3)$, logo existem 6 bijeções de A em A. É claro que a composição de duas bijeções também é uma bijeção, então vamos compor as bijeções φ e ψ para ver quais novas bijeções podemos produzir. Temos que $\varphi \circ \varphi = e$ onde e aqui denota a bijeção, ou permutação, identidade (ou seja, $e(1) = 1$, $e(2) = 2$ e $e(3) = 3$). Por outro lado temos que $\psi \circ \psi$ corresponde à permutação que passa de $(1,2,3)$ para $(3,1,2)$ e $\psi \circ \psi \circ \psi = e$. Para identificarmos as bijeções $\varphi \circ \psi$ e $\psi \circ \varphi$ lembramos que quando trabalhamos com bijeções em teoria de grupos é usual seguir a convenção usada para a composição de permutações, aplicando em primeiro lugar a f

unção escrita à esquerda e em seguida aplicando a função escrita à direita. Assim $(\varphi\circ\psi)(1)=\psi(\varphi(1))=\psi(2)=3$, e analogamente vemos que $(\varphi\circ\psi)(2)=2$ e $(\varphi\circ\psi)(3)=1$ enquanto $(\psi\circ\varphi)(1)=\varphi(\psi(1))=\varphi(2)=1$, $(\psi\circ\varphi)(2)=3$ e $(\psi\circ\varphi)(3)=2$. Como já temos 6 bijeçõesestassãotodososelementosde G .Assim $G=\{e,\ \varphi,\psi,\psi\circ\psi,\varphi\circ\psi,\psi\circ\varphi\}$ e resumimos no quadro abaixo os resultados encontrados até agora, representado as bijeções como permutações (a partir de agora omitiremos o sinal de composição, e também escrevemos ψ^2 para representar $\psi\circ\psi$, φ^3 para representar $\varphi\circ\varphi\circ\varphi$, etc.):

e	$(1,2,3) \rightarrow (1,2,3)$
φ	$(1,2,3) \rightarrow (2,1,3)$
ψ	$(1,2,3) \rightarrow (2,3,1)$
ψ^2	$(1,2,3) \rightarrow (3,1,2)$
$\varphi\psi$	$(1,2,3) \rightarrow (3,2,1)$
$\psi\varphi$	$(1,2,3) \rightarrow (1,3,2)$

Como a composição de bijeções é uma bijeção podemos tomar a composição como operação no conjunto G. Além disso a composição é uma operação associativa, e é claro que a bijeção e é elemento neutro para a operação de composição. Assim, para mostrar que G é grupo, só falta mostrar que todo elemento de G tem um inverso com relação à composição. Mas da tabela acima é fácil identificar os inversos: por exemplo, o inverso do elemento ψ tem que ser uma bijeção ψ^{-1} tal que $\psi\psi^{-1}=e$, logo temos que ter $\psi^{-1}(\psi(1))=\psi^{-1}(2)=1$, e analogamente $\psi^{-1}(3)=2$ e $\psi^{-1}(1)=3$. Escrevendo ψ^{-1} como permutação de $(1,2,3)$ temos que ψ^{-1} é a permutação $(1,2,3)\rightarrow(3,1,2)$, ou seja $\psi^{-1}=\psi^2$. Procedendo da mesma forma temos que $\varphi^{-1}=\varphi$, $(\psi^2)^{-1}=\psi$, $(\varphi\psi)^{-1}=\varphi\psi$

e $(\psi\varphi)^{-1} = \psi\varphi$. É claro que sabendo que $\psi^{-1} = \psi^2$ e $\varphi^{-1} = \varphi$ podemos usar a Proposição 1.2.5 e deduzir que $(\varphi\psi)^{-1} = \psi^{-1}\varphi^{-1} = \psi^2\varphi$ e avaliando $\psi^2\varphi$ em 1, 2 e 3 vemos que $\psi^2\varphi = \varphi\psi$. Faça isso como exercício e mostre também que $(\psi\varphi)^{-1} = \varphi^{-1}\psi^{-1} = \varphi\psi^2 = \psi\varphi$.

Para identificar alguns subgrupos de G podemos usar a Proposição 2.1.8 (3), já que G é grupo finito. Observamos no início que $\varphi^2 = e$ logo $H = \{e, \varphi\}$ é um subgrupo de G, pois $e^2 = e \in H$, $e\,\varphi = \varphi\, e = \varphi \in H$ e $\varphi^2 = e \in H$; observe que H é um grupo cíclico. De maneira análoga temos que $N = \{e, \psi, \psi^2\}$ também é um subgrupo de G e também é cíclico. Outros subgrupos são $I = \{e, \varphi\psi\}$ e $J = \{e, \psi\varphi\}$ (use a Proposição 2.1.8 (3) para verificar isso!) e também são cíclicos. Observamos finalmente que esse exemplo

pode ser generalizado: pode-se mostrar que o conjunto das bijeções de $\{1, 2, ..., n\}$ (ou de qualquer conjunto com n elementos), juntamente com a operação de composição, forma um grupo que é usualmente denotado por S_n (e tem $n!$ elementos – faça isso como exercício!). Assim o grupo descrito acima é o S_3 e é assim que vamos nos referir a ele de agora em diante.

2.2 Classes laterais

Veremos agora uma importante interação entre relação de equivalência e subgrupos. A partir de agora vamos utilizar a notação habitual em teoria de grupo e escrever ab, ao invés de $a.b$, para indicar a operação entre elementos a e b de um grupo G (embora eventualmente ainda usemos o ponto para indicar a operação do grupo), também

eventualmente nos referiremos a essa operação como “produto” embora saibamos que em cada exemplo ela tem uma definição.

Seja G um grupo e H um subgrupo de G. Temos que H define uma relação de equivalência R sobre G da seguinte maneira (lembrando que R deve ser um subconjunto de $G \times G$ que satisfaz as condições da Definição 1.1.6): tomamos R como sendo formado pelos pares ordenados $(a,b) \in G \times G$ tais que $a^{-1}b \in H$, ou seja $R = \{ (a,b) \in G \times G \mid a^{-1} b \in H \}$.

Vejamos que R é de fato uma relação de equivalência. Inicialmente observamos que para todo $a \in G$ vale que $(a,a) \in R$ pois $a^{-1} a = e \in H$ para todo $a \in G$. Isso mostra que vale o item (i) da Definição 1.1.6. Suponha agora que $(a,b) \in R$, então vale que $a^{-1}b \in H$. Como H é um subgrupo temos que $(a^{-1}b)^{-1} \in H$, e da Proposição 1.2.5 vem que $(a^{-1}b)^{-1} = b^{-1} \ (a^{-1})^{-1} = \ b^{-1} a$. Assim $b^{-1} a \in H$ e da definição de R temos que $(b,a) \in R$. Isso mostra que vale o item (ii) da Definição 1.1.6. Finalmente suponha que $(a,b) \in R$ e $(b,c) \in R$. Então, pela definição de R devemos ter $a^{-1}b \in H$ e $b^{-1}c \in H$, e como H é um subgrupo vale que $(a^{-1}b).(b^{-1} c) \in H$, ou seja, $a^{-1}c \in H$. Agora, pela definição de R temos que $(a,c) \in R$. Isso mostra o item (iii) da Definição 1.1.6 e completa a prova de que R é de fato uma relação de equivalência. Observe que na definição de R poderíamos ter escrito $b^{-1} a \in H$ ao invés de $a^{-1} b \in H$ porque como H é subgrupo temos $b^{-1} a \in H$ se e só se $a^{-1} b \in H$.

Na literatura sobre grupos não é usual proceder como fizemos acima e denotar por R a

relação de equivalência definida pela escolha dos pares (a,b) da maneira indicada acima. A notação e a terminologia usual é a seguinte: dado H um subgrupo de G diz-se que dois elementos a e b de G são *congruentes módulo* H se $a^{-1}b \in H$, e se denota esse fato escrevendo $a \equiv b \mod H$.

Lembramos que a classe de equivalência de um elemento $a \in G$ segundo a relação R é o conjunto dos elementos $b \in G$ tais que $(a,b) \in R$, ou seja, usando a terminologia indicada acima, a classe de $a \in G$ é formada pelos elementos $b \in G$ tais que a e b de G são congruentes módulo H. É claro que, independentemente da descrição adotada, temos que a classe de $a \in G$ é o conjunto $\{b \in G \mid a^{-1} b \in H\}$. Temos então o seguinte importante resultado.

Lema 2.2.1: A classe de equivalência de $a \in G$ segundo a relação definida acima é o conjunto $\{a\,h \in G \mid h \in H\}$.

Prova. De fato, dado $b \in G$ tal que $a^{-1} b \in H$ temos que $a^{-1} b = h$ para algum $h \in H$ e logo $b = a\,h$; por outro lado se $b = a\,h$, com $h \in H$ então $a^{-1} b = h \in H$ e logo b está na classe de equivalência de $a \in G$. Isso mostra que $\{b \in G \mid a^{-1} b \in H\} = \{a\,h \in G \mid h \in H\}$

□

Devido ao lema acima a classe de equivalência de $a \in G$, segundo a relação definida acima, é denotada por $a\,H$, e um tal conjunto é chamado de *classe lateral à esquerda, de* H *em* G. Essa nomenclatura "à esquerda" vem do fato de que podemos definir uma relação de equivalência similar, cujas classes de equivalência são conjuntos da forma

Ha. De fato, seja S a relação sobre G definida por

$$S = \{(a,b) \in G \times G \mid b\ a^{-1} \in H\}\ .$$

Não é difícil verificar, de maneira similar ao que foi feito acima, que S é uma relação de equivalência (faça isso como exercício!). Também como acima temos um lema descrevendo as classes de equivalência de S.

Lema 2.2.2: A classe de equivalência de $a \in G$ segundo a relação S definida acima é o conjunto $\{ha \in G \mid h \in H\}$.

Prova. De fato, dado $b \in G$ tal que $ba^{-1} \in H$ temos que $b\,a^{-1} = h$ para algum $h \in H$ e logo $b = h\,a$; por outro lado se $b = h\,a$, com $h \in H$ então $b\,a^{-1} = h \in H$ e logo b está na classe de equivalência de $a \in G$. Isso mostra que $\{b \in G \mid b\,a^{-1} \in H\} = \{ha \in G \mid h \in H\}$

□

De maneira análoga ao que fizemos anteriormente, denotamos o conjunto $\{ha \in G \mid h \in H\}$ por Ha, para todo $a \in G$, e essas classes laterais são chamadas de *classes laterais à direita, de H em G.*

Quando a operação de G é denotada por $+$ (como por exemplo, no grupo dos números reais ou dos inteiros – veja o Exemplo 2.1.2 (1)) e H é um subgrupo de G então denotamos a classe lateral à esquerda de um elemento $a \in G$ como $a + H$ e a classe lateral à direita como $H + a$.

É importante lembrar sempre que as classes laterais à esquerda (bem como aquelas à direita) são classes de equivalência de uma relação de equivalência sobre G, e portanto

podemos utilizar resultados que obtivemos no estudo dessas relações. Por exemplo, da Proposição 1.1.11 podemos concluir que G é a união das classes $a\,H$, onde a percorre G, e da mesma forma $G=\bigcup_{a\in G} H\,a$, lembrando que duas classes $H\,a$ e $H\,b$ ou coincidem (caso $(a,b)\in S$) ou são disjuntas (caso $(a,b)\notin S$) – também temos que classes $a\ H$ e $b\,H$ ou coincidem (caso $(a,b)\in R$) ou são disjuntas (caso $(a,b)\notin R$). Essas afirmações são consequência das proposições 1.1.12 e 1.1.13.

É claro que se G for um grupo abeliano vale que $a\,H=H\,a$ para todo $a\in G$, pois como G é abeliano em particular temos $a\,h=h\,a$ para todo h em H. No entanto, pode acontecer que $a\,H=H\,a$ mesmo que aconteça $a\,h\neq h\,a$ para algum h em H, pois $a\,H=H\,a$ é uma igualdade *de conjuntos*. Isso vai ficar claro no exemplo a seguir.

Exemplo 2.2.3. Retomamos o exemplo 2.1.9 onde apresentamos o grupo S_3. Vimos ali que $H=\{e,\varphi\}$ é um subgrupo de S_3, vamos calcular as classes de equivalência à esquerda de H – ou seja, vamos calcular os conjuntos $a\ H=\{a\,c\in S_3\,|\,c\in H\}$ para todo a de S_3. Temos (usando que $\varphi^2=e$, $\psi^2\varphi=\varphi\psi$ e $\varphi\psi^2=\psi\varphi$, que são relações vistas no exemplo 2.1.9) que $e\,H=\{e.e,e.\varphi\}=\{e,\varphi\}$, $\varphi\,H=\{\varphi.e,\varphi.\varphi\}=\{\varphi,e\}$, $\psi\,H=\{\psi.e,\psi.\varphi\}=\{\psi,\psi\varphi\}$, $\psi^2\,H=\{\psi^2.e,\psi^2.\varphi\}=\{\psi^2,\psi^2\varphi\}=\{\psi^2,\varphi\psi\}$, $\varphi\psi\,H=\{\varphi\psi.e,\varphi\psi.\varphi\}=\{\varphi\psi,\varphi.\psi\varphi\}=\{\varphi\psi,\varphi.\varphi\psi^2\}=\{\varphi\psi,\varphi^2\psi^2\}=\{\varphi\psi,\psi^2\}$, $\psi\varphi\,H=\{\psi\,\varphi.e,\psi\,\varphi.\varphi\}=\{\psi\,\varphi,\psi\varphi^2\}=\{\psi\,\varphi,\psi\}$. Assim, temos 3 classes de equivalência à esquerda distintas, a saber, $e\,H=\varphi\,H=\{e,\varphi\}$, $\psi\,H=\psi\varphi H=\{\psi,\psi\varphi\}$, $\psi^2\,H=\varphi\psi H=\{\psi^2,\varphi\psi\}$. Vamos calcular agora as classes laterais à direita de H, ou seja, vamos

calcular os conjuntos $Ha = \{h\,a \in S_3 \mid h \in H\}$ para todo a de S_3. Temos como acima que $He = H\varphi = \{e, \varphi\}$, e ainda $H\psi = \{e\psi, \varphi\psi\} = \{\psi, \varphi\psi\}$, $H\psi^2 = \{e\psi^2, \varphi\psi^2\} = \{\psi^2, \psi\varphi\}$, $H\varphi\psi = \{e.\varphi\psi, \varphi.\varphi\psi\} = \{\varphi\psi, \psi\}$ e $H\psi\varphi = \{e.\psi\varphi, \varphi.\psi\varphi\} = \{\psi\varphi, \varphi\psi.\varphi\} = \{\psi\varphi, \psi^2\varphi.\varphi\} = \{\psi\varphi, \psi^2\varphi^2\} = \{\psi\varphi, \psi^2\}$. Temos novamente três classes de equivalência, a saber $He = H\varphi = \{e, \varphi\}$, $H\psi = H\varphi\psi = \{\psi, \varphi\psi\}$ e $H\psi^2 = H\psi\varphi = \{\psi^2, \psi\varphi\}$. Comparando as classes à esquerda e à direita vemos que $He = eH$ e $H\varphi = \varphi H$, mas $H\psi \neq \psi H$, $H\psi^2 \neq \psi^2 H$, etc.. Vamos agora calcular as classes à esquerda e à direita de outro subgrupo de S_3, a saber, $N = \{e, \psi, \psi^2\}$. É fácil verificar que $eN = \psi N = \psi^2 N = \{e, \psi, \psi^2\}$ (usando que $\psi^3 = e$, conforme visto no exemplo 2.1.9) e ainda $\varphi N = \{\varphi e, \varphi\psi, \varphi\psi^2\} = \{\varphi, \varphi\psi, \psi\varphi\}$, $\varphi\psi N = \{\varphi\psi e, \varphi\psi\psi, \varphi\psi\psi^2\} = \{\varphi\psi, \varphi\psi^2, \varphi\psi^3\} = \{\varphi\psi, \psi\varphi, \varphi\}$ e $\psi\varphi N = \{\psi\varphi e, \psi\varphi\psi, \psi\varphi\psi^2\} = \{\psi\varphi, \varphi\psi^2\psi, \varphi\psi^2\psi^2\} = \{\psi\varphi, \varphi\psi^3, \varphi\psi^3\psi\} = \{\psi\varphi, \varphi, \varphi\psi\}$. Temos então duas classes laterais à esquerda, de N em S_3, que são $eN = \psi N = \psi^2 N = \{e, \psi, \psi^2\}$ e $\varphi N = \varphi\psi N = \psi\varphi N = \{\varphi, \varphi\psi, \psi\varphi\}$. De forma análoga, pode-se mostrar (faça como exercício!) que $Ne = N\psi = N\psi^2 = \{e, \psi, \psi^2\}$ e $N\varphi = N\varphi\psi = N\psi\varphi = \{\varphi, \varphi\psi, \psi\varphi\}$. Assim, nesse caso, temos que $aN = Na$ para todo a em S_3. Tomando $a = \varphi$ observamos que não vale $\varphi h = h\varphi$ para todo h em N (por exemplo, $\varphi\psi \neq \psi\varphi$), no entanto o conjunto dos elementos $\{\varphi e, \varphi\psi, \varphi\psi^2\}$ é o mesmo dos elementos $\{e\varphi, \psi\varphi, \psi^2\varphi\}$ (pois ambos são iguais a $\{\varphi, \varphi\psi, \psi\varphi\}$).

