Álgebra

Sandro Marcos Guzzo

Cascavel
5 de maio de 2024

Sumário

Introdução

Espaço para uma introdução...

Capítulo 1

Relações, aplicações e operações

Neste capítulo serão abordadas as principais propriedades envolvendo relações e aplicações. Este estudo é fundamental para os capítulos que se seguem, pois estaremos sempre em contato com algumas destas definições e suas propriedades.

1.1 Terminologia básica dos conjuntos

Começaremos nosso estudo com uma introdução aos aspectos básicos dos conjuntos, e para tanto, dispensaremos o uso de numerações para escrever as definições e resultados. Também não enunciaremos proposições ou teoremas, e as principais propriedades envolvendo estes fatos serão deixadas como exercício. Recomenda-se ao leitor com pouca habilidade neste assunto resolver tais exercícios.

Um *conjunto* é entendido como sendo uma coleção ou reunião de objetos. Tais objetos são denominados *elementos* do conjunto. Tradicionalmente representaremos conjuntos usando letras maiúsculas e elementos usando letras minúsculas.

Um conjunto ficará totalmente identificado quando forem listados todos os seus elementos, ou quando for dada uma regra ou lei de formação que premita decidir se um certo elemento faz parte do conjunto. Tanto a listagem quanto a indicação da regra são tradicionalmente feitas entre entre chaves.

Exemplo 1.1. Os conjuntos $\{a, e, i, o, u\}$ e $\{1, 2, 3\}$ estão identificados pela listagem de seus elementos. Os conjuntos $\{x; \quad x \text{ é um país da Europa}\}$ e $\{y; \quad y \text{ é um inseto}\}$ estão identificados por uma lei de formação. ■

O símbolo de reticências é comumente utilizado para dar ideia de repetição ou de continuação dos elementos de um conjunto.

Exemplo 1.2. O conjunto $\{a, b, c, \ldots, y, z\}$, é entendido como sendo o conjunto das letras do alfabeto. O conjunto $\{1, 2, 3, 4, \ldots\}$ é entendido como sendo o conjunto dos números inteiros positivos. O conjunto $\{1, 2, 3, \ldots, 1000\}$ é entendido como sendo o conjunto dos números inteiros positivos menores ou iguais a 1000. ■

Para dizer que um objeto x é um dos elementos do conjunto A, ou que o conjunto A contém o elemento x, escrevemos $x \in A$ e dizemos que "x pertence a A". Para negar este fato, isto é, para dizer que o objeto x não é um elemento do conjunto A, ou que o conjunto A não contém o elemento x, escrevemos $x \notin A$ e dizemos que "x não pertence a A".

Um conjunto que possui um único elemento é dito *conjunto unitário*. Cuidado para não confundir $\{a\}$ com $\{\{a\}\}$. O conjunto $\{a\}$ é unitário cujo único elemento é a. O conjunto $\{\{a\}\}$ é também unitário porém seu único elemento é o conjunto (também unitário) $\{a\}$. Observe que também é unitário o conjunto $\{\{a, b\}\}$.

O conjunto que não possui elemento algum, é dito um *conjunto vazio*, e representado pelo símbolo $\emptyset$, ou ainda, por $\{\ \}$. Cuidado para não confundir $\emptyset$ com $\{\emptyset\}$. O primeiro conjunto é o conjunto vazio. O segundo conjunto não é vazio e sim um conjunto unitário cujo único elemento é o conjunto vazio.

Dados dois conjuntos A e B, quando (todos) os elementos do conjunto A também são elementos do conjunto B, então escrevemos $A \subset B$, e dizemos que A está contido em B, ou ainda, A é subconjunto de B. Equivalentemente podemos escrever $B \supset A$, e dizer que B contém A. De qualquer forma, temos

$$A \subset B \quad \text{se e somente se} \quad x \in A \quad \Rightarrow \quad x \in B,$$

ou ainda pela contrapositiva equivalente,

$$A \subset B \quad \text{se e somente se} \quad x \notin B \quad \Rightarrow \quad x \notin A.$$

A relação $\subset$ é chamada de relação de *inclusão de conjuntos*. Decorre imediatamente dessa definição que $A \subset A$ para qualquer que seja o conjunto A. Também se A, B e C são conjuntos que satisfazem $A \subset B$ e $B \subset C$, então temos que $A \subset C$.

Se o conjunto A possuir algum elemento que não está no conjunto B, então escrevemos $A \not\subset B$, e dizemos que A não está contido em B, ou ainda, A não é subconjunto de B. Equivelentemente podemos escrever $B \not\supset A$ e dizer que B não contém A. De qualquer forma,

$$A \not\subset B \quad \text{se e somente se} \quad \text{existe } x \in A, \text{ com } x \notin B.$$

Consideramos também que $\emptyset \subset A$ qualquer que seja o conjunto A. Isto pode não parecer muito natural pois, ao escrever $\emptyset \subset A$, devemos pensar que todos os elementos do conjunto vazio (os quais não existem) também pertencem ao conjunto A. A ideia central de afirmar que $\emptyset \subset A$ é porque a negação disso é mais contraditória ainda. Para que $\emptyset \not\subset A$ deveria existir algum elemento $x \in \emptyset$ de forma que $x \notin A$, o que é claramente impossível.

Dois conjuntos A e B são considerados iguais, se possuem os mesmos elementos. Isto significa que o conjunto A possui (todos) os elementos de B, e reciprocamente, o conjunto B possui (todos) os elementos de A. Isto motiva a definição,

$$A = B \quad \text{se e somente se} \quad B \subset A \quad \text{e} \quad A \subset B.$$

Naturalmente para que A e B não sejam iguais, isto é, $A \neq B$, é preciso que $A \not\subset B$ ou $B \not\subset A$. Nestes termos para que $A \neq B$ é preciso que exista um elemento $x \in A$ com $x \notin B$ ou que exista $x \in B$ com $x \notin A$.

Decorre diretamente da definição de igualdade entre conjuntos que é irrelevante a ordem com que os elementos de um conjunto é listada ou a quantidade de vezes que um elemento aparece na listagem.

Exemplo 1.3. São verdadeiras as igualdades $\{a, a, b\} = \{b, a\}$. De fato, todos os elementos de um conjunto pertencem ao outro conjunto. ■

Sejam A e B dois conjuntos. A reunião dos elementos do conjunto A e dos elementos do conjunto B é o conjunto, representado por $A \cup B$, e chamado de união (ou reunião) de A com B, ou de A unido com B. Então, um elemento do conjunto $A \cup B$ é um elemento do conjunto A, ou um elemento do conjunto B. Desta forma,

$$A \cup B = \{x; \quad x \in A \quad \text{ou} \quad x \in B\},$$

e desta forma,

$$x \in (A \cup B) \quad \text{se e somente se} \quad x \in A \quad \text{ou} \quad x \in B.$$

A negação desta última afirmação nos fornece

$$x \notin (A \cup B) \quad \text{se e somente se} \quad x \notin A \quad \text{e} \quad x \notin B.$$

É consequência imediata da definição de união de conjuntos que $A \cup B = B \cup A$ e que $A \cup (B \cup C) = (A \cup B) \cup C$, quaisquer que sejam os conjuntos A, B e C. Além disso, valem as inclusões $A \subset A \cup B$ e $B \subset A \cup B$ para quaisquer conjuntos A e B.

Ao conjunto dos elementos que estão simultaneamente nos conjuntos A e B, chamaremos de intersecção de A com B, e representaremos por $A \cap B$. Temos então,

$$A \cap B = \{x; \quad x \in A \quad \text{e} \quad x \in B\},$$

e assim,

$$x \in (A \cap B) \quad \text{se e somente se} \quad x \in A \quad \text{e} \quad x \in B.$$

Como consequência disso temos que

$$x \notin (A \cap B) \quad \text{se e somente se} \quad x \notin A \quad \text{ou} \quad x \notin B.$$

É consequência imediata da definição de interseção de conjuntos que $A \cap B = B \cap A$ e que $A \cap (B \cap C) = (A \cap B) \cap C$, quaisquer que sejam os conjuntos A, B e C. Além disso, valem as inclusões $A \cap B \subset A$ e $A \cap B \subset B$ para quaisquer conjuntos A e B.

Dois conjuntos A e B são ditos *disjuntos* se não possuírem nenhum elemento em comum, isto é, se $A \cap B = \emptyset$.

Dados dois conjuntos A e B, a diferença entre A e B, representada por $(A - B)$, ou por $(A \setminus B)$, é entendida como o conjunto dos elementos que pertencem a A e não pertencem a B, isto é,

$$(A - B) = \{x; \quad x \in A \quad \text{e} \quad x \notin B\},$$

ou ainda,

$$x \in (A - B) \quad \text{se e somente se} \quad x \in A \quad \text{e} \quad x \notin B.$$

Claramente

$$x \notin (A - B) \quad \text{se e somente se} \quad x \notin A \quad \text{ou} \quad x \in B.$$

Dado um conjunto E e um subconjunto $A \subset E$, o conjunto complementar de A em E é o conjunto de todos os elementos que pertencem a E, e não pertencem a A. O conjunto complementar será denotado por $\complement A$, ou por $A^{C(E)}$, ou simplesmente A^C quando não houver possibilidade de confusão com o conjunto E. Temos então,

$$A^C = \{x \in E; \quad x \notin A\},$$

e isto significa que,

$$x \in A^C \quad \text{se e somente se} \quad x \in E \quad \text{e} \quad x \notin A.$$

Claro que

$$x \notin A^C \quad \text{se e somente se} \quad x \notin E \quad \text{ou} \quad x \in A.$$

Observe que $A^{C(E)} = (E - A)$, mas cuidado para não confundir as duas definições. A diferença é definida para quaisquer conjuntos, enquanto o complementar somente é definido quando $A \subset E$.

Dados dois conjuntos A e B, o conjunto $A \times B$ é chamado de produto cartesiano, ou produto direto, de A com B. Os elementos do conjunto $A \times B$ são pares ordenados, com a primeira coordenada um elemento do conjunto A, e a segunda coordenada um elemento do conjunto B. Simbolicamente

$$A \times B = \{(a, b); \quad a \in A, \quad b \in B\},$$

e desta forma,

$$(a, b) \in A \times B \quad \text{se e somente se} \quad a \in A \quad \text{e} \quad b \in B.$$

Evidentemente

$$(a, b) \notin A \times B \quad \text{se e somente se} \quad a \notin A \quad \text{ou} \quad b \notin B.$$

Quando tomamos o produto cartesiano de um conjunto por ele mesmo, então simplificamos a notação, escrevendo A^2 para significar $A \times A$.

1.2 Números inteiros

O conjunto dos números inteiros tem importância fundamental para nossos estudos. Nesta seção vamos relembrar algumas propriedades deste conjunto e principalmente das operações de adição e multiplicação de números inteiros.

Como veremos mais adiante, o conjunto dos números inteiros pode ser construído a partir do conjunto dos números naturais $\mathbb{N} = \{0, 1, 2, 3, \dots\}$[1], e as propriedades envolvendo as

[1]Existe muita divergência sobre o fato de que o número 0 seja um número natural. Alguns autores não o consideram assim. Para os nossos estudos vamos considerar, como indicado, que 0 é um elemento de $\mathbb{N}$.

operações de adição e multiplicação também decorrem das propriedades desta construção. Tal construção será feita em um dos próximos capítulos, mas não terá o enfoque que daremos nesta seção.

O conjunto ordenado dos números inteiros,

$$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, \dots\},$$

é dotado de (pelo menos) duas operações, chamadas de adição e de multiplicação, representadas respectivamente por $+$ e $\cdot$, que possuem as seguintes propriedades:

i) $a + (b + c) = (a + b) + c$,
ii) $a + b = b + a$,
iii) $a + 0 = 0 + a = a$,
iv) $a + (-a) = (-a) + a = 0$,
v) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
vi) $a \cdot b = b \cdot a$,
vii) $1 \cdot a = a \cdot 1 = a$,
viii) $a \cdot (b + c) = a \cdot b + a \cdot c$,
ix) $(a \cdot b) = 0$ se, e somente se, $a = 0$ ou $b = 0$,
x) Se $a \cdot b = a \cdot c$ e $a \neq 0$, então $b = c$,

para quaisquer números inteiros a, b e c.

A operação de multiplicação será subentendida quando apresentados dois números inteiros sem qualquer sinal separando-os. Isto significa que ab será entendido como $a \cdot b$, para quaisquer inteiros a e b.

As operações de adição e multiplicação, quando restritas ao conjunto dos números naturais, ainda admitem algumas destas propriedades, visto que $\mathbb{N} \subset \mathbb{Z}$. Para ser mais preciso, das propriedades listadas acima, apenas a propriedade (iv) não é satisfeita no conjunto dos números naturais.

Definição 1.1. Sejam a e b dois números inteiros com $b \neq 0$. Dizemos que b divide a ou que a é divisível por b, se e somente se, existir um número inteiro k unicamente determinado, de forma que

$$a = k \cdot b = kb. \tag{1.1}$$

Se existir o número k que satisfaz a igualdade (1.1), escrevemos $b|a$, e dizemos que a é um múltiplo de b, e que b é um divisor de a. Se não existir um número inteiro k que satisfaz a igualdade (1.1), então dizemos que b não divide a, ou que a não é múltiplo de b, e neste caso escrevemos $b \nmid a$.

Na Definição 1.1 exigimos que $b \neq 0$. Note que se $b = 0$, então a igualdade $a = bk = 0k = 0$, só ficaria válida para $a = 0$. Mas por outro lado, se também $a = 0$, então o número k não fica unicamente determinado. Em outros termos, dizemos que 0 não divide número inteiro algum. Mas note que nada impede que a seja igual a zero. De fato, se $a = 0$, para qualquer $b \neq 0$ a igualdade $a = 0 = bk$ traz $k = 0$, unicamente determinado. Por isso, dizemos que qualquer número inteiro não nulo divide 0, ou ainda, 0 é múltiplo de qualquer número inteiro não nulo.

Deste ponto em diante, sempre que usarmos a expressão $b|a$ estaremos supondo implicitamente que b é não nulo, exatamente como a definição pede.

Teorema 1.2 (Algoritmo da divisão de Euclides)**.** *Dados dois números inteiros a e $b \neq 0$, então existem $q, r \in \mathbb{Z}$, unicamente determinados, chamados respectivamente de quociente e resto da divisão Euclidiana, tais que,*

$$a = qb + r \quad com \quad 0 \leq r < |b|.$$

Prova. Primeiro mostraremos a existência dos números q e r. Vamos considerar dois casos. Primeiro o caso em que a é múltiplo de b. Neste caso, de acordo com a Definição 1.1, a igualdade fica satisfeita com $r = 0$.

Para o segundo caso, isto é, o caso em que a não é múltiplo de b, vamos separar novamente nos casos $b > 0$ e $b < 0$.

Se $b > 0$, tomemos o conjunto dos múltiplos de b,

$$M_b = \{\ldots, -4b, -3b, -2b, -b, 0, b, 2b, 3b, 4b, \ldots\}.$$

Como a não é múltiplo de b, então devemos ter que a está entre dois múltiplos consecutivos de b. Então $qb < a < (q+1)b$, donde $qb < a < qb + b$, ou equivalentemente, $0 < a - qb < b$. Tomando $r = a - qb$ temos que $a = qb + (a - qb) = qb + r$, e como $0 < a - qb < b$, vem $0 < r < b = |b|$.

Se por outro lado $b < 0$, o conjunto dos múltiplos de b agora é,

$$M_b = \{\ldots, 4b, 3b, 2b, b, 0, -b, -2b, -3b, -4b, \ldots\}.$$

Novamente, como a não é múltiplo de b, a está entre dois múltiplos consecutivos de b, isto é, $qb < a < (q-1)b$. Segue que $qb < a < qb - b$, ou equivalentemente, $0 < a - qb < -b$. Tomando $r = a - qb$, temos que $a = qb + (a - qb) = qb + r$, e já que $0 < a - qb < -b$, então, $0 < r < -b = |b|$.

Agora mostraremos que os números q e r são únicos. Supondo então q_1, q_2, r_1 e r_2 tais que $a = q_1 b + r_1 = q_2 b + r_2$. Então

$$(q_1 - q_2)b = r_2 - r_1,$$

com $0 \leq r_1, r_2 < |b|$. Isto significa que $b|(r_2 - r_1)$, e como $-b < r_2 - r_1 < b$, temos que $r_2 - r_1 = 0$, donde segue que $r_2 = r_1$. Desta forma $(q_1 - q_2)b = 0$, e como $b \neq 0$ segue que $(q_1 - q_2) = 0$, donde também $q_1 = q_2$. □

Um fato importante é que, se $b|a$, então o número r da igualdade $a = qb + r$ é igual a zero. Também, se $b \nmid a$, então o número r deve ser estritamente positivo.

Proposição 1.3. *Se a, b e c são números inteiros arbitrários (não nulos conforme o caso exigir), então valem as seguintes propriedades:*

i) $a|a$;

ii) Se $a|b$ e $b|a$, então $a = \pm b$;
iii) Se $a|b$ e $b|c$, então $a|c$;
iv) $(ac)|(bc)$, se e somente se, $a|b$;
v) Se $a|b$ e $a|c$ então, $a|(bx + cy)$ para quaisquer $x, y \in \mathbb{Z}$;
vi) Se $a|b$ e $c|d$, então $(ac)|(bd)$.

Prova. A propriedade (i) é imediata pois $a = 1a$, isto é, existe $k = 1 \in \mathbb{Z}$, tal que, $a = ka$.

Para provar (ii), como $a|b$ e $b|a$, então existem $m, n \in \mathbb{Z}$ de forma que $b = ma$ e $a = nb$. Desta forma,

$$b = ma = m(nb) = (mn)b,$$

e como $b \neq 0$, então $1 = mn$. Mas isto só será possível se $m = n = \pm 1$, donde $a = \pm b$.

Para (iii), suponhamos $a|b$ e $b|c$. Então temos, $b = am$ e $c = bn$ com $m, n \in \mathbb{Z}$. Desta forma $c = bn = (am)n = a(mn)$ e, como $(mn) \in \mathbb{Z}$, temos que $a|c$.

A condição (iv) é imediata. Observe que exigimos $ac \neq 0$ e então $c \neq 0$. Temos então que $(ac)|(bc)$ se e somente se $bc = kac$ para algum $k \in \mathbb{Z}$, se e somente se $b = ka$ para algum $k \in \mathbb{Z}$, se e somente se $a|b$.

Para provarmos (v), suponha que $a|b$ e $a|c$. Assim, existem $m, n \in \mathbb{Z}$ de forma que $b = am$ e $c = an$. Para quaisquer $x, y \in \mathbb{Z}$, temos que

$$(bx + cy) = (am)x + (an)y = a(mx) + a(ny) = a(mx + ny),$$

e como $(mx + ny) \in \mathbb{Z}$, temos que $a|(bx + cy)$.

Para a última afirmação, suponha $a|b$ e $c|d$. Então existem $m, n \in \mathbb{Z}$ que satisfazem $b = ma$ e $d = nc$. Desta forma,

$$(bd) = (ma)(nc) = (mn)(ac),$$

e como $mn \in \mathbb{Z}$, segue que $(ac)|(bd)$. Isto finaliza esta demonstração. □

Dados dois números inteiros a e b, consideremos o conjunto dos múltiplos de a, dado por,

$$M_a = \{ka; \quad k \in \mathbb{Z}\} = \{0, \pm a, \pm 2a, \pm 3a, \dots\},$$

e o conjunto dos múltiplos de b, dado por,

$$M_b = \{kb; \quad k \in \mathbb{Z}\} = \{0, \pm b, \pm 2b, \pm 3b, \dots\}.$$

É bastante claro que estes conjuntos possuem elementos em comum além de 0. Os números $\pm ab$ são elementos de M_a e também de M_b, e um deles deve ser positivo. Ao menor elemento positivo (não nulo portanto) comum aos dois conjuntos M_a e M_b, isto é, o menor número inteiro positivo, múltiplo simultaneamente de a e de b, chamaremos de *mínimo múltiplo comum* entre a e b, e representamos por $\text{mmc}(a, b)$. Se algum dos números a ou b for igual a zero, e somente neste caso, então definimos $\text{mmc}(a, b) = 0$. Como $\text{mmc}(a, b) \in M_a$ e $\text{mmc}(a, b) \in M_b$ então $a|\,\text{mmc}(a, b)$ e também $b|\,\text{mmc}(a, b)$, sempre que a e b forem não nulos. Apresentamos a seguir a definição formal de $\text{mmc}(a, b)$.

Definição 1.4. Dados dois inteiros a e b não nulos, dizemos que o natural m é o mínimo múltiplo comum entre a e b, e representamos por $m = \text{mmc}(a, b)$, se e somente se

i) $a|m$ e $b|m$;

ii) Se $a|n$ e $b|n$, para algum outro $n \in \mathbb{N}$, então $m|n$.

Se $a = 0$ ou $b = 0$, então definimos $\text{mmc}(a, b) = 0$.

A condição (i) da definição anterior diz essencialmente que $m = \text{mmc}(a, b)$ é múltiplo comum de a e de b. A condição (ii) diz que este múltiplo comum é o "menor" dentre todos, isto é, se existir algum outro múltiplo comum diferente de m, este deve ser "maior" do que m. Note que as expressões "menor" e "maior" podem ser usadas no contexto da ordem dos inteiros ou dos naturais. Isto porque, sendo m e n naturais, dizer que $m|n$ obriga $m \leq n$.

Dados dois números inteiros a e b, consideremos o conjunto dos divisores de a, dado por

$$D_a = \{\pm 1, \pm a_1, \pm a_2, \ldots, \pm a\},$$

e o conjunto dos divisores de b, dado por

$$D_b = \{\pm 1, \pm b_1, \pm b_2, \ldots, \pm b\}.$$

Estes conjuntos também possuem elementos em comum. O número 1 é um elemento que pertence aos dois conjuntos simultaneamente. Ao maior elemento, comum aos dois conjuntos D_a e D_b, isto é, o maior número inteiro, divisor ao mesmo tempo de a e de b, chamaremos de *máximo divisor comum* entre a e b, e representamos por $\text{mdc}(a, b)$. Se os números a e b forem ambos iguais a zero, e somente neste caso, definimos $\text{mdc}(a, b) = 0$. Desta forma, quando $\text{mdc}(a, b) \neq 0$, teremos $\text{mdc}(a, b)|a$ e também $\text{mdc}(a, b)|b$. Além disso, é fato também que $\text{mdc}(a, b) \geq 0$. A definição formal de $\text{mdc}(a, b)$ é a que se segue.

Definição 1.5. Dados dois inteiros a e b, não simultaneamente nulos, dizemos que o natural d é o máximo divisor comum entre a e b, e representamos por $d = \text{mdc}(a, b)$, se

i) $d|a$ e $d|b$;

ii) Se $n|a$ e $n|b$, para algum outro $n \in \mathbb{N}$, então $n|d$.

Se $a = 0$ e $b = 0$, então definimos $\text{mdc}(a, b) = 0$.

Notemos que a condição (i) da definição anterior nos diz essencialmente que $d = \text{mdc}(a, b)$ é um divisor comum de a e de b. A condição (ii) garante que este divisor comum é o "maior" dentre todos os divisores comuns, isto é, se existir algum outro divisor comum diferente de d, este deve ser "menor" do que d.

Definição 1.6. Um número inteiro p, não nulo e diferente de ± 1, é dito um número primo se o conjunto D_p, de seus divisores inteiros, é o conjunto

$$D_p = \{\pm 1, \pm p\},$$

isto é, se p é divisível apenas por ± 1 e por $\pm p$.

Definição 1.7. Dois números inteiros não nulos, a e b, são ditos primos entre si, se e somente se, $\text{mdc}(a, b) = 1$.

Proposição 1.8. *Se a e b são números inteiros não nulos, então existem números inteiros m e n tais que*

$$\text{mdc}(a, b) = ma + nb.$$

Prova. Tomemos $d = \text{mdc}(a, b)$ e S o conjunto de números positivos da forma $xa + yb$, isto é,

$$S = \{xa + yb; \quad x, y \in \mathbb{Z} \quad \text{e} \quad xa + yb > 0\}.$$

Este conjunto não é vazio pois, sendo a e b não simultaneamente nulos, então a, $-a$, b ou $-b$, está em S. Mas sendo S um conjunto de números positivos, deve haver um destes números que é o menor entre eles. Tomemos $k = \min\{S\} > 0$. Como $k \in S$, então existem $m, n \in \mathbb{Z}$ que satisfazem $k = ma + nb$. Como $d|a$ e também $d|b$ temos pela propriedade (v) da Proposição (1.3) que $d|(ma + nb) = k$, e então $d|k$.

Por outro lado, afirmamos que $k|a$. De fato, do algoritmo da divisão de Euclides, existem $q, r \in \mathbb{Z}$, de tal forma que $a = qk + r$, com $0 \leq r < k$. Mas,

$$r = a - qk = a - q(ma + nb) = a - qma - qnb = (1 - qm)a + (-qn)b.$$

Isto obriga $r = 0$ pois caso contrário, isto é, se $0 < r < k$ teríamos $r \in S$ e uma contradição com o fato de que $k = \min\{S\}$. Segue que de fato $r = 0$ e com isso $a = qk$ e $k|a$ como afirmado. Um processo análogo mostrará que $k|b$ também, e então k é um divisor comum de a e de b. Então da condição (ii) da definição de mdc temos que $k|d$. Da propriedade (ii) da Proposição 1.3, temos que $d = \pm k$, e como k e d são ambos positivos, segue que $d = k$, isto é, $\text{mdc}(a, b) = d = k = ma + nb$. □

Proposição 1.9. *Sejam a e b números inteiros não nulos. Então a e b são primos entre si, se se somente se, existem números inteiros m e n tais que*

$$ma + nb = 1.$$

Prova. Se a e b são primos entre si, então $\text{mdc}(a, b) = 1$ e a proposição anterior garante a igualdade desejada.

Reciprocamente, suponha que existem $m, n \in \mathbb{Z}$ tais que $am + bn = 1$. Seja $d = \text{mdc}(a, b) > 0$. Como $d|a$ e $d|b$, da propriedade (v) da Proposição 1.3, temos que $d|(ma + nb)$, isto é, $d|1$. Segue que d é um divisor positivo de 1, donde $d = 1$ e $\text{mdc}(a, b) = d = 1$. □

Lema 1.10. *Sejam a, b e c números inteiros, com a e b não nulos e primos entre si. Se $a|c$ e $b|c$ então $(ab)|c$.*

Prova. Da Proposição (1.9), existem números inteiros m e n tais que $1 = ma + nb$. Então temos que $(ma + nb)c = c$, ou ainda, $mac + nbc = c$. Como $a|c$ e $b|c$, do item (iv) da Proposição 1.3, temos que $(ab)|(bc)$ e $(ab)|(ac)$. Do item (v) da mesma Proposição 1.3, temos que $(ab)|(mac + nbc)$, ou seja, $(ab)|c$. □

Lema 1.11. *Sejam a e b dois números inteiros, com $d = \text{mdc}(a, b)$. Então se*

$$a = md \qquad e \qquad b = nd$$

temos que m e n são primos entre si, ou seja, $\text{mdc}(m, n) = 1$.

Prova. Suponha que $k = \text{mdc}(m, n)$, então k é divisor de m e n, isto é, $k|m$ e $k|n$. Da propriedade (iv) da Proposição 1.3 temos que $(kd)|(md)$ e $(kd)|(nd)$, isto é, $(kd)|a$ e $(kd)|b$. Mas como d é o máximo entre os divisores comuns de a e b, da definição de máximo divisor comum, devemos ter $kd|d$. Do item (iv) da Proposição (1.3) temos $k|1$, donde $k = \pm 1$. Mas devendo ser $k \geq 0$, segue que $k = 1$. □

Teorema 1.12. *Para quaisquer a e b inteiros, tem-se*

$$\text{mmc}(a, b) \cdot \text{mdc}(a, b) = |ab|.$$

Prova. Se $a = 0$ ou $b = 0$, então a igualdade é óbvia pois $\text{mmc}(a, b) = 0$, e também $ab = 0$. Suponha agora $a \neq 0$ e $b \neq 0$. Neste caso $d = \text{mdc}(a, b) > 0$ e $m = \text{mmc}(a, b) > 0$, então é suficiente verificar a expressão para a e b também positivos. Suponha então $a > 0$ e $b > 0$. Como $d|a$, $d|b$ e também $d|ab$, então existem $x, y, z \in \mathbb{Z}$, todos positivos, de forma que

$$a = xd, \qquad b = yd, \qquad \text{e} \qquad ab = zd.$$

Do Lema 1.11, x e y são primos entre si. Temos então que

$$zd = ab = (xd)(yd) = xydd,$$

e como $d \neq 0$ temos $z = xyd$, ou seja, $z = xb = ay$. Desta forma, $a|z$ e $b|z$, e da definição de mínimo múltiplo comum, $m|z$.

Por outro lado, como $d|a$ e $a|m$, então $d|m$, isto é, $m = kd$ para algum $k \in \mathbb{Z}$. Como $a|m$, isto é, $(xd)|(kd)$, então do item (iv) da Proposição 1.3 segue que $x|k$. Pelos mesmos motivos, como $b|m$ então $(yd)|(kd)$ e $y|k$. Como x e y são primos entre si, então do Lema 1.10, $(xy)|k$ e também $(xyd)|(kd)$, ou seja, $z|m$. Assim $m|z$ e $z|m$ e sendo z e m ambos positivos, concluímos que $z = m$, e portanto $ab = zd = md = \text{mmc}(a, b) \cdot \text{mdc}(a, b)$. □

Corolário 1.13. *Se a e b são dois números inteiros primos entre si, então* $\text{mmc}(a, b) = |ab|$.

Teorema 1.14 (Primeiro princípio de indução finita)**.** *Seja S um subconjunto de $\mathbb{N}$, tal que*

i) $0 \in S$,

ii) $n + 1 \in S$ *para qualquer* $n \in S$,

então $S = \mathbb{N}$.

Prova. Mostraremos que o complementar S^C, de S em $\mathbb{N}$, é vazio. Suponha por absurdo, que $S^C \neq \emptyset$. Como $\mathbb{N}$ é um conjunto que possui um elemento mínimo, então qualquer subconjunto não vazio de $\mathbb{N}$ também possui um menor elemento. Existe então um elemento $k \in S^C$ de forma que $k = \min(S^C)$. Pela hipótese (i), $k \neq 0$ pois como $0 \in S$ então $0 \notin S^C$. Então $k \geq 1$. Sendo assim, k e também $k - 1$ são ainda números naturais, e claro $k - 1 < k$. Como k é mínimo em S^C, então $k - 1 \notin S^C$, e assim $k - 1 \in S$. Mas neste caso, da hipótese (ii), temos que $(k - 1) + 1 \in S$, isto é, $k \in S$. Isto contradiz o fato de que $k \in S^C$. Decorre que S^C é vazio, e portanto $S = \mathbb{N}$. □

Em outras palavras o teorema afirma que qualquer subconjunto de $\mathbb{N}$, que contenha o 0, e contenha o sucessor de qualquer um de seus elementos, deve ser igual ao próprio $\mathbb{N}$.

Este resultado é bastante forte e útil para nós. Entretanto, é bastante provável que a maioria dos alunos não conheça o princípio de indução finita desta forma. No que se segue também precisaremos do princípio de indução finita com outra formulação. Enunciaremos então o que precisaremos.

Corolário 1.15 (Primeiro princípio de indução finita)**.** *Seja $\mathcal{A}$ uma afirmação sobre os números naturais. Suponha que*

i) $\mathcal{A}$ é verdadeira para o natural 0,

ii) $\mathcal{A}$ ser verdadeira para o natural n, implicar que $\mathcal{A}$ é verdadeira para $n+1$,

então, $\mathcal{A}$ será verdadeira para todos os naturais.