O exemplo acima ilustra vários conceitos que já vimos sobre classes de equivalência. Por exemplo, vimos que $\varphi N = \{\varphi, \varphi\psi, \psi\varphi\}$ e que as classes à esquerda de $\varphi\psi$ e de $\psi\varphi$ (que juntamente com φ formam o conjunto $\{\varphi, \varphi\psi, \psi\varphi\}$) coincidem com a classe à esquerda de φ (ou seja, $\varphi N = \varphi\psi N = \psi\varphi N$). Isso não é por acaso, claro, é simplesmente uma ilustração da Proposição 1.1.12, pois como $\varphi\psi \in \varphi N$ vem dessa proposição que $\varphi N = \varphi\psi N$. Confira essas "coincidências" para as outras classes no exemplo acima. Além disso vimos como uma relação de equivalência particiona S_3 como uma união de conjuntos disjuntos (um fato observado logo após a prova da Proposião 1.1.13). Por exemplo, as classes laterais à esquerda, de H em S_3, particionam S_3 da forma $S_3 = \{e, \varphi\} \cup \{\psi, \psi\varphi\} \cup \{\psi^2, \varphi\psi\}$, as classes laterais à direita de H em S_3 particionam S_3 da forma $S_3 = \{e, \varphi\} \cup \{\psi, \varphi\psi\} \cup \{\psi^2, \psi\varphi\}$ enquanto as classes laterais à esquerda (ou à direita) de N em S_3 particionam S_3 da forma $S_3 = \{e, \psi, \psi^2\} \cup \{\varphi, \varphi\psi, \psi\varphi\}$.

Exemplo 2.2.4. . Vimos no Exemplo 2.1.5 (2) que $5\mathrm{Z} = \{m5 \mid m \in \mathrm{Z}\}$ é um subgrupo do grupo dos números inteiros Z. Como Z é um grupo abeliano temos que as classes laterais à esquerda e à direita de $5\mathrm{Z}$ em Z coincidem, ou seja $a + 5\mathrm{Z} = 5\mathrm{Z} + a$ para todo $a \in \mathrm{Z}$. Do Lema 2.2.1 sabemos que a classe de um elemento $a \in \mathrm{Z}$ é $a + 5\mathrm{Z} = \{a + m\,5 \mid m \in \mathrm{Z}\}$. Assim temos que

$0 + 5\mathrm{Z} = \{0 + m\,5 \mid m \in \mathrm{Z}\} = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$; $1 + 5\mathrm{Z} =$

$\{1+m\ 5 \mid m \in Z\} = \{\ldots,-14,-9,-4,1,6,11,16,\ldots\}$; $2+5\,Z = \{2+m\ 5 \mid m \in Z\} =$

$\{\ldots,-13,-8,-3,2,7,12,17,\ldots\}$; $3+5\,Z = \{3+m\ 5 \mid m \in Z\} =$

$\{\ldots,-12,-7,-2,3,8,13,18,\ldots\}$; $4+5\,Z = \{4+m\ 5 \mid m \in Z\} =$

$\{\ldots,-11,-6,-1,4,9,14,19,\ldots\}$;

e essas são todas as classes laterais à esquerda de $5Z$ em Z. De fato, vemos que essas classes laterais são exatamente as classes de equivalência que aparecem no Exemplo 1.1.14 (c), e ali vemos que o número de classes de equivalência distintas é cinco. Essa coincidência entre classes laterais à esquerda $5Z$ em Z e as classes de equivalência do Exemplo 1.1.14 (c) não é um acaso: se olharmos, no início da seção 2.2, a definição da relação de equivalência sobre Z definida pelo subgrupo $5Z$ veremos que um par ordenado $(a,b) \in Z \times Z$ está na relação se e só se $b-a \in 5Z$, ou seja, se e só se $b-a$ é um múltiplo de 5, que é justamente a relação que aparece no Exemplo 1.1.14 (c).

Um outro fato que podemos observar do exemplo acima é que as classes laterais (à esquerda ou à direita) de um subgrupo têm exatamente o mesmo número de elementos do subgrupo. Isso é um fato geral, que provamos a seguir.

Lema 2.2.5. Seja G um grupo finito, seja H um subgrupo de G e seja $a \in G$. Então tanto aH quanto Ha têm o mesmo número de elementos de H.

Prova. Temos que $aH = \{a\,h \in G \mid h \in H\}$, logo o número de elementos em aH é menor do que o número de elementos de H se e só se $ac = ad$ para distintos elementos c e d de H, no entanto se $ac = ad$ então multiplicando a igualdade à esquerda por a^{-1} temos

$c = d$. Assim não acontece $ac = ad$ para distintos elementos c e d de H e portanto H e aH têm o mesmo número de elementos. De maneira similar (faça como exercício!) mostra-se que H e Ha têm o mesmo número de elementos. □

Como consequência desse lema e do fato das diferentes classes laterais darem uma partição temos o seguinte importante resultado, conhecido como teorema de Lagrange e assim denominado em homenagem ao matemático francês Joseph-Louis Lagrange (1736-1813) que o provou pela primeira vez. (Lembramos que $|A|$ denota o número de elementos de um conjunto A.)

Teorema (Lagrange) 2.2.6. Seja G um grupo finito e seja H um subgrupo de G. Então $|G|$ é um múltiplo de $|H|$.

Prova. Sabemos que as classes laterais à esquerda, de H em G, formam uma partição de G, ou seja, podemos escrever $G = a_1H \cup \cdots \cup a_n H$, onde $a_1, \ldots, a_n \in G$ e $a_iH \cap a_jH$ é o conjunto vazio se $i \neq j$. Do lema acima temos que $|a_iH| = |H|$ para todo $i = 1, \ldots, n$ logo $|G| = n|H|$, e portanto $|G|$ é um múltiplo de $|H|$. □

Exemplo 2.2.7. Observe que o grupo S_3, apresentado no Exemplo 2.1.9 e que tem 6 elementos, segundo o teorema acima só admite subgrupos de ordem 1, 2, 3 ou 6. É claro que S_3 é um subgrupo de si mesmo e tem 6 elementos, por outro lado o conjunto $\{e\}$ também é um subgrupo de S_3 e tem um elemento. Temos ainda que os subgrupos H, I e J têm dois elementos cada enquanto que N tem três elementos. Isso mostra que

todas as possibilidades de ordem para semigrupos são realizadas efetivamente, mas essa **não** é a regra geral em teoria de grupos. De fato existem inúmeros exemplos de grupos que não têm subgrupos com cardinalidade igual a determinado divisor de $|G|$.

Dado um grupo G, um subgrupo H de G e um elemento $a \in G$ pode acontecer que aH seja diferente de Ha (veja, por exemplo, no exemplo 2.2.3 que $H\psi \neq \psi H$), e pode acontecer que dado um subgrupo N seja verdade que $Na = aN$ para todo $a \in G$ (veja, ainda no exemplo 2.2.3 que $Na = aN$ para todo $a \in S_3$). Esse último fato é bastante importante em teoria de grupos e leva à seguinte definição.

Definição 2.2.8. Seja G um grupo e seja H um subgrupo de G. Dizemos que H é subgrupo normal de G se $aH = Ha$ para todo $a \in G$.

Se H é subgrupo normal de G então denotamos esse fato escrevendo $H \lhd G$. Observe que da definição das classes laterais aH e Ha temos que H é subgrupo normal de G se e só se temos a igualdade $\{ah \in G \mid h \in H\} = \{ha \in G \mid h \in H\}$ para todo $a \in G$.

Dado um subgrupo H de G para todo elemento $a \in G$ definimos o conjunto $aHa^{-1} = \{aha^{-1} \in G \mid h \in H\}$. Temos então o seguinte resultado.

Teorema 2.2.9. Seja G um grupo e seja H um subgrupo de G. Então H é subgrupo normal de G se e só se $aHa^{-1} = H$ para todo $a \in G$.

Prova. Suponha que H é subgrupo normal de G e seja $a \in G$. Da definição acima temos que $\{ah \in G \mid h \in H\} = \{ha \in G \mid h \in H\}$. Essa igualdade de conjuntos *não* significa que $ah = ha$ para todo $h \in H$ (como vimos no final do exemplo 2.2.3), ela significa que

para cada $h_1 \in H$ existe $h_2 \in H$ tal que $a\, h_1 = h_2\, a$ (e logo $\{a\, h \in G \mid h \in H\} \subset \{h\, a \in G \mid h \in H\}$) bem como dado $h_3 \in H$ existe $h_4 \in H$ tal que $h_3\, a = a\, h_4$ (e logo $\{h\, a \in G \mid h \in H\} \subset \{a\, h \in G \mid h \in H\}$). Assim como para cada $h_1 \in H$ existe $h_2 \in H$ tal que $a\, h_1 = h_2\, a$ temos, multiplicando à direita por a^{-1} que $a\, h_1\, a^{-1} = h_2 \in H$ para cada $h_1 \in H$, ou seja, $a\, H\, a^{-1} \subset H$. Por outro lado, dado $h_3 \in H$ temos que existe $h_4 \in H$ tal que $h_3\, a = a\, h_4$ e novamente multiplicando à direita por a^{-1} obtemos $h_3 = a\, h_4\, a^{1} \in a\, H\, a^{-1}$ logo $H \subset a\, H\, a^{-1}$ o que completa a prova de que $a\, H\, a^{-1} = H$ para todo $a \in G$.

Suponha agora que $a\, H\, a^{-1} = H$ para todo $a \in G$. Essa igualdade de conjuntos significa que para cada $h_1 \in H$ existe $h_2 \in H$ tal que $a\, h_1\, a^{-1} = h_2$. Vamos mostrar que $a\, H = H\, a$

Dado um elemento $a\, h_1 \in a\, H$ temos que $a\, h_1\, a^{-1} = h_2$ para algum $h_2 \in H$ e multiplicando à direita por a temos que $a\, h_1 = h_2\, a \in H\, a$ logo $a\, H \subset H\, a$. De maneira análoga, considere um elemento $h_3\, a \in H\, a$. Observe que como $a\, H\, a^{-1} = H$ para todo $a \in G$, e lembrando que $(a^{-1})^{-1} = a$ (veja a Proposição 1.2.5), temos que também vale que $a^{-1}\, H\, a = H$ para todo $a \in G$. Assim dado $a^{-1}\, h_3\, a \in a^{-1}\, H\, a$ existe $h_4 \in H$ tal que $a^{-1}\, h_3\, a = h_4$ e logo $h_3\, a = a\, h_4 \in a\, H$, ou seja, $H\, a \subset a\, H$, o que completa a prova de que $a\, H = H\, a$ e portanto o subgrupo H é normal. □

O próximo resultado mostra que não precisamos mostrar que $a\, H\, a^{-1} = H$ para todo $a \in G$ para mostrar que um subgrupo é normal, basta mostrar que $a\, H\, a^{-1} \subset H$ para

todo $a \in G$.

Proposição 2.2.10. Seja G um grupo e seja H um subgrupo de G. Então $a\,H\,a^{-1} = H$ para todo $a \in G$ se e só se $a\,H\,a^{-1} \subset H$ para todo $a \in G$.

Prova. É claro que se $a\,H\,a^{-1} = H$ então vale $a\,H\,a^{-1} \subset H$, para todo $a \in G$. Suponha então que vale $a\,H\,a^{-1} \subset H$, para todo $a \in G$, e vamos mostrar que $H \subset a\,H\,a^{-1}$. Como na prova do teorema acima temos que se vale $a\,H\,a^{-1} \subset H$, para todo $a \in G$, então vale $a^{-1}\,H\,a \subset H$ para todo $a \in G$. Assim, dado $h_1 \in H$ e $a \in G$ existe $h_2 \in H$ tal que $a^{-1}\,h_1\,a = h_2$, logo multiplicando à esquerda por a e à direita por a^{-1} temos $h_1 = a\,h_2\,a^{-1} \in a\,H\,a^{-1}$ o que mostra que $H \subset a\,H\,a^{-1}$ para todo $a \in G$. □

A importância de H ser um subgrupo normal está no fato de que, nesse caso, se pode definir um produto no conjunto das classes laterais à esquerda (ou equivalentemente, à direita) . De fato, seja G um grupo e seja H um subgrupo normal de G. Observe que, dadas classes $a\,H$ e $b\,H$, se definimos o produto $a\,H\,.bH$ da maneira "óbvia", ou seja, $a\,H\,.bH = \{ah_1bh_2 \mid h_1, h_2 \in H\}$ temos que como $H\,b = b\,H$ dado $h_1 \in H$ existe $h_3 \in H$ tal que $h_1\,b = b\,h_3$ logo $a\,h_1\,b\,h_2 = a\,b\,h_3h_2 \in ab\,H$ (pois H é subgrupo e de $h_2 \in H$ e $h_3 \in H$ temos $h_3h_2 \in H$), ou seja, $a\,H\,.bH \subset ab\,H$; por outro lado dado $a\,b\,h \in a\,b\,H$ temos que $a\,b\,h = a\,e\,b\,h \in a\,H\,.b\,H$ pois H é um subgrupo e o elemento neutro e de G está também em H, assim $a\,H\,.bH = ab\,H$. Vamos mostrar que com essa operação o conjunto das classes laterais à esquerda (que, lembramos, é o mesmo das classes

laterais à direita, pois H é um subgrupo normal de G) forma um grupo. Vejamos que a operação é associativa: dadas classes laterais aH, bH e cH temos que $(aH.bH).cH = (ab\ H).cH = (abc)H$ e $aH.(bH.cH) = aH.(bcH) = (abc)H$, assim $(aH.bH).cH = aH.(bH.cH)$ e o produto de classes, como definido, é associativo. Vejamos agora que eH é o elemento neutro desse produto (onde e é o elemento neutro de G): de fato, para toda classe lateral aH temos $eH.aH = ea\ H = aH$. Finalmente, dada uma classe lateral aH temos que $a^{-1}H$ também é uma classe lateral e $a\ H.a^{-1}\ H = e\ H$ e portanto $a^{-1}H$ é o inverso da classe aH. Antes de darmos um exemplo, observamos que se a operação do grupo G é denotada por $+$ e H é um subgrupo normal de G então denotamos a operação entre as classes laterais de H também por $+$, escrevendo $(a+H)+(b+H) = (a+b)\ H$ (veja também a observação feita no segundo parágrafo após o Lema 2.2.2).

Exemplo 2.2.11. Vimos no Exemplo 2.1.5 (2) que $5Z = \{m5 \mid m \in Z\}$ é um subgrupo do grupo dos números inteiros Z e no Exemplo 2.2.4 vimos que o conjunto das distintas classes laterais de $5Z$ em Z, que denotaremos por $Z/5Z$, é igual a $\{0+5Z\ ,\ 1+5Z\ ,\ 2+5Z\ ,\ 3+5Z,\ 4+5Z\}$. Do que foi feito acima temos que $Z/5Z$ é um grupo com a operação dada por $(a+5Z) + (b+5Z) = (a+b)+5Z$. Assim, por exemplo, temos que $(1+5Z) + (2+5Z) = 3+5Z$ e $(2+5Z) + (2+5Z) = 4+5Z$. Observe no entanto que $(3+5Z) + (3+5Z) = 6+5Z$, mas $6+5Z$ não aparece na lista de elementos de

$Z/5Z$! Acontece que como $6-1=5$ é múltiplo de 5, a classe de 6 é a mesma classe de 1 (veja a figura que ilustra o Exemplo 1.1.14 (c)) e portanto $6+5Z=1+5Z$. Abaixo colocamos a tabela com os resultados das possíveis somas de classes em $Z/5Z$.

$+$	$0+5Z$	$1+5Z$	$2+5Z$	$3+5Z$	$4+5Z$
$0+5Z$	$0+5Z$	$1+5Z$	$2+5Z$	$3+5Z$	$4+5Z$
$1+5Z$	$1+5Z$	$2+5Z$	$3+5Z$	$4+5Z$	$0+5Z$

$2+5Z$	$2+5Z$	$3+5Z$	$4+5Z$	$0+5Z$	$1+5Z$
$3+5Z$	$3+5Z$	$4+5Z$	$0+5Z$	$1+5Z$	$2+5Z$
$4+5Z$	$4+5Z$	$0+5Z$	$1+5Z$	$2+5Z$	$3+5Z$

Obesrve que, como já visto acima, temos $(4+5Z)+(4+5Z)=8+5Z=3+5Z$ pois $8-3=5$ é múltiplo de 5.

Esse exemplo foi interessante porque nos chamou a atenção para o fato de que uma classe lateral pode ter várias "notações", ou como se diz na literatura, pode "admitir vários representantes" (é usual dizer que a é um representante da classe lateral aH).

Já poderíamos ter pensando nisso, pois classes laterais são classes de equivalência e sabemos que uma mesma classe de equivalência pode ser representada usando diferentes elementos (como, por exemplo, feito no Exemplo 1.1.14 (c) e (d)). Esse fato nos leva a refletir sobre a definição de soma de classes. No exemplo acima temos que $6+5Z=1+5Z$ e $8+5Z=3+5Z$. Da definição de soma de classes temos que $(1+5Z)+(3+5Z)=4+5Z$, mas $(6+5Z)+(8+5Z)=14+5Z$. Como as classes que estão sendo somadas são as mesmas, só não teremos uma contradição se $14+5Z=4+5Z$, e de fato essa igualdade se verifica porque $14-4=10$ é um múltiplo de 5.

Mas, e na teoria geral? Será que o resultado do produto de classes laterais (de subgrupos normais, claro) independe dos representantes usados para denotar essas classes?

Ou seja, dado um grupo G e H um subgrupo normal de G, se $a\,H = c\,H$ e $b\,H = d\,H$ é verdade que $ab\,H = cd\,H$? A resposta é: Sim! Mas isso tem que ser provado, e é o que fazemos agora. Como $a\,H = c\,H$ temos que $c^{-1}a \in H$, e como $b\,H = d\,H$ temos $d^{-1}b \in H$. Sejam $h_1 = c^{-1}a$ e $h_2 = d^{-1}b$, temos então que $a = c\,h_1$ e $b = d\,h_2$ logo $a\,b = c\,h_1\,d\,h_2$, onde h_1 e h_2 são elementos de H. Como H é subgrupo normal de G temos que $d\,H = H\,d$, ou seja, existe h_3 em H tal que $h_1 d = d\,h_3$. Assim $c\,h_1\,d\,h_2 = c\,d\,h_3\,h_2$ e temos $a\,b = c\,d\,h_3\,h_2$ (observe que $h_3\,h_2 \in H$ pois H é subgrupo) logo $(c\,d)^{-1}\,a\,b = h_3\,h_2 \in H$ e portanto $ab\,H = cd\,H$.

Resumimos o que fizemos acima no seguinte resultado.

Teorema 2.2.12. Seja G um grupo e seja H um subgrupo normal de G. O conjunto das classes laterais à esquerda de H em G forma um grupo com a operação definida por $a\,H\,.\,bH = ab\,H$. Essa operação está bem definida, no sentido de que não depende dos representantes utilizados para simbolizar as classes. Mais especificamente, se $a\,H = c\,H$ e $b\,H = d\,H$ então vale $a\,H\,.\,bH = c\,H\,.\,d\,H$. Como H é um subgrupo normal de G o conjunto das classes laterais à direita coincide com o das classes laterais à esquerda e também forma um grupo, sendo que nesse caso a operação é dada por $Ha\,.\,Hb = H\,ab$

Essa operação também é bem definida, e se $H\,a = H\,c$ e $H\,b = H\,d$ então $H\,a\,.\,H\,b = H\,c\,.\,H\,d$.

O grupo das classes laterais de H em G é normalmente denotado por G/H e é chamado de *grupo quociente de* G *por* H.

Observe que o grupo das classes laterais, mencionado no Teorema acima, trata de objetos de uma outra natureza, distinta do grupo original. Podemos "ver" isso na figura do Exemplo 1.1.14 (c). Ali, podemos imaginar que o conjunto dos inteiros foi divido em cinco pedaços (como uma pizza, talvez!). O grupo quociente $Z/5Z$, que aparece no Exemplo 2.2.11, tem como elementos esses "pedaços", esses são os cinco elementos de $Z/5Z$, já que cada "pedaço" contém exatamente os elementos de uma classe lateral. E ao escrevermos $(1+5\,Z)+(2+5\,Z)=3+5\,Z$ estamos dizendo que o pedaço que contém o 1 somado ao pedaço que contém o 2 tem como resultado o pedaço que contém o 3. Se escrevemos $1+5\,Z=6+5\,Z$ isso pode ser interpretado como a afimação de que o pedaço que contém o 1 é o mesmo que contém 6, e escrevendo $2+5\,Z=-8+5\,Z$ vemos que o pedaço que contém 2 é o mesmo que contém -8. Temos que $(6+5\,Z)+(-8+5\,Z)=-2+5\,Z$ e esse deve ser o mesmo resultado da soma $(1+5\,Z)+(2+5\,Z)$ e de fato vemos que -2 e 3 estão no mesmo pedaço. Isso mostra mais uma vez que a operação $(a+5\,Z)+(b+5\,Z)=(a+b)+5\,Z$ está bem definida como "soma de pedaços", mesmo que para realizá-la tenhamos que utilizar os valores de determinados inteiros que estão em cada pedaço. É isso que significa a boa definição da operação entre classes laterais de um subgrupo normal.

O exemplo 2.2.11 pode ser generalizado da seguinte maneira. Seja n um número inteiro positivo e seja $nZ=\{mn \mid m\in Z\}$ o subconjunto dos múltiplos de n. Como observado

no Exemplo 2.1.5 (2) temos que $n\mathrm{Z}$ é um subgrupo de Z, e como Z é um grupo abeliano temos que $n\mathrm{Z}$ é subgrupo normal de Z. Pelo que fizemos acima, sabemos que o conjunto das classes laterais, digamos à esquerda, de $n\mathrm{Z}$ em Z, forma um grupo com a operação $(a+H)+(b+H)=(a+b)\ H$, para todos inteiros a e b. Do lema 2.2.1 e da definição da relação de equivalência mencionada nesse lema temos que $a+H=b+H$ se e só se $b-a\in H$, ou seja, se e só se $b-a$ é um múltiplo de n. Lembrando que duas classes de equivalência ou coincidem ou são disjuntas temos que as classes de $0,1,\ldots,n-1$ são disjuntas: de fato se a e b são elementos distintos no conjunto $\{0,1,\ldots,n-1\}$ então $b-a$ não é um múltiplo de n. Mais ainda, dado um número inteiro m temos que a classe de m coincide com a classe de um dos elementos do conjunto $\{0,1,\ldots,n-1\}$: isso é verdade pois dividindo m por n pode-se encontrar inteiros q e r tais que $m=q\,n+r$ e $r\in\{0,1,\ldots,n-1\}$. Assim $m-r=q\,n$ é um múltiplo de n e portanto a classe de m e de r coincidem. Isso mostra que existem exatamente n classes laterais no grupo quociente $\mathrm{Z}/n\mathrm{Z}$, a saber: $0+n\mathrm{Z}$, $1+n\mathrm{Z}$, ..., $(n-1)+n\mathrm{Z}$. Faça você mesmo um exemplo numérico tomando, por exemplo $n=2$ (e observe que nesse caso você terá duas classes, uma com todos os números pares e outra com todos os números ímpares), $n=3$, etc.

MÓDULO 3

Homomorfismo de grupo e introdução à teoria dos anéis

HOMOMORFISMO DE GRUPO E INTRODUÇÃO À TEORIA DOS ANEIS

Até agora estudamos grupos "isoladamente", ou seja, não procuramos relações entre um grupo e outro. Nesse módulo estudaremos aplicações entre gupos, e também uma estrutura similar à do grupo, mas sobre a qual estão definidas duas operações, e não apenas uma.

3.1 Homomorfismos de grupos

Definição 3.1.1. Sejam F e G dois grupos, e denotemos por $.$ e $\bullet$ as operações de F e G respectivamente. Uma aplicação $\phi : F \to G$ é chamada de *homomorfismo* entre os grupos F e G se para todos elementos a e b de F temos que $\phi(a.b) = \phi(a) \bullet \phi(b)$.

Exemplos 3.1.2.

i) Seja $\Re$ o grupo formado pelos números reais, com a operação de soma usual, e seja $\Re^*$ o grupo formado pelos números reais não nulos, com a operação de multiplicação usual (veja o Exemplo 1.2.2 (1)). Seja $\phi : \Re \to \Re^*$ a aplicação exponencial, ou seja, $\phi(a) = e^a$ para todo $a \in \Re$. Temos que ϕ é um homomorfismo entre os grupos $\Re$ e $\Re^*$ pois $\phi(a+b) = e^{a+b} = e^a.e^b = \phi(a).\phi(b)$.

ii) Seja Z grupo dos inteiros com operação de adição usual (que denotaremos por $+$) e seja $Z/5Z$ o grupo quociente de Z pelo subgrupo $5Z$ (veja o Exemplo 2.2.11) , com a operação de soma de classes laterais, que também denotaremos por $+$. Seja $\phi : Z \to Z/5Z$ a aplicação dada por $\phi(a) = a + 5Z$, para todo a em Z. Temos que ϕ é

homomorfismo de grupos pois $\phi(a+b)=(a+b)+5\mathrm{Z}=(a+5\mathrm{Z})+(b+5\mathrm{Z})=\phi(a)+\phi(b)$

iii) Seja Z grupo dos inteiros com operação de adição usual (que denotaremos por $+$) e sejam $\phi:\mathrm{Z}\to\mathrm{Z}$ e $\psi:\mathrm{Z}\to\mathrm{Z}$ as operações definidas respectivamente por $\phi(a)=3a$ e $\psi(a)=a+3$ para todo a em Z. Temos que ϕ é um homomorfismo de grupos pois $\phi(a+b)=3(a+b)=3a+3b=\phi(a)+\phi(b)$. No entanto ψ *não* é homomorfismo de grupos pois de modo geral $\psi(a+b)=(a+b)+3\neq(a+3)+(b+3)$, por exemplo $\psi(2)=5$, $\psi(1)=4$ e logo não vale $\psi(1+1)=\psi(1)+\psi(1)$.

Não raramente encontrarmos na literatura alguma frase explicando que um homomorfismo de grupos é uma aplicação "que respeita as operações dos grupos no domínio e no contradomínio". Esse "respeito" é simplesmente porque, da defínção de um homomorfismo $\phi:F\to G$, vemos que se conhecemos as imagens dos elementos a e b de F então a imagem de $a.b$ já fica determinada como sendo $\phi(a)\bullet\phi(b)$.

No que se segue não usaremos mais notações diferentes para as operações de F e G, mesmo sabendo que em exemplos essas operações são em geral distintas. Continuaremos a utilizar a prática já estabelecida acima de indicar o resultado do produto de a por b em F simplesmente por ab, bem como indicar o resultado do produto de c e d em G simplesmente por cd. Assim, uma aplicação $\phi:F\to G$ será um homomorfismo de grupos se e só se $\phi(ab)=\phi(a)\,\phi(b)$ para todos a e b em F.

Lema 3.1.3. Seja $\phi : F \to G$ um homomorfismo de grupos, e sejam e_F e e_G os elementos neutros de F e G, respectivamente. Então $\phi(e_F) = e_G$.

Prova. Como $e_F\, e_F = e_F$ temos que $\phi(e_F) = \phi(e_F\, e_F) = \phi(e_F)\,\phi(e_F)$. Temos também que $\phi(e_F)$ é um elemento de G e como tal tem um inverso, que denotaremos por $\phi(e_F)^{-1}$. Multiplicando a igualdade $\phi(e_F) = \phi(e_F)\,\phi(e_F)$ à esquerda por $\phi(e_F)^{-1}$ temos $e_G = e_G\,\phi(e_F) = \phi(e_F)$, o que prova o Lema. □

Lema 3.1.4. Seja $\phi : F \to G$ um homomorfismo de grupos, e seja $a \in F$. Então $\phi(a^{-1}) = \phi(a)^{-1}$ para todo $a \in F$.

Prova. Dado $a \in F$ temos que $\phi(a)\,\phi(a^{-1}) = \phi(a\,a^{-1}) = \phi(e_F) = e_G$ e $\phi(a^{-1})\,\phi(a) = \phi(a^{-1}a) = \phi(e_F) = e_G$ logo $\phi(a^{-1}) = \phi(a)^{-1}$. □

O lema 3.1.3 acima mostra que dado um homomorfismo $\phi : F \to G$ o conjunto dos elementos de F que são levados em e_G por ϕ é não vazio, pois contém pelo menos e_F Esse é um subconjunto bastante importante de F, que destacamos a seguir.

Definição 3.1.5. O conjunto $Ker(\phi) := \{a \in F \mid \phi(a) = e_G\}$ é chamado de *núcleo* do homomorfismo ϕ.

O núcleo de um homomorfismo ϕ é simbolizado por $Ker(\phi)$ porque esse conceito apareceu com matemáticos alemães, e núcleo em alemão é "kernel". Observe também que utilizamos acima o símbolo $:=$. Esse é um símbolo de igualdade, mas mais do que isso, significa que não há, no texto, um motivo anterior que justifique essa igualdade, e que na verdade o conceito que está do lado do símbolo de $=$ que tem os dois pontos está sendo definido pelo que aparece do outro lado do símbolo $=$. Por isso às vezes se diz que $:=$ significa "igual por definição" (e não igual devido a um motivo anterior).

Exemplos 3.1.6. Vamos determinar o núcleo dos homomorfismos que aparecem nos itens (i) e (ii) dos Exemplos 3.1.2.

(i) No primeiro exemplo temos $\phi : \Re \to \Re^*$ definida por $\phi(a) = e^a$ para todo $a \in \Re$. O elemento identidade de $\Re^*$ é o número 1 e se $e^a = 1$ então temos que ter $a = 0$. Isso mostra que nesse caso $Ker(\phi) = \{ 0 \}$.

(ii) Nesse caso temos que $\phi : \mathrm{Z} \to \mathrm{Z}/5\mathrm{Z}$ é definido por $\phi(a) = a + 5\mathrm{Z}$, para todo a em Z. O elemento neutro de $\mathrm{Z}/5\mathrm{Z}$ é a classe $0 + 5\mathrm{Z}$. Além disso se $a + 5\mathrm{Z} = 0 + 5\mathrm{Z}$ é porque $a - 0 \in 5\mathrm{Z}$, ou seja, a é um múltiplo de 5. Isso mostra que se a está no núcleo então a é um múltiplo de 5. Por outro lado, se $m5$ é um múltiplo de 5 temos que $\phi(m5) = m5 + 5\mathrm{Z} = 0 + 5\mathrm{Z}$ pois $m5 - 0 \in 5\mathrm{Z}$. Isso mostra que todo múltiplo de 5 está no núcleo e portanto $Ker(\phi) = 5\mathrm{Z}$.

O próximo resultado mostra a importância do núcleo de um homomorfismo.

Proposição 3.1.7. Seja $\phi : F \to G$ um homomorfismo de grupos. O núcleo de ϕ é um subgrupo normal de F.

Prova. Seja H o núcleo do homomorfismo ϕ. Para provar que H é um subgrupo de F vamos usar a Proposição 2.1.3. Assim, dados a e b em H devemos mostrar que $a\,b \in H$ para isso aplicamos ϕ em $a\,b$ obtendo $\phi(a\,b) = \phi(a)\,\phi(b) = e_G\,e_G = e_G$ e portanto $a\,b \in H$ Devemos mostrar ainda que $a^{-1} \in H$, e como $\phi(a^{-1}) = \phi(a)^{-1} = (e_G)^{-1} = e_G$ temos de fato que $a^{-1} \in H$. Isso completa a prova de que H é um subgrupo de F. Para mostrarmos que H é subgrupo normal de F, pelo Teorema 2.2.9 e Proposição 2.2.10, basta mostrar que $a\,H\,a^{-1} \subset H$ para todo $a \in F$. Seja $a \in F$ e seja $a\,h\,a^{-1} \in a\,H\,a^{-1}$, onde $h \in H$, temos que $\phi(a)\phi(h)\,\phi(a^{-1}) = \phi(a)\,e_G\,\phi(a^{-1}) = \phi(a)\,\phi(a^{-1}) = \phi(a\,a^{-1}) = \phi(e_F) = e_G$. Isso mostra que $a\,h\,a^{-1} \in H$ e logo $a\,H\,a^{-1} \subset H$, o que completa a prova de que H é um subgrupo normal de F. □

Exemplos 3.1.8. No Exemplo 3.1.6 (i) o núcleo do homomorfismo ϕ é o conjunto $\{0\}$ que de fato é um subgrupo (dito trivial, veja o Exemplo 2.1.5 (i)) do grupo dos números reais $\Re$ com a adição usual. E como $\Re$ é um grupo abeliano temos que todo subgrupo de $\Re$ é normal. Já no Exemplo 3.1.6 (ii) o núcleo do homomorfismo ϕ é o conjunto $5\mathbb{Z}$ dos inteiros que são múltiplos de 5, e já vimos no Exemplo 2.1.7 (1) que esse é um subgrupo do grupo dos inteiros $\mathbb{Z}$. Como $\mathbb{Z}$ é um grupo abeliano, temos que todo subgrupo de $\mathbb{Z}$ é normal. Para dar um exemplo onde o domínio do homomorfismo não

é um grupo abeliano vamos considerar um homomorfismo ϕ cujo domínio é S_3 e cujo contradomínio é o grupo $G=\{\alpha,\beta\}$ apresentado no Exemplo 1.2.2 (4) – veja ali a tabela que dá o resultado das operações com os elementos de G e confira que o elemento neutro de G é α. Definimos o homomorfismo $\phi: S_3 \to G$ como sendo dado por $\phi(e)=\alpha$, $\phi(\psi)=\alpha$, $\phi(\psi^2)=\alpha$, $\phi(\varphi)=\beta$, $\phi(\varphi\psi)=\beta$ e $\phi(\psi\varphi)=\beta$. Deixamos ao leitor a tarefa de verificar que ϕ de fato é um homomorfismo (e então você terá que verificar coisas como $\phi(\varphi)\phi(\varphi\psi)=\beta\,\beta=\alpha$, e $\phi(\varphi\,\varphi\psi)=\phi(\varphi^2\,\psi)=\phi(e\,\psi)=\phi(\psi)=\alpha$ e portanto $\phi(\varphi)\phi(\varphi\psi)=\phi(\varphi\,\varphi\psi)$). Da própria definição de ϕ temos que $Ker(\phi)=\{e,\psi,\psi^2\}$; vimos no Exemplo 2.1.9 que $N=\{e,\psi,\psi^2\}$ é um subgrupo de S_3, e dos cálculos feitos no (final do) Exemplo 2.2.3 temos que N é subgrupo normal de S_3 (veja também o ultimo parágrafo antes da Definição 2.2.8).