Prova. Seja P o conjunto daqueles números naturais tais que $\mathcal{A}$ seja verdadeira. De outra forma,

$$P = \{n \in \mathbb{N}; \quad \mathcal{A} \text{ é válida para } n\}.$$

É claro que $P \subset \mathbb{N}$. Da hipótese (i), temos que $\mathcal{A}$ é válida para 0, então $0 \in P$. Além disso, se $n \in P$, então $\mathcal{A}$ é válida para n, e da hipótese (ii) $\mathcal{A}$ também vale para o natural $n+1$, e então $n+1 \in P$. Notemos então que o conjunto P satisfaz as hipóteses do teorema (1.14) e portanto a sua conclusão, isto é, $P = \mathbb{N}$. Decorre então que, $\mathcal{A}$ é verdadeira para todos os números naturais. □

Outra forma bastante usual de enunciado do princípio de indução finita, é a que se segue, que não será demonstrada. A sua demonstração é também baseada no teorema (1.14), e o leitor interessado poderá fazê-lo. Embora com alguma modificação continuaremos nos referindo a este como o primeiro princípio de indução finita.

Corolário 1.16. *Suponha $\mathcal{A}$ uma afirmação sobre os números naturais. Se*

i) $\mathcal{A}$ é verdadeira para um certo $k_0 \in \mathbb{N}$ e,

ii) $\mathcal{A}$ ser verdadeira para o natural $k > k_0$, implicar que $\mathcal{A}$ é verdadeira para $k+1$,

então, a afirmação $\mathcal{A}$ será verdadeira para todo número natural maior ou igual a k_0.

Definição 1.17. Dado um número inteiro a, uma decomposição de a, ou uma fatoração de a, é um conjunto de números inteiros $\{q_1, q_2, \ldots, q_n\}$, tal que $a = q_1 q_2 \ldots q_n$. Cada um dos números inteiros q_i, $(1 \leq i \leq n)$, é dito um fator da decomposição.

Uma fatoração em si, não é algo muito importante quando não colocamos regras para os fatores da decomposição. Neste caso, um certo número inteiro pode admitir muitas decomposições. Como exemplo, consideremos o número inteiro 360. Podemos escrever,

$$360 = 9 \cdot 40 = 5 \cdot 6 \cdot 12 = 4 \cdot 6 \cdot 15 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5,$$

entre outras decomposições possíveis. Uma decomposição bastante importante é quando consideramos que os fatores da decomposição são obrigatoriamente números primos. Neste caso existirá uma só decomposição possível (exceto por reposicionamento entre os fatores). Este resultado é conhecido como Teorema Fundamental da Aritmética.

Teorema 1.18 (Teorema Fundamental da Aritmética)**.** *Se a é um número inteiro, com $a \neq 0$ e $a \neq \pm 1$, e*

$$\{p_1, p_2, \ldots, p_m\} \qquad e \qquad \{q_1, q_2, \ldots, q_n\},$$

são duas fatorações para a, com p_i e q_j primos, então $m = n$ e existe uma permutação $i \leftrightarrow j$, tal que, $p_i = q_j$ para todo $1 \leq i \leq m$.

Prova. Ver se é interessante escrever esta demonstração... □

1.3 Relações

Definição 1.19. Sejam E e F dois conjuntos não vazios. Uma *relação binária* ou simplesmente *relação* de E em F é qualquer subconjunto R de $E \times F$, isto é, R é relação de E em F, se e somente se $R \subset E \times F$.

Representamos uma relação através de letras maiúsculas (como R, S, T), ou por símbolos (como $\simeq$, $\sim$, $\approx$, $\leq$, $\preccurlyeq$), embora os símbolos sejam preferidos para representar relações de equivalência ou de ordem, que veremos mais adiante. Note que, embora E e F sejam não vazios, nada impede que tenhamos uma relação vazia de E em F.

Para qualquer par ordenado $(a, b) \in R$ dizemos que $a \in E$ está relacionado com $b \in F$ pela relação R. Podemos também escrever aRb para dizer que $(a, b) \in R$. Para indicar que o elemento $a \in E$ não está relacionado com o elemento $b \in F$, escrevemos $(a, b) \notin R$, ou $a \not R b$.

Poderíamos definir de uma forma mais geral, relações n-árias, como subconjuntos

$$R \subset E_1 \times E_2 \times \cdots \times E_n,$$

onde os n conjuntos E_i, $i = 1, 2, \ldots, n$, são todos não vazios. Como não é do nosso interesse o estudo de relações que não sejam binárias, usaremos o termo *relação* e entenderemos que sempre será uma relação binária.

Definição 1.20. Seja R uma relação de E em F. O *domínio* de R é o subconjunto de E, denotado por $D(R)$, formado por todos os elementos de E que estão relacionados com algum elemento de F. Simbolicamente

$$D(R) = \{a \in E; \quad (a, b) \in R \quad \text{para algum} \quad b \in F\}.$$

Em outras palavras, o domínio de uma relação é o conjunto de todos os elementos de E que figuram na primeira coordenada de cada par de elementos de R.

Definição 1.21. Dada uma relação R de E em F, a *imagem* de R é o subconjunto de F, denotado por $Im(R)$, formado por todos os elementos de F que estão relacionados por algum elemento de E. Simbolicamente

$$Im(R) = \{b \in F; \quad (a, b) \in R \quad \text{para algum} \quad a \in E\}.$$

Em outras palavras, a imagem de uma relação é o conjunto de todos os elementos de F que figuram na segunda coordenada de cada par de elementos de R.

Exemplo 1.4. Sobre os conjuntos, $E = \{-1, 0, 1\}$ e $F = \{0, 1, 2, 3, 4\}$, podemos definir as seguintes relações de E em F:

$R_1 = \{(-1,0),(-1,1),(-1,2),(-1,3),(-1,4)\}$,
$R_2 = \{(0,0)\}$,
$R_3 = \{(-1,2),(0,3),(1,4)\}$.

Nestes casos, temos
$D(R_1) = \{-1\}$, e $Im(R_1) = \{0,1,2,3,4\} = F$,
$D(R_2) = Im(R_2) = \{0\}$,
$D(R_3) = \{-1,0,1\} = E$, e $Im(R_3) = \{2,3,4\}$. ■

Exemplo 1.5. Considere a relação R, de $E = \{2,3,5\}$ em $F = \{5,7,10,12,15\}$, dada pela lei de formação

$$xRy \quad \Leftrightarrow \quad (x,y) \in R \quad \Leftrightarrow \quad x|y,$$

isto é, x está relacionado com y, se e somente se, x é um divisor de y. Neste caso,

$$R = \{(2,10),(2,12),(3,12),(3,15),(5,5),(5,10),(5,15)\},$$

e para esta relação temos $D(R) = \{2,3,5\}$ e $Im(R) = \{5,10,12,15\}$. ■

Quando os conjuntos E e F são subconjuntos de $\mathbb{R}$ é comum (e útil) a representação de uma relação R sob a forma de um gráfico cartesiano. Quando os conjuntos E e F são constituídos de poucos elementos é útil a representação da relação R através de um diagrama de flechas (Diagrama de Venn).

Definição 1.22. Seja R uma relação de E em F. A *relação inversa* de R, denotada por R^{-1}, é uma relação de F em E e definida por,

$$R^{-1} = \{(b,a) \in F \times E; \quad (a,b) \in R\}.$$

Isto significa que aRb, se e somente se, $bR^{-1}a$, ou ainda, $(a,b) \in R$, se e somente se, $(b,a) \in R^{-1}$. Observe também que $R = \emptyset$, se e somente se, $R^{-1} = \emptyset$. A representação gráfica de R^{-1} caracteriza-se por uma reflexão dos pontos $(a,b) \in R$ pela reta $y = x$. A representação de R^{-1} pelo diagrama de flechas, caracteriza-se por uma inversão no sentido das flechas.

Proposição 1.23. *Se R é uma relação de E em F, então*
i) $D(R) = Im(R^{-1})$,
ii) $D(R^{-1}) = Im(R)$,
iii) $(R^{-1})^{-1} = R$.

Prova. Os três itens são trivialmente satisfeitos se R for uma relação vazia, pois neste caso, todos os conjuntos envolvidos serão vazios também. Suponhamos então R não vazia. Para (i) temos,

$$\begin{aligned} x \in D(R) \quad &\Leftrightarrow \quad (x,y) \in R \quad \text{para algum} \quad y \in F \\ &\Leftrightarrow (y,x) \in R^{-1} \quad \text{para algum} \quad y \in F \quad \Leftrightarrow \quad x \in Im(R^{-1}), \end{aligned}$$

mostrando que $D(R) = Im(R^{-1})$. A prova de (ii) é análoga. Para (iii), temos

$$(x,y) \in R \quad \Leftrightarrow \quad (y,x) \in R^{-1} \quad \Leftrightarrow \quad (x,y) \in (R^{-1})^{-1},$$

o que encerra a demonstração. □

Definição 1.24. Dadas as relações R de E em F, e S de F em G, definimos a *relação composta* de R com S, como sendo a relação de E em G, denotada por $(S \circ R)$, dada por

$$(S \circ R) = \{(x, z) \in E \times G; \quad \text{existe} \quad y \in F \quad \text{com} \quad (x, y) \in R \quad \text{e} \quad (y, z) \in S\}.$$

Observe que se $R = \emptyset$, ou $S = \emptyset$, então $(S \circ R) = \emptyset$. Entretanto, é possível que tenhamos $(S \circ R) = \emptyset$ sem que necessariamente $R = \emptyset$ ou $S = \emptyset$. Como exemplo disto, considere $E = F = G = \{0, 1, 2\}$, e $R = \{(0, 1)\}$ e $S = \{(0, 2)\}$. É obvio que R e S são não vazias, mas $(S \circ R) = \emptyset$.

Proposição 1.25. *Sejam E, F e G conjuntos não vazios Se R e S são relações de E em F e de F em G respectivamente, então*

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

Prova. Mostraremos primeiramente que $(S \circ R)^{-1} \subset R^{-1} \circ S^{-1}$. Suponha $(z, x) \in (S \circ R)^{-1}$, então $(x, z) \in (S \circ R)$, e da definição de composta, existe $y \in F$ tal que,

$$(x, y) \in R \quad \text{e} \quad (y, z) \in S,$$

donde

$$(z, y) \in S^{-1} \quad \text{e} \quad (y, x) \in R^{-1},$$

e novamente da definição de composta, $(z, x) \in (R^{-1} \circ S^{-1})$. Para mostrar a segunda inclusão, $(R^{-1} \circ S^{-1}) \subset (S \circ R)^{-1}$, é suficiente tomar as implicações anteriores na ordem inversa. Segue a igualdade entre os conjuntos. □

Vamos agora estudar as principais propriedades envolvidas em uma relação. Este estudo faz-se necessário para o desenvolvimento de relações de equivalência, que é um dos principais objetivos nesta seção. Para isto, consideremos que os conjuntos E e F são iguais, isto é, as relações R são relações de um conjunto E em E, e neste caso dizemos simplesmente que R é uma relação em E, ou sobre E.

Definição 1.26. Uma relação R, sobre um conjunto não vazio E é dita *reflexiva* se xRx para todo $x \in E$, ou equivalentemente se $(x, x) \in R$, para todo $x \in E$.

Isto significa que qualquer elemento de E se relaciona consigo mesmo através de R. Dizer que R não é reflexiva significa que existe pelo menos um elemento x de E tal que $(x, x) \notin R$.

Definição 1.27. Dizemos que uma relação R, sobre um conjunto não vazio E, é *simétrica* se, para quaisquer $x, y \in E$ com xRy, tem-se também yRx, ou equivalentemente, se $(x, y) \in R$, então $(y, x) \in R$.

Isto significa que para qualquer par ordenado (x, y) que esteja na relação, deverá ser encontrado o par simétrico (y, x) também na relação. Para que R não seja simétrica, basta que exista um par (x, y) em R e o par simétrico (y, x) não esteja em R.

Definição 1.28. Uma relação R sobre um conjunto não vazio E é dita *antissimétrica* se, para todos $x, y \in E$ com xRy e yRx tem-se obrigatoriamente $x = y$, ou ainda, se $(x, y) \in R$ e $(y, x) \in R$ então $x = y$.

Esta definição nos diz que os únicos pares (x, y) em R de forma que (y, x) também estejam em R devem ser os pares com coordenadas iguais. Se forem encontrados elementos distintos $x, y \in E$ de forma que ambos os pares (x, y) e (y, x) estejam em R, então R não é antissimétrica.

A contrapositiva da definição anterior é mais fácil de ser verificada. Dados $x, y \in E$ com $x \neq y$, a relação R é antissimétrica se, e somente se, $(x, y) \notin R$ ou $(y, x) \notin R$. Isto significa que para elementos distintos x e y de E, pelo menos um dos pares, (x, y) ou (y, x), não deve ser encontrado na relação.

Cuidado: dizer que R não é simétrica não significa que R é antissimétrica, e vice-versa. São duas definições distintas, que não se excluem mutuamente. Veja o próximo exemplo.

Exemplo 1.6. No conjunto $A = \{a, b, c\}$ definimos as relações $R_1 = \{(a, a), (b, b), (c, c)\}$, $R_2 = \{(a, b), (b, a)\}$, $R_3 = \{(a, b), (b, b)\}$ e $R_4 = \{(a, b), (a, c), (c, a)\}$. Nestes termos, R_1 é simétrica e é antissimétrica. R_2 é simétrica e não é antissimétrica. R_3 não é simétrica e é antissimétrica. R_4 não é simétrica e não é antissimétrica. ■

Definição 1.29. Uma relação R sobre um conjunto não vazio E, é dita *transitiva* se para todos $x, y, z \in E$ com xRy e yRz, tem-se também xRz, isto é, se $(x, y) \in R$ e $(y, z) \in R$ então $(x, z) \in R$.

Para que R não seja transitiva, basta encontrar dois pares de elementos (x, y) e (y, z) ambos em R de forma que (x, z) não esteja em R.

Exemplo 1.7. Considere E o conjunto de todas as retas do plano. Em E defina as relações R e S dadas por

$$rRs \quad \Leftrightarrow \quad r \parallel s \qquad \text{e} \qquad rSs \quad \Leftrightarrow \quad r \perp s,$$

ou seja, R é a relação de paralelismo entre retas e S é a relação de perpendicularidade entre retas do plano. Temos então que, R é reflexiva, pois $r \parallel r$ para qualquer reta r do plano, R é simétrica pois se $r \parallel s$ então é claro que $s \parallel r$, R não é antissimétrica, pois retas distintas r e s podem cumprir $r \parallel s$ e $s \parallel r$, e R é transitiva, pois se $r \parallel s$ e $s \parallel t$ temos obrigatoriamente $r \parallel t$. Para a relação S, temos que S não é reflexiva pois para qualquer reta r do plano $r \not\perp r$, S é simétrica pois se $r \perp s$ então é claro que $s \perp r$, S não é antissimétrica, pois retas distintas r e s podem cumprir $r \perp s$ e $s \perp r$, e S não é transitiva, pois se $r \perp s$ e $s \perp t$ não garante que $r \perp t$. Muito pelo contrário, teremos $r \parallel t$. ■

Exemplo 1.8. Dado $E = \{a, b, c, d\}$ e a relação R em E, definida por

$$R = \{(a, a), (b, b), (c, c), (a, c), (c, d), (a, d)\},$$

então, R não é reflexiva pois $d \in E$ e $(d, d) \notin R$, R não é simétrica pois $(c, d) \in R$ e no entanto $(d, c) \notin R$, R é antissimétrica pois os únicos pares (x, y) de R, em que o simétrico (y, x) também está em R, são os pares com as duas coordenadas iguais, e R é transitiva pois

$$\begin{aligned}
&(a, a), (a, c) \in R, \quad \text{e também} \quad (a, c) \in R;\\
&(a, a), (a, d) \in R, \quad \text{e também} \quad (a, d) \in R;\\
&(c, c), (c, d) \in R, \quad \text{e também} \quad (c, d) \in R;
\end{aligned}$$

$$(a,c),(c,c) \in R, \quad \text{e também} \quad (a,c) \in R;$$
$$(a,c),(c,d) \in R, \quad \text{e também} \quad (a,d) \in R.$$

■

Exemplo 1.9. Considere E qualquer conjunto (não vazio) e $R = \emptyset$ uma relação sobre E. Temos que, R não é reflexiva pois existe $x \in E$ e $(x,x) \notin R$, R é simétrica pois para negar este fato deveríamos ter $(a,b) \in R$ e $(b,a) \notin R$, R é antissimétrica pois para negar este fato, deveríamos ter pares (x,y) e (y,x) de R com elementos distintos x e y de E, e R é transitiva pois para negar este fato deveríamos ter algum (a,c) e algum (c,d) em R com $(a,d) \notin R$. ■

Proposição 1.30. *Se R é uma relação não vazia sobre um conjunto E, então*

i) R é reflexiva, se e somente se, R^{-1} é reflexiva,

ii) R é simétrica, se e somente se, R^{-1} é simétrica,

iii) R é antissimétrica, se e somente se, R^{-1} é antissimétrica,

iv) R é transitiva, se e somente se, R^{-1} é transitiva.

Prova. Mostraremos primeiro as quatro implicações diretas. Para (i), suponha que R é reflexiva. Então para todo $x \in E$, temos $(x,x) \in R$, ou ainda, $(x,x) \in R^{-1}$. Sendo assim, R^{-1} é reflexiva. Para mostrarmos (ii), suponha R simétrica. Se $(x,y) \in R^{-1}$, então $(y,x) \in R$ e como R é simétrica, $(x,y) \in R$ e então $(y,x) \in R^{-1}$ e segue que R^{-1} é simétrica. Para (iii), seja R antissimétrica. Se $(x,y),(y,x) \in R^{-1}$, então $(y,x),(x,y) \in R$, e sendo R antissimétrica segue que $x = y$ mostrando que R^{-1} é também antissimétrica. Para (iv), suponhamos R transitiva e tomemos $(x,y),(y,z) \in R^{-1}$. Então $(z,y) \in R$ e $(y,x) \in R$. Como R é transitiva, segue que $(z,x) \in R$ e portanto $(x,z) \in R^{-1}$ o que mostra que R^{-1} é transitiva. Para as quatro implicações contrárias, basta usar as respectivas implicações diretas e o fato de que $(R^{-1})^{-1} = R$. □

1.4 Relações de equivalência

Definição 1.31. Uma relação R sobre um conjunto não vazio E é dita uma *relação de equivalência* sobre E, se R for reflexiva, simétrica e transitiva. Isto é,

i) para todo $x \in E$, tem-se xRx,

ii) para todos $x, y \in E$ tais que xRy, tem-se yRx,

iii) para todos $x, y, z \in E$ tais que xRy e yRz, tem-se xRz.

Uma relação de equivalência determina em um conjunto, uma "lei", que permite decidir quando dois elementos deste conjunto são equivalentes, ou seja, dois elementos são iguais quando observados por esta relação. Deste ponto em diante, usaremos letras maiúsculas para representar uma relação de equivalência somente quando a relação for expressa como subconjunto de $E \times E$, uma vez que as letras maiúsculas são mais comuns para representar conjuntos. Usaremos símbolos como $\sim$, $\simeq$, $\approx$, $\cong$, $\equiv$, entre outros possíveis, para representar relações de equivalência.

Exemplo 1.10. A relação $R = \emptyset$ sobre qualquer conjunto E não vazio, não é relação de equivalência, pois como já verificado, R não é reflexiva. ■

Exemplo 1.11. Seja $E = \mathbb{Z}^*$ o conjunto dos números inteiros não nulos, e a relação $R : xRy \Leftrightarrow x|y$, a relação de divisibilidade entre inteiros (não nulos). R não é relação de equivalência. De fato, R é reflexiva, pois $x|x$ para todo inteiro não nulo x. Também R é transitiva pois se $x|y$ e $y|z$, então claramente $x|z$. Entretanto, R não é simétrica, pois podemos obter dois números inteiros não nulos x e y, de forma que $x|y$ e no entando $y \nmid x$. ■

Exemplo 1.12. Tomando $E = \{B; B \text{ é subconjunto de } \mathbb{R}^2\}$ e R é a relação de inclusão de conjuntos, isto é, $ARB \Leftrightarrow A \subset B$. R não é relação de equivalência, pois embora R seja reflexiva e transitiva, R não é simétrica. De fato, é possível obter dois conjuntos A e B, satisfazendo $A \subset B$, sem que necessariamente $B \subset A$. ■

Exemplo 1.13. Considere o conjunto $E = \mathbb{Z} \times \mathbb{Z}^* = \{(a, b); \quad a, b \neq 0 \in \mathbb{Z}\}$, e a relação $\equiv$ dada por

$$(a, b) \equiv (c, d) \quad \Leftrightarrow \quad ad = bc.$$

Esta é a conhecida relação de igualdade entre frações. É uma relação de equivalência. Para tornar este importante exemplo completo, vejamos os detalhes. Para qualquer $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, temos claramente $ab = ba$, e da definição de $\equiv$, temos $(a, b) \equiv (a, b)$, o que mostra a reflexividade de $\equiv$. Sejam agora $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$ tais que $(a, b) \equiv (c, d)$. Então $ad = bc$, e assim, tem-se também que $cb = da$. Segue da definição de $\equiv$ que $(c, d) \equiv (a, b)$. Com isso $\equiv$ é simétrica. Para finalizar, sejam $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z}^*$ tais que $(a, b) \equiv (c, d)$ e também $(c, d) \equiv (e, f)$. Então temos $ad = bc$, e também, $cf = de$. Multiplicando a primeira igualdade por f e a segunda por b, temos que $adf = bcf$ e $bcf = bde$. Destas duas igualdades temos que $adf = bde$, e como $d \neq 0$ temos, do axioma (x) dos números inteiros, que $af = be$. Isto significa que $(a, b) \equiv (e, f)$, o que mostra a transitividade de $\equiv$. ■

Notemos então que, se $\sim$ é a uma relação de equivalência sobre um conjunto $E \neq \emptyset$, dado qualquer elemento $a \in E$, da reflexividade de $\sim$, temos que $a \sim a$. Isto significa que pelo menos o elemento a deve estar relacionado consigo mesmo. Mas pode ocorrer que outros elementos do conjunto E também estejam relacionados com o elemento a. A coleção de todos os elementos de E que estão relacionados com este elemento a é chamada de classe de equivalência de $a \in E$. A próxima definição formaliza este conceito.

Definição 1.32. Seja $\sim$ uma relação de equivalência sobre um conjunto não vazio E. A *classe de equivalência* de um elemento $a \in E$, módulo $\sim$, é o subconjunto de E denotado por $\overline{a}$ e dado por

$$\overline{a} = \{x \in E; \quad x \sim a\},$$

ou seja, $\overline{a}$ é o subconjunto de todos os elementos relacionados com a por $\sim$.

Uma classe de equivalência é então um conjunto que reúne todos os elementos que são equivalentes entre si no conjunto E. Observe que como $\sim$ é uma relação reflexiva, então para qualquer $a \in E$ tem-se obrigatoriamente $a \sim a$ e da definição anterior segue que $a \in \overline{a}$. O conjunto de todas as classes de equivalência módulo $\sim$, de E, indicado por $\frac{E}{\sim}$, é chamado de *conjunto quociente* de E pela relação $\sim$. Então

$$\frac{E}{\sim} = \{\overline{a}; \quad a \in E\}.$$

Proposição 1.33. *Seja $\sim$ uma relação de equivalência sobre $E \neq \emptyset$ e $a, b \in E$. São equivalentes as afirmações*

i) $a \sim b$,
ii) $a \in \overline{b}$,
iii) $b \in \overline{a}$,
iv) $\overline{a} = \overline{b}$.

Prova. Como a relação $\sim$ é simétrica, decorre imediatamente da definição de classe de equivalência que

$$a \in \overline{b} \quad \Leftrightarrow \quad a \sim b \quad \Leftrightarrow \quad b \sim a \quad \Leftrightarrow \quad b \in \overline{a},$$

e desta forma, (i), (ii) e (iii) são equivalentes.

Mostraremos agora que (i) e (iv) são equivalentes. Suponha então $a \sim b$, e mostraremos a dupla inclusão dos conjuntos $\overline{a}$ e $\overline{b}$. Seja $x \in \overline{a}$. Então $x \sim a$, e como $a \sim b$, temos da transitividade de $\sim$, que $x \sim b$. Segue que $x \in \overline{b}$, e isto prova que $\overline{a} \subset \overline{b}$. Suponha agora $x \in \overline{b}$, ou equivalentemente $x \sim b$. Como $a \sim b$, da simetria de $\sim$ temos que $b \sim a$ também. Como $x \sim b$ e $b \sim a$, da transitividade de $\sim$ temos que $x \sim a$. Assim, $x \in \overline{a}$ mostrando que $\overline{b} \subset \overline{a}$, e conseguentemente a igualdade $\overline{a} = \overline{b}$. Suponha agora $\overline{a} = \overline{b}$. Como claramente temos $a \in \overline{a}$, então temos também $a \in \overline{b}$, e da definição de classe de equivalência $a \sim b$. Isto encerra a demonstração. □

O próximo resultado é muito importante para os estudos que virão. Em sua essência, o próximo resultado diz que o conjunto E pode ser escrito como reunião de classes de equivalência, duas a duas disjuntas.

Proposição 1.34. *Seja $\sim$ uma relação de equivalência sobre um conjunto E não vazio. Então temos que*

i) Para todo $a \in E$, $\overline{a} \neq \emptyset$,
ii) Para todos $a, b \in E$, ou $\overline{a} = \overline{b}$ ou $\overline{a} \cap \overline{b} = \emptyset$,
iii) $E = \bigcup_{a \in E} \overline{a}$.

Prova. O item (i) é imediato, pois como $\sim$ é relação de equivalência, então $\sim$ é reflexiva. Isto significa que para qualquer $a \in E$, temos $a \sim a$, e desta forma que, $a \in \overline{a}$, para todo $a \in E$.

Provaremos agora (ii). Suponha que $\overline{a} \cap \overline{b} \neq \emptyset$, e mostraremos que ocorre obrigatoriamente a igualdade entre as classes $\overline{a}$ e $\overline{b}$. Já que a intersecção é não vazia, então existe $x \in E$ que satisfaz $x \in \overline{a}$ e $x \in \overline{b}$. Então, da proposição anterior, temos $\overline{x} = \overline{a}$ e também $\overline{x} = \overline{b}$. É claro então que $\overline{a} = \overline{x} = \overline{b}$.

Para provar (iii), mostraremos a dupla inclusão dos conjuntos. Observemos que dado qualquer $x \in E$ temos que $x \in \overline{x}$, e portanto x está em alguma classe de equivalência de E. Como consequência disto, x estará na união de todas as classes de equivalência de E, isto é, $x \in \bigcup_{a \in E} \overline{a}$. Isto mostra a inclusão $E \subset \bigcup_{a \in E} \overline{a}$. Para a inclusão contrária, note que cada classe de equivalência $\overline{a}$ de um elemento $a \in E$, é formada apenas por elementos de E. A união de todas as classes continuará sendo formada por elementos de E. Desta forma, é imediato que $\bigcup_{a \in E} \overline{a} \subset E$. Isto termina esta demonstração. □

Exemplo 1.14. Consideremos o conjunto $E = \{a, b, c, d\}$ e a relação de equivalência R sobre E determinada por seus pares ordenados

$$R = \{(a,a), (b,b), (c,c), (d,d), (a,b), (b,a), (c,d), (d,c)\}.$$

As classes de equivalência, dos elementos de E, são então $\overline{a} = \{a, b\}$, $\overline{b} = \{b, a\} = \overline{a}$, $\overline{c} = \{c, d\}$, e $\overline{d} = \{d, c\} = \overline{c}$. Temos portanto apenas duas classes de equivalência distintas. Daí

$$\frac{E}{R} = \{\{a, b\}, \{c, d\}\} = \{\overline{a}, \overline{c}\}.$$

■

Exemplo 1.15. Considerando $A = \{1, 2, 3, 4, 5, 6\}$ e a relação $\approx$ dada por

$$x \approx y \qquad \Leftrightarrow \qquad 2|(x - y).$$

Como $2|(x - x)$ para qualquer $x \in A$, então $x \approx x$ para todo $x \in A$ e temos a reflexividade de $\approx$. Dados $x, y \in A$ com $x \approx y$, então da definição da relação $2|(x - y)$. Das propriedades de divisibilidade temos $2|(y - x)$ e então $y \approx x$, donde $\approx$ é simétrica. Sejam $x, y, z \in A$ com $x \approx y$ e $y \approx z$, então da definição da relação, $2|(x - y)$ e $2|(y - z)$. Das propriedades de divisibilidade, segue que $2|((x-y)+(y-z))$, ou melhor $2|(x-z)$ e então $x \approx z$, e fica mostrada a transitividade de $\approx$.

As classes de equivalência são portanto

$$\begin{array}{ll} \overline{1} = \{1, 3, 5\}, & \overline{2} = \{2, 4, 6\}, \\ \overline{3} = \{1, 3, 5\} = \overline{1}, & \overline{4} = \{2, 4, 6\} = \overline{2}, \\ \overline{5} = \{1, 3, 5\} = \overline{1}, & \overline{6} = \{2, 4, 6\} = \overline{2}. \end{array}$$

Desta forma,

$$\frac{A}{\approx} = \{\overline{1}, \overline{2}\}.$$

■

O próximo exemplo é uma generalização deste último. Constitui um dos exemplos mais importantes de relação de equivalência, chamada *congruência módulo m nos inteiros.*

Exemplo 1.16. No conjunto dos números inteiros $\mathbb{Z}$, escolhemos um inteiro arbitrário $m \geq 2$, e definimos a relação $\sim$ dada por

$$x \sim y \quad \Leftrightarrow \quad x \equiv y (\text{mod } m) \quad \Leftrightarrow \quad m|(x - y).$$

A expressão $x \equiv y (\text{mod } m)$ deve ser lida como: "x é congruente a y módulo m", ou ainda, "x é equivalente a y módulo m". É fácil ver que esta relação é de equivalência. Vejamos os detalhes. Primeiro temos que $m|0$ e então $m|(x - x)$ para todo $x \in \mathbb{Z}$, logo, $x \sim x$ para todo $x \in \mathbb{Z}$, isto é, $\sim$ é reflexiva. Suponha agora $x \sim y$, e então, $m|(x - y)$. Do item (v) da proposição (1.3), m divide qualquer múltiplo de $(x - y)$. Em particular $m|((-1) \cdot (x - y))$, ou ainda, $m|(y - x)$. Desta forma, $y \sim x$, mostrando que $\sim$ é simétrica. Também, sejam $x, y, z \in \mathbb{Z}$ com $x \sim y$ e $y \sim z$, isto é, $m|(x - y)$ e $m|(y - z)$. Então temos do item (v) da proposição (1.3)

que m divide a soma $(x-y)+(y-z)$, isto é, $m|(x-z)$ e temos portanto $x \sim z$, mostrando a transitividade de $\sim$. Desta forma $\sim$ é de fato uma relação de equivalência.

Observe que dizer que $x \sim y$, ou equivalentemente $m|(x-y)$, significa que os restos da divisão euclidiana de x e de y por m, são iguais. De fato, do algoritmo de Euclides, temos que existem q_1, q_2, r_1 e r_2 tais que $x = q_1m + r_1$ e $y = q_2m + r_2$, com $0 \leq r_1, r_2 < m$. Como $m|(x-y)$ então $m|[(q_1-q_2)m+(r_1-r_2)]$. Como m divide uma soma, e divide uma das parcelas desta soma, então obrigatoriamente, m divide a outra parcela desta soma também. Isto é, $m|(r_1-r_2)$ e em outras palavras (r_1-r_2) é um múltiplo de m. Mas como $0 \leq r_1, r_2 < m$, então $-m < r_1 - r_2 < m$, e o único múltiplo de m que está estritamente entre $-m$ e m é 0. Segue que $r_1 - r_2 = 0$, ou ainda, $r_2 = r_1$, provando a nossa afirmação. A recíproca é obviamente verdadeira, isto é, se os restos r_1 e r_2 são iguais, então $(x-y) = q_1m+r_1-q_2m-r_2 = (q_1-q_2)m$ e então $m|(x-y)$.