Todo homomorfismo é, em particular, uma aplicação, e como tal pode ou não ser injetor – lembrando que uma aplicação $\Theta: A \to B$ entre conjuntos A e B é injetora se sempre que a_1 e a_2 estão em A e $a_1 \neq a_2$ temos $\Theta(a_1)\neq\Theta(a_2)$, ou equivalentemente, se sempre que $\Theta(a_1)=\Theta(a_2)$ vale que $a_1=a_2$. O próximo resultado mostra que quando trabalhamos com homomorfismos existe uma outra maneira de se verificar a injetividade.

Proposição 3.1.9 Seja $\phi: F \to G$ um homomorfismo de grupos. Temos que ϕ é um homomorfismo injetor se e só se $Ker(\phi)=\{e_F\}$.

Prova. Suponha que ϕ seja um homomorfismo injetor, ou seja, que se $\phi(a)=\phi(b)$

então vale $a = b$, onde a e b são elementos de F. Seja c um elemento do núcleo de ϕ, então vale que $\phi(c) = e_G$. Por outro lado do Lema 3.1.3 temos que $\phi(e_F) = e_G$, logo $\phi(c) = \phi(e_F)$ e da hipótese vem que $c = e_F$, portanto $Ker(\phi) = \{e_F\}$. Suponha agora que $Ker(\phi) = \{e_F\}$ e sejam a e b elementos de F tais que $\phi(a) = \phi(b)$. Multiplicando essa igualdade à direita por $\phi(b)^{-1}$ temos $\phi(a)\ \phi(b)^{-1} = \phi(b)\ \phi(b)^{-1}$, ou seja, $\phi(a)\ \phi(b^{-1}) = e_G$, e como ϕ é homomorfismo temos $\phi(a\,b^{-1}) = e_G$. Assim $a\,b^{-1} \in Ker(\phi)$ e portanto $a\,b^{-1} = e_F$. Multiplicando essa igualdade à direita por b chegamos a $a = b$, e logo ϕ é um homomorfismo injetor. □

Exemplo 3.1.10. No Exemplo 3.1.6 (i) temos que o núcleo do homomorfismo é apenas o 0 (que é elemento neutro da adição dos reais) e de fato o homomorfismo é injetor (pois a função exponencial é injetora). Já no Exemplo 3.1.6 (ii) temos que o núcleo do homomorfismo tem infinitos elementos já que é formado pelos inteiros que são múltiplos de 5, e de fato o homomorfismo não é injetor (pois, por exemplo, $\phi(5) = 5 + 5Z = 0 + 5Z = \phi(0)$).

Definição 3.1.11 A *imagem* de um homomorfismo de grupos $\phi : F \to G$ é o conjunto $\mathrm{Im}(\phi) := \{\phi(a) \in G \mid a \in F\}$.

Outra propriedade importante de um homomorfismo de grupos é que sua imagem é um subgrupo do contradomínio. É o que provamos a seguir.

Lema 3.1.12. Seja $\phi : F \to G$ um homomorfismo de grupos. Então $\mathrm{Im}(\phi)$ é um subgrupo de G.

Prova. Vamos usar a Proposição 2.1.3 para provar o lema. Dados os elementos $\phi(a)$ e $\phi(b)$ em $\mathrm{Im}(\phi)$ temos que $\phi(a)\phi(b) = \phi(a\,b) \in \mathrm{Im}(\phi)$, além disso do Lema 3.1.4 vem que $\phi(a)^{-1} = \phi(a^{-1}) \in \mathrm{Im}(\phi)$. Isso prova que $\mathrm{Im}(\phi)$ é subgrupo de G. □

Definição 3.1.13. Dizemos que um homomorfismo de grupos $\phi : F \to G$ é um *isomorfismo* se ϕ é injetor e sobrejetor. Quando existe um isomorfismo entre grupos F e G dizemos que esses grupos são *isomorfos*.

Exemplo 3.1.14. Já notamos, no Exemplo 3.1.10, que o homomorfismo do Exemplo 3.1.6 (i) é injetor, e é fácil de ver que sua imagem é o conjunto dos números reais positivos $\Re_+^*$. Observe que $\Re_+^*$ é um subgrupo dos números reais não nulos $\Re^*$ com a operação de multiplicação usual (veja o Exemplo 1.2.2 (1)): de fato, dados dois números reais positivos seu produto é um número real positivo, e dado um número real positivo seu inverso multiplicativo é também um número real positivo. Assim, se modificamos o homomorfismo do Exemplo 3.1.6 (i) mudando apenas o contradomínio, ou seja, se consideramos $\tilde{\phi} : \Re \to \Re_+^*$ dado por $\tilde{\phi}(a) = e^a$ para todo $a \in \Re$, temos que $\tilde{\phi}$ é um isomorfismo, pois é injetor (já que o núcleo é apenas o zero) e é sobrejetor.

O próximo teorema traz um dos mais importantes resultados da teoria de grupos que envolvem homomorfismos.

Teorema 3.1.15. (Teorema do homomorfismo para grupos). Seja $\phi : F \to G$ um homomorfismo de grupos. Então o grupo quociente $F / Ker(\phi)$ é isomorfo ao grupo $\mathrm{Im}(\phi)$, e a aplicação $\psi : F / Ker(\phi) \to \mathrm{Im}(\phi)$ dada por $a\ Ker(\phi) \mapsto \phi(a)$ está bem definida e é um isomorfismo entre $F / Ker(\phi)$ e $\mathrm{Im}(\phi)$.

Prova. Inicialmente observamos que, como visto na Proposição 3.1.7 o núcleo de ϕ é um subgrupo normal de F e portanto faz sentido considerar o grupo quociente $F / Ker(\phi)$. Esse grupo é formado pelas classes laterais $a\ Ker(\phi)$ onde $a \in F$. A aplicação ψ é definida como $\psi(a\ Ker(\phi)) = \phi(a)$ e vejamos que está bem definida, ou seja, não depende do elemento escolhido para representar a classe. De fato, se a classe de $a \in F$ é a mesma classe de $a' \in F$, e logo temos $a\ Ker(\phi) = a'Ker(\phi)$, então $(a')^{-1} a \in Ker(\phi)$. Assim, $\phi((a')^{-1} a) = e_G$, onde e_G é o elemento neutro de G, ou seja, $e_G = \phi((a')^{-1})\phi(a)$ e de $\phi((a')^{-1}) = \phi(a')^{-1}$ (v. Lema 3.1.4) temos $e_G = \phi(a')^{-1}\phi(a)$ e multplicando ambos os lados por $\phi(a')$ vem que $\phi(a') = \phi(a)$. Isso prova que $\psi(a' Ker(\phi)) = \psi(a\ Ker(\phi))$ sempre que $a\ Ker(\phi) = a'Ker(\phi)$ e portanto a aplicação ψ dá o mesmo resultado independentemente do representante escolhido para simbolizar o elemento de $a\ Ker(\phi)$ em resumo, ψ está bem definida. Vamos mostrar agora que ψ é um homomorfismo de grupos, é injetora e sobrejetora. Sejam $a\ Ker(\phi)$ e $b\ Ker(\phi)$ elementos de $F / Ker(\phi)$, temos que $a\ Ker(\phi).b\ Ker(\phi) = ab\ Ker(\phi)$, logo $\psi(a\ Ker(\phi).b\ Ker(\phi)) = \psi(ab\ Ker(\phi)) = \phi(ab)$, por outro lado $\psi(a\ Ker(\phi))$.

$\psi(b\ Ker(\phi)) = \phi(a)\ \phi(b)$ e como $\phi(a)\ \phi(b) = \phi(a\,b)$ temos que $\psi(a\ Ker(\phi))$. $\psi(b\ Ker(\phi)) = \psi(ab\ Ker(\phi))$ o que prova que ψ é um homomorfismo de grupos. Para mostrar que ψ é injetora basta mostrar que seu núcleo consiste apenas no elemento neutro de $F / Ker(\phi)$ que é $e_F\ Ker(\phi)$. Seja então $a\ Ker(\phi)$ tal que $\psi(a\ Ker(\phi)) = e_G$, nesse caso $\phi(a) = e_G$ e portanto $a \in Ker(\phi)$, daí vem que $a\ Ker(\phi) = e_F\ Ker(\phi)$ e portanto ψ é injetora. Para mostrar que ψ é sobrejetora seja $c \in \mathrm{Im}(\phi)$, temos então que $c = \phi(a)$ para algum $a \in F$ e logo, pela definição de ψ temos que $\psi(a\ Ker(\phi)) = \phi(a) = c$, o que prova que ψ é sobrejetora. □

Exemplos 3.1.16.

i) Vimos no Exemplo 3.1.6 (ii) que o núcleo do homomorfismo $\phi : \mathrm{Z} \to \mathrm{Z}/5\mathrm{Z}$ definido por $\phi(a) = a + 5\mathrm{Z}$ para todo a em Z é $Ker(\phi) = 5\,\mathrm{Z}$. Observe que $\mathrm{Im}(\phi) = \mathrm{Z}/5\mathrm{Z}$, logo pelo Teorema do homomorfismo para grupos temos que $\psi : \mathrm{Z}/5\mathrm{Z} \to \mathrm{Z}/5\mathrm{Z}$ dada por $\psi(a + 5\mathrm{Z}) = \ a + 5\mathrm{Z}$ é um isomorfismo. Nesse caso a aplicação do Teorema resultou num fato óbvio.

ii) Para um exemplo menos óbvio considere o grupo quociente $\mathrm{Z}/2\mathrm{Z}$. Conforme mencionado no final do módulo 2 esse grupo tem apenas duas classes, a saber $0 + 2\mathrm{Z}$ e $1 + 2\mathrm{Z}$ (que consistem, respectivamente, como subconjuntos de Z, no conjunto dos números pares e dos números ímpares). A tabela de soma desses elementos é:

$(0 + 2\mathrm{Z}) + (0 + 2\mathrm{Z}) = 0 + 2\mathrm{Z}$, $(0 + 2\mathrm{Z}) + (1 + 2\mathrm{Z}) = 1 + 2\mathrm{Z}$, $(1 + 2\mathrm{Z}) + (0 + 2\mathrm{Z}) = 1 + 2\mathrm{Z}$ e $(1 + 2\mathrm{Z}) + (1 + 2\mathrm{Z}) = 0 + 2\mathrm{Z}$. Vimos no Exemplo 2.2.3 que $N = \{e, \psi, \psi^2\}$ é um subgrupo

de $S_3 = \{e,\ \varphi, \psi, \psi^2, \varphi\psi, \psi\varphi\}$ (a definição de S_3 está no Exemplo 2.1.9). Seja $\phi : S_3 \to \mathrm{Z}/2\mathrm{Z}$ a aplicação dada por $\phi(e) = \phi(\psi) = \phi(\psi^2) = 0 + 2\mathrm{Z}$ e $\phi(\varphi) = \phi(\varphi\psi) = \phi(\psi\varphi) = 1 + 2\mathrm{Z}$. Deixamos como exercício ao leitor verificar que ϕ de fato é homomorfismo mostrando que $\phi(a\,b) = \phi(a) + \phi(b)$ para todos a e b em S_3; por exemplo, no Exemplo 2.1.9 vimos que $\psi^2\varphi = \varphi\psi$, assim $\phi(\psi^2\varphi) = \phi(\varphi\psi) = 1 + 2\mathrm{Z}$, e de $\phi(\psi^2) = 0 + 2\mathrm{Z}$ e $\phi(\varphi) = 1 + 2\mathrm{Z}$ temos que $\phi(\psi^2\varphi) = \phi(\psi^2) + \phi(\varphi)$. Da definição de ϕ temos que $Ker(\phi) = N$ e que ϕ é sobrejetora, logo, do teorema do homomorfismo para grupos vem que S_3 / N é isomoformo a $\mathrm{Z}/2\mathrm{Z}$, sendo um isomorfismo dado por $a\,N \mapsto \phi(a)$ para todo $a\,N$ em S_3 / N (lembrando que no Exemplo 2.2.3 já havíamos visto que S_3 / N tem apenas duas classes distintas, que podem ser denotadas por $e\,N$ e $\varphi\,N$).

O Teorema 3.1.15 é também chamado de "Primeiro teorema do homomorfismo para grupos". Isso porque existem outros dois teoremas sobre homomorfismos que, juntamente com o aqui apresentado, formam a base da teoria de homomorfismos de grupos. Você poderá saber mais sobre homomorfismos de grupos se consultar, por exemplo, o livro Tópicos de Álgebra, de I. Herstein.

3.2. Anéis

Vamos estudar agora estruturas algébricas que têm duas operações definidas sobre elas, lembrando que uma operação sobre um conjunto é uma maneira de combinar dois elementos desse conjunto produzindo um terceiro. O estudo de anéis, como objeto

abstrato, veio da observação de que muitos conjuntos com os quais trabalhamos frequentemente têm duas operações definidas sobre eles, e com propriedades semelhantes, como por exemplo, o conjunto dos inteiros, o conjunto dos números reais, o conjunto das matrizes quadradas, o conjunto dos polinômios, etc. Esses exemplos citados têm uma soma e uma multiplicação definidas em cada um deles, e são grupos comutativos com relação à soma. Além disso, a soma e a multiplicação se relacionam através da propriedade que chamamos de distributividade. Esse fatos levaram à seguinte definição.

Definição 3.2.1. Um conjunto não vazio A sobre o qual estão definidas duas operações, que simbolizaremos por $+$ e $.$, e chamaremos respectivamente de soma e produto, é um *anel* se para todos a , b e c em A valem:

i) $(a+b)+c=a+(b+c)$ (ou seja, a adição é associativa);

ii) existe em A um elemento, que denotaremos por 0 , tal que $a+0=0+a=a$;

iii) existe em A um elemento denotado por $-a$ tal que $a+(-a)=(-a)+a=0$;

iv) $a+b=b+a$ (ou seja, a adição é comutativa);

v) $(a.b).c=a.(b.c)$ (ou seja, o produto é associativo);

vi) $a.(b+c)=a.b+a.c$ e $(b+c).a=b.a+c.a$ (ou seja, o produto se distribui com relação à soma)

Observe que se A é um anel, então A com a operação de soma é um grupo comutativo. Isso é uma consequência das condições (i) a (iv) acima.

Se, além das condições acima, também vale que $a.b=b.a$ para todos a e b em A então A é dito um *anel comutativo*. Se, além das condições acima, também vale que

existe um elemento, que denotaremos por 1, tal que $a.1=1.a=a$ para todo a em A então A é dito ser um *anel com unidade*. Neste texto assumiremos sempre que num anel com unidade vale $1\neq 0$, evitando assim o (trivial e) único exemplo de anel com unidade em que temos $1=0$ que é o anel A que consiste apenas em um elemento $A=\{0\}$, e tem as operações + e . , onde $0+0=0$ e $0.0=0$.

Exemplos 3.2.2.

i) O conjunto Z dos inteiros, com as operações usuais de soma e produto, forma um anel comutativo e com unidade.

ii) O conjunto das matrizes 2×2 com entradas reais, considerado com as operações usuais de soma e produto, forma um anel não comutativo, mas com unidade. De fato, a matriz identidade faz o papel do elemento identidade, e sabemos que o produto de matrizes não é comutativo.

iii) O conjunto $2Z$ dos inteiros pares, com as operações usuais de soma e produto de inteiros, forma um anel comutativo que não tem unidade. De fato todas as condições (i) a (vi) são satisfeitas e sabemos que o produto de inteiros é comutativo. No entanto não existe em $2Z$ um elemento $u\in 2Z$ tal que $a.u=u.a=a$ para todo $a\in 2Z$.

iv) O conjunto das matrizes 2×2 cujas entradas são inteiros pares, considerado com as operações usuais de soma e produto, forma um anel não comutativo e sem unidade.

v) O conjunto dos polinômios com coeficientes reais, munido das operações usuais de soma e produto de polinômios, forma um anel comutativo e com unidade.

vi) O conjunto dos números racionais, com as operações usuais de soma e produto, forma

um anel comutativo e com unidade.

Lema 3.2.3. Seja A um anel.

i) Apenas o elemento 0 tem a propriedade de que $a+0=0+a=a$ para todo a em A

ii) Dado a em A o elemento $-a$ tal que $a+(-a)=0$ é único.

iii) Se A for anel com unidade o elemento 1 é o único tal que $a.1=1.a=a$ para todo a em A (e é chamado de *unidade* do anel).

iv) Para todo a em A temos $a.0=0.a=0$.

v) Se A for anel com unidade e denotarmos o inverso aditivo de a em A por $-a$ então vale que $a.(-1)=(-1).a=-a$.

Prova. i) Seja $0'$ um elemento de A tal que $a+0'=0'+a=a$ para todo a em A, então em particular temos que $0+0'=0$. Por outro lado, pela propriedade que 0 tem, em particular vale que $0+0'=0'$, e portanto $0'=0$.

ii) Seja b um elemento de A tal que $a+b=0$ então temos $b=0+b=(-a+a)+b=-a+(a+b)=-a+0=-a$, ou seja $b=-a$.

iii) A prova da unicidade de 1 é idêntica à que foi feita na Proposição 1.2.3.

iv) Dado a em A temos $a.0=a.(0+0)=a.0+a.0$. É claro que $a.0$ é um elemento de A e logo tem um inverso com relação à adição, que denotaremos por $-(a.0)$, somando esse elemento em ambos os lados da igualdade temos $0=a.0$. De forma análoga se mostra que $0=0.a$.

v) Temos $a.(-1)+a=a.(-1)+a.1=a.(-1+1)=a.0=0$, onde na última igualdade

utilizamos o item (iv). Isso mostra que $a.(-1) = -a$. De forma análoga se mostra que $(-1).a = -a$. □

Definição 3.2.4. Seja A um anel e B um subconjunto não vazio de A. Se B, com as mesmas operações definidas sobre A, é um anel, dizemos que B é *subanel* de A.

Lema 3.2.5. Seja A um anel com as operações de soma, denotada por $+$, e multiplicação, denotada por $.$, e seja B um subconjunto não vazio de A tal que:

i) $a+b \in B$ e $a.b \in B$ para todos a e b em B;

ii) para todo a em B temos $-a$ em B.

Então B é um subanel de A.

Prova. Em princípio teríamos que provar que as condições (i) a (iv) da Definição 3.2.1 são satisfeitas, mas é claro que (i), (iv), (v) e (vi) não precisam ser verificadas, pois são propriedades das operações e sabemos que A é anel com essas mesmas operações. Por outro lado, a condição (iii) está satisfeita por hipótese. Assim temos que verificar apenas a condição (ii) mas isso é fácil, já que pelo item (ii) da hipótese dado a em B temos $-a$ em B e pelo item (i) da hipótese temos $a+(-a) = 0 \in B$. □

A partir de agora frequentemente vamos indicar o produto de elementos a e b de um anel A apenas por ab, sem colocar o símbolo " . " do produto entre os elementos.

Num anel é possível acontecer que $a \neq 0$, $b \neq 0$ e $ab = 0$, como mostram os exemplos abaixo.

Exemplo 3.2.6. Seja M o anel das matrizes 2×2 cujas entradas são números reais. Temos que $a=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$ e $b=\begin{pmatrix}0 & 0\\ 1 & 2\end{pmatrix}$ são matrizes não nulas mas $a.b=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$.

Isso motiva a seguinte definição.

Definição 3.2.7. Dizemos que um anel A é um *domínio* (ou também *domínio de integridade*) quando o produto de quaisquer dois elementos não nulos tem como resultado um elemento não nulo. Equivalentemente, A é um domínio se sempre que $a\,b=0$ (com a e b em A) temos $a=0$ ou $b=0$.

Vimos no final do módulo 2 que o conjunto das classes laterais à esquerda de $H=n\mathbb{Z}$ em $\mathbb{Z}$, que é denotado por $\mathbb{Z}/n\mathbb{Z}$, forma um grupo com a operação $(a+H)+(b+H)=(a+b)\ H$, para todos inteiros a e b. É fácil verificar que esse grupo é comutativo. Veremos agora que podemos dar a $\mathbb{Z}/n\mathbb{Z}$ uma estrutura de anel comutativo com unidade, se definimos uma operação de produto de classes através de $(a+H).(b+H)=(a.b)+\ H$. Em primeiro lugar é preciso verificar que esse produto está bem definido, ou seja, se $a+H=a'+\ H$ e $b+H=b'+\ H$ então temos que ter $(a.b)+H=(a'.b')+H$ (lembre-se das considerações que fizemos nos dois parágrafos que precedem o Teorema 2.2.12). E, de fato, como $a+H=a'+\ H$ temos $a-a'=n\,z_1$ para algum inteiro z_1, da mesma forma de $b+H=b'+\ H$ temos $b-b'=n\,z_2$ para algum inteiro z_2. Assim $(a-a')(b-b')=n\,z_1\,n\,z_2$, ou seja, $a\,b-a\,b'-b\,a'+a'\,b'=n\,z_1\,n\,z_2$. Somando e subtraindo $a'\,b'$ do lado esquerdo temos

$a\,b + a'\,b' - a'\,b' - a\,b' - b\,a' + a'\,b' = n\,z_1\,n\,z_2$ que podemos reescrever como $a\,b - a'\,b' + (a' - a)b' - (b - b')a' = n\,z_1\,n\,z_2$. Assim temos $a\,b - a'\,b' + (-n\,z_1)b' - (n\,z_2)a' = n\,z_1\,n\,z_2$, logo $a\,b - a'\,b' = n\,z_1\,b' + n\,z_2\,a' + n\,z_1\,n\,z_2 \in H = n\,\mathrm{Z}$, e portanto $a\,b + H = a'\,b' + H$. Isso mostra que o produto definido é de fato um produto de classes de equivalência e não depende da representação escolhida para denotar cada classe. Já sabemos que $\mathrm{Z}/n\mathrm{Z}$ é um grupo comutativo com a operação de soma de classes, de modo que as condições (i) a (iv) da Definição 3.2.1 estão satisfeitas. Da definição de produto de classes temos que $((a+H)\,.\,(b+H)).(c+H) = (a\,b+H)\,.\,(c+H) = a\,b\,c + H$ e por outro lado $(a+H)\,.\,((b+H).(c+H)) = (a+H)\,.\,(b\,c+H) = a\,b\,c + H$, e portanto vale (v). Finalmente temos que $(a+H)\,.\,((b+H)+(c+H)) = (a+H)\,.\,((b+c)+H) = a\,(b+c) + H =$ $(ab+ac) + H = (a+H)\,.\,(b+H) + (a+H)\,.\,(c+H)$ (deixamos a verificação dessa última igualdade para você, leitor, bem como a verificação de que $((a+H)+(b+H))\,.\,(c+H) = (a+H)\,.\,(c+H) + (b+H)\,.\,(c+H)$). Isso mostra que vale (vi) e portanto $\mathrm{Z}/n\mathrm{Z}$ é um anel com as operações de soma e produto de classes. Como o produto definido acima é claramente comutativo, o anel é comutativo. Também é claro que $((a+H)\,.\,(b+H)).(c+H) = (a\,b+H)\,.\,(c+H) = a\,b\,c + H$ para todo $a + H \in \mathrm{Z}/n\mathrm{Z}$, logo $\mathrm{Z}/n\mathrm{Z}$ é anel comutativo com unidade.

Exemplos 3.2.8. Vamos fazer as tabelas de soma e de multiplicação no anel $Z/4Z$.

Lembramos que, como observado no parágrafo final do módulo 2, toda classe em $Z/4Z$ é igual a uma das seguintes classes: $0+4Z$, $1+4Z$, $2+4Z$ e $3+4Z$ (reveja também as contas feitas no Exemplo 2.2.11). Utilizando as definições de soma e de produto de classes, e fatos como $4+4Z=0+4Z$ pois $4-0=4\in 4Z$, $5+4Z=1+4Z$ pois $5-1=4\in 4Z$, etc. temos as tabelas:

$+$	$0+4Z$	$1+4Z$	$2+4Z$	$3+4Z$
$0+4Z$	$0+4Z$	$1+4Z$	$2+4Z$	$3+4Z$
$1+4Z$	$1+4Z$	$2+4Z$	$3+4Z$	$0+4Z$
$2+4Z$	$2+4Z$	$3+4Z$	$0+4Z$	$1+4Z$
$3+4Z$	$3+4Z$	$0+4Z$	$1+4Z$	$2+4Z$

e

$\cdot$	$0+4Z$	$1+4Z$	$2+4Z$	$3+4Z$
$0+4Z$	$0+4Z$	$0+4Z$	$0+4Z$	$0+4Z$
$1+4Z$	$0+4Z$	$1+4Z$	$2+4Z$	$3+4Z$
$2+4Z$	$0+4Z$	$2+4Z$	$0+4Z$	$2+4Z$
$3+4Z$	$0+4Z$	$3+4Z$	$2+4Z$	$1+4Z$

Observando a tabela de multiplicação vemos que $(2+4Z).(2+4Z)=0+4Z$, e como $2+4Z\neq 0+4Z$ temos que $Z/4Z$ não é domínio (pois encontramos dois elementos não nulos cujo produto é o zero do anel, a saber, $0+4Z$).

Vamos agora fazer a tabela de multiplicação para $Z/5Z$, já que a tabela de soma já feita no Exemplo 2.2.11.

$\cdot$	$0+5\,\mathrm{Z}$	$1+5\,\mathrm{Z}$	$2+5\,\mathrm{Z}$	$3+5\,\mathrm{Z}$	$4+5\,\mathrm{Z}$
$0+5\,\mathrm{Z}$	$0+5\,\mathrm{Z}$	$0+5\,\mathrm{Z}$	$0+5\,\mathrm{Z}$	$0+5\,\mathrm{Z}$	$0+5\,\mathrm{Z}$
$1+5\,\mathrm{Z}$	$0+5\,\mathrm{Z}$	$1+5\,\mathrm{Z}$	$2+5\,\mathrm{Z}$	$3+5\,\mathrm{Z}$	$4+5\,\mathrm{Z}$
$2+5\,\mathrm{Z}$	$0+5\,\mathrm{Z}$	$2+5\,\mathrm{Z}$	$4+5\,\mathrm{Z}$	$1+5\,\mathrm{Z}$	$3+5\,\mathrm{Z}$
$3+5\,\mathrm{Z}$	$0+5\,\mathrm{Z}$	$3+5\,\mathrm{Z}$	$1+5\,\mathrm{Z}$	$4+5\,\mathrm{Z}$	$2+5\,\mathrm{Z}$
$4+5\,\mathrm{Z}$	$0+5\,\mathrm{Z}$	$4+5\,\mathrm{Z}$	$3+5\,\mathrm{Z}$	$2+5\,\mathrm{Z}$	$1+5\,\mathrm{Z}$

Novamente expressamos todos os resultados em termos das classes $0+5\,\mathrm{Z}$, $1+5\,\mathrm{Z}$, $2+5\,\mathrm{Z}$, $3+5\,\mathrm{Z}$ e $4+5\,\mathrm{Z}$, por exemplo, $(4+5\mathrm{Z}).(3+5\mathrm{Z}) = 12+5\mathrm{Z} = 2+5\mathrm{Z}$, sendo a primeira igualdade devido à definição de produto de classes e a segunda ao fato de que $12-2=10\in 5\mathrm{Z}$. Observando a tabela vemos que o elemento $0+5\,\mathrm{Z}$ nunca aparece como resultado do produto de dois elementos não nulo, logo $\mathrm{Z}/5\mathrm{Z}$ é um domínio.

Pensando com mais vagar, poderíamos ter antecipado que $\mathrm{Z}/4\,\mathrm{Z}$ não é domínio. Isso porque sabemos que os elementos de $\mathrm{Z}/n\,\mathrm{Z}$ podem ser escritos como por exemplo $0+n\,\mathrm{Z}$, $1+n\,\mathrm{Z}$, ..., $(n-1)+n\,\mathrm{Z}$, e quando o número inteiro positivo n não é primo ele se fatora como o produto de dois números inteiros positivos menores do que ele, digamos $n=a.b$, logo os elementos $a+n\,\mathrm{Z}$ e $b+n\,\mathrm{Z}$ são não nulos e temos $(a+n\,\mathrm{Z})(b+n\,\mathrm{Z}) = ab+n\,\mathrm{Z} = n+n\,\mathrm{Z} = 0+n\,\mathrm{Z}$, e portanto $\mathrm{Z}/n\,\mathrm{Z}$ não é domínio. Assim, por exemplo, $\mathrm{Z}/6\,\mathrm{Z}$ não é domínio pois $3+6\,\mathrm{Z}$ e $2+6\,\mathrm{Z}$ são elementos não nulos de $\mathrm{Z}/6\,\mathrm{Z}$ e $(3+6\,\mathrm{Z})\,(2+6\,\mathrm{Z}) = 6+6\,\mathrm{Z} = 0+6\,\mathrm{Z}$. O próximo resultado determina

quando $\mathrm{Z}/n\mathrm{Z}$ é domínio.

Proposição 3.2.9. Seja n um inteiro positivo. Temos que $\mathrm{Z}/n\mathrm{Z}$ é domínio se e só se n é primo.

Prova. Suponha inicialmente que $\mathrm{Z}/n\mathrm{Z}$ seja domínio. Pelo raciocínio feito logo antes dessa Proposição o inteiro n não pode ser composto, ou seja, não pode admitir fatoração como um produto de inteiros positivos ambos menores do que n. Assim n se fatora, como produto de inteiros positivos, apenas como $n = 1.n$ e portanto n é primo. Suponha agora por hipótese que n seja um número primo e suponha por absurdo que $\mathrm{Z}/n\mathrm{Z}$ não seja domínio. Nesse caso existem $a+n\,\mathrm{Z}$ e $b+n\,\mathrm{Z}$ em $\mathrm{Z}/n\mathrm{Z}$, com a e b inteiros positivos menores do que n tais que $(a+n\,\mathrm{Z})(b+n\,\mathrm{Z}) = ab+n\,\mathrm{Z} = 0+n\,\mathrm{Z}$. Daí vem que $ab-0 \in n\mathrm{Z}$, ou seja, ab é múltiplo de n, ou equivalentemente, que n divide ab. Como n é primo temos, por uma propriedade de números primos, que n divide a ou n divide b mas ambas as possibilidades são falsas pois a e b são inteiros positivos menores do que n. Chegamos assim a um absurdo e portanto $\mathrm{Z}/n\mathrm{Z}$ é domínio. □

Definição 3.2.10. Seja A um anel com unidade. Dizemos que um elemento $a \in A$ é *invertível* se existe um elemento $b \in A$ tal que $ab = ba = 1$ (e logo b será invertível também). O elemento b é chamado de *inverso* de a (às vezes se usa também *inverso multiplicativo* de a).

O próximo resultado mostra que se existe o inverso de um elemento então ele é único.

Lema 3.2.11. Seja A um anel com unidade, seja $a \in A$ e suponha que existem elementos $b \in A$ e $c \in A$ tais que $a\,b = b\,a = 1$ e $a\,c = c\,a = 1$, então $b = c$.

Prova. Temos que $b = b\,.\,1 = b\,.\,(a\,.\,c) = (b\,.\,a)\,.\,c = 1\,.\,c = c$. □

Quando, num anel A com unidade, um elemento $a \in A$ tem inverso é usual denotar esse inverso por a^{-1}.

É claro que a unidade 1 é invertível pois $1\,.\,1 = 1$, e -1 também é invertível pois, utilizando o item (v) do Lema 3.2.3 temos $(-1)\,.\,(-1) = -(-1) = 1$.

Alguns livros usam *inversível* para denotar elementos como os definidos acima.

Afinal, é inversível ou invertível? Ou os dois estão certos? O certo é *invertível*, e só. Essa é a palavra que está nos dicionários há mais de 100 anos, e que quer dizer *aquilo que tem inverso ou pode ser invertido*. É claro que muitas palavras que usamos não estão no dicionário – gírias, por exemplo, acabam no dicionário só depois de certo tempo. No entanto não há necessidade de se criar uma palavra nova, como *inversível*, para ter exatamente o mesmo significado de uma palavra que já existe.

Exemplo 3.2.12. Observando as tabelas do Exemplo 3.2.8 vemos que em $\mathbb{Z}/4\mathbb{Z}$ apenas os elementos $1+4\mathbb{Z}$ e $3+4\mathbb{Z}$ são invertíveis. Esses são os invertíveis óbvios já que $3+4\mathbb{Z} = (-1)+4\mathbb{Z}$. Por outro lado todos os elementos não nulos de $\mathbb{Z}/5\mathbb{Z}$ são invertíveis.

Essa propriedade do anel $Z/5Z$ merece destaque.

Definição 3.2.13. Seja A um anel com unidade e com a propriedade de que todo elemento não nulo é invertível. Então dizemos que A é um *corpo*.

Exemplos 3.2.14. O conjunto dos números racionais munido das operações usuais de soma e multiplicação é claramente um anel com unidade (que, no caso, é o número 1). Além disso, todo número racional não nulo tem um inverso multiplicativo, que é também um número racional. Assim, o conjunto dos números racionais é um corpo. O mesmo raciocínio se aplica ao conjunto dos números reais, que também é um corpo. Já o conjunto dos números inteiros, munido das operações usuais de soma e multiplicação, *não* é um corpo, pois, por exemplo o inteiro 2 não tem outro inteiro como inverso multiplicativo – observe na Definição 3.2.10 que o inverso de um elemento a deve estar no mesmo anel que esse elemento. Assim, o número 2 não tem inverso, quando considerado como elemento do conjunto dos inteiros, e tem inverso quando considerado como elemento do conjunto dos racionais (ou dos reais).

Teorema 3.2.15. Se A é um corpo então A é um domínio.

Prova. Sejam a e b elementos de A tais que $a\,b = 0$. Segundo a Definição 3.2.7 devemos mostrar que $a = 0$ ou $b = 0$. Se $a = 0$ a prova acabou, suponha então que $a \neq 0$. Como A é corpo temos que existe o inverso de a em A e multiplicando ambos os lados de $a\,b = 0$, à esquerda, por a^{-1} temos $a^{-1}(a\,b) = a^{-1}0 = 0$ e portanto $(a^{-1}a)\,b = b = 0$, o que conclui a prova. □

O conjunto dos elementos invertíveis de um anel com unidade A é denotado por A^* e não é vazio, já que $1 \in A$. Observe que se A é um corpo então A^* consiste de todos os elementos de A exceto o 0. Isso às vezes causa alguma confusão porque, em livros de Cálculo, por exemplo, onde se trabalha constantemente com o conjunto $\Re$ dos reais e às vezes com o conjunto Q dos racionais, encontramos as igualdades (corretas, claro) $\Re^* = \Re - \{0\}$ e $Q^* = Q - \{0\}$ e por isso o estudante fica com a impressão que o asterisco na posição de expoente significa que o zero foi retirado do conjunto. Mas isso não é verdade: por exemplo, temos que $Z^* = \{-1, 1\}$ pois os únicos invertíveis do anel dos inteiros são -1 e 1.