Assim, podemos construir as classes de equivalência $\overline{n}$ para cada $n \in \mathbb{Z}$, que consiste de todos os números inteiros relacionados com n, isto é, todos os números inteiros que deixam o mesmo resto que n na divisão euclidiana por m. Temos então,

$$\begin{aligned}
\overline{0} &= \{0, \pm m, \pm 2m, \pm 3m, \dots\} \\
\overline{1} &= \{1, 1 \pm m, 1 \pm 2m, 1 \pm 3m, \dots\} \\
\overline{2} &= \{2, 2 \pm m, 2 \pm 2m, 2 \pm 3m, \dots\} \\
&\vdots \\
\overline{m-1} &= \{m-1, (m-1) \pm m, (m-1) \pm 2m, (m-1) \pm 3m, \dots\} \\
&= \{-1, -1 \pm m, -1 \pm 2m, -1 \pm 3m, \dots\} = \overline{-1} \\
\overline{m} &= \{m, m \pm m, m \pm 2m, m \pm 3m, \dots\} \\
&= \{0, \pm m, \pm 2m, \pm 3m, \dots\} = \overline{0}
\end{aligned}$$

e a partir daí as classes se repetem, e portanto, temos m classes de equivalência distintas, chamadas classes de equivalência módulo m. O conjunto destas classes de equivalência, denotado por $\mathbb{Z}_m$, é

$$\mathbb{Z}_m = \frac{\mathbb{Z}}{\sim} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}.$$

■

1.5 Relações de ordem

Definição 1.35. Uma relação R sobre um conjunto $E \neq \emptyset$ é chamada *relação de ordem parcial* sobre E, se R for reflexiva, antissimétrica e transitiva, isto é,

i) xRx para todo $x \in E$,

ii) se xRy e yRx então $x = y$, e

iii) se xRy e yRz então tem-se xRz,

e se isto acontecer, o conjunto E é dito um conjunto *parcialmente ordenado* pela relação R.

Uma relação de ordem R define no conjunto E, uma ordem entre os seus elementos, informando quem vem antes de quem (ou quem precede quem), e da mesma forma, quem vem

depois de quem (ou quem sucede quem). Mas observe que pode acontecer que alguns elementos de E não estejam necessariamente relacionados entre si. Para denotar relações de ordem é comum o uso de símbolos como $\preceq$, $\prec$, $\preccurlyeq$, $\trianglelefteq$, $\lhd$, $\leq$ ou $<$.

É comum também o uso das notações invertidas. Escrever $a \preccurlyeq b$ é equivalente a escrever $b \succcurlyeq a$, e dizemos em ambos os casos, que a precede b (ou a é predecessor de b), e que b sucede a (ou b é sucessor de a), pela relação $\preccurlyeq$.

Dada uma relação de ordem denotada por algum símbolo como $\preceq$ ou $\leq$, geralmente notações como $a \prec b$ e $a < b$ (ou mesmo $b \succ a$ e $b > a$), são usadas para indicar que a precede estritamente b, isto é, a precede b, mas não é igual a b. Para estas mesmas notações, também podemos dizer que b sucede a estritamente, isto é, b sucede a mas não é igual a a. Mas cuidado! Nestes termos a relação $\prec$ ou $<$ não pode ser reflexiva e portanto não é uma relação de ordem.

Definição 1.36. Sejam E um conjunto não vazio, e $\preccurlyeq$ uma relação de ordem parcial sobre E. Dois elementos a e b em E são ditos *comparáveis* por $\preccurlyeq$ se

$$a \preccurlyeq b \qquad \text{ou} \qquad b \preccurlyeq a.$$

Definição 1.37. Uma relação de ordem $\preccurlyeq$ sobre um conjunto não vazio E é dita *relação de ordem total* quando para quaisquer a e b em E tem-se

$$a \preccurlyeq b \qquad \text{ou} \qquad b \preccurlyeq a,$$

isto é, quaisquer a e b em E são comparáveis. Neste caso, dizemos que E é um conjunto *totalmente ordenado.*

Exemplo 1.17. Consideremos $E = \{0, 1, 2\}$, e $R = \{(0,0), (1,1), (2,2), (0,1), (0,2)\}$. É fácil ver que R é reflexiva, é antissimétrica e também transitiva. E assim, R é uma relação de ordem parcial. Entretanto R não é relação de ordem total, pois podemos encontrar elementos em E que não se relacionam entre si. Os elementos 1 e 2 estão em E, e no entanto não temos $1R2$, nem $2R1$. ■

Exemplo 1.18. Tomemos $E = \{B; B \text{ é subconjunto de } \mathbb{R}^2\}$, e a relação $\preccurlyeq$ de inclusão, isto é,

$$A \preccurlyeq B \quad \Leftrightarrow \quad A \subset B.$$

Esta relação é reflexiva ($A \subset A$, para todo $A \in E$), transitiva (se $A \subset B$ e $B \subset C$ então $A \subset C$) e antissimétrica (se $A \subset B$ e $B \subset A$, então $A = B$), logo $\preccurlyeq$ é uma relação de ordem parcial sobre o conjunto E. Mas é claro que é possível encontrar dois subconjuntos A e B do plano, tais que $A \not\subset B$ e $B \not\subset A$, e assim $\preccurlyeq$ não é relação de ordem total. ■

Exemplo 1.19. Consideremos o conjunto dos inteiros $\mathbb{Z}$, e uma relação sobre $\mathbb{Z}$, definida da seguinte forma,

$$a \leq b \quad \Leftrightarrow \quad b = a + n, \quad \text{para algum} \quad n \in \mathbb{N}.$$

Veja que $\leq$ é reflexiva, pois $a = a + 0$, para todo $a \in \mathbb{Z}$, e assim $a \leq a$, para todo $a \in \mathbb{Z}$. Também se $a, b \in \mathbb{Z}$ satisfazem $a \leq b$ e $b \leq a$, então $b = a + n$ e também $a = b + m$, para $m, n \in \mathbb{N}$. Temos então que $b = a + n = (b + m) + n$, e desta forma $0 = m + n$. Mas no conjunto dos naturais, esta

equação só será verdadeira se $m = n = 0$ e então $a = b$, o que mostra a anti-simetria de $\leq$. Se $a, b, c \in \mathbb{Z}$, com $a \leq b$ e $b \leq c$, então temos $b = a + n$ e $c = b + m$, para $m, n \in \mathbb{N}$. Sendo assim, $c = b+n = (a+n)+m = a+(m+n)$. Como $(m+n) \in \mathbb{N}$, então da definição, temos que $a \leq c$, e segue a transitividade de $\leq$. Por tudo isto, $\leq$ é uma relação de ordem (parcial) sobre $\mathbb{Z}$. Além disso, dados arbitrários $a, b \in \mathbb{Z}$, então $a - b$ ou $b - a$ é positivo, e portanto pertence a $\mathbb{N}$. Se $(a - b) \in \mathbb{N}$ então colocamos $a = b + (a - b)$ e temos que $b \leq a$. Se por outro lado $(b - a) \in \mathbb{N}$, então colocamos $b = a + (b - a)$ e temos $a \leq b$. Segue que $\leq$ é relação de ordem total em $\mathbb{Z}$. ■

Definição 1.38. Seja E um conjunto parcialmente ordenado pela relação de ordem $\preccurlyeq$, e A um subconjunto não vazio de E. Um elemento $L \in E$ é dito um *limite superior* para A, se

$$x \preccurlyeq L \quad \text{para todos} \quad x \in A,$$

e um elemento $l \in E$ é dito um *limite inferior* para A se

$$l \preccurlyeq x \quad \text{para todos} \quad x \in A.$$

Definição 1.39. Seja E um conjunto parcialmente ordenado pela relação de ordem $\preccurlyeq$, e A um subconjunto não vazio de E. Se existir $M \in A$ que satisfaz

$$x \preccurlyeq M \quad \text{para todos} \quad x \in A,$$

então M é chamado de máximo de A. Se existir $m \in A$ que satisfaz

$$m \preccurlyeq x \quad \text{para todos} \quad x \in A,$$

então m é chamado de mínimo de A.

Observe que um máximo de A é um limite superior que pertence a A e um mínimo de A é um limite inferior que pertence a A. Além disso, o máximo de um conjunto A, se existir, é único. De fato se M_1, M_2 são dois máximos de A. Como M_1 é máximo de A, então

$$x \preccurlyeq M_1 \quad \text{para todos} \quad x \in A.$$

Mas como $M_2 \in A$ então $M_2 \preccurlyeq M_1$. Da mesma forma, como M_2 é máximo de A, então

$$x \preccurlyeq M_2 \quad \text{para todos} \quad x \in A,$$

e como $M_1 \in A$ então $M_1 \preccurlyeq M_2$. Da antissimetria de $\preccurlyeq$ segue que $M_1 = M_2$.

Definição 1.40. Seja E um conjunto (parcialmente) ordenado pela relação de ordem $\preccurlyeq$, e A um subconjunto não vazio de E. Se o conjunto dos limites superiores de A possuir elemento mínimo, este mínimo é chamado de supremo de A. Se o conjunto dos limites inferiores de A possuir elemento máximo, este máximo é chamado de ínfimo de A.

Definição 1.41. Um elemento $M \in A$ é um elemento *maximal* de A se, para qualquer $x \in A$,

$$M \preccurlyeq x \quad \Rightarrow \quad M = x.$$

Um elemento $m \in A$ é um elemento *minimal* de A se, para qualquer $x \in A$,

$$x \preccurlyeq m \quad \Rightarrow \quad m = x.$$

Em outras palavras, M é elemento maximal de A se o único sucessor de M for ele próprio. Analogamente m é elemento minimal de A se o único predecessor de m for ele próprio.

Exemplo 1.20. Seja $E = \mathbb{R}$ com a relação de ordem usual $\leq$ e $A = [-2, 2)$, então temos que os limites superiores de A são os números do conjunto $[2, \infty)$. Os limites inferiores são os números do conjunto $(-\infty, -2]$. O máximo não existe. O mínimo é -2. O supremo é 2. O ínfimo é -2. O elemento minimal é -2. O elemento maximal não existe. ■

Exemplo 1.21. Consideremos $E = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ munido da relação de ordem $\preccurlyeq$ dada pela divisibilidade de naturais, isto é,

$$x \preccurlyeq y \quad \Leftrightarrow \quad x|y.$$

Sugerimos ao leitor mostrar que a divisibilidade é de fato uma relação de ordem parcial em $\mathbb{N}$. Considerando $A = \{2, 4, 6\}$, temos para A: Os limites superiores 12 e 36; Os limites inferiores 1 e 2; O máximo não existe; O mínimo 2; O supremo 12; O ínfimo 2; O elemento minimal 2; Os elementos maximais 4 e 6. ■

Exemplo 1.22. Dado $E = \{a, b, c, d\}$ e a relação de ordem

$$R = \{(a, a), (b, b), (c, c), (d, d), (a, c), (c, d), (a, d)\}.$$

Para o subconjunto $A = \{c, d\}$, temos: O limite superior d; Os limites inferiores a e c; O máximo d; O mínimo c; O ínfimo c; O supremo d; O elemento maximal d; O elemento minimal c. ■

1.6 Aplicações

Nesta seção vamos estudar uma classe especial de relações, que serão chamadas de aplicações. Usaremos preferencialmente letras minúsculas para indicar relações que são aplicações.

Definição 1.42. Dados E e F conjuntos não vazios, uma relação f de E em F, é dita uma *aplicação* de E em F se

i) $D(f) = E$, e

ii) para cada $a \in E = D(f)$, existe um único $b \in F$ tal que $(a, b) \in f$.

Como o elemento b é unicamente determinado, podemos expressar b em termos do seu correspondente $a \in E$. Assim, se f é uma aplicação, e somente neste caso, escrevemos $b = f(a)$ para indicar que $(a, b) \in f$, e além disso, o elemento $b \in F$ é dito imagem do elemento $a \in E$ pela aplicação f. Escrevemos $f : E \to F$ para indicar que f é uma aplicação de E em F. O conjunto F é chamado de *contra-domínio* de f, denotado também por $Cd(f)$.

Lembremos que sendo f uma relação, o conjunto $Im(f)$ já foi definido por

$$Im(f) = \{b \in F; \quad b = f(a) \quad \text{para algum} \quad a \in E\}.$$

Definição 1.43. Dizemos que duas aplicações $f : E \to F$ e $g : X \to Y$ são iguais, e escrevemos $f = g$, se e somente se,

i) $E = X$,
ii) $F = Y$ e
iii) $f(a) = g(a)$ para todo $a \in E$.

Note que esta definição de igualdade de aplicações não difere da definição de igualdade de funções dada nos cursos de Cálculo. No Cálculo, diz-se que, duas funções f e g são iguais se (e somente se) $D(f) = D(g)$, $Cd(f) = Cd(g)$, e $f(x) = g(x)$ para todo x no domínio das funções. Mas para o nosso caso, já temos $D(f) = E = D(g)$, e $Cd(f) = F = Cd(g)$, e por isto a igualdade entre f e g se reduz à igualdade dos valores pontuais.

Exemplo 1.23. Dados dois conjuntos $E = \{1, 2, 3\}$ e $F = \{0, 1, 2, 3, 4\}$, consideremos as relações f e g de E em F, dadas por

$$f = \{(1, 0), (1, 1), (2, 2), (3, 4)\} \quad \text{e} \quad g = \{(1, 4), (2, 3), (3, 0)\},$$

então, $D(f) = \{1, 2, 3\} = E$, mas o elemento $1 \in E$ tem dois correspondentes em F, isto é, não é único o elemento $b \in F$ tal que $(1, b) \in f$, logo f não é aplicação. Para g, temos $D(g) = \{1, 2, 3\} = E$, além disso para todo $a \in E$, é único o elemento $b \in F$ tal que $(a, b) \in g$, e então g é aplicação. ■

Definição 1.44. Seja $f : E \to F$ uma aplicação, e A um subconjunto de E. Chama-se *imagem direta* de A por f, o subconjunto de F, representado por $f(A)$, formado pelas imagens de elementos de A. Simbolicamente

$$\begin{aligned} f(A) &= \{y \in F; \quad y = f(x) \quad \text{para algum} \quad x \in A\} \\ &= \{f(x); \quad x \in A\}. \end{aligned}$$

No caso em que $A = E$, o conjunto $f(A) = f(E)$ é precisamente o conjunto imagem da aplicação.

Definição 1.45. Sejam, $f : E \to F$ uma aplicação e B um subconjunto de F. Chama-se *imagem inversa* de B por f o subconjunto de E, indicado por $f^{-1}(B)$, e determinado por

$$f^{-1}(B) = \{x \in E; \quad f(x) \in B\},$$

isto é, o subconjunto de todos os elementos de E, com imagem em B.

Se $A = \emptyset$, então $f(A) = \emptyset$. Se $B = \emptyset$ então $f^{-1}(B) = \emptyset$. Note que $x \in f^{-1}(B)$, se e somente se, $f(x) \in B$, e também se $x \in A$ então $f(x) \in f(A)$, mas $f(x) \in f(A)$ não garante que $x \in A$. O que se garante da definição é que se $f(x) \in f(A)$ então $f(x) = f(a)$ para algum $a \in A$. O próximo exemplo se refere a este fato.

Exemplo 1.24. Sejam $E = F = \mathbb{R}$ e $f : E \to F$ dada por

$$f = \{(x, x^2); \quad x \in \mathbb{R}\} \subset \mathbb{R} \times \mathbb{R}.$$

Observe que $(x, x^2) \in f$ significa que $f(x) = x^2$. Tomemos $A = [0, 2] \subset \mathbb{R}$, e $x = -1$. Temos então que $f(A) = f([0, 2]) = [0, 4]$, e $f(x) = f(-1) = 1$. Sendo assim, vemos que $f(-1) \in f(A)$, e no entanto $-1 \notin A$. Mas como mencionado no parágrafo anterior, como $f(-1) = 1 \in f(A)$ então existe $a \in A$, mais precisamente $a = 1 \in A$, de forma que $f(-1) = f(1) = 1 \in f(A)$. ■

Definição 1.46. Seja $f : E \to F$ uma aplicação. Dizemos que f é uma aplicação *injetora* se para quaisquer $x, y \in E$, tais que $f(x) = f(y)$ tem-se $x = y$. Equivalentemente, f é injetora, se para quaisquer $x, y \in E$, tais que $x \neq y$ tem-se $f(x) \neq f(y)$.

A definição acima, significa que elementos distintos devem possuir imagens distintas. Para dizer que uma aplicação f é injetora, é comum também escrever que f é 1-1, e dizer que f é um a um. Para dizer que f não é injetora, basta então encontrar elementos distintos x e y com imagens $f(x)$ e $f(y)$ iguais.

Definição 1.47. Seja $f : E \to F$ uma aplicação. Dizemos que f é uma aplicação *sobrejetora* se para todo $y \in F$, existe $x \in E$, tal que $f(x) = y$.

Note que o conjunto dos elementos $y \in F = Cd(f)$, para os quais existe $x \in E$ tal que $f(x) = y$ é o conjunto imagem da aplicação. A definição anterior diz que para que a aplicação seja sobrejetora, esta condição deve ser satisfeita para todo $y \in Cd(f)$ e portanto uma aplicação será sobrejetora se e somente se $Im(f) = Cd(f)$. Mas $Im(f)$ é, por definição, sempre um subconjunto de $Cd(f)$. Então o trabalho de provar que f é sobrejetora, resume-se em mostrar que $Cd(f) \subset Im(f)$. Para dizer que f não é sobrejetora, basta encontrar algum $y \in F$ que não é imagem de nenhum $x \in E$.

Definição 1.48. Uma aplicação f, é dita *bijetora*, se f for simultaneamente injetora e sobrejetora.

Exemplo 1.25. A aplicação $f : \mathbb{R} \to \mathbb{C}$ que a cada real x associa o complexo $f(x) = x - xi$ é injetiva, pois

$$f(x) = f(y) \quad \Rightarrow \quad x - xi = y - yi \quad \Rightarrow \quad x = y.$$

Por outro lado, f não é sobrejetiva, pois $1 + 3i \in \mathbb{C}$, e não existe $x \in \mathbb{R}$ que satisfaz $f(x) = x - xi = 1 + 3i$. ■

Exemplo 1.26. Considerando

$$\mathcal{M} = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}; \quad a, b \in \mathbb{R} \right\}$$

o conjunto das matrizes diagonais de ordem 2, e a aplicação $f : \mathcal{M} \to \mathbb{R}$, definida por $f(A) = \det A$. A aplicação f não é injetiva pois as matrizes

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \qquad \text{e} \qquad B = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$$

possuem o mesmo determinante, isto é, $f(A) = 2 = f(B)$ e no entanto $A \neq B$. Por outro lado, f é sobrejetiva, pois para cada $x \in \mathbb{R}$, a matriz

$$A = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$$

satisfaz $f(A) = \det A = x$. ■

Suponha que E e F sejam não vazios e $f : E \to F$ é uma aplicação. Então f é uma relação. Sendo assim, podemos falar que a relação f possui relação inversa f^{-1} de F em E. Entretanto, pode ocorrer que a relação f^{-1} não seja uma aplicação. O teorema seguinte, nos dá condições, para que possamos afirmar quando f^{-1} é também uma aplicação.

Teorema 1.49. *Seja $f : E \to F$ uma aplicação entre os conjuntos não vazios E e F. Então f é bijetora, se e somente se, f^{-1} é uma aplicação de F em E.*

Prova. Suponha então que f seja bijetora. Como f^{-1} é uma relação de F em E, é imediato que $D(f^{-1}) \subset F$. Para provar que também $F \subset D(f^{-1})$, seja então $y \in F$. Como f é sobrejetora, existe $x \in E$ tal que $f(x) = y$. Desta forma, $(x, y) \in f$, e então, $(y, x) \in f^{-1}$ donde $y \in D(f^{-1})$. Segue que todo elemento de F está no domínio de f^{-1}. Dado agora $y \in F = D(f^{-1})$, mostraremos que é único o elemento $x \in E$ tal que $(y, x) \in f^{-1}$. Para isto, consideremos $x_1, x_2 \in E$, satisfazendo $(y, x_1) \in f^{-1}$ e $(y, x_2) \in f^{-1}$. Assim, temos que $(x_1, y) \in f$ e $(x_2, y) \in f$, e sendo f uma aplicação, escrevemos $y = f(x_1)$ e $y = f(x_2)$, e então $f(x_1) = f(x_2)$. Mas como f é injetora, segue que $x_1 = x_2$. Isto mostra que f^{-1} é aplicação, o que conclui esta demonstração.

Suponha agora $f^{-1} : F \to E$ uma aplicação. Sejam $x, y \in E$ com $f(x) = f(y)$. É claro que temos $(x, f(x)) \in f$ e $(y, f(y)) \in f$. Então, $(f(x), x) \in f^{-1}$ e $(f(y), y) \in f^{-1}$. Mas como $f(x) = f(y)$, então temos que $(f(x), x), (f(x), y) \in f^{-1}$, e sendo f^{-1} uma aplicação, é única a imagem do elemento $f(x)$ por f^{-1}. Segue que $x = y$.

Para provar que f é sobrejetora, seja $y \in F$. Como f^{-1} é uma aplicação então $F = D(f^{-1})$ e assim $y \in D(f^{-1})$, donde existe $x \in E$ tal que $(y, x) \in f^{-1}$. Mas isto significa que $(x, y) \in f$ e portanto existe $x \in E$ tal que $y = f(x)$. Segue que f é sobrejetora, e consequentemente bijetora. □

Um resultado mais forte do que o último teorema pode ser obtido. Se uma aplicação f é bijetora, além de f^{-1} ser uma aplicação, pode-se provar que f^{-1} é também bijetora. Este é o objetivo do próximo teorema.

Teorema 1.50. *Seja $f : E \to F$ uma aplicação. f é bijetora se, e somente se, $f^{-1} : F \to E$ é bijetora.*

Prova. Suponha f bijetora. Sejam $x, y \in F$ tais que $f^{-1}(x) = f^{-1}(y)$. Então $(x, f^{-1}(x)) \in f^{-1}$ e $(y, f^{-1}(y)) \in f^{-1}$, e como $f^{-1}(x) = f^{-1}(y)$ temos que $(x, f^{-1}(x)), (y, f^{-1}(x)) \in f^{-1}$. Assim, temos que $(f^{-1}(x), x), (f^{-1}(x), y) \in f$. De outra forma, $x = f(f^{-1}(x))$ e também $y = f(f^{-1}(x))$. Como f é aplicação, a imagem de $f^{-1}(x) \in E$ por f é única, isto é, $x = y$, mostrando a injetividade de f^{-1}.

Seja $x \in E$ arbitrário. Como f é aplicação, $D(f) = E$ e assim, $x \in D(f)$, isto é, existe $y \in F$ tal que $f(x) = y$, e então, $(x, y) \in f$ ou ainda $(y, x) \in f^{-1}$. Segue que existe $y \in F$ de forma que $(y, x) \in f^{-1}$, ou ainda, $x = f^{-1}(y)$, mostrando a sobrejetividade de f^{-1}. Segue portanto que f^{-1} é bijetora.

Suponha agora f^{-1} bijetora, então da primeira parte, a inversa de f^{-1} é bijetora, isto é, $(f^{-1})^{-1}$ é bijetora. Mas como $(f^{-1})^{-1} = f$ (Ver proposição 1.23) então f é bijetora. □

Quando $f : E \to F$ é uma aplicação bijetora, temos então que $f^{-1} : F \to E$ é também uma aplicação bijetora, e além disso,

$$y = f(x) \qquad \Leftrightarrow \qquad (x, y) \in f \qquad \Leftrightarrow \qquad (y, x) \in f^{-1} \qquad \Leftrightarrow \qquad x = f^{-1}(y).$$

Tomando as igualdades $y = f(x)$ e $x = f^{-1}(y)$, e substituindo x e y de uma igualdade para outra, obtemos ainda que, para qualquer $x \in E$ tem-se $f^{-1}(f(x)) = x$ e para qualquer $y \in F$ tem-se $f(f^{-1}(y)) = y$.

Já definimos anteriormente a relação composta de duas relações. Estamos agora interessados em saber em que situações a composta é de fato uma aplicação e também em que situações é uma aplicação bijetora.

Proposição 1.51. *Sejam $f : E \to F$ e $g : F \to G$ duas aplicações. A relação composta de f com g, indicada por $(g \circ f) \subset E \times G$, é também uma aplicação.*

Prova. Primeiro temos que mostrar que $D(g \circ f) = E$. Seja então $x \in E$. Como f é uma aplicação $E = D(f)$ e então $x \in D(f)$, logo existe $y \in F$ tal que $(x, y) \in f$. Como g é aplicação temos que $D(g) = F$ e para este $y \in F$ existe $z \in G$ tal que $(y, z) \in g$. Neste caso da definição de relação composta $(x, z) \in (g \circ f)$ e portanto $x \in D(g \circ f)$.

Dado agora $x \in D(g \circ f) = E$, queremos mostrar que é único o elemento $z \in G$ tal que $(x, z) \in (g \circ f)$. Suponha que z_1 e z_2 satisfazem $(x, z_1) \in (g \circ f)$ e $(x, z_2) \in (g \circ f)$. Então da definição de relação composta existem $y_1, y_2 \in F$ tais que

$$\begin{aligned} &(x, y_1) \in f \quad \text{e} \quad (y_1, z_1) \in g, \qquad \text{e} \\ &(x, y_2) \in f \quad \text{e} \quad (y_2, z_2) \in g. \end{aligned}$$

Como f é uma aplicação então $y_1 = y_2$ e escrevendo $y = y_1 = y_2$, temos que

$$(y, z_1) \in g \quad \text{e} \quad (y, z_2) \in g,$$

e como g é uma aplicação segue que $z_2 = z_1$. Isto posto temos que a composta $g \circ f$ é uma aplicação. □

A aplicação composta $(g \circ f) : E \to G$ tem o mesmo domínio de f e o mesmo contradomínio de g. Um fato importante, é que se $f : E \to F$ e $g : F \to E$ são duas aplicações, então estão definidas as composições $(g \circ f)$ e $(f \circ g)$, mas em geral, $(g \circ f) \neq (f \circ g)$.

Observemos que $(g \circ f)(x) = g(f(x))$ para todo $x \in E$. De fato, sendo $f : E \to F$ e $g : F \to G$ duas aplicações, então $(g \circ f) : E \to G$ é uma aplicação. Assim, dado qualquer $x \in E = D(g \circ f)$, temos que existe $z \in G$ tal que $z = (g \circ f)(x)$. De outra forma, $(x, z) \in (g \circ f)$ e da definição de composição de relações, existe $y \in F$ tal que $(x, y) \in f$ e $(y, z) \in g$, e consequentemente, $z = g(y)$ e $y = f(x)$. Logo,

$$(g \circ f)(x) = z = g(y) = g(f(x)),$$

para todo $x \in E = D(g \circ f)$.

Lema 1.52. *Se $f : E \to F$ e $g : F \to G$ são sobrejetoras, então $(g \circ f) : E \to G$ é sobrejetora.*

Prova. Seja $z \in G$. Como g é sobrejetora, existe $y \in F$ tal que $g(y) = z$. Sendo $y \in F$ e f sobrejetora, existe $x \in E$ tal que $f(x) = y$. Então

$$(g \circ f)(x) = g(f(x)) = g(y) = z,$$

e segue então que $(g \circ f)$ é sobrejetora. □

Lema 1.53. *Se $f : E \to F$ e $g : F \to G$ são injetoras, então $(g \circ f) : E \to G$ é injetora.*

Prova. Sejam $x, y \in E$ tais que $(g \circ f)(x) = (g \circ f)(y)$. Então $g(f(x)) = g(f(y))$ e como g é injetora, segue que $f(x) = f(y)$ e sendo f injetora, temos que $x = y$, mostrando que $(g \circ f)$ é injetora. □

O próximo teorema é uma junção dos resultados dos dois últimos lemas. Optamos por enunciar os dois lemas em separado, apenas para evidenciar os resultados individuais.

Teorema 1.54. *Se $f : E \to F$ e $g : F \to G$ são bijetoras, então $(g \circ f) : E \to G$ é bijetora.*

No caso em que f e g forem bijetoras, então a composta $(g \circ f)$ é invertível, e a sua inversa $(g \circ f)^{-1}$ é dada, de acordo com o teorema 1.25, por $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Definição 1.55. Seja E um conjunto não vazio. A aplicação identidade em E, que será denotada por Id_E, é a aplicação $Id_E : E \to E$ dada por

$$Id_E(x) = x \qquad \text{para todo} \qquad x \in E,$$

ou equivalentemente,

$$Id_E = \{(x, x); \quad x \in E\}.$$

Quando não houver dúvidas sobre o conjunto E envolvido, a aplicação identidade será representada simplesmente por Id, e então $Id(x) = x$, para todo $x \in E$. Claramente a aplicação identidade, $Id : E \to E$, é bijetora para qualquer conjunto $E \neq \emptyset$.

Lembremos que se $f : E \to F$ é uma aplicação bijetora, então para quaisquer $x \in E$ e $y \in F$, temos que $f^{-1}(f(x)) = x$, e $f(f^{-1}(y)) = y$, e desta forma temos claramente que, se $f : E \to F$ é bijetora, então $(f^{-1} \circ f) = Id_E$ e $(f \circ f^{-1}) = Id_F$. A recíproca desta ideia é tratada no próximo teorema.

Teorema 1.56. *Seja $f : E \to F$ uma aplicação. Se existirem aplicações $g, h : F \to E$ tais que $(g \circ f) = Id_E$ e $(f \circ h) = Id_F$, então f é bijetora. Além disso $h = g = f^{-1}$.*

Prova. Suponha então $(g \circ f) = Id_E$ e $(f \circ h) = Id_F$. Seja $y \in F$ arbitrário. Então como $(f \circ h)(y) = y$, ou $f(h(y)) = y$, segue que existe $x = h(y) \in E$ tal que $f(x) = y$, donde se conclui que f é sobrejetora. Sejam agora $x_1, x_2 \in E$ com $f(x_1) = f(x_2)$. Como g é aplicação temos que $g(f(x_1)) = g(f(x_2))$ ou ainda $(g \circ f)(x_1) = (g \circ f)(x_2)$. Mas como $(g \circ f) = Id_E$, temos que

$$x_1 = (g \circ f)(x_1) = (g \circ f)(x_2) = x_2,$$

o que mostra que f é injetora. E assim, f é bijetora.

Mostraremos agora que $g = f^{-1} = h$. Da bijetividade de f temos que $f^{-1} : F \to E$ é aplicação. Como $F = D(g) = D(h) = D(f^{-1})$ e também $E = Cd(g) = Cd(h) = Cd(f^{-1})$, resta mostrar que $h(y) = f^{-1}(y)$ e que $g(y) = f^{-1}(y)$ para todo $y \in F$. De fato, dado $y \in F$ arbitrário,

$$f^{-1}(y) = f^{-1}((f \circ h)(y)) = f^{-1}(f(h(y))) = (f^{-1} \circ f)(h(y)) = h(y),$$

e também

$$f^{-1}(y) = (g \circ f)(f^{-1}(y)) = g(f(f^{-1}(y))) = g((f^{-1} \circ f)(y)) = g(y).$$

□

Este último teorema poderia ter sido enunciado em duas partes. Observe que para provar que f é sobrejetora, usamos a existência de uma aplicação h tal que $(f \circ h) = Id_F$. Para provar que f é injetora, usamos a existência de uma aplicação g tal que $(g \circ f) = Id_E$.

Definição 1.57. Seja $f : E \to F$ uma aplicação, e suponha E e F conjuntos parcialmente ordenados pelas relações de ordem $\overset{R}{\preccurlyeq}$ e $\overset{S}{\preccurlyeq}$ respectivamente. Dizemos que f é uma aplicação *crescente* se

$$a \overset{R}{\preccurlyeq} b \quad \Rightarrow \quad f(a) \overset{S}{\preccurlyeq} f(b) \quad \text{para quaisquer } a, b \in E,$$

e que f é uma aplicação *decrescente* se

$$a \overset{R}{\preccurlyeq} b \quad \Rightarrow \quad f(a) \overset{S}{\succcurlyeq} f(b) \quad \text{para quaisquer } a, b \in E.$$

Em qualquer um dos casos, f é dita uma aplicação *monótona*.

Na definição anterior, podemos remover a possibilidade de que $a = b$, e também a possibilidade de que $f(a) = f(b)$. Neste caso as relações de ordem passam a ser consideradas no sentido estrito, e temos então a definição de aplicações estritamente crescente e estritamente decrescente.

Definição 1.58. Sejam E e F conjuntos parcialmente ordenados pelas relações de ordem $\overset{R}{\preccurlyeq}$ e $\overset{S}{\preccurlyeq}$ respectivamente. Dizemos que $f : E \to F$ é uma aplicação *estritamente crescente* se

$$a \overset{R}{\prec} b \quad \Rightarrow \quad f(a) \overset{S}{\prec} f(b) \quad \text{para quaisquer } a, b \in E,$$

e que f é uma aplicação *estritamente decrescente* se

$$a \overset{R}{\prec} b \quad \Rightarrow \quad f(a) \overset{S}{\succ} f(b) \quad \text{para quaisquer } a, b \in E.$$

Proposição 1.59. *Seja E um conjunto totalmente ordenado pela relação de ordem $\preceq$. Se uma aplicação $f : E \to F$ é estritamente crescente, ou decrescente, então f é injetora.*

Prova. Suponha f estritamente crescente. Sejam $x, y \in E$ com $x \neq y$, então $x \prec y$, ou $x \succ y$, e como f é estritamente crescente temos que $f(x) \prec f(y)$, ou $f(x) \succ f(y)$ respectivamente. Em ambos os casos se confirma que $f(x) \neq f(y)$ e portanto f é injetora. O segundo caso, com f estritamente decrescente, é demonstrado de forma análoga. □

1.7 Operações

Nos capítulos que se seguirão, torna-se importantíssimo o uso de operações definidas nos conjuntos de estudo. Esta seção é dedicada aos aspectos fundamentais das operações e também de suas principais propriedades. Será uma seção útil para o restante deste texto.

Definição 1.60. Se E é um conjunto não vazio, então uma operação sobre E, ou uma lei de composição interna para E, é qualquer aplicação $f : E \times E \to E$.

Observe que, como aplicação, f deve satisfazer $D(f) = E \times E$, e isto significa que cada par ordenado $(x, y) \in E \times E$ deve estar associado a um único elemento $z = f(x, y) \in E$, chamado de resultado da operação de x com y.

É comum a representação de operações por símbolos como $*$, $+$, $\cdot$, $\oplus$ ou $\odot$. Assim, uma operação $*$ sobre um conjunto E é uma aplicação $* : E \times E \to E$, sendo que escrevemos $x * y$ para designar o elemento $*(x, y) \in E$, resultado da operação de x com y. Também, x e y são denomidados respectivamente primeiro termo ou o termo à esquerda e segundo termo ou termo à direita da operação. Quando não houver necessidade de ordem, podemos dizer simplesmente que x e y são as parcelas, ou os termos, da operação.

Vamos agora estudar as principais propriedades envolvendo as operações.

Definição 1.61. Dizemos que uma operação $*$, definida sobre um conjunto não vazio E, é associativa, ou que $*$ tem a propriedade associativa, se

$$(x * y) * z = x * (y * z),$$

para quaisquer $x, y, z \in E$.

Equivalentemente, em termos de uma aplicação, dizemos que $* : E \times E \to E$ é associativa, se e somente se $*(*(x, y), z) = *(x, *(y, z))$, para todos $x, y, z \in E$.

Definição 1.62. Dizemos que uma operação $*$, definida sobre um conjunto não vazio E, é comutativa, ou que $*$ tem a propriedade comutativa, se

$$x * y = y * x,$$

para quaisquer $x, y \in E$.

Também em termos de uma aplicação dizemos que $* : E \times E \to E$ é comutativa, se for satisfeita a igualdade $*(x, y) = *(y, x)$, para quaisquer $x, y \in E$.

Exemplo 1.27. Sobre o conjunto $E = \mathbb{Z}$ consideremos as aplicações

$$(x, y) \mapsto +(x, y) = x + y,$$
$$(x, y) \mapsto \cdot(x, y) = x \cdot y,$$
$$(x, y) \mapsto -(x, y) = x - y,$$

chamadas respectivamente de adição, multiplicação e diferença de números inteiros. Claramente são três aplicações de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z}$, e portanto são operações. A adição e a multiplicação são associativas e comutativas, mas a diferença não é associativa e nem comutativa. ■

Exemplo 1.28. Considere o conjunto $E = \mathbb{R}^* = \mathbb{R} - \{0\}$ e as aplicações

$$(x, y) \mapsto \div(x, y) = x \div y = \frac{x}{y},$$
$$(x, y) \mapsto \cdot(x, y) = x \cdot y,$$

chamadas respectivamente divisão e multiplicação de números reais (não nulos). A multiplicação é associativa e comutativa, mas a divisão não é associativa nem comutativa. ■

Exemplo 1.29. Seja $E = M_2(\mathbb{R})$ o conjunto das matrizes quadradas de ordem 2 com coeficientes reais, e a aplicação

$$(A, B) \mapsto \cdot(A, B) = A \cdot B,$$

chamada de multiplicação de matrizes. Esta operação é associativa mas não é comutativa. ■

Exemplo 1.30. Considerando X um conjunto não vazio, e $E = \mathcal{P}(X) = \{A; A \subset X\}$, as aplicações

$$(A, B) \mapsto \cup(A, B) = A \cup B,$$
$$(A, B) \mapsto \cap(A, B) = A \cap B,$$
$$(A, B) \mapsto -(A, B) = A - B = A \cup B^C,$$

chamadas respectivamente de união, intersecção e diferença entre conjuntos, são operações em E. A união e a intersecção são associativas e comutativas, mas a diferença não é associativa nem comutativa. ■

Exemplo 1.31. Dado $E = \mathbb{R}^{\mathbb{R}}$, o conjunto das funções de $\mathbb{R}$ em $\mathbb{R}$. A aplicação

$$(f, g) \mapsto \circ(f, g) = f \circ g,$$

define a operação de composição de funções. A composição de funções é associativa mas não é comutativa. ■

Definição 1.63. Seja $*$ uma operação sobre um conjunto não vazio E. Dizemos que $e \in E$ é *elemento neutro* para a operação $*$ se

$$x * e = e * x = x \quad \text{para todo} \quad x \in E.$$

Se apenas a condição $x * e = x$ for cumprida para todo $x \in E$ então e é dito elemento neutro pela direita de $*$ e se apenas a condição $e * x = x$ for cumprida para todo $x \in E$ então e é dito elemento neutro pela esquerda de $*$. É possível ainda que uma operação admita apenas elemento neutro à direita ou apenas elemento neutro à esquerda. Um destes exemplos é a operação de diferença de números reais, que não admite elemento neutro à esquerda mas admite elemento neutro à direita que é o número 0. Entretanto, é possível provar que se uma operação admite um elemento neutro à esquerda e também um elemento neutro à direita, então estes elementos neutros obrigatoriamente são iguais.

Proposição 1.64. *Suponha que $*$ é uma operação sobre um conjunto não vazio E, que admite elemento neutro pela esquerda e elemento neutro pela direita. Então estes elementos neutros coincidem.*

Prova. Suponha que e_1 é um elemento neutro pela esquerda de $*$ e que e_2 é um elemento neutro pela direita de $*$. Então e_1 satisfaz $e_1 * x = x$ para qualquer $x \in E$. Em particular $e_1 * e_2 = e_2$. Também e_2 satisfaz $x * e_2 = x$ para qualquer $x \in E$. Em particular $e_1 * e_2 = e_1$. Assim

$$e_1 = e_1 * e_2 = e_2,$$

concluindo que os elementos neutros pela esquerda e pela direita coincidem. □

Corolário 1.65. *Se uma operação $*$ em E admite elemento neutro, então este elemento neutro é único.*

Definição 1.66. Suponha que $*$ tem elemento neutro e em E. Dizemos que $x \in E$ é simetrizável para a operação $*$, se existir $x' \in E$, chamado de elemento simétrico de x, tal que

$$x' * x = x * x' = e.$$

Se apenas a condição $x' * x = e$ for cumprida então o elemento x é dito simetrizável pela esquerda, e se apenas a condição $x * x' = e$ for cumprida então o elemento x é dito simetrizável pela direita, para a operação $*$. Pode ocorrer que um elemento admita apenas simétrico pela direita ou apenas simétrico pela esquerda. Um exemplo disto pode ser conseguido considerando o conjunto E das funções de $[-1, 1]$ em $[-1, 1]$, e em E considere a operação de composição de funções. Este conjunto possui elemento neutro para esta operação que é a função identidade. Dada

$$\begin{aligned} f : [-1, 1] &\to [-1, 1] \\ x &\mapsto f(x) = 2x^2 - 1 \end{aligned}$$

podemos verificar que

$$\begin{aligned} g : [-1, 1] &\to [-1, 1] \\ x &\mapsto g(x) = \sqrt{\frac{x+1}{2}} \end{aligned}$$

satisfaz

$$(f \circ g)(x) = f(g(x)) = 2\left(\sqrt{\frac{x+1}{2}}\right)^2 - 1 = x,$$

para todo $x \in [-1, 1]$. Desta forma, f é simetrizável pela direita, sendo g o elemento simétrico pela direita de f. Mas note que g não é o elemento simétrico de f pela esquerda. De fato,

$$(g \circ f)(x) = g(f(x)) = \sqrt{\frac{(2x^2 - 1) + 1}{2}} = \sqrt{x^2} = |x|.$$

Mas poderia existir alguma outra função h de forma que $(h \circ f)(x) = x$ para todo $x \in [-1, 1]$? A resposta é não. Se existisse uma tal função h, então de acordo com o teorema 1.56, f seria bijetora. Como f não é bijetora, então f não pode admitir simétrico pela esquerda.

Podemos verificar que se a operação for associativa e admite elemento neutro, e se x é um elemento simetrizável pela esquerda e simetrizável pela direita, então os simétricos à direita e à esquerda coincidem.

Proposição 1.67. *Suponha que $*$ é uma operação associativa e que possui elemento neutro e. Se $x \in E$ admite simétrico pela direita e admite simétrico pela esquerda, então estes simétricos coincidem.*

Prova. Denotemos x' o simétrico de x pela esquerda, isto é, $x' * x = e$. Denotemos também x'' o simétrico de x pela direita, isto é, $x * x'' = e$. Então

$$x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x'',$$

e portanto os simétricos de x pela direita e pela esquerda coincidem. □

Corolário 1.68. *Suponha que $*$ é uma operação associativa e que admite elemento neutro e. Se $x \in E$ é simetrizável então o elemento simétrico de x é único.*

Deste ponto em diante, para padronizar a notação, se um elemento $x \in E$ for simetrizável, e o simétrico for único, então a notação x' sempre indicará o elemento simétrico de x.

Proposição 1.69. *Seja $*$ uma operação sobre E, com elemento neutro e, então*

i) Se x é simetrizável, x' é simetrizável e $(x')' = x$,

ii) Se $*$ é associativa e x e y são simetrizáveis, então $(x*y)$ é simetrizável e $(x*y)' = y' * x'$.

Prova. Para o item (i), se x é simetrizável, então existe $x' \in E$ tal que $x * x' = x' * x = e$. Mas esta mesma igualdade, nos diz que para o elemento $x' \in E$, existe um elemento $x \in E$ tal que $x * x' = x' * x = e$. Portanto $x' \in E$ é simetrizável com seu simétrico sendo o elemento x, isto é, $(x')' = x$. Para mostrar (ii), suponha x e y simetrizáveis. Como

$$(x * y) * (y' * x') = x * (y * y') * x' = x * e * x' = x * x' = e,$$

e também

$$(y' * x') * (x * y) = y' * (x' * x) * y = y' * e * y = y' * y = e,$$

então da definição de elemento simetrizável, segue que, o elemento $(x * y)$ é simetrizável, sendo $(y' * x')$ o seu simétrico, isto é, $(x * y)' = y' * x'$. □

O conjunto de todos os elementos simetrizáveis de E para a operação $*$ é denotado por $U_*(E)$, ou seja,

$$x \in U_*(E) \quad \Leftrightarrow \quad x \text{ é simetrizável,}$$

ou ainda,

$$U_*(E) = \{x \in E; \quad x * x' = x' * x = e \quad \text{para algum} \quad x' \in E\}.$$

Definição 1.70. Sejam $*$ uma operação sobre $E \neq \emptyset$, e $a \in E$. Dizemos que a é *regular à esquerda* para a operação $*$ se

$$a * x = a * y \quad \Rightarrow \quad x = y,$$

para quaisquer $x, y \in E$, e que a é *regular à direita* para $*$ se

$$x * a = y * a \quad \Rightarrow \quad x = y,$$

para quaisquer $x, y \in E$. Se as duas condições acontecem, então a é dito simplesmente um *elemento regular* para $*$ em E.

Um elemento regular é um elemento que pode ser "simplificado" à direita e à esquerda de uma igualdade envolvendo a operação $*$ de E. O conjunto dos elementos de E regulares para a operação $*$ é denotado por $R_*(E)$, isto é,

$$a \in R_*(E) \quad \Leftrightarrow \quad a \text{ é regular para a operação } *,$$

ou ainda,

$$R_*(E) = \{a \in E; \quad a * x = a * y \quad \Rightarrow \quad x = y, \quad \text{para quaisquer} \quad x, y \in E\}.$$

Proposição 1.71. *Se $*$ é uma operação associativa em um conjunto E não vazio, e admite elemento neutro e, então todo elemento simetrizável é regular para a operação $*$.*

Prova. Seja $a \in E$ um elemento simetrizável, mostraremos que a é regular (à esquerda). Suponha então $a * x = a * y$ para quaisquer $x, y \in E$. Assim

$$\begin{aligned} x = e * x &= (a' * a) * x = a' * (a * x) \\ &= a' * (a * y) = (a' * a) * y = e * y = y. \end{aligned}$$

Segue que a é elemento regular à esquerda. Analogamente prova-se que a é regular à direita, e portanto a é elemento regular para a operação $*$. □

Definição 1.72. Sejam $\circ$ e $*$ duas operações definidas sobre um conjunto $E \neq \emptyset$. Dizemos que $\circ$ é *distributiva à esquerda* com relação a $*$ se

$$x \circ (y * z) = (x \circ y) * (x \circ z),$$

e que $\circ$ é *distributiva à direita* com relação a $*$ se

$$(x * y) \circ z = (x \circ z) * (y \circ z),$$

para quaisquer que sejam $x, y, z \in E$. Se ocorrerem as duas igualdades então dizemos simplesmente que $\circ$ é *distributiva* com relação a $*$.

Note que se a operação $\circ$ for comutativa, então distributividade à direita implica em distributividade à esquerda e reciprocamente.

Definição 1.73. Seja E um conjunto (não vazio) munido de uma operação $*$. Um subconjunto $A \subset E$ não vazio, é dito *fechado* para a operação $*$, ou $*$ é dita fechada em A, se (e somente se) $x * y \in A$ quaisquer que sejam $x, y \in A$.

Observe que, um subconjunto A de E, ser fechado para uma operação $*$ significa que $*$ define uma operação sobre A.

Exemplo 1.32. Considerando o conjunto $E = \mathbb{R}$ dos números reais. O subconjunto $A = \mathbb{N} \subset E$ dos números naturais é fechado para o produto e a soma, mas não é fechado para a diferença. O subconjunto $B = \mathbb{Q}$ dos números racionais, é fechado para a soma, o produto e a diferença. O conjunto $C = \mathbb{R} - \mathbb{Q}$ dos números irracionais não é fechado para a soma, para o produto e para a diferença. ■

Exemplo 1.33. Seja $E = \mathbb{R}^{\mathbb{R}} = \{f : \mathbb{R} \to \mathbb{R}; \quad f \text{ é função}\}$ o conjunto das funções de $\mathbb{R}$ em $\mathbb{R}$ com a composição de funções. O subconjunto $I \subset E$ das funções injetoras é fechado para a composição, pois sabemos que a composta de duas funções injetoras é ainda injetora. ■

Exemplo 1.34. Consideremos o conjunto $E = M_2(\mathbb{R})$ das matrizes de ordem 2×2 com coeficientes reais, e o subconjunto $M = \{A \in E; \quad \det(A) \neq 0\} \subset E$. O conjunto M não é fechado para a soma de matrizes, pois é possível encontrar duas matrizes A e B, invertíveis, tais que sua soma é uma matriz não invertível. No entanto este conjunto é fechado para o produto de matrizes, pois é conhecido que se A e B são inversíveis, o produto $A \cdot B$ é inversível também, isto é, $A \cdot B \in M$. ■

Quando o conjunto $E = \{a_1, a_2, \ldots, a_n\}$ possui poucos elementos, é comum representar os resultados da operação $x * y$ em uma tabela. Nesta tabela, colocamos na primeira linha, e na primeira coluna, os elementos de E, que chamaremos respectivamente de linha fundamental e coluna fundamental, ou linha e coluna das entradas, e serão numeradas como linha 0 e coluna 0.

$*$	a_1	a_2	$\cdots$	a_m
a_1				
a_2				
$\vdots$				
a_m				

No interior da tabela, são encontrados os elementos a_{ij} obtidos por $a_{ij} = a_i * a_j$ para $1 \leq i, j \leq m$. Desta forma temos

$*$	a_1	a_2	$\cdots$	a_j	$\cdots$	a_m
a_1	a_{11}	a_{12}	$\cdots$	a_{1j}	$\cdots$	a_{1m}
a_2	a_{21}	a_{22}	$\cdots$	a_{2j}	$\cdots$	a_{2m}
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_i	a_{i1}	a_{i2}	$\cdots$	a_{ij}	$\cdots$	a_{im}
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_m	a_{m1}	a_{m2}	$\cdots$	a_{mj}	$\cdots$	a_{mm}

Exemplo 1.35. Se $E = \{1, -1, i, -i\} \subset \mathbb{C}$, com a operação $x * y = x \cdot y$, o produto usual de complexos, temos,

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

■

Exemplo 1.36. Considerando $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$ um conjunto de funções de $\mathbb{R}$ em $\mathbb{R}$, dadas por $f_1(x) = x$, $f_2(x) = |x|$, $f_3(x) = -x$ e $f_4(x) = -|x|$, com a operação de composição de

funções usual, temos

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_2	f_2	f_2
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_4	f_4	f_4

■

Suponha que uma operação $*$ seja dada pela sua tábua, sem especificar explicitamente a lei de composição. Algumas propriedades desta operação podem ser detectadas observando a sua tábua.

A comutatividade de $*$ é dada pela lei $x * y = y * x$ para quaisquer $x, y \in E$. Se $x = a_i$ e $y = a_j$ então $x * y = y * x$ significa que $a_i * a_j = a_j * a_i$ e portanto $a_{ij} = a_{ji}$. Desta forma, a propriedade comutativa ocorre quando a tabela for simétrica com relação à sua diagonal principal.

A existência de um elemento neutro $e \in E$ à esquerda e à direita é dada pelas leis $e * x = x$ e $x * e = x$ respectivamente para qualquer $x \in E$. Se $e = a_i$ e $x = a_j$ então $e * x = x$ se resume em $a_{ij} = a_i * a_j = a_j$. Desta forma o elemento neutro à esquerda será o elemento a_i da coluna fundamental, cuja linha é igual a linha fundamental. Isto é,

	a_1	a_2	a_3	$\cdots$	a_m
$\vdots$					
$e = a_i$	a_1	a_2	a_3	$\cdots$	a_m
$\vdots$					

Analogamente, se $x = a_i$ e $e = a_j$ então $x * e = x$ significa que $a_{ij} = a_i * a_j = a_i$, e assim, o elemento neutro à direita será o elemento da linha fundamental, cuja coluna é igual à coluna fundamental. Isto é,

	$\cdots$	$e = a_j$	$\cdots$
a_1		a_1	
a_2		a_2	
$\vdots$		$\vdots$	
a_m		a_m	

Caso exista um elemento neutro em E para a operação $*$, então, os elementos simetrizáveis de E são os elementos x tais que existe um x' que satisfaz $x * x' = x' * x = e$, e assim, procuramos os a_i e a_j em E tais que $a_i * a_j$ e $a_j * a_i$ sejam iguais a e, isto é, $a_{ij} = a_{ji} = e$, ou ainda, o elemento neutro aparece nas linhas e colunas de a_i e a_j em posições simétricas, com

relação à diagonal principal. Na tábua, temos

$*$	a_1	$\cdots$	a_i	$\cdots$	a_j	$\cdots$	a_m
a_1	a_{11}		a_{1i}		a_{1j}		a_{1m}
$\vdots$			$\vdots$		$\vdots$		
a_i	a_{i1}	$\cdots$		$\cdots$	e		
$\vdots$			$\vdots$				
a_j	a_{j1}	$\cdots$	e				
$\vdots$							
a_m	a_{m1}						a_{mm}

Finalmente os elementos regulares também podem ser localizados na tábua. O elemento a é um elemento regular à esquerda se $a * x = a * y$ implicar que $x = y$, para quaisquer $x, y \in E$. Equivalentemente, se $x \neq y$ devemos ter $a * x \neq a * y$. Isto significa que os diferentes elementos a_i quando operados com a resultam em elementos distintos também, e assim, procuramos na tábua qualquer elemento a que encabeça uma linha constituída de elementos todos distintos

	a_1	a_2	$\cdots$	a_m
a	a_{k_1}	a_{k_2}	$\cdots$	a_{k_m}

sendo que $a_{k_i} \neq a_{k_j}$ se $1 \leq i \neq j \leq m$. O elemento a será o elemento regular à esquerda para a operação de E. Analogamente, o elemento regular à direita será o elemento a cuja coluna é constituída de elementos todos distintos, isto é,

	a
a_1	a_{k_1}
a_2	a_{k_2}
$\vdots$	
a_m	a_{k_m}

desde que $a_{k_i} \neq a_{k_j}$ quando $1 \leq i \neq j \leq m$, e neste caso, o elemento a será dito elemento regular à direita para a operação definida em E. Se a linha e a coluna do elemento a forem ao mesmo tempo constituídas de elementos todos distintos, então o elemento a é dito simplesmente elemento regular para a operação $*$.

Exemplo 1.37. Considere $E = \{a, b, c, d\}$ com a operação $*$ dada pela tábua,

$*$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

então temos que $*$ é comutativa, pois a tábua é simétrica com relação à diagonal principal. O elemento neutro à direita e à esquerda é b, pois as coluna e a linha encabeçadas por b são

iguais às coluna e linha fundamental respectivamente. Os elementos simetrizáveis são b, pois é o elemento neutro, e os elementos c e d pois o elemento neutro b aparece nas linhas e colunas de c e d em posição simétrica. Os elementos regulares são b, c e d, pois as linhas e colunas encabaçadas por estes elementos são constituídas de elementos distintos. ■

Capítulo 2

Grupos

Neste capítulo começamos o estudo das estruturas algébricas, especificamente a que chamaremos de grupo. Uma estrutura algébrica pode ser entendida como uma $(n+1)$-upla ordenada $(C, *_1, *_2, \ldots, *_n)$, composta de um conjunto não vazio C, e n operações em C, com $n \geq 1$. Uma estrutura $(C, *_1, *_2, \ldots, *_n)$, é classificada de acordo com a quantidade de operações, e principalmente, de acordo com as propriedades que estas operações possuírem.

Um conjunto G não vazio, munido de uma operação $*$, que satisfaz a lei associativa é chamado de *semigrupo*. Um conjunto M não vazio, munido de uma operação $*$, que satisfaz a lei associativa, e que admite um elemento neutro $0_M \in M$, é dito um *monóide*.

A notação $(M, *)$ denota que M munido da operação $*$ é um monóide. Em virtude de considerarmos uma única operação em M, o elemento 0_M é dito também elemento neutro de M. Devemos tomar o cuidado de não confundir o número 0 com o elemento 0_M que representa um elemento qualquer do conjunto M, que satisfaz a condição $m * 0_M = 0_M * m = m$ para todo $m \in M$. Este elemento neutro é comumente identificado pelo símbolo e_M, ou simplesmente e, quando não houver possibilidade de confusão.

Se além das duas condições da definição anterior, a operação $*$ for comutativa, então M é dito um *monóide comutativo* .

Um subconjunto $S \subset M$ de um monóide $(M, *)$, é dito um *submonóide* se ele próprio for um monóide. De outra forma, se $0_M \in S$, e se S for fechado para a operação $*$, isto é, $a * b \in S$ para todos $a, b \in S$.

Exemplo 2.1. O conjunto $\mathbb{N}$ com a operação de adição de números é um monóide. O elemento neutro é o número 0 ($0_M = 0$). O mesmo conjunto $\mathbb{N}$ com a operação de produto de números também é um monóide. Neste caso, o elemento neutro é o número 1 ($0_M = 1$). Note que a adição e a multiplicação de números são operações associativas. ■

Exemplo 2.2. (O monóide das transformações de um conjunto $\mathcal{A}$) Suponha dado um conjunto não vazio $\mathcal{A}$. O conjunto $\mathcal{T}(\mathcal{A})$, das transformações $f : \mathcal{A} \to \mathcal{A}$, com a operação de composição de transformações é um monóide, pois a composição de transformações é associativa e $\mathcal{T}(\mathcal{A})$ admite um elemento neutro que é a transformação identidade $f(x) = x$ para todo $x \in \mathcal{A}$. Se o conjunto $\mathcal{A}$ possui pelo menos dois elementos distintos, então $\mathcal{T}(\mathcal{A})$ é certamente não comutativo. Tente

verificar esta última afirmação. ■

Exemplo 2.3. Os conjuntos $M = \mathbb{Z}_m$, com a operação de multiplicação de classes de equivalência módulo m, é um monóide comutativo para qualquer $2 \leq m \in \mathbb{N}$. De fato, já mostramos que a multiplicação é uma operação associativa e comutativa em $\mathbb{Z}_m$, e o elemento neutro é $0_M = \overline{1}$. ■

2.1 Grupos e subgrupos

Definição 2.1. Seja G um conjunto não vazio e $*$ uma operação em G. Dizemos que G, com a operação $*$, é um *grupo* se

i) $*$ é associativa, isto é, $a * (b * c) = (a * b) * c$ para todos $a, b, c \in G$,

ii) $*$ admite elemento neutro, isto é, existe $e_G \in G$, tal que, $a * e_G = e_G * a = a$, para todo $a \in G$, e

iii) todo $a \in G$ é simetrizável, isto é, dado qualquer $a \in G$, existe $a' \in G$, tal que, $a * a' = a' * a = e_G$.

Podemos dizer que G é grupo sobre a operação $*$, ou ainda a operação $*$ define em G uma estrutura de grupo, uma vez que G só torna-se grupo devido às propriedades da operação $*$ envolvida. O mesmo conjunto G, pode não ser um grupo, se considerada alguma outra operação. Deste ponto em diante, poderemos algumas vezes afirmar que um conjunto não vazio G é um grupo. Isto significará que existe uma operação sobre a qual G torna-se um grupo.

É comum usar a notação na forma de par ordenado $(G, *)$ e a expressão "grupo $(G, *)$", para dizer que o conjunto G é um grupo com a operação $*$.

O elemento neutro e_G é também denotado por 0_G, e apesar disto, nem sempre é o número 0. Também usamos simplesmente e ou 0 quando não houver possibilidade de confusão com o grupo G envolvido. Usaremos preferencialmente a notação e pois a notação 0 pode causar confusão quando o elemento neutro não é o número 0. Deste ponto em diante, e sempre representará o elemento neutro para a operação de um grupo.

Observe que, um conjunto não vazio com uma operação associativa é um semigrupo. Um semigrupo com elemento neutro, é um monóide. Um monóide com todos os elementos simetrizáveis, é um grupo.

Definição 2.2. Dado um grupo $(G, *)$, dizemos que G é *grupo abeliano*[1] ou *grupo comutativo* se a operação $*$ for comutativa, isto é, $a * b = b * a$ para todos $a, b \in G$.

A teoria envolvendo os grupos abelianos é muito importante. Alguns autores dedicam capítulo separado para o estudo dos grupos abelianos. Como veremos adiante, alguns resultados sobre grupos, serão válidos apenas para os grupos abelianos.

[1] O nome grupo abeliano é devido ao matemático norueguês Niels Henrik Abel (Ver A.1).