O estudo de corpos é uma parte importante da matemática, com inúmeras aplicações na álgebra e fora dela. A apresentação dos fatos básicos dessa teoria já tomaria todo um semestre de estudo, se não mais. Existe uma farta bibliografia sobre o assunto, e o aluno interessado pode iniciar seus estudos pela monografia de Otto Endler denominada "Teoria dos Corpos" que pode ser comprada a partir do site do IMPA (*https://institucional.impa.br/livros/index.action* , acessado em agosto de 2015) ou baixado gratuitamente também do site do IMPA (*http://www.impa.br/opencms/pt/biblioteca/pm/PM_19.pdf* acessado em agosto de 2015). Aliás, no site das publicações do IMPA (*http://www.impa.br/opencms/pt/biblioteca/biblioteca_colecoes* acessado em agosto de 2015) o estudante encontrará muitos textos sobre as diversas áreas da matemática, que podem ser baixados para seu uso pessoal.

MÓDULO 4

Teoria de anéis com unidades e corpos de frações

TEORIA DE ANÉIS COM UNIDADE E CORPOS DE FRAÇÕES.

Nesse módulo desenvolveremos a teoria iniciada no final do módulo anterior, estudando também relações entre anéis (ou seja, homomorfismos de anéis). Um conceito importante que iremos apresentar é o de ideal de um anel. Também mostraremos como construir determinado corpo a partir de um domínio. Como seria apropriado para um módulo final, utilizaremos aqui conceitos estudados em todos os módulos anteriores, tais como relação de equivalência, grupos e anéis.

4.1 Homomorfismos de anéis e anéis quocientes

Definição 4.1.1 . Seja A um anel e seja B um subconjunto não vazio de A. Dizemos que B é um subanel de A se B é um anel com as mesmas operações de A.

É claro que para B ser subanel as operações de A têm que ser operações sobre B, ou seja, dados elementos a e b em B temos que ter $a+b$ e $a\,b$ em B.

Exemplo 4.1.2. Vimos no Exemplo 3.2.2 (vi) que o conjunto Q dos números racionais forma um anel com as operações usuais de soma e de produto. Essas operações também são operações sobre o conjunto Z dos inteiros (pois soma de inteiros é um inteiro e produto de inteiros é um inteiro), e Z com essas operações é um anel, logo Z é um subanel de Q.

Vimos no Lema 3.2.5 um critério para verificar se determinado subconjunto de um anel

é um subanel. Agora veremos outro critério que será usado mais adiante.

Proposição 4.1.3. Seja A um anel e seja B um subconjunto não vazio de A. Temos que B é um subanel de A se e só se para todos a e b em B temos $a-b$ e ab em B.

Prova. Suponha que B é um anel com as mesmas operações de A e sejam a e b elementos de B. Como o produto é uma operação sobre B temos que $ab \in B$, por outro lado $-b \in B$ e logo $a-b=a+(-b) \in B$.

Suponha agora que para todos a e b em B temos $a-b$ e ab em B. Em princípio temos que mostrar que as condições da Definição 3.2.1 estão satisfeitas. No entanto as condições (i), (iv), (v) e (vi) dependem apenas das operações, que são as mesmas do anel A, então essas condições estão satisfeitas. Para mostrar (ii) observe que dado a em B por hipótese temos $a-a \in B$, ou seja, $0 \in B$. Nesse caso, ainda por hipótese temos que $0-a \in B$, ou seja, $-a \in B$, e portanto vale (iii). Isso completa a demonstração de que B é um anel com as mesmas operações de A. □

Definição 4.1.4 . Seja A um corpo e seja B um subconjunto não vazio de A. Dizemos que B é um subcorpo de A se B é um corpo com as mesmas operações de A.

Como acima, entendemos aqui que para B ser subcorpo de A um pré-requisito tem que ser que as operações de A sejam também operações sobre B, ou seja, dados elementos a e b em B temos que ter $a+b$ e ab em B.

Exemplo 4.1.5. É fácil verificar que o conjunto $\Re$ dos números reais forma um corpo

com as operações usuais de soma e multiplicação. Temos também que essas operações também são operações sobre o conjunto Q dos racionais (pois soma de racionais é um número racional e o produto de números racionais é um racional), além disso Q é um corpo com essas operações logo Q é um subcorpo de $\Re$.

Proposição 4.1.6. Seja A um corpo e seja B um subconjunto não vazio de A, com mais de um elemento. Temos que B é um subcorpo de A se e só se para todos a e $b \neq 0$ em B temos $a-b$ e $a\,b^{-1}$ em B.

Prova. Suponha que B seja um subcorpo de A e sejam a e b elementos de B, com $b \neq 0$. Como B é corpo temos que $-b$ e b^{-1} são elementos de B, e logo $a-b=a+(-b)\in B$ e $a\,b^{-1}\in B$.

Suponha agora que para todos a e $b \neq 0$ em B temos $a-b$ e $a\,b^{-1}$ em B. Vamos mostrar inicialmente que todo elemento não nulo de B tem seu inverso também em B e depois vamos mostrar que B é um anel usando a Proposição 4.1.3. Sabemos que B tem mais de um elemento, logo tem um elemento não nulo, e seja c um tal elemento. Da hipótese vem então que $c-c=0\in B$ e $c\,c^{-1}=1\in B$. Seja b um elemento qualquer não nulo de B, temos novamente pela hipótese, que $1.b^{-1}=b^{-1}\in B$. Usaremos agora a Proposição 4.1.3 para mostrar que B é anel. Sejam a e b elementos de B, se $b=0$ então $a\,b=a.0=0\in B$, se $b\neq 0$ então pelo que acabamos de provar temos $b^{-1}\in B$ e por hipótese $a\,(b^{-1})^{-1}=a\,b\in B$, temos também por hipótese que $a-b\in B$, logo da

Proposição 4.1.3 temos que B é anel. Isso completa a prova de que B é corpo. □

O próximo resultado mostra que em corpos vale a chamada "lei do corte".

Proposição 4.1.7. Seja A um corpo e seja a um elemento não nulo de A. Se $a\,b = a\,c$ então $b = c$ (essa propriedade é chamada de "lei do corte").

Prova. Temos por hipótese que $a\,b = a\,c$ e que $a \neq 0$, como A é um corpo existe em A o inverso multiplicativo de a, que denotamos por a^{-1}. Multiplicando a igualdade à esquerda por a^{-1} temos $a^{-1}(a\,b) = a^{-1}(a\,c)$ logo $(a^{-1}a)\,b = (a^{-1}a)\,c$ e portanto $b = c$.

□

A lei do corte não é suficiente para caracterizar corpos, mas é suficiente para caracterizar domínios.

Proposição 4.1.8. Seja A um anel. Temos que A é um domínio se e só se sempre que $a \neq 0$ e que $a\,b = a\,c$ temos $b = c$ (onde a, b e c são elementos de A).

Prova. Suponha que A seja domínio, que $a \neq 0$ e que $a\,b = a\,c$. Dessa última igualdade vem que $a\,b - a\,c = 0$ e logo que $a\,(b - c) = 0$. Como $a \neq 0$ e A é domínio temos que ter $b - c = 0$, ou seja, $b = c$.

Suponha agora que sempre vale a lei do corte, queremos mostrar que A é domínio e vamos usar a condição da Definição 3.2.7. Suponha que a e b sejam elementos de A tais que $a\,b = 0$. Se $a = 0$ acabamos, se $a \neq 0$ então como $a\,b = 0 = a\,0$ da lei do corte vem que $b = 0$ e acabamos. Isso completa a demonstração da Proposição. □

Vimos no Teorema 3.2.15 que todo corpo é um domínio. Utilizando as duas Proposições acima é possível dar uma outra demonstração desse fato. Pare, pense e descubra como é essa demonstração.

Vamos agora estudar aplicações entre anéis, chamadas, como na teoria de grupos, de homomorfismos. Aqui também a definição exigirá que a aplicação "respeite" as operações nos anéis que estão em seu domínio e contradomínio (recorde a observação feita após os Exemplos 3.1.2). Da mesma forma que fizemos quando trabalhamos com homomorfismos de grupos (veja a observação no parágrafo antes do Lema 3.1.3) não vamos denotar por símbolos diferentes as operações nos anéis que estão no domínio e contradomínio de um homomorfismo, ainda que essas operações sejam distintas. A soma em qualquer dos anéis será indicada por " $+$ " e o produto por " . ", ou simplesmente será indicado escrevendo os fatores um após o outro.

Definição 4.1.9. Sejam A e B anéis. Uma aplicação $\phi: A \to B$ é chamada de *homomorfismo de anéis* se para todos elementos a e b em A temos que $\phi(a+b) = \phi(a) + \phi(b)$ e $\phi(a\,b) = \phi(a)\,\phi(b)$. Quando A e B são anéis com unidade exigimos também que onde 1_A e 1_B denotam, respectivamente, as unidades de A e de B. Como no caso de homomorfismo de grupos, definimos o *núcleo* de ϕ como sendo $Ker(\phi) := \{a \in A \mid \phi(a) = 0\}$.

Exemplo 4.1.10. Seja Z o anel dos inteiros e seja $Z/5Z$ o anel quociente que aparece no Exemplo 2.2.11 e no Exemplo 3.2.8. Seja $\phi: Z \to Z/5Z$ a aplicação definida por

$\phi(n) = n + 5\mathrm{Z}$ para todo $n \in \mathrm{Z}$. Temos que ϕ é um homomorfismo de anéis com unidade, pois para todos n e m em Z temos $\phi(n+m) = (n+m) + 5\mathrm{Z} = (n + 5\mathrm{Z}) + (m + 5\mathrm{Z}) = \phi(n) + \phi(m)$, e também que $\phi(n\,m) = (n\,m) + 5\mathrm{Z} = (n + 5\mathrm{Z})\,(m + 5\mathrm{Z}) = \phi(n)\,\phi(m)$. Por último observamos que $\phi(1) = 1 + 5\mathrm{Z}$, e portanto a imagem da unidade de Z por ϕ é a unidade de $\mathrm{Z}/5\mathrm{Z}$.

É claro que se A e B são anéis, então também são grupos comutativos com a operação de adição. Assim, se $\phi : A \to B$ é um homomorfismo de anéis, como vale $\phi(a + b) = \phi(a) + \phi(b)$ para todos a e b em A, temos que ϕ também é homomorfismo de grupos (se consideramos A e B como grupos). Temos então que o núcleo $Ker(\phi)$ é um subgrupo de A. Esse subgrupo tem a seguinte relação com a operação de produto em A: para todo a em $Ker(\phi)$ e todo c em A vale que $c\,a$ e $a\,c$ são elementos de $Ker(\phi)$. De fato, se $\phi(a) = 0$ então $\phi(c\,a) = \phi(c)\,\phi(a) = \phi(c).0 = 0$ e logo $c\,a \in Ker(\phi)$, e da mesma forma mostramos que $\phi(a\,c) = 0$ e logo $a\,c \in Ker(\phi)$. Essas observações levam à seguinte definição.

Definição 4.1.11. Seja A um anel e seja $I \subset A$ um subconjunto não vazio. Dizemos que I é um *ideal* de A se para todos a e b em I vale que $a + b \in I$ e para todo c em A vale que $c\,a$ e $a\,c$ são elementos de I.

Exemplos 4.1.12.

i) Seja $\phi : A \to B$ um homomorfismo de anéis, pelo raciocínio feito logo antes da Definição acima temos que o núcleo $Ker(\phi)$ é um ideal de A.

ii) Seja M o conjunto das matrizes 2×2 com entradas inteiras, ou seja, $M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}; a,b,c,d \in \mathrm{Z} \right\}$ e seja I o subconjunto de M formado pelas matrizes onde todas as entradas são números inteiros pares. É claro que se $M_1, M_2 \in I$ então $M_1 + M_2 \in I$ e se $M_3 \in M$ é fácil verificar que $M_1 M_3, M_3 M_1 \in I$, logo I é um ideal de M.

iii) Seja Z o anel dos inteiros e seja n um número inteiro. O conjunto $n\mathrm{Z} = \{mn \mid m \in \mathrm{Z}\}$ dos múltiplos de n é um ideal de Z. De fato, a soma de dois múltiplos de n é um múltiplo de n e o produto de um inteiro qualquer por um múltiplo de n é um múltiplo de n.

iv) Num anel A o conjunto unitário $I = \{0\}$ é um ideal de A já que $0 + 0 = 0$ e para todo $c \in A$ temos $c.0 = 0$. Observe também que o próprio anel A é um ideal de A pois é fácil ver que se $I = A$ as condições na definição acima são satisfeitas. Esses dois ideais, $\{0\}$ e A, são chamados de *ideais triviais* de A.

Como esse texto traz apenas uma introdução à teoria dos anéis, a partir de agora, com o objetivo de simplificar a exposição, vamos trabalhar apenas com anéis comutativos e com unidade. Muitos resultados que vamos provar valem também para anéis não comutativos ou sem unidade, mas as provas em nosso caso serão mais simples. Assim, a partir de agora, "anel" significa "anel comutativo com unidade". Dessa forma, para provar, por exemplo, que um subconjunto não vazio I de um anel A é um ideal temos que provar que para todos a e b em I vale que $a+b \in I$ e para todo c em A vale que $c\,a$ está em I (não precisamos nos preocupar com $a\,c$ pois $a\,c = c\,a$).

Nos próximos resultados tratamos de domínios (que, como são anéis, também considerados a partir de agora como sendo comutativos com unidade)

Proposição 4.1.13. Seja A um domínio formado por um número finito de elementos. Então A é um corpo.

Prova. Seja n o número de elementos de A, escrevemos então $A = \{a_1, \ldots, a_n\}$. Seja $a_i \in A$ um elemento não nulo de A, queremos mostrar que a_i tem inverso multiplicativo em A. Observe que se $a_j \neq a_k$ então $a_i\,a_j \neq a_i\,a_k$ pois se $a_i\,a_j = a_i\,a_k$ pela lei do corte teríamos $a_j = a_k$. Assim o conjunto $\{a_i\,a_1, \ldots, a_i\,a_n\}$ tem n elementos distintos e todos pertencem a A logo temos que ter $A = \{a_i\,a_1, \ldots, a_i\,a_n\}$. Como A é anel com unidade, para algum índice t temos que ter $a_i\,a_t = 1$ e logo a_t é o inverso de a_i. □

Corolário 4.1.14. Seja p um inteiro positivo primo. Temos que $\mathbb{Z}/p\mathbb{Z}$ é um corpo.

Prova. Como p é primo temos da Proposição 3.2.9 que $\mathbb{Z}/p\mathbb{Z}$ é um domínio. Sabemos também que $\mathbb{Z}/p\mathbb{Z}$ é formado por p elementos (a saber, as classes de equivalência $0+p\mathbb{Z}$, ... , $(p-1)+p\mathbb{Z}$) logo $\mathbb{Z}/p\mathbb{Z}$ é um domínio que tem um número finito de elementos e como consequência do resultado anterior temos que $\mathbb{Z}/p\mathbb{Z}$ é corpo. □

Na matemática um Corolário é uma consequência imediata de um resultado anterior. Um Lema é um resultado auxiliar. Uma Proposição é um resultado mais forte, mas não tão forte quanto o de um Teorema.

Seja A um anel e seja $I \subset A$ um ideal de A. Sabemos que dados a e b em I vale que $a+b \in I$. Observe que $-1 \in A$ já que estamos supondo que A tem unidade 1, e como A é um grupo com relação à adição temos que ter o inverso aditivo de 1 em A também, e como I é ideal vale que $-1.a = -a \in A$. Isso mostra (confira a Proposição 2.1.3) que I é um subgrupo de A. Como A é um grupo comutativo com relação à adição temos que I é um subgrupo normal de A que, conforme já vimos, define uma relação R de equivalência sobre A dada por $(a,b) \in R$ se e somente se $b-a \in I$. Vimos também que as classes de equivalência dessa relação são os conjuntos da forma $a+I = \{a+h \mid h \in I\}$, ou seja, as classes laterais à esquerda, de I em A (veja o Lema

2.2.1 e o parágrafo seguinte a esse Lema). E sabemos ainda que tais conjuntos formam um grupo com a operação de soma de classes definida por $(a+I)+(b+I)=(a+b)+I$

(veja o parágrafo que precede o Exemplo 2.2.11). No presente caso esse grupo é claramente comutativo

pois $(b+I)+(a+I)=(b+a)+I=(a+b)+I$, já que a soma em A é comutativa.