Exemplo 2.4. Os conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, com a operação de adição de números, representada pelo sinal $+$, são grupos. Todos eles são também abelianos (comutativos). O conjunto $\mathbb{N}$ com esta operação não é grupo. Embora $+$ seja associativa e possua elemento neutro, o elemento neutro é o único elemento simetrizável em $\mathbb{N}$ pela operação $+$. Consideremos agora os conjuntos $\mathbb{Q}^*$, $\mathbb{R}^*$ e $\mathbb{C}^*$, com a operação de produto de números, representada por $\cdot$. Estes conjuntos são grupos abelianos. Note que agora o elemento neutro é o número 1. Observe que $\mathbb{Z}^*$ não é grupo pois 1 e -1 são os únicos elementos simetrizáveis de $\mathbb{Z}^*$ para $\cdot$. ■

Exemplo 2.5. O conjunto $\mathcal{M} = M_{n\times n}(\mathbb{R})$, das matrizes quadradas de ordem $n \geq 2$ com coeficientes reais, com a operação de adição usual de matrizes é um grupo abeliano. De fato a adição de matrizes é associativa, o elemento neutro e deste conjunto é a matriz nula que representaremos por 0, e para cada matriz $A \in \mathcal{M}$ existe a matriz oposta $-A \in \mathcal{M}$, que satisfaz $A + (-A) = 0$. ■

Exemplo 2.6. O conjunto das funções $\mathcal{F} = \mathbb{R}^{\mathbb{R}} = \{f : \mathbb{R} \to \mathbb{R}\}$ com a operação de soma de funções é um grupo. O elemento neutro e para esta operação é a função identicamente nula $e = 0_{\mathcal{F}} = f$, onde $f(x) = 0$ para todo $x \in \mathbb{R}$. É um grupo abeliano. Note que este mesmo conjunto com a operação de composição de funções não é grupo, pois embora a composição de funções seja associativa e admita elemento neutro (a função identidade) nem todo elemento de $\mathcal{F}$ é simetrizável, isto é, é invertível. O conjunto das funções invertíveis $F = \{f : \mathbb{R} \to \mathbb{R}; f \text{ possui inversa}\}$ com a operação de composição de funções é um grupo. O elemento neutro $e = 0_F$ deste grupo é a função identidade $Id(x) = x$. Não é um grupo abeliano, pois em geral $f \circ g \neq g \circ f$. ■

Exemplo 2.7. O que vamos apresentar agora é um dos exemplos mais importantes de grupo, chamado grupo das classes de equivalência $\mathbb{Z}$ módulo m. Dado $m \geq 2$ um número inteiro, consideremos o conjunto $G = \mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$, como construído na seção 1.4. Lembremos que para cada $a \in \mathbb{Z}$ temos $\overline{a} = \{x \in \mathbb{Z};\, x \sim a\}$, sendo que $x \sim a$, se e somente se $m|(x-a)$. Também como verificado na proposição 1.33, temos que $x \sim a$, se e somente se, $\overline{a} = \overline{x}$. Vamos definir neste conjunto uma operação e verificar que esta operação torna este conjunto um grupo. Para cada $\overline{a}, \overline{b} \in \mathbb{Z}_m$, definimos a soma $\overline{a} + \overline{b}$ por

$$\overline{a} + \overline{b} = \overline{a+b}.$$

Observe que no primeiro membro temos a soma de duas classes, enquanto no segundo membro a soma incide sobre os representantes a e b. Uma pergunta natural surge agora. Já que a não é o único elemento que está na classe $\overline{a}$, perguntamos se a soma ainda é a mesma, no sentido da relação de equivalência, tomando outro elemento da classe $\overline{a}$ (ou da classe $\overline{b}$). O que faremos então é mostrar que a operação está bem definida, isto é, dados $a \sim x$ e $b \sim y$ mostraremos que $\overline{a} + \overline{b} = \overline{x} + \overline{y}$. Se $a \sim x$ e $b \sim y$ então $m|(a-x)$ e $m|(b-y)$, e assim $m|(a-x+b-y)$ ou $m|((a+b)-(x+y))$ e da definição da relação segue que $(a+b) \sim (x+y)$ ou ainda, $\overline{a+b} = \overline{x+y}$. Então $\overline{a} + \overline{b} = \overline{a+b} = \overline{x+y} = \overline{x} + \overline{y}$, e a operação está bem definida. Agora, dados $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, temos

$$\begin{aligned}(\overline{a} + \overline{b}) + \overline{c} &= \overline{a+b} + \overline{c} = \overline{(a+b)+c} \\ &= \overline{a+(b+c)} = \overline{a} + \overline{b+c} = \overline{a} + (\overline{b} + \overline{c}),\end{aligned}$$

e também

$$\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a},$$

donde segue a associatividade e a comutatividade de $+$. Procuramos agora um elemento neutro para $+$, isto é, desejamos encontrar $x \in \mathbb{Z}$, de forma que $\overline{x} \in \mathbb{Z}_m$ satisfaça $\overline{a} + \overline{x} = \overline{x} + \overline{a} = \overline{a}$ para todo $\overline{a} \in \mathbb{Z}_m$. Da igualdade $\overline{a} + \overline{x} = \overline{a}$ vem que $\overline{a+x} = \overline{a}$ e da definição de relação que $m|(a + x - a)$, ou ainda, $m|x$. Em outras palavras x é múltiplo de m, isto é, $x = km$ para qualquer $k \in \mathbb{Z}$. Mas os elementos da forma km são pertencentes à classe $\overline{0}$, e portanto $e = \overline{x} = \overline{0}$. Finalmente vamos mostrar que todo $\overline{a} \in \mathbb{Z}_m$ é simetrizável. Dado $\overline{a} \in \mathbb{Z}_m$ procuramos um elemento $x \in \mathbb{Z}$, de forma que $\overline{x} = (\overline{a})'$, chamado simétrico de $\overline{a}$, e que satisfaz $\overline{a} + \overline{x} = \overline{x} + \overline{a} = e = \overline{0}$. Desta igualdade, segue que $\overline{a} + \overline{x} = \overline{0}$, ou ainda, $\overline{a+x} = \overline{0}$ e da definição de relação $m|(a + x - 0)$. Em outras palavras, $a + x$ é múltiplo de m, isto é, $a + x = km$ para $k \in \mathbb{Z}$, donde segue que $x = (-a) + km$. Os números da forma $(-a) + km$ são pertencentes à classe $\overline{-a}$ ou ainda à classe $\overline{m-a}$, já que $(-a) + km = (m - a) + (k - 1)m$. Segue que todo elemento $\overline{a} \in \mathbb{Z}_m$ é simetrizável sendo $\overline{m-a}$ o seu simétrico. Isto posto, os conjuntos $\mathbb{Z}_m$ são grupos abelianos sob a operação de soma de classes para qualquer inteiro $m \geq 2$. ■

Exemplo 2.8. Vamos verificar agora que a operação de multiplicação (de classes de equivalência) não torna o conjunto $G = \mathbb{Z}_m$ um grupo. Dado $m \geq 2$, consideremos em $\mathbb{Z}_m$ a operação de multiplicação de classes

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{ab},$$

que primeiro, precisamos mostrar que está bem definida. De fato, dados $a \sim x$ e $b \sim y$, então $m|(a - x)$ e $m|(b - y)$, e assim $m|(a - x)b$ e $m|(b - y)x$, donde $m|[(a - x)b + (b - y)x]$. Isto é, $m|(ab - xb + bx - yx)$ ou $m|(ab - xy)$ e da definição da relação segue que $(ab) \sim (xy)$ ou ainda, $\overline{ab} = \overline{xy}$.

É fácil ver (como no caso da adição) que $\cdot$ é associativa e comutativa. Desejamos agora obter $x \in \mathbb{Z}$, tal que $\overline{x} \in \mathbb{Z}_m$ satisfaça $\overline{a} \cdot \overline{x} = \overline{a}$ para todo $\overline{a} \in \mathbb{Z}_m$. Desta igualdade, temos que $\overline{ax} = \overline{a}$ e da definição da relação $m|(ax - a)$ ou $m|a(x - 1)$. Mas como $\overline{a}$ é arbitrário em $\mathbb{Z}_m$, não há garantias que m divide a, mais ainda, pode ocorrer que $\text{mdc}(a, m) = 1$. Sendo assim, pedimos que $m|(x - 1)$, ou ainda $x \sim 1$ o que é equivalente a $\overline{x} = \overline{1}$. Segue que $\overline{1}$ é o elemento neutro para a multiplicação de classes. Apesar disto, $\overline{0} \cdot \overline{x} = \overline{0 \cdot x} = \overline{0}$ para qualquer $\overline{x} \in \mathbb{Z}_m$, e assim $\overline{0}$ não é simetrizável em $\mathbb{Z}_m$ para a operação $\cdot$, já que não existe $\overline{x} \in \mathbb{Z}_m$ tal que $\overline{0} \cdot \overline{x} = \overline{1}$. Portanto $\mathbb{Z}_m$ com a operação de multiplicação não é um grupo.

Contudo, podem existir elementos (não nulos) simetrizáveis para a operação de multiplicação em $\mathbb{Z}_m$. Dado $\overline{a} \in \mathbb{Z}_m$, queremos investigar em que situação existe $x \in \mathbb{Z}$, de forma que $\overline{x} \in \mathbb{Z}_m$ satisfaça $\overline{x} \cdot \overline{a} = \overline{1}$, ou ainda $\overline{xa} = \overline{1}$. Mas isto significa que $m|(xa - 1)$, ou ainda que $(xa - 1)$ é múltiplo de m. Desta forma, existe $k \in \mathbb{Z}$ tal que $(xa - 1) = km$. Em resumo, dados $a, m \in \mathbb{Z}$, queremos que existam $x, k \in \mathbb{Z}$, tais que $xa + (-k)m = 1$. De acordo com o corolário 1.9, existem x e k que cumprem esta igualdade se e somente se $\text{mdc}(a, m) = 1$. Desta forma, dado $\overline{a} \in \mathbb{Z}_m$ temos que $\overline{a}$ admite simétrico pela operação multiplicação se e somente se $mdc(a, m) = 1$, isto é, se e somente se a e m forem primos entre si. Em particular, se m for um número primo então todo $\overline{a} \in \mathbb{Z}_m$, com $\overline{a} \neq \overline{0}$, cumpre $\text{mdc}(a, m) = 1$ e portanto, se m é um número primo, todo $\overline{a}$ não nulo é simetrizável para a multiplicação de classes em $\mathbb{Z}_m$. Segue que,

se $m \geq 2$ for um número primo, $\mathbb{Z}_m^* = \{\overline{1}, \overline{2}, \ldots, \overline{m-1}\}$ é um grupo abeliano sobre a operação de multiplicação de classes. ■

Proposição 2.3. *Seja $(G, *)$ um grupo. Então,*

i) o elemento neutro e_G é único,

ii) para qualquer $a \in G$, o simétrico a' é único, e além disso $(a')' = a$,

iii) para quaisquer $a, b \in G$, $(a * b)' = b' * a'$,

iv) todo elemento $a \in G$ é regular para a operação $*$.

As demonstrações destes quatro itens já foram feitas nos Corolários (1.65) e (1.68) e nas Proposições (1.69) e (1.71). Estamos apenas reescrevendo para evidenciar a sua validade em um grupo.

Estamos agora procurando subconjuntos S não vazios, de um grupo G, de forma que S seja ele próprio um grupo.

Definição 2.4. Seja $(G, *)$ um grupo e S um subconjunto não vazio de G. S é dito um *subgrupo* de G, se

i) S é fechado para a operação $*$, isto é, $a * b \in S$ para todos $a, b \in S$.

ii) $(S, *)$ também é grupo.

É imediato que $S_1 = \{e_G\}$ e $S_2 = G$ são subgrupos de G. São chamados de subgrupos triviais de G.

Definição 2.5. Um subgrupo M de um grupo $(G, *)$ é dito um subgrupo maximal se, $M \neq G$ e o único subgrupo de G que contém M, e é diferente de M, for o próprio G. Isto é, se S é um subgrupo de G, com $M \subsetneq S \subset G$, então $S = G$.

Proposição 2.6. *Seja S um subgrupo de um grupo $(G, *)$. Então os elementos neutros de S e de G são os mesmos, e se $a \in S \subset G$ então o simétrico de a é o mesmo em S e em G.*

Prova. Para a primeira afirmação, sejam e_S e e_G os elementos neutros para a operação $*$ em S e em G respectivamente. Observemos que $e_S * e_S = e_S$ em S, e que $e_S * e_G = e_S$ em G. Desta forma $e_S * e_S = e_S * e_G$ e da regularidade de $e_S \in S \subset G$, temos que $e_S = e_G$.

Para a segunda afirmação, dado $a \in S \subset G$ arbitrário, sejam a_S e a_G os simétricos de a em S e em G respectivamente. Então,

$$a_S = a_S * e = a_S * (a * a_G) = (a_S * a) * a_G = e * a_G = a_G.$$

□

O próximo resultado nos oferece um método mais rápido e bastante seguro para afirmar quando um subconjunto não vazio, $S \subset G$, é um subgrupo de G.

Teorema 2.7. *Seja $(G, *)$ um grupo. Um subconjunto não vazio $S \subset G$ é um subgrupo de G, se e somente se, $(a * b') \in S$ para todos $a, b \in S$.*

Prova. Suponha S subgrupo de G. Então para quaisquer $a, b \in S$, temos também $b' \in S$, e sendo S fechado para a operação $*$ segue que $a * b' \in S$.

Reciprocamente, suponha que $(a * b') \in S$ para todos $a, b \in S$. Primeiro observamos que como S herdou a operação $*$ de G e $*$ é associativa em G, então $*$ é também associativa em S. Como $S \neq \emptyset$, então existe $a \in S$, e por hipótese $(a * a') \in S$, isto é, $e \in S$. Então S possui o elemento neutro e. Se $a \in S$, então como já sabemos $e \in S$, e por hipótese, $(e * a') \in S$, isto é, $a' \in S$. Então todo elemento de S admite simétrico. Dados $a, b \in S$, do passo anterior, $b' \in S$, e por hipótese, $(a * (b')') \in S$, isto é, $(a * b) \in S$ e então S é fechado para a operação $*$. Segue que S é também um grupo, e portanto um subgrupo de G. □

Definição 2.8. Considere um grupo $(G, *)$. Dado um elemento $a \in G$, e um subconjunto $B \subset G$, definimos o subconjunto a operado com B, denotado por $a * B$, como sendo

$$a * B = \{a * b; \quad b \in B\}.$$

Da mesma forma, definimos o subconjunto $B * a$, dito B operado com a, como sendo

$$B * a = \{b * a; \quad b \in B\}.$$

Assim, dizer que $x \in a * B$, significa que existe $y \in B$ tal que $x = a * y$, e dizer que $x \in B * a$ significa que existe $y \in B$ tal que $x = y * a$. Se $B = \emptyset$ então $a * B = B * a = \emptyset$ para qualquer elemento $a \in G$, e se a é o elemento neutro de G, então $a * B = B * a = B$. De qualquer forma, é obrigatório que $a * B \subset G$ e também $B * a \subset G$.

Definição 2.9. Dado um grupo $(G, *)$, e dois subconjuntos $A, B \subset G$. Definimos o subconjunto A operado com B, denotado por $A * B$ como sendo

$$A * B = \{a * b; \quad \text{para todos} \quad a \in A \quad \text{e} \quad b \in B\}.$$

Desta forma, todo elemento $x \in A * B$, é escrito na forma $x = a * b$ para algum $a \in A$ e algum $b \in B$. Note também que se $A = \emptyset$ ou $B = \emptyset$ então temos $A * B = \emptyset$. Além disso, se G for abeliano, então $A * B = B * A$. Um outro fato importante é que se A e B forem subgrupos do grupo G, então $A * B$ também será subgrupo de G e além disso, $A \subset (A * B) \subset G$ e também $B \subset (A * B) \subset G$. Deixaremos a prova destes fatos como exercício.

2.2 Homomorfismos e isomorfismos

Definição 2.10. Dados $(G, *)$ e $(H, \circ)$, dois grupos, uma aplicação $\varphi : G \to H$ é dita um *homomorfismo* de G em H, se

$$\varphi(a * b) = \varphi(a) \circ \varphi(b),$$

para todos $a, b \in G$.

Se φ for um homomorfismo de um grupo G no mesmo grupo G, então φ é chamada de *endomorfismo*. Se φ é um homomorfismo injetor então φ é chamada de *monomorfismo*. Se φ é homomorfismo sobrejetor, então φ é dita um *epimorfismo*. Cuidado para não confundir homomorfismo com homeomorfismo. Um homeomorfismo é uma aplicação contínua que admite inversa também contínua.

Definição 2.11. Uma aplicação $\eta : G \to H$ é dita um *isomorfismo* de G em H, se η for um homomorfismo bijetor. No caso de existir um isomorfismo η entre os grupos G e H, então dizemos que G e H são *isomorfos*, e representamos este fato escrevendo $G \approx H$.

Um isomorfismo $\eta : G \to G$ de um grupo G nele mesmo, é chamado de *automorfismo.*

Exemplo 2.9. Se $(G, *)$ e $(H, \cdot)$ são grupos, então a aplicação $\varphi : G \to H$ dada por $\varphi(x) = 0_H = e_H$ para todo $x \in G$, é um homomorfismo. É chamado de homomorfismo trivial. ■

Exemplo 2.10. Sejam $G = (\mathbb{R}, +)$ e $H = (\mathbb{R}_+^*, \cdot)$ os grupos dos reais aditivos e multiplicativos respectivamente. A aplicação definida por

$$\begin{array}{rcl} \varphi : G & \to & H \\ x & \mapsto & \varphi(x) = e^x \end{array}$$

é um homomorfismo. De fato $\varphi(x + y) = e^{x+y} = e^x \cdot e^y = \varphi(x) \cdot \varphi(y)$ para todos $x, y \in \mathbb{R}$. É ainda um homomorfismo bijetor. ■

Exemplo 2.11. Considerando $G = (\mathbb{R} \times \mathbb{R}, +)$ com a soma induzida pelo produto cartesiano, e $H = (\mathbb{R}, +)$ com a operação de adição usual. A aplicação

$$\begin{array}{rcl} \eta : G & \to & H \\ (x, y) & \mapsto & \eta(x, y) = x - y \end{array}$$

é um homomorfismo, pois

$$\eta((x, y) + (z, w)) = \eta(x + z, y + w) = x + z - y - w = \eta(x, y) + \eta(z, w),$$

é sobrejetor, mas não é injetor. ■

Exemplo 2.12. Considerando $G = (\mathbb{C}^*, \cdot)$ e $H = (\mathbb{R}^*, \cdot)$ dois grupos, a aplicação

$$\begin{array}{rcl} f : G & \to & H \\ z & \mapsto & f(z) = |z| \end{array}$$

é um homomorfismo, pois dados quaisquer $z, w \in \mathbb{C}^*$, temos que $f(z \cdot w) = |z \cdot w| = |z| \cdot |w| = f(z) \cdot f(w)$. Não é um homomorfismo injetor e nem sobrejetor. ■

Proposição 2.12. *Sejam $\varphi : (G, *) \to (H, \cdot)$ e $\eta : (H, \cdot) \to (S, \oplus)$ dois homomorfismos. Então a composta $\eta \circ \varphi$ é também um homomorfismo entre os grupos $(G, *)$ e $(S, \oplus)$.*

Prova. Sejam $x, y \in G$. Então

$$\begin{aligned} (\eta \circ \varphi)(x * y) &= \eta(\varphi(x * y)) = \eta(\varphi(x) \cdot \varphi(y)) \\ &= \eta(\varphi(x)) \oplus \eta(\varphi(y)) = (\eta \circ \varphi)(x) \oplus (\eta \circ \varphi)(y), \end{aligned}$$

que prova que $(\eta \circ \varphi)$ é um homomorfismo. □

Corolário 2.13. *A aplicação composta de dois isomorfismos é também um isomorfismo.*

Proposição 2.14. *Se $\varphi : G \to H$ é um homomorfismo bijetor entre os grupos $(G, *)$ e $(H, \circ)$, então, $\varphi^{-1} : H \to G$ é também um homomorfismo.*

Prova. Sejam $x, y \in H$, então como φ é sobrejetor, existem $a, b \in G$ tais que $\varphi(a) = x$ e $\varphi(b) = y$, e consequentemente $\varphi^{-1}(x) = a$ e $\varphi^{-1}(y) = b$. Assim

$$\varphi^{-1}(x \cdot y) = \varphi^{-1}(\varphi(a) \circ \varphi(b)) = \varphi^{-1}(\varphi(a * b)) = a * b = \varphi^{-1}(x) * \varphi^{-1}(y),$$

que prova que φ^{-1} é um homomorfismo. □

Corolário 2.15. *A aplicação inversa de um isomorfismo é também um isomorfismo.*

Proposição 2.16. *Dados dois grupos $(G, *)$ e $(H, \circ)$, e $\varphi : G \to H$ um homomorfismo. Então,*
i) $\varphi(e_G) = e_H$,
ii) $\varphi(a') = (\varphi(a))'$ para todo $a \in G$.

Prova. Para provar (i), como $e_G \in G$ então $\varphi(e_G) \in H$ e sendo H um grupo, existe $(\varphi(e_G))' \in H$, de forma que $\varphi(e_G) \circ (\varphi(e_G))' = e_H$. Desta forma,

$$\begin{aligned} e_H = \varphi(e_G) \circ (\varphi(e_G))' &= \varphi(e_G * e_G) \circ (\varphi(e_G))' \\ &= (\varphi(e_G) \circ \varphi(e_G)) \circ (\varphi(e_G))' \\ &= \varphi(e_G) \circ \big(\varphi(e_G) \circ (\varphi(e_G))'\big) = \varphi(e_G) \circ e_H = \varphi(e_G). \end{aligned}$$

Para mostrar (ii), basta provar que dado $a \in G$ tem-se $\varphi(a') \circ \varphi(a) = \varphi(a) \circ \varphi(a') = e_H$. De fato,

$$\varphi(a) \circ \varphi(a') = \varphi(a * a') = \varphi(e_G) = e_H,$$

e também

$$\varphi(a') \circ \varphi(a) = \varphi(a' * a) = \varphi(e_G) = e_H.$$

Desta forma o elemento $\varphi(a)$ é simetrizável em H sendo $\varphi(a')$ o seu simétrico. Em outras palavras, $(\varphi(a))' = \varphi(a')$. □

O próximo resultado garante que imagem direta e imagem inversa de subgrupo, por um homomorfismo, é subgrupo também.

Proposição 2.17. *Sejam $(G, *)$ e $(H, \circ)$ dois grupos e $\varphi : G \to H$ um homomorfismo entre G e H. Então,*

i) Se S é subgrupo de G, então $\varphi(S)$ é subgrupo de H.

ii) Se S é subgrupo de H, então $\varphi^{-1}(S)$ é subgrupo de G, onde $\varphi^{-1}(S)$ significa imagem inversa de S por φ.

Prova. Para provarmos (i), suponha S um subgrupo de G, então S é não vazio, e assim $\varphi(S)$ é não vazio em H. Além disso, dados $x, y \in \varphi(S)$, existem $a, b \in S$, tais que $x = \varphi(a)$ e $y = \varphi(b)$. Então,

$$x \circ y' = \varphi(a) \circ (\varphi(b))' = \varphi(a) \circ \varphi(b') = \varphi(a * b'),$$

e como S é subgrupo, $a * b' \in S$, decorre que $x \circ y' = \varphi(a * b') \in \varphi(S)$, e pela proposição (2.7), $\varphi(S)$ é subgrupo de H.

Para provar (ii), suponha S subgrupo de H. Sejam $x, y \in \varphi^{-1}(S)$, então $\varphi(x) \in S$ e $\varphi(y) \in S$, e como S é subgrupo de H, temos que $\varphi(x) \circ (\varphi(y))' \in S$. Mas $\varphi(x) \circ (\varphi(y))' = \varphi(x * y')$ e então $\varphi(x * y') \in S$, donde $x * y' \in \varphi^{-1}(S)$, e portanto da proposição (2.7), $\varphi^{-1}(S)$ é subgrupo de G. □

Uma consequência imediata desta proposição é que se $\varphi : (G, *) \to (H, \circ)$ é um homomorfismo, então $Im(\varphi) = \varphi(G)$, é um subgrupo de H.

Definição 2.18. Sejam $(G, *)$ e $(H, \circ)$ dois grupos e $\varphi : G \to H$ um homomorfismo. O *núcleo* de φ, denotado por $N(\varphi)$ ou $Ker(\varphi)$, é o conjunto

$$Ker(\varphi) = \{x \in G; \quad \varphi(x) = e_H\},$$

de todos os elementos de G que são levados em e_H pela aplicação φ.

A notação $Ker(\varphi)$ vem do termo inglês kernel que significa núcleo. Observe que $x \in Ker(\varphi)$ se, e somente se, $\varphi(x) = e_H$. Como já vimos, um homomorfismo φ sempre satisfaz $\varphi(e_G) = e_H$, e então $e_G \in Ker(\varphi)$, o que assegura que $Ker(\varphi)$ é sempre um conjunto não vazio. Além disso, se $\varphi : G \to H$ é o homomorfismo trivial, isto é, $\varphi(x) = e_H$ para todo $x \in G$, então $Ker(\varphi) = G$.

Proposição 2.19. *Se $\varphi : G \to H$, é um homomorfismo entre os grupos $(G, *)$ e $(H, \circ)$, então $Ker(\varphi)$ é um subgrupo de G.*

Prova. Uma vez que $Ker(\varphi) \neq \emptyset$, suponha $x, y \in Ker(\varphi)$, isto é, $\varphi(x) = \varphi(y) = e_H$. Assim,

$$\varphi(x * y') = \varphi(x) \circ \varphi(y') = \varphi(x) \circ (\varphi(y))' = e_H \circ (e_H)' = e_H,$$

o que mostra que $(x * y') \in Ker(\varphi)$. Sendo x e y arbitrários, segue da proposição (2.7) que $Ker(\varphi)$ é subgrupo de G. □

Proposição 2.20. *Sejam $(G, *)$ e $(H, \circ)$ dois grupos e $\varphi : G \to H$ um homomorfismo. Então, φ é injetor, se e somente se $Ker(\varphi) = \{e_G\}$.*

Prova. Suponha φ um homomorfismo injetor. Vamos mostrar a dupla inclusão dos conjuntos. Como já comentado anteriormente, $e_G \in Ker(\varphi)$, o que assegura a inclusão $\{e_G\} \subset Ker(\varphi)$. Dado agora $x \in Ker(\varphi)$ temos, $\varphi(x) = e_H = \varphi(e_G)$, e como φ é injetor, temos $x = e_G$ e então $Ker(\varphi) \subset \{e_G\}$.

Suponha agora que $Ker(\varphi) = \{e_G\}$. Sejam $x, y \in G$ tais que $\varphi(x) = \varphi(y)$. Então

$$\varphi(x * y') = \varphi(x) \circ (\varphi(y))' = \varphi(y) \circ (\varphi(y))' = e_H,$$

e assim, $(x * y') \in Ker(\varphi)$, mas como $Ker(\varphi) = \{e_G\}$, devemos ter $(x * y') = e_G$, e então

$$x = x * e_G = x * (y' * y) = (x * y') * y = e_G * y = y,$$

o que prova que φ é injetor. □

2.3 Grupos de translações

Nesta seção vamos construir um dos mais importantes exemplos de grupo, chamado de grupo das translações de um grupo G.

Definição 2.21. Seja $(G, *)$ um grupo e fixemos um elemento $a \in G$. A aplicação

$$\begin{aligned} T_a : G &\to G \\ x &\mapsto T_a(x) = a * x \end{aligned}$$

é chamada translação à esquerda determinada pelo elemento a. Da mesma forma a translação à direita pelo elemento a, é a aplicação $T_a(x) = x * a$.

Consideremos o conjunto de todas as translações T_a de G em G, com $a \in G$, representado por,

$$\mathcal{F}(G) = \{T_a; \quad a \in G\},$$

e chamado de conjunto das translações de G. Queremos mostrar que o conjunto $\mathcal{F}(G)$ juntamente com a composição de aplicações é um grupo. Os próximos resultados tratarão destas questões, e para isso, padronizaremos estes resultados usando as translações pela esquerda e apenas comentaremos as adaptações necessárias para o caso das translações pela direita.

Proposição 2.22. *Sejam $(G, *)$ um grupo e $a, b \in G$. Então*

i) $T_a = T_b$, se e somente se, $a = b$;

ii) $T_a \circ T_b = T_{a*b}$;

iii) Se $e \in G$ é o elemento neutro de G, então T_e é a aplicação identidade de G.

Prova. Para provar (i) notemos que $D(T_a) = G = D(T_b)$ e também $Cd(T_a) = G = Cd(T_b)$. Assim

$$\begin{aligned} T_a = T_b \quad &\Leftrightarrow \quad T_a(x) = T_b(x) \quad \text{para todo} \quad x \in G \\ \Leftrightarrow \quad a * x = b * x \quad &\text{para todo} \quad x \in G \quad \Leftrightarrow \quad a = b. \end{aligned}$$

Para a segunda afirmação, claramente temos que $D(T_a \circ T_b) = G = D(T_{a*b})$, $Cd(T_a \circ T_b) = G = Cd(T_{a*b})$, e também

$$(T_a \circ T_b)(x) = T_a(T_b(x)) = T_a(b * x) = a * (b * x) = (a * b) * x = T_{a*b}(x),$$

para todo $x \in G$. Segue da definição de igualdade de aplicações que $(T_a \circ T_b) = T_{a*b}$.

Para o último item, designando $Id_G : G \to G$ a aplicação identidade de G, temos que $D(T_e) = G = D(Id_G)$, $Cd(T_e) = G = Cd(Id_G)$ e também

$$T_e(x) = e * x = x = Id_G(x),$$

para todo $x \in G$. Segue da definição de igualdade de aplicações que $T_e = Id_G$. □

Para as translações à direita é preciso um ajuste nesta última proposição. Para trasnlações pela direita é válida a igualdade $T_a \circ T_b = T_{b*a}$. As demais propriedades não necessitam de ajustes, sendo válidas também para translações à direita.

Proposição 2.23. *Para cada elemento $a \in G$ a translação T_a é uma aplicação bijetora, e além disso, $(T_a)^{-1} = T_{a'}$.*

Prova. Notemos que a aplicação $T_{a'} : G \to G$ satisfaz

$$(T_a \circ T_{a'})(x) = T_a(T_{a'}(x)) = T_a(a' * x) = a * a' * x = x,$$

e

$$(T_{a'} \circ T_a)(x) = T_{a'}(T_a(x)) = T_{a'}(a * x) = a' * a * x = x,$$

para todo $x \in G$, provando que T_a admite inversas pela direita e pela esquerda. Segue do Teorema 1.56 que T_a é bijetora e além disso $(T_a)^{-1} = T_{a'}$. □

Este último resultado é válido na íntegra para as translações à direita. Nenhuma adequação é necessária.

Teorema 2.24. *Seja $(G, *)$ um grupo. O conjunto de todas as translações pela esquerda definidas por elementos de G, $\mathcal{F}(G) = \{T_a; \quad a \in G\}$, é um grupo com a composição de aplicações.*

Prova. Primeiramente notemos que $\mathcal{F}(G)$ é um conjunto não vazio, pois como G é não vazio, existe pelo menos um $a \in G$ e portanto existe pelo menos uma aplicação T_a definida. Também segue do item (ii) da Proposição 2.22 que a composição é fechada em $\mathcal{F}(G)$, isto é, dados $T_a, T_b \in \mathcal{F}(G)$, temos que $T_a \circ T_b = T_{a*b} \in \mathcal{F}(G)$.

Como já sabemos, a composição de aplicações é uma operação associativa. Também $\mathcal{F}(G)$ possui elemento neutro para a composição de aplicações, pois o elemento neutro da composição de aplicações é a aplicação identidade e $Id_G = T_e \in \mathcal{F}(G)$. Dada $T_a \in \mathcal{F}(G)$, sabemos que o elemento que cumpre a definição de simétrico de T_a é a aplicação $(T_a)^{-1}$ e como $(T_a)^{-1} = T_{a'} \in \mathcal{F}(G)$, então T_a é simetrizável sendo $(T_a)' = (T_a)^{-1} = T_{a'}$.

Segue que $\mathcal{F}(G)$ é grupo com a composição de aplicações. □

Desta forma o conjunto $\mathcal{F}(G)$ com a operação de composição de aplicações, é um grupo, chamado de *grupo das translações* de um grupo G. Tanto o conjunto das translações pela esquerda quanto o conjunto das translações pela direita. Fica claro que este grupo não é necessariamente abeliano já que dados $T_a, T_b \in \mathcal{F}(G)$, em geral

$$(T_a \circ T_b)(x) = a * b * x \neq b * a * x = (T_b \circ T_a)(x),$$

para todos $x \in G$, donde em geral $T_a \circ T_b \neq T_b \circ T_a$. Entretanto, se G for abeliano então $a * b = b * a$ para todos $a, b \in G$ e neste caso teremos $(T_a \circ T_b) = (T_b \circ T_a)$, quaisquer que sejam $T_a, T_b \in \mathcal{F}(G)$.

A respeito deste grupo de translações, temos um teorema muito importante, que é devido a Arthur Cayley[2].

[2]Ver apêndice A.5

Teorema 2.25 (Teorema de Cayley)**.** *Um dado grupo $(G, *)$ é isomorfo ao grupo das translações (à esquerda) $(\mathcal{F}(G), \circ)$.*

Prova. Tomemos a aplicação

$$\begin{aligned} \varphi : G &\to \mathcal{F}(G) \\ a &\mapsto \varphi(a) = T_a \end{aligned}$$

e mostraremos que esta aplicação é um isomorfismo. Para cada $T_a \in \mathcal{F}(G)$ escolhemos $a \in G$ e claramente temos $\varphi(a) = T_a$, o que mostra a sobrejetividade de φ. Sejam $a, b \in G$, com $\varphi(a) = \varphi(b)$. Isto é $T_a = T_b$, e da proposição 2.22 temos que $a = b$, que prova que φ é injetora.

Resta mostrar que φ é homomorfismo. Dados então $a, b \in G$, temos da proposição 2.22 que $T_{a*b} = T_a \circ T_b$, e segue disto que

$$\varphi(a * b) = T_{a*b} = T_a \circ T_b = \varphi(a) \circ \varphi(b),$$

o que prova que φ é homomorfismo. Portanto φ é isomorfismo, e escrevemos $G \approx \mathcal{F}(G)$. □

Observe que se consideradas as translações à direita então na demonstração do teorema anterior teríamos

$$\varphi(a * b) = T_{a*b} = T_b \circ T_a = \varphi(b) \circ \varphi(a),$$

e portanto a aplicação φ definida na última demonstração não é homomorfismo para as translações à direita (a menos que G fosse comutativo). Isto não significa que G não seja isomorfo ao grupo das translações à direita. Significa apenas que esta aplicação não é homomorfismo, mas nada impede de existir outra aplicação entre estes dois grupos que venha a ser homomorfismo. De fato, no caso de translações pela direita, a aplicação

$$\begin{aligned} \varphi : G &\to \mathcal{F}(G) \\ a &\mapsto \varphi(a) = T_{a'} \end{aligned}$$

é um isomorfismo. A bijetividade seguirá de forma convencional e como para as translações pela direita é válida a igualdade $T_a \circ T_b = T_{b*a}$, temos que

$$\varphi(a * b) = T_{(a*b)'} = T_{b'*a'} = T_{a'} \circ T_{b'} = \varphi(a) \circ \varphi(b),$$

e o isomorfismo procurado para o caso das translações pela direita.

2.4 Grupos cíclicos

Definição 2.26. Sejam $(G, *)$ um grupo e $a \in G$. Definimos a n-ésima potência inteira de a dada recursivamente por

$$a^n = \begin{cases} e_G & \text{se} \quad n = 0 \\ a^{n-1} * a & \text{se} \quad n > 0 \\ (a')^{-n} & \text{se} \quad n < 0. \end{cases}$$

Exemplo 2.13. Considere $(G, *) = (\mathbb{Z}_7, +)$ o grupo das classes de equivalência módulo 7, com a operação usual de adição. Escolhemos $a = \overline{4} \in \mathbb{Z}_7$. Então

$$\overline{4}^5 = \overline{4} + \overline{4} + \overline{4} + \overline{4} + \overline{4} = \overline{20} \equiv \overline{6},$$

$$(\overline{4})^{-5} = (\overline{4}')^5 = (\overline{3})^5 = \overline{3} + \overline{3} + \overline{3} + \overline{3} + \overline{3} = \overline{15} \equiv \overline{1}.$$

■

Exemplo 2.14. Considere o grupo de matrizes $\mathcal{M} = \{A, B, C, D\}$, onde,

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

com a operação usual de produto de matrizes. Considerando o elemento $B \in \mathcal{M}$, temos

$$B^3 = B \cdot B \cdot B = B,$$

$$B^{-4} = (B')^4 = (B)^4 = B \cdot B \cdot B \cdot B = A.$$

■

Exemplo 2.15. Tomamos o grupo $\mathcal{F} = \{f : \mathbb{R} \to \mathbb{R}; \quad f(x) = ax + b, \quad a \in \mathbb{R}^*, b \in \mathbb{R}\}$, com a composição de funções. Dada $g \in \mathcal{F}$ a função $g(x) = 2x - 3$, temos que $g^3 = g \circ g \circ g$ é a função dada por

$$\begin{aligned} g^3(x) &= (g \circ g \circ g)(x) = g(g(g(x))) \\ &= g(g(2x-3)) = g(2(2x-3)-3) \\ &= g(4x-9) = 2(4x-9) - 3 = 8x - 21. \end{aligned}$$

Também a função $g^{-2} = (g')^2 = g^{-1} \circ g^{-1}$ é a função

$$\begin{aligned} g^{-2}(x) &= (g^{-1} \circ g^{-1})(x) = g^{-1}(g^{-1}(x)) \\ &= g^{-1}(\tfrac{1}{2}x + \tfrac{3}{2}) = \tfrac{1}{2}(\tfrac{1}{2}x + \tfrac{3}{2}) + \tfrac{3}{2} = \tfrac{1}{4}x + \tfrac{9}{4}. \end{aligned}$$

■

Proposição 2.27. *Seja $(G, *)$ um grupo. Então para qualquer $a \in G$ e quaisquer $m, n \in \mathbb{Z}$,*

i) $a^1 = a$,
ii) $a^n = a^{n-1} * a = a * a^{n-1}$,
iii) $a^{m+n} = a^m * a^n$,
iv) $a^n = (a^{-n})' = (a')^{-n}$,
v) $a^{-n} = (a^n)' = (a')^n$,
vi) $(a^m)^n = a^{mn}$.

Prova. A demonstração de (i) é imediata da definição, $a^1 = a^0 * a = e_G * a = a$.

Para provar (ii), provaremos primeiro que $a^n = a^{n-1} * a$ para todo $n \in \mathbb{Z}$. Se $n = 0$ temos claramente $a^{-1} * a = (a')^1 * a = a' * a = e_G = a^0$. A própria definição de potência já contempla o caso $n > 0$ para esta igualdade. Agora se $n < 0$ então

$$a^n = (a')^{-n} = (a')^{-n} * (a' * a) = ((a')^{-n} * a') * a = ((a')^{-n+1}) * a = a^{n-1} * a.$$

Agora a igualdade $a^n = a * a^{n-1}$ para todo $n \in \mathbb{Z}$. Procederemos primeiro por indução sobre $n \geq 0$. Para $n = 0$ temos imediatamente $a * a^{-1} = a * (a')^1 = a * a' = e_G = a^0$. Supondo a igualdade $a^n = a * a^{n-1}$ temos que

$$a^{n+1} = a^n * a = (a * a^{n-1}) * a = a * (a^{n-1} * a) = a * a^n.$$

Para o caso $n < 0$, temos que,

$$a^n = (a')^{-n} = (a * a') * (a')^{-n} = a * (a' * (a')^{-n}) = a * (a')^{-n+1} = a * a^{n-1}.$$

Para provarmos (iii), supomos $m \in \mathbb{Z}$, e usaremos primeiro indução finita sobre $n \geq 0$. Para $n = 0$, então

$$a^m * a^0 = a^m * e_G = a^m = a^{m+0}.$$

Suponha agora que o resultado seja válido para n, isto é, $a^{m+n} = a^m * a^n$. Desta forma, temos

$$\begin{aligned} a^m * a^{n+1} &= a^m * (a^n * a) \\ &= (a^m * a^n) * a \\ &= a^{m+n} * a = a^{(m+n)+1} = a^{m+(n+1)}. \end{aligned}$$

Supondo agora que $m, n \in \mathbb{Z}$, escolhemos $p \in \mathbb{Z}$ de forma que $p > 0$ e $p + n > 0$, e então

$$\begin{aligned} a^{m+n} &= a^{m+n} * e_G = a^{m+n} * (a^p * (a^p)') \\ &= (a^{m+n} * a^p) * (a^p)' = a^{m+n+p} * (a^p)' \\ &= (a^m * a^{n+p}) * (a^p)' = (a^m * (a^n * a^p)) * (a^p)' \\ &= (a^m * a^n) * (a^p * (a^p)') = (a^m * a^n) * e_G = a^m * a^n. \end{aligned}$$

Para (iv) provaremos primeiro a igualdade $a^n = (a')^{-n}$ para todo $n \in \mathbb{Z}$. Notemos que se $n = 0$ então a igualdade é trivialmente satisfeita. Se $n < 0$ então a própria definição de potência já garante a igualdade. Se $n > 0$ então $-n < 0$ e novamente da definição de potência

$$(a')^{-n} = ((a')')^{-(-n)} = a^n.$$

Para prova a igualdade $a^n = (a^{-n})'$ para todo $n \in \mathbb{Z}$ basta usar o item anterior e ver que

$$a^{-n} * a^n = a^{-n+n} = a^0 = e_G = a^{n-n} = a^n * a^{-n}.$$

Desta forma temos que o simétrico de a^{-n} é precisamente a^n, isto é, $a^n = (a^{-n})'$.

O item (v) não necessita de demonstração. É apenas o item anterior reorganizado substituindo-se n por $-n$.

Para a demonstração de (vi), suponhamos primeiro que $n \geq 0$ e então usaremos indução finita sobre n. Para $n = 0$, temos

$$(a^m)^0 = e_G = a^0 = a^{0 \cdot m}.$$

Suponha agora o resultado válido para n, isto é, $(a^m)^n = a^{mn}$. Temos então,

$$a^{m(n+1)} = a^{mn+m} = a^{mn} * a^m = (a^m)^n * a^m = (a^m)^{n+1}.$$

Para finalizar, resta verificar o resultado para $n < 0$. Neste caso,

$$(a^m)^n = ((a^m)^{-n})' = (a^{m\cdot(-n)})' = (a^{-mn})' = a^{mn},$$

o que conclui esta demonstração. □

Definição 2.28. Sejam $(G, *)$ um grupo e $a \in G$. O conjunto de todas as potências inteiras de a é denotado por $\langle a \rangle$. De outra forma,

$$\langle a \rangle = \{a^m; \quad m \in \mathbb{Z}\} = \{\dots, a^{-3}, a^{-2}, a^{-1}, a^0, a, a^2, a^3, a^4, \dots\},$$

ou ainda

$$\langle a \rangle = \{\dots, (a^3)', (a^2)', a', e_G, a, a^2, a^3, a^4, \dots\}.$$

Proposição 2.29. *Dado um grupo $(G, *)$ e $a \in G$ um elemento fixo, o conjunto $\langle a \rangle$ é subgrupo de G. Além disso, $\langle a \rangle$ é abeliano.*

Prova. É claro que $\langle a \rangle \neq \emptyset$ já que $a \in \langle a \rangle$. Também, se $x, y \in \langle a \rangle$, então $x = a^m$ e $y = a^n$ para algum $m, n \in \mathbb{Z}$. E assim,

$$x * y' = a^m * (a^n)' = a^m * a^{-n} = a^{m-n},$$

e como $(m-n) \in \mathbb{Z}$ temos $a^{m-n} \in \langle a \rangle$, isto é, $x * y' \in \langle a \rangle$ e pela proposição (2.7), $\langle a \rangle$ é subgrupo de G. Além disso, dados $x, y \in \langle a \rangle$ arbitrários, temos que existem $m, n \in \mathbb{Z}$ tais que $x = a^m$ e $y = a^n$. Desta forma,

$$x * y = a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m = y * x,$$

donde $\langle a \rangle$ é abeliano. □

Definição 2.30. Um grupo $(G, *)$ é dito um grupo *cíclico*, se existir um elemento $a \in G$, tal que

$$\langle a \rangle = G,$$

e neste caso dizemos que a é o gerador de G, ou ainda que G é gerado por a.

Observe que é imediato da última proposição que sendo $\langle a \rangle$ abeliano, então quando G é cíclico, da igualdade $G = \langle a \rangle$ segue que G é abeliano. O recíproco não é verdadeiro. Existem grupos que são abelianos e não são cíclicos. Um exemplo disto é o grupo $(\mathbb{Q}, +)$, dos números racionais com a operação de adição, que como já mencionado, é abeliano e não é cíclico (ver próximo exemplo).

Exemplo 2.16. O conjunto dos números inteiros com a operação adição é um grupo cíclico, pois

$$\begin{aligned}\langle 1 \rangle &= \{\dots, 1^{-3}, 1^{-2}, 1^{-1}, 0, 1, 1^2, 1^3, 1^4, \dots\} \\ &= \{\dots, (-1)^3, (-1)^2, (-1)^1, 0, 1, 1^2, 1^3, 1^4, \dots\} = \mathbb{Z}.\end{aligned}$$

Podemos notar que também $\langle -1\rangle = \mathbb{Z}$. Já o grupo dos racionais com a operação de adição, não é cíclico. De fato, podemos mostrar que $\langle x\rangle \neq \mathbb{Q}$, para qualquer que seja $x \in \mathbb{Q}$, isto é, dado qualquer número racional x sempre haverá outro número racional que não é gerado por x. De fato, dado $x \in \mathbb{Q}^*$, então $x = \frac{m}{n}$ com $m, n \in \mathbb{Z}^*$. O número $\frac{m}{2n}$ não é gerado por x, um vez que não existe $k \in \mathbb{Z}$ satisfazendo

$$\frac{m}{2n} = \frac{1}{2}\frac{m}{n} = x^k = k\frac{m}{n}.$$

■

Exemplo 2.17. Considerando $G = \{1, -1, i, -i\}$ com a operação de produto usual de complexos, observamos que

$$\langle 1\rangle = \{1\}, \qquad \langle -1\rangle = \{1, -1\}, \qquad \langle i\rangle = \{1, i, -1, -i\}, \qquad \langle -i\rangle = \{1, -i, -1, i\}.$$

Portanto i e $-i$ são dois geradores de G, o que garante que G é um grupo cíclico. ■

Exemplo 2.18. O grupo de matrizes $\mathcal{M} = \{A, B, C, D\}$, onde

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

com a operação de produto de matrizes não é cíclico. De fato,

$$\langle A\rangle = \{A\}, \qquad \langle B\rangle = \{A, B\}, \qquad \langle C\rangle = \{A, C\} \qquad \text{e} \qquad \langle D\rangle = \{A, D\},$$

ou seja, nenhum dos elementos de $\mathcal{M}$ gera todo o conjunto $\mathcal{M}$. ■

Consideremos um grupo $(G, *)$ com elemento neutro e, e $a \in G$ um elemento qualquer de G. Já sabemos que $a^0 = e$. Então, pode ocorrer que:

i) $a^k = e$ somente para $k = 0$, ou

ii) $a^k = e$ para algum outro $k \in \mathbb{Z}$ com $k \neq 0$.

Se (i) ocorre, isto é,

$$a^k = e \quad \text{se e somente se} \quad k = 0,$$

então dizemos que a tem *período* zero, ou *ordem* zero, e escrevemos $o(a) = 0$. Neste caso, $\langle a\rangle$ será um grupo cíclico infinito. De fato, considerando a aplicação

$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle a\rangle \\ m &\mapsto \varphi(m) = a^m \end{aligned}$$

temos que, para todo $y \in \langle a\rangle$, $y = a^k$ para algum $k \in \mathbb{Z}$, e portanto escolhemos $x = k \in \mathbb{Z}$ de forma que $\varphi(x) = \varphi(k) = a^k = y$, e assim, φ é sobrejetora. Sejam $m, n \in \mathbb{Z}$ tais que $\varphi(m) = \varphi(n)$, isto é, $a^m = a^n$. Então

$$a^{m-n} = a^m * a^{-n} = a^n * (a^n)' = e.$$

Mas $a^{m-n} = e$ significa que $m - n = 0$, e assim, $m = n$ o que mostra que φ é injetora, e portanto bijetora. Assim, a cada k distinto em $\mathbb{Z}$ corresponde um a^k distinto em $\langle a\rangle$. Escrevemos então,

$$\langle a\rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, \ldots\},$$

e concluímos que, se a tem ordem 0, então $\langle a\rangle$ é um grupo cíclico infinito. Além disso, para quaisquer $m, n \in \mathbb{Z}$,

$$\varphi(m+n) = a^{m+n} = a^m * a^n = \varphi(m) * \varphi(n),$$

que prova que φ é homomorfismo. Segue que φ é isomorfismo e então $\langle a\rangle \approx \mathbb{Z}$. Note que neste caso G é também infinito já que $\langle a\rangle \subset G$.

Suponha agora que (ii) acontece, isto é, $a^k = e$ para algum outro $0 \neq k \in \mathbb{Z}$. Então é fácil ver que existirão infinitos inteiros satisfazendo esta condição. Pelo menos os múltiplos inteiros de k satisfazem esta condição. Dentre estes múltiplos de k, estão os múltiplos positivos. Ao menor número inteiro positivo k tal que $a^k = e$ chamaremos de *período*, ou *ordem*, de a, e representaremos por $o(a) = k$.

Neste caso, $\langle a\rangle$ será um grupo cíclico finito, com exatamente k elementos. Mostraremos primeiro que $\{e, a, a^2, a^3, \ldots, a^{k-1}\}$ tem exatamente k elementos distintos. Suponha (por absurdo) que existam dois destes elementos iguais, isto é, existem $0 \leq n < m < k$ tais que $a^m = a^n$. Então

$$a^{m-n} = a^m * a^{-n} = a^n * a^{-n} = e,$$

e isto é uma contradição pois $0 < m - n < k$ e k deveria ser o menor número inteiro positivo satisfazendo $a^k = e$. Desta forma, $\{e, a, a^2, a^3, \ldots, a^{k-1}\}$ possui k elementos distintos.

Mostraremos agora que $\langle a\rangle = \{e, a, a^2, a^3, \ldots, a^{k-1}\}$. Como $\langle a\rangle = \{a^m; m \in \mathbb{Z}\}$ então é imediato que $\{e, a, a^2, a^3, \ldots, a^{k-1}\} \subset \langle a\rangle$. Para a segunda inclusão, seja $x \in \langle a\rangle$, então $x = a^m$ para algum $m \in \mathbb{Z}$. Pelo algoritmo da divisão de Euclides, existem únicos $q, r \in \mathbb{Z}$ tais que $m = kq + r$ com $0 \leq r < k$. Então,

$$x = a^m = a^{kq+r} = (a^k)^q * a^r = e^q * a^r = a^r,$$

e como $0 \leq r < k$ então $x = a^m = a^r \in \{e, a, a^2, a^3, \ldots, a^{k-1}\}$ o que completa a segunda inclusão, mostrando que

$$\langle a\rangle = \{e, a, a^2, a^3, \ldots, a^{k-1}\}.$$

Do exposto acima, lembremos que, a ordem de um elemento $a \in G$, é o menor número inteiro positivo k tal que $a^k = e$. Caso não exista tal inteiro positivo, então dizemos que a ordem de a é zero. Em qualquer caso, temos que $a^{o(a)} = e$.

Da mesma forma que o subgrupo $\langle a\rangle = \{a^m; m \in \mathbb{Z}\}$ foi obtido tomando-se as potências de um único elemento $a \in G$, podemos construir subgrupos a partir de uma coleção de k elementos de um grupo $(G, *)$. Dado $L = \{a_1, a_2, \ldots, a_k\} \subset G$, o conjunto gerado pelos elementos a_i, é denotado por $\langle L\rangle = \langle a_1, a_2, \ldots, a_k\rangle$ e determinado por

$$\langle L\rangle = \langle a_1, a_2, \ldots, a_k\rangle = \{a_1^{m_1} * a_2^{m_2} * a_3^{m_3} * \cdots * a_k^{m_k}; \quad m_1, m_2, \ldots, m_k \in \mathbb{Z}\}.$$

O conjunto acima, gerado pelos elementos a_i, com $1 \leq i \leq k$, é um subgrupo de G. A prova deste fato é deixada como exercício.

2.5 Classes laterais e o Teorema de Lagrange

Definição 2.31. Dado um grupo G, definimos a ordem de G, denotada por $o(G)$ ou $|G|$, como sendo o número de elementos de G. Se G é infinito, dizemos que a ordem de G é infinita.

Note que se $\langle a \rangle$ for um grupo finito, então $o(\langle a \rangle) = o(a)$.

Definição 2.32. Seja H um subgrupo de um grupo $(G, *)$. Dado $a \in G$, definimos a *classe lateral à esquerda* de a módulo H, como sendo o subconjunto de G,

$$a * H = \{a * h; \quad \text{para todo} \quad h \in H\}.$$

Analogamente, a *classe lateral à direita* de a módulo H, é o conjunto

$$H * a = \{h * a; \quad \text{para todo} \quad h \in H\}.$$

Se G for um grupo abeliano então a classe à direita de a módulo H, coincide com a classe à esquerda de a módulo H. Além disso deve ficar claro que qualquer classe lateral $a * H$ ou $H * a$ não é necessariamente um subgrupo de G, mas ainda assim, é um conjunto obrigatoriamente não vazio. De fato, se $e \in G$ é o elemento neutro de G então $e \in H$ e portanto $a = a * e \in a * H$ e também $a = e * a \in H * a$.

Estabeleceremos agora alguns resultados sobre as classes laterais, e para não sermos repetitivos, enunciaremos estes resultados apenas para classes laterais à esquerda. Mas ocorre também a validade destes resultados para as classes laterais à direita, com pequenos ajustes em alguns casos.

Proposição 2.33. *Se H é subgrupo de $(G, *)$ e a e b são elementos de G, então $a * H = b * H$ se e somente se $a' * b \in H$.*

Prova. Suponha $a * H = b * H$. Sabemos que $b \in b * H$ e então, $b \in a * H$, isto é, $b = a * h$ para algum $h \in H$. Assim, $(a' * b) = h \in H$.

Reciprocamente, suponha $(a' * b) \in H$. Mostraremos que $a * H = b * H$, mostrando a dupla inclusão dos conjuntos. Tomemos $x \in a * H$, então $x = a * h$ para algum $h \in H$. Assim $x = a * h = b * (b' * a * h)$ e como $(a' * b) \in H$ então $(a' * b)' * h \in H$ ou ainda $(b' * a * h) \in H$ o que prova que $x = b * (b' * a * h) \in b * H$.

Suponha agora $x \in b * H$. Temos que $x = b * k$ com $k \in H$. Então $x = a * (a' * b * k)$ e como $(a' * b) \in H$ então $(a' * b * h) \in H$, donde $x = a * (a' * b * h) \in a * H$, o que termina a demonstração. □

Para classes laterais pela direita módulo H, podemos provar que $H * a = H * b$ se e somente se $(a * b') \in H$. Não faremos esta demonstração porque é análoga à proposição anterior.

Definição 2.34. Para um grupo $(G, *)$ qualquer e um subgrupo H de G, a quantidade de classes laterais à esquerda distintas em G módulo H, é representada por $(G : H)$ e chamada de *índice* de G em H.

Exemplo 2.19. Considerando o grupo $G = \{1, -1, i, -i\}$ com a operação de produto de complexos, e o subgrupo $H = \{1, -1\}$, temos

$$\begin{aligned} 1 \cdot H &= 1 \cdot \{1, -1\} = \{1, -1\} = H, \\ (-1) \cdot H &= (-1) \cdot \{1, -1\} = \{-1, 1\} = H, \\ i \cdot H &= i \cdot \{1, -1\} = \{i, -i\}, \\ (-i) \cdot H &= (-i) \cdot \{1, -1\} = \{-i, i\} = i \cdot H, \end{aligned}$$

temos portanto duas classes laterais distintas e assim, $(G : H) = 2$. ■

Exemplo 2.20. Dado o grupo $G = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ com a operação de soma de classes de equivalência, e o subgrupo $H = \{\overline{0}, \overline{3}\}$. Então

$$\begin{aligned} \overline{0} + H &= \overline{0} + \{\overline{0}, \overline{3}\} = \{\overline{0}, \overline{3}\} = H, \\ \overline{1} + H &= \overline{1} + \{\overline{0}, \overline{3}\} = \{\overline{1}, \overline{4}\}, \\ \overline{2} + H &= \overline{2} + \{\overline{0}, \overline{3}\} = \{\overline{2}, \overline{5}\}, \\ \overline{3} + H &= \overline{3} + \{\overline{0}, \overline{3}\} = \{\overline{3}, \overline{0}\} = H, \\ \overline{4} + H &= \overline{4} + \{\overline{0}, \overline{3}\} = \{\overline{4}, \overline{1}\} = \overline{1} + H, \\ \overline{5} + H &= \overline{5} + \{\overline{0}, \overline{3}\} = \{\overline{5}, \overline{2}\} = \overline{2} + H, \end{aligned}$$

temos portanto três classes laterais distintas e assim, $(G : H) = 3$. ■

Exemplo 2.21. Consideremos o grupo $(\mathbb{Z}, +)$ e fixemos $m \in \mathbb{Z}$ com $m \geq 2$. Tomemos o subgrupo

$$H = \langle m \rangle = \{\dots, -5m, -4m, -3m, -2m, -m, 0, m, 2m, 3m, 4m, 5m, \dots\}.$$

Queremos determinar as classes laterais $a + H$ para todos $a \in \mathbb{Z}$. Embora o conjunto $\mathbb{Z}$ seja infinito, vamos mostrar que existem apenas m classes laterais distintas e dado qualquer $a \in \mathbb{Z}$, a classe lateral $a + H$ recai em alguma destas m classes laterais distintas. De fato, dado qualquer $a \in \mathbb{Z}$, do algortimo da divisão de Euclides, existem $q, r \in \mathbb{Z}$ (unicamente determinados) de forma que $a = qm + r$ com $0 \leq r < m$. Nestes termos

$$a' + r = -a + r = (-q)m - r + r = (-q)m \in H,$$

e da Proposição 2.33 segue que $a + H = r + H$. Isto significa que dado qualquer inteiro a a classe lateral $a + H$ coincide com a classe lateral do resto da divisão de a por m. Como existem m restos possíveis para a divisão de um inteiro por m, segue que existem m classes laterais distintas, e são elas

$$0 + H = H, \quad 1 + H, \quad 2 + H, \quad 3 + H, \quad \dots, \quad (m-1) + H.$$

■

Exemplo 2.22. Consideremos o conjunto de matrizes, $\mathcal{M} = \{A, B, C, D\}$, onde

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

com a operação de produto de matrizes, e $\mathcal{H} = \{A, C\}$. Temos,

$$\begin{aligned} A \cdot \mathcal{H} &= \{A \cdot A, A \cdot C\} = \{A, C\} = \mathcal{H}, \\ B \cdot \mathcal{H} &= \{B \cdot A, B \cdot C\} = \{B, D\}, \\ C \cdot \mathcal{H} &= \{C \cdot A, C \cdot C\} = \{C, A\} = \mathcal{H}, \\ D \cdot \mathcal{H} &= \{D \cdot A, D \cdot C\} = \{D, B\} = B \cdot \mathcal{H}, \end{aligned}$$

e assim temos duas classes laterais distintas, isto é, $(\mathcal{M} : \mathcal{H}) = 2$. ■

Proposição 2.35. *Seja H subgrupo do grupo $(G, *)$. A união de todas as classes laterais módulo H em G, é igual a G, isto é,*

$$\bigcup_{a \in G} a * H = G.$$

Prova. Como $H \subset G$ e G é fechado para a operação $*$, então $a * H \subset G$ para cada $a \in G$. Assim

$$\bigcup_{a \in G} a * H \subset G.$$

Para a inclusão contrária, seja $x \in G$. Como já comentado anteriormente $x \in x * H$ e então

$$x =\in x * H \subset \bigcup_{a \in G} a * H,$$

concluindo esta demonstração. □

Proposição 2.36. *Se $a * H$ e $b * H$ são duas classes laterais módulo H em $(G, *)$ então, ou $a * H \cap b * H = \emptyset$, ou $a * H = b * H$.*

Prova. As duas igualdades são claramente exclusivas. Suponha $a * H \cap b * H \neq \emptyset$, então existe $x \in a * H \cap b * H$. Logo $x \in a * H$ e $x \in b * H$, e então existem $h, k \in H$ tais que $x = a * h$ e $x = b * k$. Sendo assim, $b * k = a * h$ e então $h * k' = a' * b$, e como $h, k \in H$ temos $h * k' \in H$, mostrando que $a' * b \in H$, e pela proposição 2.33 segue que $a * H = b * H$. □

Proposição 2.37. *Qualquer classe lateral $a * H$ é equipotente a H, isto é, tem a mesma quantidade de elementos de H.*

Prova. É suficiente provar que existe uma aplicação bijetora entre os conjuntos $a * H$ e H. Consideremos então

$$\begin{aligned} f : H &\to a * H \\ h &\mapsto f(h) = a * h. \end{aligned}$$

Tomemos $y \in a * H$. Então $y = a * k$ para algum $k \in H$. Basta tomar $x = k \in H$ para termos $f(x) = f(k) = a * k = y$, provando a sobrejetividade de f. Tomemos agora $x, y \in H$ com $f(x) = f(y)$. Temos então $a * x = a * y$ e da regularidade do elemento $a \in G$, temos $x = y$, provando a injetividade de f. Segue que f é bijetora, isto é, os conjuntos possuem a mesma quantidade de elementos. □

Teorema 2.38 (Teorema de Lagrange)**.** *Se G é um grupo finito e H é um subgrupo de G, então $o(H)|o(G)$ e além disso*

$$o(G) = o(H)(G : H).$$

Prova. Como $(G, *)$ é finito, então G possui uma quantidade finita de elementos. Seja m a quantidade de elementos de m, isto é, $o(G) = m$ e podemos escrever $G = \{a_1, a_2, a_3, \ldots, a_m\}$.

De acordo com a proposição 2.35, G é igual à união de todas as classes laterais módulo H, isto é,

$$G = \bigcup_{a \in G} (a * H) = (a_1 * H) \cup (a_2 * H) \cup (a_3 * H) \cup \cdots \cup (a_m * H).$$

Podemos agora descartar as lasses laterais que se repetem na união de conjuntos do segundo membro da igualdade acima. Considerando que existem k classes laterais distintas, com $0 < k \leq m$, então reorganizando os elementos $a_i \in G$, temos que

$$G = (a_1 * H) \cup (a_2 * H) \cup (a_3 * H) \cup \cdots \cup (a_k * H),$$

sendo que agora as classes laterias da união do segundo membro são distintas, isto é, não possuem elementos em comum. Observe também que nestes termos $(G : H) = k$.

Desta forma temos que

$$o(G) = o((a_1 * H) \cup (a_2 * H) \cup \cdots \cup (a_k * H)),$$

e como as classes na direita da igualdade não possuem elementos em comum entre elas, então a quantidade de elementos da união é a soma das quantidades de elementos de cada uma das partes. Segue que

$$o(G) = o(a_1 * H) + o(a_2 * H) + \cdots + o(a_k * H).$$

Além disso, como cada classe tem a mesma quantidade de elementos de H (Proposição 2.37), então

$$o(G) = o(H) + o(H) + \cdots + o(H),$$

onde no lado direito existem k parcelas iguais a $o(H)$. Logo $o(G) = o(H) \cdot k$, ou seja, $o(G) = o(H)(G : H)$, donde segue ainda que $o(H) | o(G)$. □

Corolário 2.39. *Seja G um grupo finito com $o(G) = p$ um número primo. Então G é cíclico e seus únicos subgrupos são os triviais.*

Prova. Considere $e \in G$ o elemento neutro de G. Suponha H um subgrupo arbitrário de G com $H \neq \{e\}$. Vamos então provar que $H = \langle a \rangle = G$ para algum $a \in G$. Como $H \neq \{e\}$ então existe $a \in H \subset G$ com $a \neq e$. Temos assim que $\langle a \rangle \subset H \subset G$. Já sabemos que $\langle a \rangle$ é subgrupo cíclico de G e possui pelos menos dois elementos distintos, a e e. Desta forma $o(\langle a \rangle) \geq 2$. Pelo teorema de Lagrange, $o(G) = o(\langle a \rangle)(G : \langle a \rangle)$, isto é, $p = o(\langle a \rangle)(G : \langle a \rangle)$, e sendo p um número primo, segue que

$$o(\langle a \rangle) = 1 \quad \text{e} \quad (G : \langle a \rangle) = p \qquad \text{ou} \qquad o(\langle a \rangle) = p \quad \text{e} \quad (G : \langle a \rangle) = 1.$$

Como $o(\langle a \rangle) \geq 2$, temos que necessariamente $o(\langle a \rangle) = p$. Isto significa que $\langle a \rangle$ tem p elementos distintos de G. Então $\langle a \rangle = G$ e donde segue que $\langle a \rangle = H = G$ e além disso, G é cíclico pois $\langle a \rangle$ é cíclico. □

2.6 Subgrupos normais e grupos quocientes

Definição 2.40. Um subgrupo H de um grupo $(G, *)$ é dito um *subgrupo normal* de G se as classes laterais à direita e à esquerda de qualquer elemento $a \in G$ módulo H, coincidem, isto é, se

$$a * H = H * a$$

para qualquer que seja $a \in G$. Escrevemos $H \lhd G$, para dizer que H é (subgrupo) normal em G.

Notemos que se o grupo G é abeliano (ou comutativo) então qualquer subgrupo H de G é subgrupo normal. Além disso, independentemente de G ser abaliano, podemos mostrar que os subgrupos triviais, $H = \{e_G\}$ e $S = G$ são sempre normais em G. Um grupo G será dito um grupo *simples* se não existirem subgrupos normais em G além dos subgrupos triviais.