Utilizando a notação apresentada após o Teorema 2.2.12 vamos denotar o conjunto das classes de equivalência por A/I, ou seja, $A/I=\{a+I \mid a\in A\}$. Vamos mostrar agora que, mais do que grupo comutativo, podemos dar ao conjunto A/I uma estrutura de anel (no presente caso, comutativo e com unidade) se definirmos um produto de classes laterais por $(a+I).(b+I):=(a.b)+I$. Vejamos inicialmente que esse produto está bem definido, ou seja, independe da representação escolhida para cada classe,

exatamente como fizemos após a Definição 3.2.7 quando definimos um produto de elementos de Z/nZ. Aliás aqui o raciocínio é exatamente o mesmo: supomos que $a+I=a'+I$ e $b+I=b'+I$, onde a, b, a' e b' estão em A e queremos mostrar que $(a\,b)+I=(a'b')+I$. De $a+I=a'+I$ temos que $a-a'=h_1\in I$ e de $b+I=b'+I$ temos que $b-b'=h_2\in I$ logo $(a-a')(b-b')=h_1h_2$. Expandindo o lado esquerdo e depois somando e subtraindo $a'b'$, como fizemos após a Definição 3.2.7, chegamos a $a\,b-a'b'=h_1b'+h_2a'+h_1h_2$. Como I é ideal e h_1 e h_2 são elementos de I, da definição de ideal temos que $h_1b'+h_2a'+h_1h_2\in I$. Assim $a\,b-a'b'\in I$ e portanto $(a\,b)+I=(a'b')+I$. Isso mostra que o produto está bem definido. Deixamos agora ao leitor a tarefa de verificar que A/I, munido das operações de soma e produto de

classes, é um anel que tem $0+I$ como elemento neutro da soma e $1+I$ como unidade. Esse é o chamado *anel quociente de* A *por* I.

Exemplos 4.1.15

i) Seja $\Re[X]$ o conjunto dos polinômios na variável X, ou seja, o conjunto das expressões do tipo $a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$, onde $n \in \{0, 1, 2, ...\}$ e a_0, ... , a_n são números reais. Temos que $\Re[X]$ é um anel com as operações usuais de soma e multiplicação de polinômios (que lembramos com os exemplos: $(2-3X+2X^4)+(3X+3X^4+X^5)=2+5X^4+X^5$ e $(2-3X).(X+X^2)=2(X+X^2)+(-3X)(X+X^2)=2X+2X^2+(-3)X^2+(-3)X^3=2X-X^2-3X^3$), tendo 0 como elemento neutro da soma e 1 como a unidade. Seja I o conjunto dos mútiplos de X^2+1, ou seja, $I=\{p(X).(X^2+1) \mid p(X) \in \Re[X]\}$. Assim, dados $p_1(X).(X^2+1)$ e $p_2(X).(X^2+1)$ em I e $a(X) \in \Re[X]$ temos $p_1(X).(X^2+1)+p_2(X).(X^2+1)=(p_1(X)+p_2(X))(X^2+1) \in I$ e temos ainda que $a(X)(p_1(X)(X^2+1))=(a(X)p_1(X))(X^2+1) \in I$, o que mostra que I é ideal de $\Re[X]$. Assim o anel $\Re[X]/I$ é composto pelos elementos do tipo $p(X)+I$, onde $p(X) \in \Re[X]$. Usando divisão polinomial é possível determinar precisamente as distintas classes que compõem $\Re[X]/I$. Lembramos que o grau de um polinômio não nulo é o valor da maior potência de X que efetivamente aparece no polinômio, por exemplo: $grau(1+X-4X^4)=4$, $grau(X^3+3X^7)=7$ e $grau(5)=0$. Além disso, dados

dois polinômios $p(X)$ e $g(X)$ em $\Re[X]$, com $g(X)$ não nulo, é possível encontrar polinômios $q(X)$ e $r(X)$, também em $\Re[X]$, tais que $p(X) = q(X)\,g(X) + r(X)$, onde $r(X) = 0$ ou $grau(r(X)) < grau(g(X))$. Por exemplo, tomando $p(X) = 3X^4 + X + 1$ e $g(X) = X^2 + 1$ temos $3X^4 + X + 1 = (3X^2 - 3)(X^2 + 1) + X + 4$ (e $grau(X + 4) = 1 < 2 = grau(X^2 + 1)$), tomando $p(X) = X^4 - 1$ e $g(X) = X^2 + 1$ temos $X^4 - 1 = (X^2 - 1)(X^2 + 1)$ (nesse caso $r(X) = 0$), e tomando $p(X) = X + 2$ e $g(X) = X^2 + 1$ temos $X + 2 = 0\,.\,(X^2 + 1) + (X + 2)$ (e $grau(X + 2) = 1 < 2 = grau(X^2 + 1)$). Assim, na divisão de um polinômio $p(X)$ por $X^2 + 1$ temos $p(X) = q(X)(X^2 + 1) + r(X)$ e $r(X)$ necessariamente será da forma $r(X) = a\,X + b$, com a e b números reais. Nesse caso, como $p(X) - r(X) = q(X)(X^2 + 1) \in I$ temos que $p(X) + I = r(X) + I$. Isso mostra que não precisamos considerar todas as classes $p(X) + I$, onde $p(X) \in \Re[X]$ para obter $\Re[X]/I$, podemos escrever $\Re[X]/I = \{\,(a\,X + b) + I \mid a, b \in \Re\,\}$ já que dado $p(X) \in \Re[X]$ vai existir um polinômio $r(X) = a\,X + b$ para o qual vale $p(X) + I = r(X) + I$. Além disso é fácil ver que se $a_1\,X + b_1 \neq a_2\,X + b_2$ então $(a_1\,X + b_1) + I \neq (a_2\,X + b_2) + I$ já que $(a_1\,X + b_1) - (a_2\,X + b_2)$ é um polinômio não nulo de grau no máximo 1 e logo não pode ser múltiplo de $X^2 + 1$, ou seja, $(a_1\,X + b_1) - (a_2\,X + b_2) \notin I$. Isso mostra que as distintas classes de $\Re[X]/I$ são exatamente as classes do tipo $(a\,X + b) + I$ com a e b números reais.

ii) Considere o conjunto $\mathrm{Z}[\sqrt{2}] := \{\,a + b\,\sqrt{2} \mid a, b \in \mathrm{Z}\,\}$. Observe que as operações

usuais de soma e produto de números reais são operações sobre $Z[\sqrt{2}]$, isto é, dados $a+b\sqrt{2}$ e $c+d\sqrt{2}$ em $Z[\sqrt{2}]$ temos $(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}\in Z[\sqrt{2}]$ (pois $a+c,\ b+d\ \in Z$) e $(a+b\sqrt{2}).(c+d\sqrt{2})=(a\,c+2b\,d)+(a\,d+b\,c)\sqrt{2}\in Z[\sqrt{2}]$ (pois $a\,c+2b\,d, a\,d+b\,c\in Z$). Agora não é difícil mostrar que $Z[\sqrt{2}]$ é um anel comutativo e com unidade munido dessas operações, com $0\,(=0+0\sqrt{2})$ como elemento neutro da soma e $1\ (=1+0\sqrt{2})$ como a unidade. Seja I o conjunto dos múltiplos de 2, ou seja, $I=\{2\,(a+b\sqrt{2})\ |\ a+b\sqrt{2}\in Z[\sqrt{2}]\}$. Procedendo como no exemplo acima mostra-se que I é um ideal (faça os detalhes!), portanto podemos considerar o anel quociente $Z[\sqrt{2}]/I$. Esse anel consiste de todas as classes do tipo $(a+b\sqrt{2})+I$ com $a+b\sqrt{2}$ em $Z[\sqrt{2}]$. Como fizemos com $Z/5Z$ e no exemplo acima, também aqui é possível determinar um certo conjunto de classes cuja união é igual a $Z[\sqrt{2}]/I$. De fato, seja $a+b\sqrt{2}$ em $Z[\sqrt{2}]$, se a e b são pares então $a=2a'$, $b=2b'$ e $a+b\sqrt{2}=2\,(a'+b'\sqrt{2})$ com $a'+b'\sqrt{2}\in Z[\sqrt{2}]$, assim $a+b\sqrt{2}\in I$ e $(a+b\sqrt{2})+I=0+I$. Suponha agora que a seja par e b seja ímpar, nesse caso $a=2a'$ e $b=2b'+1$, com a' e b' inteiros, e temos que $a+b\sqrt{2}=2a'+(2b'+1)\sqrt{2}=\ 2(a'+b'\sqrt{2})+\sqrt{2}$, logo $(a+b\sqrt{2})-\sqrt{2}\in I$ e portanto $(a+b\sqrt{2})+I=\sqrt{2}+I$. Assumimos agora que a seja ímpar e b seja par, nesse caso $a=2a'+1$ e $b=2b'$, com a' e b' inteiros, e temos que $a+b\sqrt{2}=(2a'+1)+2b'\sqrt{2}=1+2(a'+b'\sqrt{2})$, logo $(a+b\sqrt{2})-1\in I$ e portanto

$(a+b\sqrt{2})+I=1+I$. Por último, vamos supor que a e b sejam ímpares, nesse caso $a=2a'+1$ e $b=2b'+1$, com a' e b' inteiros, e temos que $a+b\sqrt{2}=(2a'+1)+(2b'+1)\sqrt{2}=2(a'+b'\sqrt{2})+(1+\sqrt{2})$, logo $(a+b\sqrt{2})-(1+\sqrt{2})\in I$ e portanto $(a+b\sqrt{2})+I=(1+\sqrt{2})+I$. Assim temos que $\mathrm{Z}[\sqrt{2}]/I=\{(a+b\sqrt{2})+I \mid a+b\sqrt{2}\in \mathrm{Z}[\sqrt{2}]\}=\{0+I,1+I,\sqrt{2}+I,(1+\sqrt{2})+I\}$.

Compare o que fizemos no exemplo 4.1.15 (i) e o que fizemos no (final do) Exemplo 1.1.10 (d) e veja como os raciocínios são semelhantes, ambos baseados em um argumento de divisão, e com as distintas classes sendo caracterizadas pelo resto. Isso não é uma coincidência, e pode ser explicada pelo estudo dos assim chamados *domínios euclidianos*. Até o que fizemos no exemplo 4.1.15 (ii), apesar de não envolver explicitamente algum tipo de divisão, pode ser explicado pelo estudo de domínios euclidianos. Você encontra mais sobre isso no livro *Elementos de Álgebra, de A. Garcia e Y. Lequain*, editado pelo IMPA.

Continuamos nosso estudo de homomorfismos de anéis.

Definição 4.1.16. A *imagem* de um homomorfismo de anéis $\phi: A\to B$ é o conjunto $\mathrm{Im}(\phi):=\{\phi(a)\in B \mid a\in A\}$.

Proposição 4.1.17. Seja $\phi: A\to B$ é um homomorfismo de anéis. Então $\mathrm{Im}(\phi)$ é um subanel de B.

Prova. Vamos usar o Lema 3.2.5 para provar a Proposição. Dados os elementos $\phi(a)$ e $\phi(b)$ em $\mathrm{Im}(\phi)$ temos que $\phi(a) + \phi(b) = \phi(a+b) \in \mathrm{Im}(\phi)$ e $\phi(a)\phi(b) = \phi(a\,b) \in \mathrm{Im}(\phi)$. Por outro lado $\phi(-a) + \phi(a) = \phi(-a+a) = \phi(0) = 0$, logo $-\phi(a) = \phi(-a) \in \mathrm{Im}(\phi)$ o que completa a prova. □

Definição 4.1.18. Dizemos que um homomorfismo de anéis $\phi : A \to B$ é um *isomorfismo* se ϕ é injetor e sobrejetor. Quando existe um isomorfismo entre anéis A e B dizemos que esses anéis são *isomorfos*.

Já observamos, no Exemplo 4.1.12 (i) que o núcleo de um homomorfismo é um ideal do anel que está no domínio do homomorfismo. Vamos apresentar agora um resultado para anéis análogo ao do Teorema 3.1.15.

Teorema 4.1.19 (Teorema do homomorfismo para anéis) Seja $\phi : A \to B$ um homomorfismo de anéis. Então o anel quociente $A / Ker(\phi)$ é isomorfo ao anel $\mathrm{Im}(\phi)$, e a aplicação $\psi : A / Ker(\phi) \to \mathrm{Im}(\phi)$ dada por $a + Ker(\phi) \mapsto \phi(a)$ está bem definida e é um isomorfismo entre $A / Ker(\phi)$ e $\mathrm{Im}(\phi)$.

Prova. Podemos aplicar o Teorema 3.1.15 pois A e B em particular são grupos (com a operação de adição) e como ϕ é homomorfismo de anéis, também é, em particular, homomorfismo de grupos. Assim temos que a aplicação ψ está bem definida e é um isomorfismo de grupos. Falta então apenas provar que

$\psi(\,(a + Ker(\phi)\,).(b + Ker(\phi)\,)) = \psi(\,a + Ker(\phi)\,).\psi(\,a + Ker(\phi)\,)$ mas isso é fácil já

que $\psi(\,(a+Ker(\phi))\,.\,(b+Ker(\phi))\,)=\psi(\,a\,b+Ker(\phi)\,)=\phi(a\,b)=\phi(a\,)\,\phi(b\,)=$ $\psi(\,a+Ker(\phi)\,)\,.\,\psi(\,b+Ker(\phi)\,)$. Isso prova que ψ é homomorfismo de anéis e como já sabemos que ψ é sobrejetor e injetor temos que ψ é isomorfismo de anéis. □

4.2 Ideais e corpos de frações

Nessa seção aprofundamos um pouco o estudo da relação entre ideais e anéis quocientes e mostramos uma importante construção que se pode fazer com um domínio, chamada de corpo de frações do domínio. Continuamos a supor que "anel" significa "anel comutativo com unidade" (e em particular os domínios também são comutativos com unidade).

Vimos nos Exemplos 4.1.15 ideais formados por múltiplos de um elemento no anel. Esses são um tipo especial de ideais, sobre os quais apresentamos alguns resultados.

Proposição 4.2.1. Seja A um anel e seja $a\in A$. O conjunto $(a)\coloneqq\{\,a\,b\mid b\in A\,\}$ dos múltiplos de a em A é um ideal de A.

Prova. Sejam $a\,b_1$ e $a\,b_2$ elementos de (a), temos que $a\,b_1+a\,b_2=a\,(b_1+b_2)\in(a)$. Por outro lado, dado $c\in A$ temos que $c\,(a\,b_1)=(c\,b_1)\,a\in(a)$ logo (a) é ideal de A.

□

Definição 4.2.2. Seja $I\subset A$ um ideal de A. Dizemos que I é um *ideal principal* se existe $a\in I$ tal que $I=(a)$. O elemento $a\in I$ é dito ser um *gerador* de I, e se diz também que I é gerado por a.

Exemplos 4.2.3.

i) O ideal $n\mathrm{Z} = \{mn \mid m \in \mathrm{Z}\}$ do anel dos inteiros, que apareceu no Exemplo 4.1.12 (iii) é claramente um ideal principal gerado por $n \in \mathrm{Z}$.

ii) Já observamos que, dado um anel A, o próprio anel é um ideal de si mesmo, no Exemplo 4.1.12 (iv). E observamos agora que A, como ideal, é principal já que $A = (1)$ (pois dado $a \in A$ temos $a = a.1$). O gerador de um ideal em geral não é único. Por exemplo, temos também que $A = (-1)$ já que dado $a \in A$ vale que $a = (-a).(-1)$, ou seja, qualquer elemento de A é um múltiplo de -1. O outro ideal trivial, $I = \{0\}$, também é claramente principal já que $I = (0)$. Esse é um caso em que o gerador é único até porque o ideal só tem um elemento!

iii) Seja $\Re[X]$ o anel dos polinômios com coeficientes reais (veja o Exemplo 4.1.15 (i)) e seja $I = \{\, p(X) \in \Re[X] \mid p(1) = 0 \,\}$ o conjunto dos polinômios que se anulam quando substituímos X por 1. Observe que I é um ideal de $\Re[X]$: de fato, dados polinômios $p_1(X)$ e $p_2(X)$ em I se definimos $s(X) := p_1(X) + p_2(X)$ temos que $s(1) = p_1(1) + p_2(1) = 0 + 0 = 0$ logo $s(X) \in I$, e por outro lado dado $a(X) \in \Re[X]$ e definindo $t(X) := a(X)\, p_1(X)$ temos que $t(1) = a(1).0 = 0$ logo $t(X) \in I$. Um dos polinômios que está em I é claramente $m(X) = X - 1$ e temos que qualquer múltiplo desse polinômio também está em I. Considere agora um polinômio qualquer $p(X)$

em I, conforme recordamos no Exemplo 4.1.15 (i) podemos dividir $p(X)$ por $X-1$ obtendo um quociente $q(X)$ e um resto $r(X)$ tal que $p(X)=q(X)(X-1)+r(X)$, onde $r(X)=0$ ou $grau(r(X))<grau(X-1)=1$. Assim ou $r(X)=0$ ou o grau de $r(X)$ é zero, e de qualquer forma temos que $r(X)$ é um número real $r(X)=k$. Fazendo $X=1$ na igualdade $p(X)=q(X)(X-1)+k$ e lembrando que $p(X)\in I$ temos $0=q(1).0+k$, ou seja, $k=0$. Isso mostra que $p(X)=q(X)(X-1)$, e portanto o ideal I é exatamente o conjunto dos múltiplos do polinômio $X-1$ (ou, usando a notação apresentada na Proposição 4.2.1, temos $I=(X-1)$). Descobrimos assim que I é ideal principal, embora ele não tenha sido definido como o conjunto dos múltiplos de um polinômio.