Exemplo 2.23. Consideremos o conjunto $\mathcal{M}$ das matrizes quadradas de ordem 2, com determinante não nulo,

$$\mathcal{M} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}; \quad a, b, c, d \in \mathbb{R},\ ad - bc \neq 0 \right\},$$

que com a operação de multiplicação de matrizes é um grupo. No grupo $(\mathcal{M}, \cdot)$ consideremos o subgrupo

$$\mathcal{H} = \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}; \quad x, y \in \mathbb{R}^* \right\}.$$

Mostraremos que $\mathcal{H}$ não é (em geral) subgrupo normal. Seja $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}$ uma matriz qualquer. Mostraremos que em geral $A \cdot \mathcal{H} \neq \mathcal{H} \cdot A$. De fato, dada

$$H = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \in \mathcal{H},$$

temos que

$$A \cdot H = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} ax & by \\ cx & dy \end{pmatrix}.$$

Agora, para que $A \cdot H$ pertença ao conjunto $\mathcal{H} \cdot A$, deverá existir uma matriz $K = \begin{pmatrix} m & 0 \\ 0 & n \end{pmatrix} \in \mathcal{H}$ de forma que $A \cdot H = K \cdot A$. Isto é,

$$\begin{pmatrix} ax & by \\ cx & dy \end{pmatrix} = \begin{pmatrix} m & 0 \\ 0 & n \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} am & bm \\ cn & dn \end{pmatrix}.$$

Mas isto acarretará que $ax = am$, $by = bm$, $cx = cn$ e $dy = dn$ para quaisquer $a, b, c, d \in \mathbb{R}$ com $ad - bc \neq 0$. Note que para que o subgrupo $\mathcal{H}$ seja um subgrupo normal, a igualdade $A \cdot H = K \cdot A$ deve ocorrer para todas as matrizes $A \in \mathcal{M}$. Desta forma, obrigatoriamente teremos $m = x = n = y$, o que significa que $\mathcal{H}$ será subgrupo normal se e somente se $x = y$. Então em geral $\mathcal{H}$ não é subgrupo normal, mas

$$\mathcal{N} = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}; \quad x \in \mathbb{R}^* \right\},$$

é subgrupo normal de $\mathcal{M}$. ■

Incluir exemplo quatérnios...

A próxima proposição nos oferece outro método para determinar se um subgrupo é ou não um subgrupo normal.

Proposição 2.41. *Dado um subgrupo H de um grupo $(G,*)$, então H é subgrupo normal, se e somente se, $a*h*a' \in H$, para quaisquer $h \in H$, e $a \in G$.*

Prova. Suponhamos inicialmente que H seja subgrupo normal de G. Dados então $a \in G$ e $h \in H$ arbitrários, temos que $(a*h) \in a*H$ e como $a*H = H*a$, então $(a*h) \in H*a$. Segue que $a*h = k*a$ para algum $k \in H$. Desta forma $(a*h*a') = k$ e como $k \in H$, segue que $(a*h*a') \in H$.

Reciprocamente, suponha que $(a*h*a') \in H$ para quaisquer $a \in G$ e $h \in H$. Mostraremos primeiro que $a*H \subset H*a$. Seja $x \in a*H$, então $x = a*h$ para algum $h \in H$ e então $x = a*h = (a*h)*(a'*a) = (a*h*a')*a$, e como por hipótese, $(a*h*a') \in H$, temos que $x \in H*a$. Desta forma $a*H \subset H*a$.

Para a inclusão contrária, seja $x \in H*a$. Então $x = h*a$ para algum $h \in H$. Podemos assim escrever $x = a*(a'*h*a)$, e a prova estará terminada se $(a'*h*a) \in H$. Usando então a hipótese com $h \in H$ e $a' \in G$, temos que $(a'*h*(a')') \in H$, e portanto $(a'*h*a) \in H$. Segue que $x = a*(a'*h*a) \in a*H$, mostrando a segunda inclusão e a igualdade desejada. □

Um resultado similar ao da proposição anterior pode ser estabelecido. Um subgrupo H de um grupo $(G,*)$ é subgrupo normal, se e somente se, $(a'*h*a) \in H$ para quaisquer $a \in G$ e $h \in H$. A demonstração é análoga e então não repetiremos isto, mas poderemos utilizar igualmente as duas variações dependendo da conveniência.

Se H é subgrupo normal de G então o conjunto de todas as classes laterais módulo H em G, indicado por $\frac{G}{H}$, ou G/H, é chamado de conjunto quociente de G por H. Podemos representar este conjunto por

$$\frac{G}{H} = \{a*H; \quad a \in G\} = \{H*a; \quad a \in G\},$$

ou ainda, no caso em que G é finito,

$$\frac{G}{H} = \{a_1*H, a_2*H, \ldots, a_n*H\}.$$

Nosso intuito agora é dotar o conjunto quociente $\frac{G}{H}$ de uma operação, de modo que esta operação torne este conjunto um grupo também.

Notemos que os elementos do conjunto $\frac{G}{H}$ são precisamente os subconjuntos $a*H$, e portanto são subconjuntos de G. Desta forma, é natural a ideia de considerar no conjunto $\frac{G}{H}$ a operação de subconjuntos de G, definida em (2.9), isto é, se $(a*H),(b*H) \in \frac{G}{H}$, então,

$$(a*H)*(b*H) = \{u*v; \quad u \in (a*H), v \in (b*H)\}.$$

A próxima proposição nos dá um método mais rápido para determinar $(a*H)*(b*H)$ para quaisquer que sejam $a, b \in G$.

Proposição 2.42. *Se H é um subgrupo normal de $(G,*)$ então, para quaisquer $a,b \in G$, tem-se*

$$(a*H)*(b*H) = (a*b)*H.$$

Prova. Sejam $a,b \in G$ arbitrários. Suponha $x \in (a*H)*(b*H)$, então $x = u*v$ para algum $u \in a*H$ e $v \in b*H$. Mas desta forma, $u = a*h$ e $v = b*k$, para algum $h,k \in H$. Assim, $x = (a*h)*(b*k) = (a*b)*(b'*h*b*k)$. Como H é subgrupo normal, usando a Proposição 2.41 com $b' \in G$ e $h \in H$, temos que $b'*h*b \in H$. Como também $k \in H$, segue que $(b'*h*b*k) \in H$, donde $x = (a*b)*(b'*h*b*k) \in (a*b)*H$. Isto prova a inclusão $(a*H)*(b*H) \subset (a*b)*H$.

Seja agora $x \in (a*b)*H$, então $x = (a*b)*h$ para algum $h \in H$. Considerando $e \in G$ o elemento neutro de G, então $x = a*(b*h) = (a*e)*(b*h) \in (a*H)*(b*H)$, pois $e \in H$. Temos então que $(a*b)*H \subset (a*H)*(b*H)$, que completa a demonstração. □

Notemos que a proposição que acabamos de provar não só estabelece um método mais rápido para determinar $(a*H)*(b*H)$, como também prova que a operação entre classes laterais módulo H é fechada, já que como $(a*b) \in G$, então $(a*b)*H \in \frac{G}{H}$.

Proposição 2.43. *A operação $*$, entre classes laterais módulo H definida no conjunto $\frac{G}{H}$, está bem definida.*

Prova. Sejam $(a*H)$, $(b*H)$, $(x*H)$ e $(y*H)$ de forma que $(a*H) = (x*H)$ e $(b*H) = (y*H)$. Queremos mostrar que $(a*H)*(b*H) = (x*H)*(y*H)$, ou equivalentemente pela proposição anterior, que $(a*b)*H = (x*y)*H$. Das igualdades $(a*H) = (x*H)$ e $(b*H) = (y*H)$, a proposição 2.33 nos garante que $(a'*x) \in H$ e que $(b'*y) \in H$. Então

$$(a*b)'*(x*y) = b'*a'*x*y = b'*a'*x*b*b'*y = b'*(a'*x)*b*(b'*y),$$

e vamos olhar para o último termo desta igualdade. Temos que $(a'*x) \in H$ e sendo H um subgrupo normal, a proposição 2.41 nos garante que $(b'*(a'*x)*b) \in H$. Como também $(b'*y) \in H$ e H é fechado para a operação $*$, segue que $b'*(a'*x)*b*(b'*y) \in H$. Segue então que $(a*b)'*(x*y) \in H$ e novamente da proposição 2.33 temos que $(a*b)*H = (x*y)*H$ e a operação $*$ entre classes laterais módulo H em G está bem definida. □

Exemplo 2.24. Considerando $G = (\mathbb{Z},+)$ o conjunto dos inteiros com a operação de adição usual, e o subgrupo $H = 3\mathbb{Z}$. Como $\mathbb{Z}$ é abeliano, o subgrupo H é normal, e as classes laterais são

$$\begin{aligned}
0+H &= \{\ldots,-6,-3,0,3,6,9,\ldots\} = H,\\
1+H &= \{\ldots,-5,-2,1,4,7,10,\ldots\},\\
2+H &= \{\ldots,-4,-1,2,5,8,11,\ldots\},\\
3+H &= \{\ldots,-3,0,3,6,9,12,\ldots\} = H,\\
4+H &= \{\ldots,-2,1,4,7,10,13,\ldots\} = 1+H,
\end{aligned}$$

e a partir daí as demais classes se repetem, e temos então apenas estas três classes módulo H. Assim $\frac{G}{H} = \{H, 1+H, 2+H\}$, e podemos construir a tábua da operação de adição em $\frac{G}{H}$, que é,

$+$	H	$1+H$	$2+H$
H	H	$1+H$	$2+H$
$1+H$	$1+H$	$2+H$	H
$2+H$	$2+H$	H	$1+H$

■

Exemplo 2.25. Considere o grupo $G = (\mathbb{Z}_8, +)$ e o subgrupo $H = \{\overline{0}, \overline{4}\}$. Como G é abeliano, então o subgrupo H é normal em G. Também as classes laterais são:

$$\begin{aligned}
\overline{0} + H &= \overline{0} + \{\overline{0}, \overline{4}\} = \{\overline{0}, \overline{4}\} = H,\\
\overline{1} + H &= \overline{1} + \{\overline{0}, \overline{4}\} = \{\overline{1}, \overline{5}\},\\
\overline{2} + H &= \overline{2} + \{\overline{0}, \overline{4}\} = \{\overline{2}, \overline{6}\},\\
\overline{3} + H &= \overline{3} + \{\overline{0}, \overline{4}\} = \{\overline{3}, \overline{7}\},\\
\overline{4} + H &= \overline{4} + \{\overline{0}, \overline{4}\} = \{\overline{4}, \overline{0}\} = H,\\
\overline{5} + H &= \overline{5} + \{\overline{0}, \overline{4}\} = \{\overline{5}, \overline{1}\} = \overline{1} + H,\\
\overline{6} + H &= \overline{6} + \{\overline{0}, \overline{4}\} = \{\overline{6}, \overline{2}\} = \overline{2} + H,\\
\overline{7} + H &= \overline{7} + \{\overline{0}, \overline{4}\} = \{\overline{7}, \overline{3}\} = \overline{3} + H.
\end{aligned}$$

Temos portanto $\frac{G}{H} = \{H, \overline{1} + H, \overline{2} + H, \overline{3} + H\}$, e a tábua da operação em $\frac{G}{H}$ fica determinada por

$+$	H	$\overline{1}+H$	$\overline{2}+H$	$\overline{3}+H$
H	H	$\overline{1}+H$	$\overline{2}+H$	$\overline{3}+H$
$\overline{1}+H$	$\overline{1}+H$	$\overline{2}+H$	$\overline{3}+H$	H
$\overline{2}+H$	$\overline{2}+H$	$\overline{3}+H$	H	$\overline{1}+H$
$\overline{3}+H$	$\overline{3}+H$	H	$\overline{1}+H$	$\overline{2}+H$

Também, $(G : H) = 4$. ■

Proposição 2.44. *Se H é um subgrupo normal de G, então o conjunto $(\frac{G}{H}, *)$ com a operação entre conjuntos é um grupo, denominado grupo quociente de G por H.*

Prova. Mostraremos que a operação $*$ satisfaz todas as propriedades de grupo. Em primeiro lugar, é bastante óbvio que $\frac{G}{H}$ é um conjunto não vazio, pois G e H são não vazios e então existe pelo menos uma classe lateral $a * H \in \frac{G}{H}$. A operação $*$ é associativa em $\frac{G}{H}$. De fato, para quaisquer $a, b, c \in G$, temos

$$\begin{aligned}
(a * H) * [(b * H) * (c * H)] &= (a * H) * [(b * c) * H]\\
&= (a * (b * c)) * H\\
&= ((a * b) * c) * H\\
&= [(a * b) * H] * (c * H) = [(a * H) * (b * H)] * (c * H).
\end{aligned}$$

Vamos checar a existência de elemento neutro no conjunto $\frac{G}{H}$. Queremos determinar um elemento $x * H \in \frac{G}{H}$ tal que

$$(a * H) * (x * H) = (a * H)$$

para todo $(a*H) \in \frac{G}{H}$. Nestes termos desejamos que $(a*x)*H = (a*H)$, e da proposição 2.33 segue que $(a*x)' * a \in H$, ou ainda, $x' * a' * a \in H$, donde $x' * e_G \in H$. A mesma proposição 2.33 garante que $x*H = e_G*H = H$, o que nos diz que o elemento neutro procurado é $e_G*H = H$. Podemos verificar que $(e_G*H)*(a*H) = (a*H)$ também e portanto da definição de elemento neutro $e_{G/H} = (e_G*H) \in \frac{G}{H}$ é de fato e elemento neutro para a operação $*$ no conjunto $\frac{G}{H}$.

Vamos agora checar que todo elemento $a*H \in \frac{G}{H}$ é simetrizável. Tomemos $x*H \in \frac{G}{H}$ tal que $(a*H)*(x*H) = e_{G/H} = e_G*H$. Desta igualdade, desejamos que $(a*x)*H = e_G*H$, e da proposição 2.33 temos $(a*x)' \in H$, ou ainda, $x' * a' \in H$. Da mesma proposição 2.33 isto significa que $x*H = a'*H$, e portanto o simétrico de $a*H$ é $a'*H$, isto é, $(a*H)' = (a'*H)$. Temos portanto que a operação $*$ cumpre os axiomas da definição de grupo, sendo portanto o conjunto $\frac{G}{H}$ um grupo. □

Proposição 2.45. *Dado um grupo $(G,*)$, então qualquer subgrupo normal H de G é núcleo de algum homomorfismo definido em G.*

Prova. Consideremos o grupo $\frac{G}{H}$ e a aplicação

$$\begin{aligned} \eta : G &\to \frac{G}{H} \\ a &\mapsto \eta(a) = a*H. \end{aligned}$$

Nestas condições, temos que para todos $a, b \in G$,

$$\eta(a*b) = (a*b)*H = (a*H)*(b*H) = \eta(a)*\eta(b),$$

e então η é um homomorfismo. Mostraremos que $Ker(\eta) = H$. Dado $x \in Ker(\eta)$ temos que $x*H = \eta(x) = e_{G/H} = e_G*H$. Da proposição 2.33 segue que $(x' * e_G) \in H$e e assim $x \in H$. Para a segunda inclusão, dado $x \in H$ temos que $x * e_G \in H$. Da proposição 2.33 segue que $x*H = e_G*H$, e assim, $\eta(x) = x*H = e_G*H = e_{G/H}$, donde $x \in Ker(\eta)$. Isto mostra que $Ker(\eta) = H$. □

Proposição 2.46. *Se $(G,*)$ e $(S,\circ)$ são dois grupos e $\varphi : G \to S$ é um homomorfismo, então $Ker(\varphi)$ é um subgrupo normal de G.*

Prova. Já sabemos da Proposição (2.19) que $Ker(\varphi)$ é subgrupo de G. Resta mostrar que é normal. Sejam $a \in G$ e $h \in Ker(\varphi)$ arbitrários. Então $\varphi(h) = e_S$ o elemento neutro de S, e assim,

$$\varphi(a*h*a') = \varphi(a) \circ \varphi(h) \circ \varphi(a') = \varphi(a) \circ e_S \circ (\varphi(a))' = e_S,$$

e então, $(a*h*a') \in Ker(\varphi)$. Segue da Proposição 2.41 que $Ker(\varphi) \lhd G$. □

Como $Ker(\varphi)$ é um subgrupo normal em G, então podemos falar em grupo quociente $\frac{G}{Ker(\varphi)}$, e estamos prontos para o principal resultado desta seção.

Teorema 2.47 (Teorema Fundamental do Homomorfismo)**.** *Seja $\varphi : G \to S$ um homomorfismo entre dois grupos $(G,*)$ e $(S,\circ)$. Então*

$$\frac{G}{Ker(\varphi)} \approx Im(\varphi).$$

Prova. Mostraremos que existe um isomorfismo de $\frac{G}{Ker(\varphi)}$ em $Im(\varphi)$. Consideremos a aplicação

$$\begin{array}{rcl} f : \dfrac{G}{Ker(\varphi)} & \to & Im(\varphi) \\ a * Ker(\varphi) & \mapsto & f(a * Ker(\varphi)) = \varphi(a). \end{array}$$

Antes de qualquer coisa, faz-se necessário mostrar que esta aplicação está bem definida. Suponha $a * Ker(\varphi) = b * Ker(\varphi)$ representantes da mesma classe. Então, da Proposição (2.33), temos que $(a' * b) \in Ker(\varphi)$ e portanto, $\varphi(a' * b) = e_S$. Então $(\varphi(a))' \circ \varphi(b) = e_S$, ou ainda, $\varphi(a) = \varphi(b)$, donde $f(a * Ker(\varphi)) = f(b * Ker(\varphi))$. Segue que f está bem definida.

Sejam $a * Ker(\varphi), b * Ker(\varphi) \in \frac{G}{Ker(\varphi)}$ com $f(a * Ker(\varphi)) = f(b * Ker(\varphi))$, e então, $\varphi(a) = \varphi(b)$. Segue que

$$\varphi(a' * b) = (\varphi(a))' \circ \varphi(b) = (\varphi(a))' \circ \varphi(a) = e_S.$$

Desta forma $(a' * b) \in Ker(\varphi)$, e novamente da Proposição (2.33), segue que $a * Ker(\varphi) = b * Ker(\varphi)$. Fica mostrada a injetividade de f. Dado agora $y \in Im(\varphi)$ arbitrário, existe $a \in G$ tal que $\varphi(a) = y$. Escolhemos $x = a * Ker(\varphi) \in \frac{G}{Ker(\varphi)}$, e temos

$$f(x) = \varphi(a * Ker(\varphi)) = \varphi(a) = y,$$

que prova a sobrejetividade de f. Sendo assim, f é bijetora.

Resta apenas mostrar que f é homomorfismo. Sejam $a * Ker(\varphi), b * Ker(\varphi) \in \frac{G}{Ker(\varphi)}$. Então

$$\begin{aligned} f((a * Ker(\varphi)) * (b * Ker(\varphi))) &= f((a * b) * Ker(\varphi)) \\ &= \varphi(a * b) = \varphi(a) \circ \varphi(b) = f(a * Ker(\varphi)) \circ f(b * Ker(\varphi)), \end{aligned}$$

provando que f é homomorfismo, e portanto um isomorfismo. □

Corolário 2.48. *Se $\varphi : G \to S$ é um homomorfismo sobrejetor entre os grupos $(G, *)$ e $(S, \circ)$, então*

$$\frac{G}{Ker(\varphi)} \approx S.$$

Corolário 2.49. *Sejam H e K subgrupos de $(G, *)$ com $K \lhd G$. Então*

i) $H * K$ é subgrupo de G, com $K \lhd (H * K)$.

ii) $(H \cap K) \lhd H$, e além disso $\frac{H}{H \cap K} \approx \frac{H * K}{K}$.

Prova. Como $K \lhd G$ então $a * K = K * a$ para todo $a \in G$. Segue que

$$(H * K) = \{h * K; \quad h \in H \subset G\} = \{K * h; \quad h \in H \subset G\} = (K * H).$$

Seja e o elemento neutro de G. Para provarmos (i), notemos primeiramente que $(H * K) \neq \emptyset$, pois $e \in H$ e $e \in K$ e então $e \in (H * K)$. Suponha agora $x, y \in (H * K)$, então existem $h_1, h_2 \in H$ e $k_1, k_2 \in K$ tais que, $x = h_1 * k_1$ e $y = h_2 * k_2$. Assim,

$$x * y' = (h_1 * k_1) * (h_2 * k_2)' = (h_1 * k_1) * (k_2' * h_2') = h_1 * ((k_1 * k_2') * h_2').$$

Como $(k_1 * k_2') * h_2' \in K * H = H * K$, existem $h \in H$ e $k \in K$ de forma que

$$x * y' = h_1 * ((k_1 * k_2') * h_2') = h_1 * (h * k) = (h_1 * h) * k \in H * K.$$

Segue que $x * y' \in (H * K)$, e da Proposição (2.7), $(H * K)$ é subgrupo de G. Além disso, $K = e * K \subset (H * K)$. É imediato que $K \lhd (H * K)$, pois como $K \lhd G$, da Proposição 2.41 segue que $a * k * a' \in K$ para todos $k \in K$ e $a \in G$ e, em particular para $a \in H * K \subset G$, a mesma Proposição 2.41 garante que $K \lhd (H * K)$.

Para provar (ii), começamos tomando $h \in H \cap K$ e $a \in H \subset G$ arbitrários. Como K é normal em G então da Proposição 2.41 temos que $a * h * a' \in K$. Também, como $a, h \in H$ e H é subgrupo de G, segue que $a * h * a' \in H$ e desta forma, $a * h * a' \in H \cap K$. Segue novamente da Proposição 2.41 que que $H \cap K \lhd H$.

com $K \lhd G$. Como $H \cap K$ é subgrupo de G mostraremos que $H \cap K = Ker(\eta) \subset H$, para algum homomorfismo η. Consideremos então a aplicação

$$\begin{array}{rcl} \eta : H & \to & \dfrac{H * K}{K} \\ h & \mapsto & \eta(h) = h * K. \end{array}$$

Dados $x, y \in H$ temos,

$$\eta(x * y) = (x * y) * K = (x * K) * (y * K) = \eta(x) * \eta(y),$$

e então η é um homomorfismo.

Portanto, do teorema fundamental do homomorfismo, temos que

$$\frac{H}{Ker(\eta)} \approx Im(\eta),$$

sendo que determinaremos ainda $Ker(\eta)$ e $Im(\eta)$.

Além disso,

$$Im(\eta) =$$

Rever este homomorfismo e estas continhas... Notemos que $H * K = (H * K) * K$, pois sendo K subgrupo $K * K = K$ e então $H * K = H * (K * K) = (H * K) * K$. Além disso,

$$\frac{H * K}{K} = \{x * K; \quad \forall x \in H * K\} = (H * K) * K = H * K,$$

e como $Im(\eta) = \eta(H) = \{h * K; \quad h \in H\} = \frac{H}{K}$. Temos também,

$$\begin{array}{rcl} Ker(\eta) & = & \{h \in H; \quad \eta(h) = 0_{(H*K)/K}\} = \{h \in H; \quad h * K = 0_G * K\} \\ & = & \{h \in H; \quad (h - 0_G) \in K\} = \{h \in H; \quad h \in K\} = H \cap K. \end{array}$$

Desta forma $H \cap K$ é o núcleo de um homomorfismo, e como $Ker(\eta)$ é subgrupo normal, segue que $H \cap K$ é subgrupo normal de H. Portanto, do teorema fundamental do homomorfismo, temos que

$$\frac{H}{Ker(\eta)} \approx Im(\eta), \qquad \text{isto é,} \qquad \frac{H}{H \cap K} \approx \frac{H * K}{K}.$$

□

Exemplo 2.26. Fixado $m \in \mathbb{Z}$ com $m \geq 2$, considere os grupos $(\mathbb{Z}, +)$ e $(\mathbb{Z}_m, +)$. Vamos mostrar que $\frac{\mathbb{Z}}{m\mathbb{Z}} \approx \mathbb{Z}_m$. Representemos $a \sim b$ se e somente se $m|(a-b)$, a relação de equivalência módulo m, usada para construir a classes de equivalência em $\mathbb{Z}_m$.

Consideremos a aplicação

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \to & \mathbb{Z}_m \\ k & \mapsto & \varphi(k) = \overline{k}. \end{array}$$

Dados $x, y \in \mathbb{Z}$, temos

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

e então φ é um homomorfismo. Segue do teorema fundamental do homomorfismo que

$$\frac{\mathbb{Z}}{Ker(\varphi)} \approx Im(\varphi).$$

Vamos agora determinar $Ker(\varphi)$ e $Im(\varphi)$. Primeiro temos que

$$\begin{aligned} Ker(\varphi) &= \{x \in \mathbb{Z}; \quad \varphi(x) = \overline{0}\} \\ &= \{x \in \mathbb{Z}; \quad \overline{x} = \overline{0}\} \\ &= \{x \in \mathbb{Z}; \quad x \sim 0\} \\ &= \{x \in \mathbb{Z}; \quad m|(x-0)\} \\ &= \{x \in \mathbb{Z}; \quad x = mk, k \in \mathbb{Z}\} = \{mk, \quad k \in \mathbb{Z}\} = m\mathbb{Z}. \end{aligned}$$

Para ver que $Im(\varphi) = \mathbb{Z}_m$, vamos provar que φ é sobrejetora. Dado então $\overline{y} \in \mathbb{Z}_m$, basta tomar $x = y \in \mathbb{Z}$. Desta forma, $\varphi(x) = \overline{x} = \overline{y}$, mostrando a sobrejetividade de φ e portanto $Im(\varphi) = \mathbb{Z}_m$. Segue então que

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \approx \mathbb{Z}_m.$$

■

2.7 Subgrupos de Sylow

Como vimos anteriormente, dado um subgrupo S de um grupo finito G, então a ordem de S divide a ordem de G. Uma pergunta natural que surge é dado um grupo finito G e um divisor k da ordem de G, é possível encontrar subgrupos de G com ordem k? A resposta é não.

Como contra-exemplo, consideremos o conjunto $E = \{1, 2, 3, 4\}$ e o conjunto $\mathcal{F}$ de todas as permutações (aplicações) pares de elementos em E, isto é,

$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \quad f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix},$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \quad f_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix},$$

$$f_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \quad f_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \quad f_9 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix},$$
$$f_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad f_{11} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad f_{12} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

O conjunto de todas estas permutações, com a composição de aplicações é um grupo de ordem 12. Mas não é possível extrair dentre estas aplicações um subgrupo de ordem 6. De fato, todos os subgrupos possíveis de $\mathcal{F}$ são $\{f_1\}$, $\{f_1, f_4\}$, $\{f_1, f_9\}$, $\{f_1, f_{12}\}$, $\{f_1, f_2, f_3\}$, $\{f_1, f_5, f_7\}$, $\{f_1, f_6, f_{10}\}$, $\{f_1, f_8, f_{11}\}$, $\{f_1, f_4, f_9, f_{12}\}$ e $\mathcal{F}$. Ver se não é possível mesmo...

Embora tenhamos este exemplo, em algumas situações, é possível garantir que dado um divisor k de $o(G)$ existe um subgrupo de G com ordem k. Os principais resultados a este respeito são devidos a Sylow (Ver A.2), e os Teoremas de Sylow são agora nosso objetivo. Antes destes resultados, precisamos de alguns estudos preliminares.

Consideremos então um grupo $(G, *)$, de ordem finita, e definimos em G a relação

$$a \sim b \quad \Leftrightarrow \quad a = x' * b * x \quad \text{para algum} \quad x \in G.$$

É fácil ver que esta relação é uma relação de equivalência em G. De fato,

i) Para todo $a \in G$ tem-se $a \sim a$, pois $0_G \in G$, e $a = 0'_G * a * 0_G$. Isto significa que $\sim$ é reflexiva.

ii) Dados $a, b \in G$ com $a \sim b$, isto é, $a = x' * b * x$ para algum $x \in G$. Então temos, $a = x' * b * x$ e então $x * a * x' = b$. Segue que $b = (x')' * a * x'$ sendo que $x' \in G$, e desta forma $b \sim a$, mostrando que $\sim$ é simétrica.

iii) Sejam $a, b, c \in G$ tais que $a \sim b$ e $b \sim c$, isto é, $a = x' * b * x$ e $b = y' * c * y$, para algum $x, y \in G$. Então,

$$a = x' * (y' * c * y) * x = (x' * y') * c * (y * x) = (y * x)' * c * (y * x),$$

e como $(y * x) \in G$ segue que $a \sim c$ e a transitividade da relação $\sim$.

De *i*), *ii*) e *iii*), temos que $\sim$ define então uma relação de equivalência em G. A classe de equivalência de um elemento $a \in G$, é o conjunto de todos os elementos de G que se relacionam com a por $\sim$. Tais classes serão denotadas por C_a e dadas por,

$$C_a = \{b \in G; \quad a \sim b\} = \{b \in G; \quad b = x' * a * x \quad \text{para algum} \quad x \in G\},$$

ou ainda,

$$b \in C_a \quad \Leftrightarrow \quad b = x' * a * x, \quad \text{para algum} \quad x \in G.$$

É bastante claro que, por se tratar de uma relação de equivalência, temos $a \in C_a$ para cada $a \in G$. Também duas classes C_a e C_b quaisquer, ou são disjuntas ou são iguais. Estes fatos são devidos à proposição (1.34). Além disso, cada classe C_a é um subgrupo de G. A prova deste fato é deixada como exercício.

O procedimento que acabamos de fazer poderia ser refeito considerando uma relação sobre os subgrupos de um grupo finito G. Se S e H são dois subgrupos de G, definimos a relação

$$S \sim H \quad \Leftrightarrow \quad S = x' * H * x \text{ para algum } x \in G.$$

Esta relação também é uma relação de equivalência. É chamada de relação de conjugação de subgrupos, e dois subgrupos, S e H, serão ditos subgrupos conjugados. O conjunto

$$C_H = \{S; \quad S \sim H\} = \{S; \quad S = a' * H * a, \quad \text{para algum} \quad a \in G\},$$

é a classe de todos os subgrupos de G conjugados de H, que será chamada de classe de conjugação do subgrupo H. Observe que C_H é sempre não vazio, pois pelos menos teremos $H \in C_H$.

Definição 2.50. Dado um subgrupo H de um grupo $(G, *)$, definimos a *órbita* de H determinada pelo elemento $a \in G$, como sendo o subgrupo $\mathcal{O}_a(H) \subset G$, dado por

$$\mathcal{O}_a(H) = a' * H * a = \{a' * h * a; \quad h \in H\}.$$

O conjunto C_H é exatamente o conjunto de todas as órbitas de H em G. A órbita $\mathcal{O}_a(H)$ é também chamada de a-órbita de H em G. Quando o elemento a é um elemento que varia em um subconjunto $S \subset G$, temos a S-órbita de H, que é o conjunto

$$\mathcal{O}_S(H) = \{\mathcal{O}_a(H); \quad a \in S\} = \{a' * H * a; \quad a \in S\}.$$

Definição 2.51. Dado um grupo $(G, *)$, e um elemento $a \in G$, definimos o *centro* ou *centralizador* de a, como sendo o subconjunto de G, denotado por $Z(a)$, e dado por

$$Z(a) = \{g \in G; \quad g * a = a * g\},$$

isto é, o conjunto de todos os elementos de G que comutam com a.

Definição 2.52. Dado um grupo $(G, *)$, e S um subconjunto não vazio de G. O *centro* ou *centralizador* de S é o subconjunto denotado por $Z(S)$ e dado por

$$Z(S) = \{g \in G; \quad g * s = s * g, \quad \text{para todo} \quad s \in S\}.$$

Note que $Z(G)$ é então,

$$Z(G) = \{g \in G; \quad g * x = x * g, \quad \text{para todo} \quad x \in G\},$$

isto é, o conjunto de todos os elementos comutativos em G. Observe ainda, que se G é um grupo abeliano, então todos os elementos de G são comutativos para a operação $*$, isto é, $Z(G) = G$. Além disso, se $S = \{a\}$, então $Z(S) = Z(a)$. É comum também chamar o centralizador de *normalizador*, e denotá-lo por $N(a)$ ou $N(S)$.

Proposição 2.53. *Dado um grupo $(G, *)$ então, para qualquer $S \subset G$, o centralizador $Z(S)$, munido da mesma operação $*$, é um subgrupo de G.*

Prova. Dado então $S \subset G$, mostraremos que $Z(S)$ cumpre os axiomas da definição de grupo. Notemos primeiramente que $Z(S)$ é não vazio, pois como $s * 0_G = 0_G * s$, para todo $s \in S$, e então $0_G \in Z(S)$.