Pode-se provar que qualquer ideal no anel dos inteiros, ou no anel de polinômios $\Re[X]$ ou no anel $Z[\sqrt{2}]$ (v. Exemplo 4.1.15 (ii)) é principal. Esses fatos aparecem no estudo dos *domínios euclidianos* mencionados acima, e encontram-se demonstrados no livro de *A. Garcia e Y. Lequain* já citado.

Definição 4.2.3. Seja A um anel e $I\subset A$ um ideal de A. Dizemos que I é um *ideal primo* se sempre que $a\,b\in I$ (onde a e b são elementos de A) vale que $a\in I$ ou $b\in I$.

Exemplos 4.2.4.

i) No anel dos inteiros Z seja p um número primo e seja $I=(p)$ (ou seja, I é o ideal formado pelos múltiplos de p). Dados inteiros a e b tais que $a\,b\in I$, temos então que $a\,b$ é um múltiplo de p (em outras palavras, p divide $a\,b$) e por uma propriedade de números primos temos que ter que ou a ou b é múltiplo de p (em outras palavras, p divide a ou p divide b). Isso mostra que $I=(p)$ é um ideal primo.

ii) Seja A um anel e seja $I\subset A$ o ideal gerado por 0 (e que tem apenas esse elemento, claro). Se A for um domínio então I será ideal primo (pois se $a\,b=0$ então $a=0$ ou $b=0$) e se A não for um domínio então I não será ideal primo, pois existem em A elementos $a\neq 0$ e $b\neq 0$ tais que $a\,b=0$. □

Teorema 4.2.5. Seja A um anel e $I\subset A$ um ideal primo de A, então o anel quociente A/I e um domínio.

Prova. Já sabemos que A/I é um anel, e devemos mostrar que dados $a+I$ e $b+I$ em A/I tais que $(a+I)(b+I)=0+I$ temos que ter $a+I=0+I$ ou $b+I=0+I$. Observamos inicialmente que $(a+I)(b+I)=a\,b+I$, e de $a\,b+I=0+I$ temos que $a\,b=a\,b-0\in I$. Como I é ideal primo, de $a\,b\in I$ temos que $a\in I$ ou $b\in I$, e portanto $a+I=0+I$ ou $b+I=0+I$. □

Como último tópico do nosso curso vamos estudar uma construção que pode ser usada para se obter o corpo dos números racionais a partir dos números inteiros. Essa construção funciona para todo domínio, ou seja, a partir de um domínio vamos construir um corpo que o contém e que é o "menor" corpo com essa propriedade.

O que leva a essa construção é a constatação de que existem várias maneiras de se escrever um mesmo número racional na forma de fração. Por exemplo, temos que $\frac{2}{3}=\frac{4}{6}=\frac{14}{21}$, etc. Dadas duas frações $\frac{a}{b}$ e $\frac{c}{d}$ aprendemos que $\frac{a}{b}=\frac{c}{d}$ se e somente se $a\,d=b\,c$, e por isso sabemos que $\frac{255}{45}=\frac{2040}{360}$ e que $\frac{108}{144}\neq\frac{71}{96}$. Com a experiência que adquirimos até agora, o fato de um número racional ter diversos representantes nos leva a desconfiar que tal número talvez possa ser visto como ... uma classe de equivalência!

De fato, vimos várias vezes nesse texto que uma classe de equivalência de uma relação de

equivalência pode ser escrita de distintas formas (veja, por exemplo, a figura no Exemplo 1.1.14(c)). Vamos mostrar no que se segue que nossa suspeita é de fato verdade.

Seja D um domínio e vamos denotar por $\tilde{D}$ o conjunto dos elementos não nulos de D. Vamos definir uma relação R de equivalência sobre $D\times\tilde{D}$, o produto cartesiano de D por $\tilde{D}$. Comparando o que acabamos de escrever com a Definição 1.1.6 observe que *uma relação sobre* $D\times\tilde{D}$ significa que $D\times\tilde{D}$ faz o papel de A naquela definição, e assim a relação que queremos definir é um subconjunto de $(D\times\tilde{D})\times(D\times\tilde{D})$, ou seja, um elemento de R vai ser um par ordenado formado por pares ordenados (e portanto, um objeto do tipo $((a,b),(c,d))$). A relação vai ser definida da seguinte maneira: $((a,b),(c,d))\in R$ se e só se $a\,d=b\,c$.

Vamos verificar que essa definição de fato nos dá uma relação de equivalência sobre $D\times\tilde{D}$. Para isso temos que verificar que R satisfaz as três condições da Definição 1.1.6. Para verificar a primeira condição, como em nosso caso temos $A=D\times\tilde{D}$, o que precisamos verificar é que para todo $(a,b)\in D\times\tilde{D}$ temos que $((a,b),(a,b))\in R$, e isso de fato é verdade porque $ab=ba$. Para verificar a segunda condição precisamos verificar se o fato de termos $((a,b),(c,d))\in R$ implica que $((c,d),(a,b))\in R$. Como $((a,b),(c,d))\in R$ temos que $ad=bc$, que é o mesmo que $cb=da$, e da definição de R vemos que isso implica que $((c,d),(a,b))\in R$. Finalmente, para verificar a terceira condição da Definição 1.1.6 precisamos, em nosso caso, de mostrar que se $((a,b),(c,d))\in R$ e $((c,d),(e,f))\in R$ então vale que $((a,b),(e,f))\in R$. De $((a,b),(c,d))\in R$ temos que $ad=bc$, e de $((c,d),(e,f))\in R$ temos que $cf=de$. Multiplicando ambos os lados de $ad=bc$ por f temos $adf=bcf$, e usando no lado direito dessa igualdade que $cf=de$ temos $adf=bde$. Passando tudo para o lado esquerdo e colocando d em evidência temos $d(af-be)=0$. De $(c,d)\in D\times\tilde{D}$ temos que $d\in\tilde{D}$ e em particular $d\neq 0$. Como D é um domínio, de $d(af-be)=0$ e $d\neq 0$ temos que ter $af-be=0$ (veja a Definição 3.2.7) e logo $af=be$. Da definição de R vem dessa igualdade que $((a,b),(e,f))\in R$, o que completa a prova de que R é de fato uma relação de equivalência. Como de hábito, definimos uma relação de equivalência para trabalharmos com as classes de equivalência associadas a essa relação. No caso, temos que R vai dividir o conjunto $D\times\tilde{D}$ numa série de subconjutos, que são as

distintas classes de equivalência de seus elementos (conforme visto na Proposição 1.1.12 e nos Exemplos 1.1.14). Queremos dar uma estrutura de corpo ao conjunto das classes de equivalência de R, mas antes devemos decidir como denotar a classe de equivalência de um elemento $(a,b) \in D \times \tilde{D}$. No caso da relação de equivalência que estamos estudando ao invés de denotar a classe de equivalência de $(a,b) \in D \times \tilde{D}$ por $\overline{(a,b)}$, seguindo a notação apresentada na Definição 1.1.8, é usual denotar tal classe de equivalência por $\frac{a}{b}$. Isso vai fazer com que recuperemos igualdades familiares, por exemplo, sabemos que as classes de equivalência de (a,b) e (c,d) coincidem se e só se $((a,b),(c,d)) \in R$, ou equivalentemente, se e só se $a\,d = b\,c$ (veja a observação antes dos Exemplos 1.1.14), ou seja, temos que $\frac{a}{b} = \frac{c}{d}$ se e só se $a\,d = b\,c$.

Vamos denotar por K o conjunto das classes de equivalência da relação R, e portanto podemos escrever $K = \{\frac{a}{b} \mid a \in D, b \in \tilde{D}\}$. Queremos dar a K uma estrutura de corpo, isto é, queremos definir operações de soma e de produto em K de modo que com essas operações K seja um anel com unidade onde todos os elementos não nulos têm inverso (veja a Definição 3.2.13). As operações serão definidas da seguinte forma:

a soma de duas classes será definida por $\frac{a}{b} + \frac{c}{d} := \frac{a\,d + b\,c}{b\,d}$, e

o produto de duas classes será definido por $\frac{a}{b} \cdot \frac{c}{d} := \frac{a\,c}{b\,d}$.

Observe que, nas definições acima, como b e d estão em $\tilde{D}$ temos que b e d são não nulos, e como D é um domínio temos que bd também é um elemento não nulo, ou seja $bd \in \tilde{D}$, logo faz sentido bd aparecer no denominador tanto de $\frac{ad+bc}{bd}$ (que denota a classe de $(ad+bc,bd) \in D \times \tilde{D}$) quanto de $\frac{ac}{bd}$ (que denota a classe de $(ac,bd) \in D \times \tilde{D}$). Como definimos operações sobre classes de equivalência precisamos mostrar que o resultado não depende dos representantes escolhidos. Assim suponha que (a,b) e (a',b') estejam na mesma classe de equivalência (e portanto $\frac{a}{b}=\frac{a'}{b'}$) e que (c,d) e (c',d') estejam na mesma classe de equivalência (e portanto $\frac{c}{d}=\frac{c'}{d'}$). Vamos mostrar que $\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}$ e que $\frac{a}{b}\cdot\frac{c}{d}=\frac{a'}{b'}\cdot\frac{c'}{d'}$. De $\frac{a}{b}=\frac{a'}{b'}$ temos que $ab'=ba'$ e de $\frac{c}{d}=\frac{c'}{d'}$ temos que $cd'=dc'$. Para ver que a soma não depende dos representantes escolhidos, multiplicamos ambos os lados de $ab'=ba'$ por dd' obtendo $ab'dd'=ba'dd'$, e multiplicamos ambos os lados de $cd'=dc'$ por bb' obtendo $cd'bb'=dc'bb'$. Somando as igualdades obtidas temos $ab'dd'+cd'bb'=ba'dd'+dc'bb'$ que pode ser reescrita como $(ad+bc)b'd'=(a'd'+b'c')bd$ e essa igualdade mostra que $\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}$ ou seja, $\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}$. Para ver que o produto não depende dos representantes, multiplicamos as igualdades $ab'=ba'$ e $cd'=dc'$ obtendo $acb'd'=bda'c'$ e então podemos concluir que $\frac{ac}{bd}=\frac{a'c'}{b'd'}$, ou seja, $\frac{a}{b}\cdot\frac{c}{d}=\frac{a'}{b'}\cdot\frac{c'}{d'}$. Isso mostra que a soma e o

produto que definimos são de fato soma e produto de classes de equivalências.

Para ver que K é um anel temos que verificar as seis condições da Definição 3.2.1. Da definição das operações sobre K é fácil verificar que tanto a adição quanto a multiplicação são comutativas (faça isso, leitor!). Lembramos que D é um domínio, e em particular um anel com unidade 1 e estamos assumindo $1 \neq 0$ (veja o parágrafo antes dos Exemplos 3.2.2), assim $(0,1)$ e $(1,1)$ são elementos de $D \times \tilde{D}$ e suas classes são denotadas por $\frac{0}{1}$ e $\frac{1}{1}$, respectivamente. Temos que para todo $\frac{a}{b}$ em K vale $\frac{0}{1}+\frac{a}{b}=\frac{0.b+1.a}{1.b}=\frac{a}{b}$ e $\frac{1}{1}\cdot\frac{a}{b}=\frac{a}{b}$, logo o elemento neutro da soma é $\frac{0}{1}$ e a unidade é $\frac{1}{1}$. Deixamos a verificação da associatividade da soma e do produto para o leitor e vamos fazer aqui a verificação da distributividade. Dados $\frac{a}{b}$, $\frac{c}{d}$ e $\frac{e}{f}$ em K temos $\frac{a}{b}\cdot(\frac{c}{d}+\frac{e}{f})=\frac{a}{b}\cdot(\frac{cf+de}{df})=\frac{acf+ade}{bdf}$, por outro lado temos $\frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f}=\frac{ac}{bd}+\frac{ae}{bf}=\frac{acbf+bdae}{bdbf}$ e é fácil verficar que $\frac{acf+ade}{bdf}=\frac{acbf+bdae}{bdbf}$ mostrando que $(acf+ade)(bdbf)=(acbf+bdae)(bdf)$ (faça as contas, leitor!). Vemos assim que K é um anel (comutativo) com unidade, e para ver que K é um corpo vamos precisar do seguinte lema.

Lema 4.2.6. No anel K construído acima temos que $\frac{a}{b}=\frac{0}{1}$ se e só se $a=0$.

Prova. Se $\frac{a}{b}=\frac{0}{1}$ então vale que $a.1=b.0$, ou seja $a=0$. Se $a=0$ temos $\frac{0}{b}=\frac{0}{1}$ já que $0.1=b.0$. □

Para mostrar que K é corpo temos que mostrar que todo elemento não nulo tem inverso multiplicativo. Seja então $\frac{a}{b} \in K$ um elemento não nulo, pelo Lema acima sabemos que $a \neq 0$, ou seja, $a \in \tilde{D}$. Assim (b,a) é um elemento de $D \times \tilde{D}$, e sua classe é denotada por $\frac{b}{a}$. Temos que $\frac{a}{b} \cdot \frac{b}{a} = \frac{a.b}{b.a} = \frac{1}{1}$ sendo que a última igualdade vale porque $a\,b.1 = b\,a.1$

Isso mostra que todo elemento não nulo de K tem inverso e logo K é um corpo.

Definição 4.2.7. O corpo K construído acima é chamado de *corpo de frações do domínio* D.

Seja $\phi : D \to K$ a aplicação definida por $\phi(a) = \frac{a}{1}$ para todo $a \in D$. Temos que $\phi(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \phi(a) + \phi(b)$ (verifique a penúltima igualdade!) e $\phi(a.b) = \frac{a.b}{1} = \frac{a}{1} \cdot \frac{b}{1} = \phi(a).\phi(b)$, além disso temos que $\phi(1) = \frac{1}{1}$. Isso mostra que ϕ é um homomorfismo de anéis com unidade. Além disso se $\phi(a) = \frac{0}{1}$ então temos do Lema 4.2.6 que $a = 0$, o que mostra que $Ker(\phi) = 0$ e logo ϕ é injetor (veja a Proposição 3.1.9). É usual, quando se estuda corpos de frações, identificar os elementos de $\phi(D)$ com D e escrever $D \subset K$. Pode-se mostrar que o corpo de frações de um domínio D é o menor corpo que contém D no seguinte sentido: se K' é um corpo que contém D então existe um homomorfismo injetor de anéis $\phi : K \to K'$ de modo que $\phi(K)$ é um subcorpo de K' que contém D.

Exemplos 4.2.8. i) O exemplo clássico dessa construção é obviamente o corpo dos números racionais, que é obtido fazendo-se a construção acima tomando $D = \mathrm{Z}$, e logo $\tilde{D} = \mathrm{Z} - \{0\}$. O corpo construído então é exatamente o dos racionais, onde os elementos

são escritos como frações do tipo $\frac{a}{b}$, com a e b em Z e $b \neq 0$. A soma e a muliplicação definidas são exatamente as que conhecemos e vale que $\frac{a}{b} = \frac{c}{d}$ se e só se $ad = bc$, como aprendemos na escola.

ii) Vimos que $Z[\sqrt{2}] := \{ a + b\sqrt{2} \mid a, b \in Z \}$ é um anel (comutativo e com unidade) no Exemplo 4.1.15 (ii). É claro que $Z[\sqrt{2}]$ é um domínio pois seus elementos são, em particular, números reais e sabemos que quando multiplicamos dois reais não nulos o resultado é um real não nulo. Aplicando a construção acima para esse domínio obtemos um corpo K cujos elementos são as classes de equivalência da forma $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$, com a, b, c e d em Z e $c + d\sqrt{2} \neq 0$. Pode-se mostrar que K é isomorfo ao corpo $Q[\sqrt{2}]$ dado por $Q[\sqrt{2}] := \{ q_1 + q_2\sqrt{2} \mid q_1, q_2 \in Q \}$, onde Q é o corpo dos números racionais.

Esse texto apresentou alguns aspectos de partes da Álgebra, tendo visitado especialmente a Teoria de Grupos e a Teoria de Anéis. A Álgebra é um vasto campo na Matemática, e caso o aluno queira prosseguir em seus estudos poderia começar, por exemplo, pelo livro Tópicos de Álgebra de I. Herstein ou também pelo livro **Elementos de Álgebra,** de A. Garcia e Y. Lequain, já mencionados nesse texto. É impotante salientar que Matemática é uma disciplina que se aprende fazendo, por isso a resolução de exercícios é parte fundamental desse aprendizado. Além disso é preciso ter um treinamento para se ler corretamente um livro de Matemática, e procuramos em determinados lugares ajudar o leitor com essa leitura correta. Esperamos que o leitor desse texto tenha avançado nesse aspecto e se torne cada vez mais independente em seus estudos.

REFERÊNCIAS

BIBLIOGRAFIA BÁSICA

[1] DOMINGUES, H. H. E IEZZI, G., Álgebra Moderna, Atual Editora, São Paulo, 1982.

[2] MONTEIRO, L.H. J., Elementos de Álgebra, LTC , 1969.

[3] LANG, S., Álgebra para Graduação, Editora Ciência Moderna, Rio de Janeiro, 2008.

BIBLIOGRAFIA COMPLEMENTAR

[5] GARCIA, A.; LEQUAIN, Y. Elementos de álgebra. IMPA – Projeto Euclides, Rio de Janeiro, 2002.

[6] GONÇALVES, A. G. Introdução à álgebra. IMPA – Projeto Euclides, Rio de Janeiro, 1979.