Sejam agora $x, y \in Z(S)$, então $x * s = s * x$ e $y * s = s * y$ para todos $s \in S$. Então para qualquer $s \in S$, temos,

$$(x * y) * s = x * (y * s) = x * (s * y) = (x * s) * y = (s * x) * y = s * (x * y),$$

isto é, $(x * y) \in Z(S)$, mostrando que $Z(S)$ é fechado para a operação $*$.

Suponha $x \in Z(S)$. Temos que para qualquer $s \in S$,

$$x * s = s * x \quad \Rightarrow \quad s = x' * s * x \quad \Rightarrow \quad s * x' = x' * s,$$

mostrando que $x' \in Z(S)$. Sabendo ainda que $*$ é associativa em G, será também associativa em $Z(S) \subset G$. Destes fatos, temos que $Z(S)$ é um grupo, e portanto um subgrupo de G. □

Além do que foi feito, é também fácil ver que $Z(S)$ é um subgrupo normal de G, pois é comutativo com os elementos de G. A prova que $Z(a)$ é também um subgrupo de G é deixada como exercício, e pode ser análoga ao que acabamos de fazer.

Proposição 2.54. *Dado um subgrupo H de um grupo finito $(G, *)$, então $H \lhd Z(H)$.*

Prova. Ver isto... Acho que isto não procede porque $Z(H) \lhd G$. □

Proposição 2.55. *Dado um grupo $(G, *)$ então temos que*

$$a \in Z(G) \quad \Leftrightarrow \quad C_a = \{a\}.$$

Prova. Suponha $a \in Z(G)$. Mostraremos a dupla inclusão dos conjuntos. Primeiramente, é obvio que $a \in C_a$ e então $\{a\} \subset C_a$. Suponha agora que $x \in C_a$, então existe $g \in G$ tal que $a = g * x * g'$, ou ainda, $a * g = g * x$. Mas como $a \in Z(G)$, a comuta com qualquer elemento de G, então $g * a = g * x$ e pela lei do cancelamento, $a = x$ donde $x \in \{a\}$. Fica então mostrada a segunda inclusão e a igualdade $C_a = \{a\}$.

Suponha agora $C_a = \{a\}$. Para qualquer $g \in G$, como G é fechado para a operação $*$, temos que

$$g' * a * g \in G,$$

isto significa que existe $x \in G$ de forma que $g' * a * g = x$, ou ainda, $a = g * x * g'$, e então $x \in C_a = \{a\}$. Assim, $x = a$, e devemos ter então $g' * a * g = a$, ou ainda $a * g = g * a$ para qualquer $g \in G$. Isto mostra que $a \in Z(G)$, que completa a demonstração. □

Se um grupo G é finito, então $G = \{a_i\}_{1 \leq i \leq n}$, e como cada elemento a_i pertence a classe de equivalência C_{a_i}, então

$$G = \bigcup_{i=1}^{n} C_{a_i}.$$

Mas como já provamos, estas classes são duas a duas iguais ou totalmente distintas. Escolhemos apenas o conjunto das k classes distintas e então temos,

$$G = \bigcup_{j=1}^{k} C_{a_j} = C_{a_1} \cup C_{a_2} \cup \cdots \cup C_{a_k},$$

e desta forma

$$o(G) = o\left(\bigcup_{j=1}^{k} C_{a_j}\right) = o(C_{a_1} \cup C_{a_2} \cup \cdots \cup C_{a_k}) = \sum_{j=1}^{k} o(C_{a_j}).$$

Além disso, sabemos que se $C_{a_i} = \{a_i\}$, então $a_i \in Z(G)$ e desta forma, podemos reescrever a expressão acima, isolando os elementos que pertencem a $Z(G)$, obtendo

$$o(G) = \sum_{a_j \in Z(G)} o(C_{a_j}) + \sum_{a_j \notin Z(G)} o(C_{a_j}) = o(Z(G)) + \sum_{a_j \notin Z(G)} o(C_{a_j}).$$

Nestes termos, o que temos é

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} |C_x|,$$

que é conhecida como equação das classes.

Antes da próxima proposição, lembremos que, $(G : Z(a))$ é a quantidade de elementos (classes laterais) do conjunto quociente $\frac{G}{Z(a)}$. Mais ainda, da proposição (2.33),

$$x * Z(a) = y * Z(a) \quad \Leftrightarrow \quad (x * y') \in Z(a).$$

Proposição 2.56. *Se $(G, *)$ é um grupo finito e $a \in G$ um elemento fixo, então*

$$|C_a| = o(C_a) = (G : Z(a)).$$

Prova. Consideremos a aplicação,

$$\begin{array}{rcl} \varphi : \dfrac{G}{Z(a)} & \to & C_a \\ g * Z(a) & \mapsto & \varphi(g * Z(a)) = g' * a * g. \end{array}$$

A primeira coisa a fazer é mostrar que esta aplicação está bem definida. Suponha $g * Z(a) = h * Z(a)$ representantes da mesma classe. Então, $(g * h') \in Z(a)$, e

$$\begin{array}{rcrcl} (g * h') \in Z(a) \quad \Rightarrow & (g * h') * a & = & a * (g * h') & \Rightarrow \\ & h' * a & = & g' * a * g * h' & \Rightarrow \\ & h' * a * h & = & g' * a * g \quad \Rightarrow & \varphi(h * Z(a)) = \varphi(g * Z(a)), \end{array}$$

segue que φ está bem definida.

Para mostrar que φ é bijetiva, seja $y \in C_a$, então $a = g' * y * g$ para algum $g \in G$. Escolhemos então $x = g * Z(a) \in \frac{G}{Z(a)}$, e temos,

$$\varphi(x) = \varphi(g * Z(a)) = g' * a * g = g' * (g * y * g') * g = (g' * g) * y * (g' * g) = y,$$

e então φ é sobrejetiva. Além disso, sejam $(g * Z(a)), (h * Z(a)) \in \frac{G}{Z(a)}$ com $\varphi(g * Z(a)) = \varphi(h * Z(a))$. Mas,

$$\varphi(g * Z(a)) = \varphi(h * Z(a)) \quad \Rightarrow \quad g' * a * g = h' * a * h \quad \Rightarrow \quad h * g' * a = a * h * g',$$

e assim $(h * g')$ comuta com a, ou ainda, $(h * g') \in Z(a)$, donde $h * Z(a) = g * Z(a)$, que prova a injetividade. Desta forma a aplicação φ é bijetora, e então os conjuntos possuem a mesma quantidade de elementos, isto é, $|C_a| = (G : Z(a))$. □

Com esta proposição, a equação das classes, pode ser reescrita na forma

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} (G : Z(x)).$$

Proposição 2.57. *Se G é um p-grupo, então $Z(G)$ tem pelo menos p elementos.*

Prova. Suponha G tal que $|G| = p^k$ com p primo, e $k \in \mathbb{N}^*$. Sabemos que

$$p^k = |G| = |z(G)| + \sum_{x \notin Z(G)} |C_x|.$$

Para cada um dos elementos $x \notin Z(G)$, então temos $C_x \neq \{x\}$, isto é, $|C_x| > 1$ e da última proposição, $(G : Z(x)) > 1$. Também, como

$$|G| = |Z(x)|(G : Z(x)),$$

então $(G : Z(x))|o(G)$. Desta forma, $(G : Z(x))|p^k$ e $(G : Z(x)) > 1$, logo $(G : Z(x))$ é um múltiplo de p para todos $x \notin Z(G)$, e então $\sum_{x \notin Z(G)}(G : Z(x))$ é múltiplo de p. Assim,

$$|Z(G)| = |G| - \sum_{x \notin Z(G)} (G : Z(x)),$$

e como os dois termos do segundo membro são múltiplos de p, então o primeiro membro é múltiplo de p, isto é, $|Z(G)| = kp$. Além disso, $0_G \in Z(G)$ e então $|Z(G)| \geq 1$, e então necessariamente $k \neq 0$, mostrando que $k \geq 1$ e portanto $|Z(G)|$ tem no mínimo p elementos. □

Lema 2.58. *Seja H um subgrupo de um grupo finito G. Então*

$$|C_H| = (G : Z(H)).$$

Prova. Vamos considerar a seguinte aplicação, que mostraremos ser bijetora,

$$\begin{aligned} \varphi : \frac{G}{Z(H)} &\to C_H \\ a * Z(H) &\mapsto \varphi(a * Z(H)) = a' * H * a. \end{aligned}$$

A primeira coisa a fazer é mostrar que se trata de fato de uma aplicação bem definida. Suponha que $a * Z(H) = b * Z(H)$ sejam representantes da mesma classe. Então $(a * b') \in Z(H)$, e da definição de $Z(H)$ temos,

$$(a * b') * H = H * (a * b') \quad \Rightarrow \quad b' * H * b = a' * H * a \quad \Rightarrow \quad \varphi(b * H) = \varphi(a * H),$$

mostrando que φ está bem definida.

Consideremos agora $Y \in C_H$ um subgrupo conjugado de H, isto significa que existe $a \in G$ tal que $Y = a' * H * a$, e desta forma escolhemos $X = a * Z(H) \in \frac{G}{Z(H)}$, e temos

$$\varphi(X) = \varphi(a * Z(H)) = a' * H * a = Y,$$

que mostra a sobrejetividade de φ.

Finalmente, suponha $a*Z(H), b*Z(H) \in \frac{G}{Z(H)}$, com $\varphi(a*Z(H)) = \varphi(b*Z(H))$, então $a' * H * a = b' * H * b$, ou ainda, $H * (a * b') = (a * b') * H$ e temos então $(a * b') \in Z(H)$ donde segue que $a * Z(H) = b * Z(H)$, e fica mostrada a injetividade. Desta forma, φ é bijetora, e segue que, os conjuntos envolvidos possuem a mesma quantidade de elementos. Designando por $|C_H|$ a quantidade de elementos de C_H e por $(G : Z(H))$ a quantidade de elementos de $\frac{G}{Z(H)}$, temos $|C_H| = (G : Z(H))$. □

Definição 2.59. Seja $(G, *)$ um grupo finito. Se a ordem de G for uma potência natural de um número p primo, isto é, se

$$|G| = p^n, \quad \text{para algum} \quad n \in \mathbb{N},$$

então G é dito um *p-grupo*.

Proposição 2.60 (Teorema de Cauchy)**.** *Se $(G, *)$ é um grupo finito e p é um número primo tal que $p|o(G)$, então existe $a \in G$ com $o(a) = p$. Consequentemente $\langle a \rangle$ será subgrupo de G com $o(\langle a \rangle) = p$.*

Prova. Usaremos indução sobre $|G|$. Se $|G| = 2$ então $G = \{0_G, a\}$, e como $p|o(G) = 2$ é primo, devemos ter $p = 2$. Mas também, $a^2 = 0_G$ pois todo elemento de G é regular, donde $o(a) = 2 = p$ comprovando o resultado para $|G| = 2$. Suponha agora o resultado válido para qualquer grupo de ordem menor que n e que $o(G) = n > 2$, e p um número primo tal que $p|o(G)$. Consideraremos três casos:

i) G é cíclico. Então $G = \langle b \rangle$ para algum $b \in G$. Como $p|o(G)$, então

$$p|o(\langle b \rangle) \quad \Rightarrow \quad p|o(b) \quad \Rightarrow \quad o(b) = p^k m,$$

onde $k \geq 1$. Tomemos $a = b^{p^{k-1}m} \in \langle b \rangle$, e é claro que

$$a^p = (b^{p^{k-1}m})^p = b^{p^{k-1}mp} = b^{p^k m} = b^{o(b)} = 0_G,$$

e se $l < p$, então $p^{k-1}ml < p^{k-1}mp = p^k m = o(b)$, e então, $b^{p^{k-1}ml} \neq 0_G$, donde $a^l = b^{p^{k-1}ml} \neq 0_G$, mostrando que $o(a) = p$.

ii) G não é cíclico, mas é abeliano. Seja $b \neq 0_G \in G$. Se $p|o(b) = o(\langle b \rangle)$, então pelo item *i*) existe $a \in \langle b \rangle \subset G$ com $o(a) = p$. Se $p \nmid o(b)$, então $p \nmid o(\langle b \rangle)$ e como do Teorema de Lagrange, $|G| = |\langle b \rangle|(G : \langle b \rangle)$, devemos ter que

$$p|(G : \langle b \rangle) = o\left(\frac{G}{\langle b \rangle}\right) = \frac{o(G)}{o(\langle b \rangle)}$$

e $\frac{G}{\langle b \rangle}$ é grupo com ordem menor que $o(G) = n$ e portanto pela hipótese de indução existe um elemento $(g * \langle b \rangle) \neq (0_G * \langle b \rangle) \in \frac{G}{\langle b \rangle}$ tal que $o(g * \langle b \rangle) = p$. Do algoritmo da divisão, existem $k, r \in \mathbb{Z}$ tais que

$$o(g) = kp + r \quad \text{com} \quad 0 \leq r < p.$$

Mas,

$$(g * \langle b \rangle)^{o(g)} = g^{o(g)} * \langle b \rangle = 0_G * \langle b \rangle,$$

e então,

$$0_G * \langle b \rangle \quad = \quad (g * \langle b \rangle)^{o(g)} = (g * \langle b \rangle)^{kp+r} =$$

$$= \quad (g * \langle b\rangle)^{pk} * (g * \langle b\rangle)^r = (0_G)^k * (g * \langle b\rangle)^r = (g * \langle b\rangle)^r$$

e então $(g * \langle b\rangle)^r = (0_G * \langle b\rangle)$. Mas como $p = o(g * \langle b\rangle)$ deve ser o menor número natural não nulo tal que $(g * \langle b\rangle)^p = (0_G * \langle b\rangle)$, e como $r < p$, então devemos ter $r = 0$, donde $o(g) = kp$ e então $p|o(g) = o(\langle g\rangle)$. Novamente pelo item i) existe $a \in \langle g\rangle \subset G$ tal que $o(a) = p$.

iii) G não é abeliano. Então $Z(G) \neq G$. Se $p|o(Z(G))$ então como $Z(G)$ é abeliano, pelo item *ii*) existe $a \in Z(G) \subset G$ com $o(a) = p$. Se $p \nmid o(Z(G))$ e sendo G um grupo finito, então,

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} (G : Z(x)).$$

Sabendo que $p|o(G)$ e $p \nmid o(Z(G))$ então deve existir $b \notin Z(G)$ tal que $p \nmid (G : Z(b))$. Mas como (Teorema de Lagrange),

$$|G| = |Z(b)|(G : Z(b)),$$

então $p|o(Z(b)) < |G|$, e da hipótese de indução, segue que existe $a \in Z(b) \subset G$ com $o(a) = p$, finalizando assim a demonstração deste teorema. □

Proposição 2.61 (Primeiro Teorema de Sylow)**.** *Se p é um número primo e $(G, *)$ é um grupo finito com $|G| = mp^k$, para algum $m \neq 0, k \in \mathbb{N}$, com* $\text{mdc}(m, p) = 1$*, então existe um subgrupo S de G com ordem p^k.*

Prova. Usaremos indução finita sobre a ordem de G. Suponha $|G| = 1 = 1p^0$, então G tem um subgrupo $\{0_G\}$ com ordem $1 = p^0$. Suponha agora que o resultado seja verdadeiro para qualquer grupo de ordem menor que n, e que $|G| = n = mp^k$. Vamos considerar dois casos:

i) Se $p|o(Z(G))$. Neste caso, do Teorema de Cauchy, o centro $Z(G)$ contém um elemento a de ordem p. O subgrupo cíclico $\langle a\rangle$ também tem ordem p, e é normal em G, donde o grupo quociente $\frac{G}{\langle a\rangle}$ tem ordem $\frac{|G|}{|\langle a\rangle|} = \frac{n}{p}$. Como $p^k|n$ então $p^{k-1}|\frac{n}{p}$ que é menor que n. Portanto pela hipótese de indução $\frac{G}{\langle a\rangle}$ tem um subgrupo $\frac{H}{\langle a\rangle}$ de ordem p^{k-1}, e assim do Teorema de Lagrange,

$$|H| = |\langle a\rangle|(H : \langle a\rangle) = pp^{k-1} = p^k,$$

que conclui a demonstração para este caso.

ii) Se $p \nmid o(Z(G))$. Neste caso, consideremos a equação das classes de G, que é

$$mp^k = n = |G| = |Z(G)| + \sum (G : Z(a)), \quad \text{para todo } a \notin Z(G).$$

Mas, $p|n$ e $p \nmid o(Z(G))$, então p não divide $(G : Z(a))$, para algum $a \in G$, com $a \notin Z(G)$. Do Teorema de Lagrange,

$$mp^k = |G| = |Z(a)|(G : Z(a)),$$

mas como $p^k|o(G)$ e $p \nmid (G : Z(a))$, devemos ter $p^k|o(Z(a))$ e $|Z(a)| < |G|$. Pela hipótese de indução $Z(a)$ tem um subgrupo de ordem p^k, e isto completa a demonstração. □

Definição 2.62. Nas condições da proposição anterior, isto é, p um número primo e $(G, *)$ um grupo com $|G| = mp^k$, para $m \neq 0, k \in \mathbb{N}$ e $\text{mdc}(m, p) = 1$, então o subgrupo S de G que tem ordem p^k é dito um *p-subgrupo* de Sylow.

Proposição 2.63 (Segundo Teorema de Sylow)**.** *Se $(G, *)$ é um grupo finito, e S e H são dois p-subgrupos de Sylow, então existe $a \in G$ tal que $S = a * H * a'$, isto é, S e H são subgrupos conjugados.*

Prova. Seja S um p-subgrupo de G, onde $|G| = mp^k$, para $m \neq 0, k \in \mathbb{N}$. Consideremos o conjunto dos subgrupos conjugados de S, dado por,

$$C_S = \{a' * S * a; \quad a \in G\}.$$

Então, da proposição (2.56), temos

$$|C_S| = (G : Z(S)) = \left|\frac{G}{Z(S)}\right|.$$

Como S é um p-subgrupo de Sylow, então $|S| = p^k$, e como S

mdc $\left(\left|\frac{G}{Z(S)}\right|, p\right) = 1$ e portanto mdc$(|C_S|, p) = 1$. Suponhamos agora H um p-subgrupo de Sylow. Mostraremos que H é conjugado a K. Vamos olhar o conjunto $C(K)$ como um H-conjunto pela conjugação. Então, para qualquer $L \in C(K)$, seja

$$C_H(L) = \{hLh^{-1}; \quad h \in H\},$$

a órbita de L. Claramente, $C_H(L) \subset C(K)$, e

$$C(K) = \bigcup_{L \in C(K)} C_H(L), \quad \text{(disjuntos)},$$

onde a união varia em L um elemento de cada órbita (= classe conjugada $C_H(L)$). Temos que

$$|C_H(L)| = \text{índice de} \quad H \cap N(L) \quad \text{em} \quad H = p^s, \quad s \geq 0,$$

pois H é um p-subgrupo de Sylow. Primeiramente mostramos que $p^s = 1$ se e somente se $H = L$. Se $H = L$ então trivialmente, $p^s = 1$. Reciprocamente

$$p^s = 1 \Rightarrow H = H \cap N(L) \Rightarrow H \subset N(L) \Rightarrow HL < G \quad \text{e} \quad L \lhd HL.$$

Mas então

$$\frac{HL}{L} \approx \frac{H}{HL} \Rightarrow \frac{HL}{L} \quad \text{é um p-subgrupo} \quad \Rightarrow HL = L,$$

pois L é um p-subgrupo de Sylow. Assim, nossa afirmação $p^s = 1 \Leftrightarrow H = L$ está provada. De (??) e (??) temos

$$|C(K)| = \sum p^s.$$

Mas então (??) implica que no somatório anterior, pelo menos um termo deve ser igual a 1, e isto implica, pelo que foi estabelecido no último parágrafo, que H deve ser igual a algum conjugado L de K provando o teorema. □

Proposição 2.64 (Terceiro Teorema de Sylow)**.** *O número de p-subgrupos de Sylow do grupo $(G, *)$ é um divisor*

Prova. Como todos os p-subgrupos de Sylow em G, são conjugados a K, segue que seu número n_p é igual a $|C(K)| = |\frac{G}{N(K)}|$. Portanto n_p divide $|G|$. É também claro que existe um, e apenas um, termo na soma $\sum p^s$ que é igual a 1, assim temos de (??), que o número de conjugados de K distintos é

$$n_p = 1 + \sum_{s>0} p^s = 1 + pk \equiv 1 (\text{mod } p),$$

provando o teorema. □

2.8 Grupos e subgrupos solúveis

O que apresentaremos nesta seção é de fundamental importância na teoria de solubilidade de equações por radicais. Caso seja esquecido de mensionar alguma vez, os grupos considerados nesta seção, serão sempre finitos.

Definição 2.65. Seja $(G, *)$ um grupo finito. Uma sequência de subgrupos

$$\{0_G\} = G_k \subset G_{k-1} \subset \cdots \subset G_2 \subset G_1 \subset G_0 = G,$$

é dita uma *série normal* para o grupo G, se cada G_i é normal (e diferente) em G_{i-1}, isto é, se

$$\{0_G\} = G_k \lhd G_{k-1} \lhd \cdots \lhd G_2 \lhd G_1 \lhd G_0 = G.$$

Denotaremos também uma série normal para o grupo finito G da forma $(G_i)_{0\leq i\leq k}$, com $k \in \mathbb{N}^*$. Notemos que embora $G_i \lhd G_{i-1}$, não é necessário que cada subgrupo seja normal em G. Já que temos $G_i \lhd G_{i-1}$, podemos então associar a esta sequência de subgrupos, a sequência de grupos quocientes

$$\frac{G_0}{G_1}, \frac{G_1}{G_2}, \ldots, \frac{G_{k-2}}{G_{k-1}}, \frac{G_{k-1}}{G_k}.$$

Definição 2.66. Um grupo G é dito *solúvel* se cada um dos grupos quocientes

$$\frac{G_{i-1}}{G_i}, \quad \text{para qualquer } 1 \leq i \leq k,$$

é um grupo abeliano.

É claro que se G for grupo abeliano, então os grupos quocientes também serão abelianos, e então G será solúvel.

Definição 2.67. Uma *série de composição* para um grupo G, é uma série normal, sem repetição, onde cada grupo quociente $\frac{G_{i-1}}{G_i}$ é simples, isto é, não admite subgrupos além dos triviais. Neste caso, os grupos quocientes serão chamados de *fatores* da composição.

Em virtude do corolário (**??**), podemos dizer que uma série de composição é uma série normal onde cada G_i é subgrupo normal maximal de G_{i-1}. Um fato importante é que uma série de composição para um grupo G não é necessariamente única. Vejamos um exemplo. Tomemos $G = (\mathbb{Z}_{12}, +)$, que é um grupo abeliano. Temos então,

$$\begin{aligned}
&\{\overline{0}\} \lhd \{\overline{0}, \overline{6}\} \lhd \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} \lhd \mathbb{Z}_{12},\\
&\{\overline{0}\} \lhd \{\overline{0}, \overline{6}\} \lhd \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\} \lhd \mathbb{Z}_{12},\\
&\{\overline{0}\} \lhd \{\overline{0}, \overline{4}, \overline{8}\} \lhd \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\} \lhd \mathbb{Z}_{12}.
\end{aligned}$$

É claro que cada um dos subgrupos acima são abelianos. Cada $\frac{G_{i-1}}{G_i}$ é simples, pois em cada caso, a ordem $\left|\frac{G_{i-1}}{G_i}\right| = \frac{|G_{i-1}|}{|G_i|}$ é um número primo e portanto não admite subgrupos diferentes dos triviais (ver corolário do Teorema de Lagrange).

Proposição 2.68. *Todo grupo finito G de ordem $|G| = p^k$, com p primo e $k \in \mathbb{N}^*$, é solúvel.*

Prova. Seja G satisfazendo $|G| = p^k$ com p primo. Então como visto nas proposições (2.53) e (2.57), $Z(G)$ tem pelo menos p elementos, e é um subgrupo de G. Então é um subgrupo não trivial de G. Colocamos $C_1 = Z(G)$ e temos que $\frac{G}{C_1}$ é um p-grupo e tem centro não trivial também. Colocamos $C_2 = Z(\frac{G}{C_1})$, e da mesma forma $C_3 = Z(\frac{G}{C_2})$, e assim sucessivamente. Obtemos então

$$\{0_G\} \subsetneq C_1 \subsetneq C_2 \subsetneq C_3 \subsetneq \dots$$

Como G é finito, devemos ter $C_s = G$ para algum s. Então

$$\{0_G\} \subsetneq C_1 \subsetneq C_2 \subsetneq C_3 \subsetneq \dots C_s = G,$$

e como os centros são subgrupos normais, temos

$$\{0_G\} = C_0 \lhd C_1 \lhd C_2 \lhd \cdots \lhd C_{s-1} \lhd C_s = G,$$

que encerra a demonstração. □

Definição 2.69. Se g, h são elementos de um grupo G, definimos o comutador de g e h como sendo o elemento $c(g,h) \in G$, dado por $c(g,h) = g' * h' * g * h$.

Observe que $g*h = h*g*c(g,h)$. O comutador é uma medida da falta de comutatividade entre os elementos g e h. Se G é um grupo abeliano, ou (menos ainda), se g e h são elementos de G que comutam entre si, então o comutador $c(g,h)$ é o elemento neutro 0_G.

Definição 2.70. Dado um grupo $G = \{0_G, a_1, a_2, \dots, a_n\}$ finito, definimos o *subgrupo derivado*, ou *subgrupo comutador* de G, como sendo o subconjunto, denotado por G', gerado por todos os comutadores $c(a_i, a_j)$ de G. Simbolicamente,

$$G' = \langle c(a_i,a_j); 1 \le i,j \le n \rangle = \left\{ \sum_{1 \le i,j \le n} c(a_i,a_j)^k; \quad a_i, a_j \in G, k \in \mathbb{Z} \right\}.$$

De outra forma, o conjunto G' é o conjunto de todos os elementos da forma (repetições são permitidas)

$$c(a_1,b_1) * c(a_2,b_2) * \cdots * c(a_m,b_n), \quad a_i, b_j \in G.$$

Observe ainda, que se G é abeliano, então como já comentamos, $c(a_i,b_j) = 0_G$ para quaisquer $a_i, b_j \in G$, e portanto $G' = \{0_G\}$. Lembremos também que o subconjunto gerado por uma coleção de elementos de um grupo G, é um subgrupo de G.

Proposição 2.71. *Se H é subgrupo de um grupo finito G, então $H' \lhd G$.*

Prova. Fazer isto ... □

Decorre desta proposição que como G' é subgrupo de G, então $G' \lhd G$. Podemos assim considerar $\frac{G}{G'}$ um grupo. De forma geral, definimos o subgrupo derivado de ordem $k \ge 1$, denotado por $G^{(k)}$, dado pela fórmula recursiva,

$$G^{(k)} = \begin{cases} G', & \text{se } k = 1, \\ (G^{(k-1)})', & \text{se } k > 1. \end{cases}$$

Desta forma, como $G' \lhd G$, garante-se que $G^{(i)} = (G^{(i-1)})' \lhd G^{(i-1)}$, para cada $1 \leq i \leq k$, ou ainda,

$$G^{(k)} \lhd G^{(k-1)} \lhd G^{(k-2)} \lhd \cdots \lhd G^{(2)} \lhd G' \lhd G,$$

e a proposição (2.71) garante que $G^{(k)} \lhd G$.

Proposição 2.72. *O grupo $\frac{G}{G'}$ é abeliano e G' está contido em cada subgrupo normal K tal que $\frac{G}{K}$ é abeliano.*

Prova. Fazer isto ... □

Teorema 2.73. *Um grupo finito G é solúvel se e somente se $G^{(k)} = \{0_G\}$ para algum $k \geq 1$.*

Prova. Fazer isto ... □

Teorema 2.74. *Seja $(G, *)$ um grupo (finito) solúvel. Então*

i) Qualquer subgrupo de G é solúvel,

ii) A imagem de um subgrupo solúvel por um homomorfismo, é solúvel,

iii) Se $H \lhd G$ e os grupos H e $\frac{G}{H}$ forem solúveis, então G é solúvel.

Prova. Fazer isto ... □

Teorema 2.75 (Teorema de Jordan-Hölder)**.** *Seja G um grupo finito e*

$$\{0_G\} = G_m \lhd G_{m-1} \lhd \cdots \lhd G_2 \lhd G_1 \lhd G_0 = G$$
$$\{0_G\} = H_n \lhd H_{n-1} \lhd \cdots \lhd H_2 \lhd H_1 \lhd H_0 = G$$

duas séries de composição para G. Então estas séries são equivalentes, isto é, $m = n$ e existe uma permutação $i \leftrightarrow j$, tal que

$$\frac{G_{i-1}}{G_i} \approx \frac{H_{j-1}}{H_j}, \qquad \forall \quad 1 \leq i \leq m.$$

Prova. Usaremos indução finita sobre a ordem de G. Se $|G| = 2$ então a única série de composição que G admite é $\{0_G\} \lhd \{0_G, a\} = G$ e o teorema é trivialmente satisfeito. Suponha agora que o resultado seja válido para qualquer grupo finito com ordem menor que $|G|$, e tomemos duas séries de composição para G,

$$S_1 = (G_i)_{0 \leq i \leq m} \qquad \text{e} \qquad S_2 = (H_j)_{0 \leq j \leq n}.$$

Se $G_1 = H_1$ então como a ordem de $G_1 = H_1$ é menor que a ordem de G, o resultado vale para G_1 e então $m = n$ e existe uma permutação de índices tais que $\frac{G_{i-1}}{G_i} \approx \frac{H_{j-1}}{H_j}$, e como também $\frac{G}{G_1} \approx \frac{G}{H_1}$ então o resultado fica provado neste caso.

Se $G_1 \neq H_1$ então tomemos $K = G_1 \cap H_1$. Como $G_1 \lhd G$ e $H_1 \lhd G$, então pelo corolário (**??**) temos que $K = G_1 \cap H_1$ é normal maximal de G_1 e de H_1. Pelo teorema (2.74), temos que K é solúvel, e denotemos

$$\{0_G\} = K_r \lhd K_{r-1} \lhd \cdots \lhd K_1 \lhd K_0 = K,$$

a série de composição de K. Desta forma temos,

$$S_3 : \qquad \{0_G\} = K_r \lhd K_{r-1} \lhd \cdots \lhd K_1 \lhd K_0 = K \lhd G_1 \lhd G_0 = G,$$

$$S_4 : \qquad \{0_G\} = K_r \lhd K_{r-1} \lhd \cdots \lhd K_1 \lhd K_0 = K \lhd H_1 \lhd H_0 = G.$$

Como $G_1 \lhd G$ e $H_1 \lhd G$, temos que $(G_1 * H_1) \lhd G$, e como $G_1 \subset (G_1 * H_1)$ e também $H_1 \subset (G_1 * H_1)$ são distintos e maximais em G, então devemos ter $(G_1 * H_1) = G$.

Então, do teorema (2.49) temos que

$$\frac{H_1}{G_1 \cap H_1} \approx \frac{G_1 * H_1}{G_1} = \frac{G}{G_1}, \quad \text{e também} \quad \frac{G_1}{G_1 \cap H_1} \approx \frac{H_1 * G_1}{H_1} = \frac{G}{H_1},$$

isto é,

$$\frac{H_1}{K} \approx \frac{G}{G_1}, \quad \text{e} \quad \frac{G_1}{K} \approx \frac{G}{H_1},$$

e então as sequências S_3 e S_4 são equivalentes.

Além disso, da hipótese de indução, como G_1 tem ordem menor do que $|G|$, então a sequência S_1 é equivalente a S_3 e também como H_1 tem ordem menor que $|G|$, então S_2 é equivalente a S_4, mostrando que S_1 é equivalente a S_2, e concluindo esta demonstração. □

Usaremos agora o Teorema de Jordan-Hölder para mostrar que todo número inteiro maior ou igual a 2, se decompõe de forma única (a menos de permutações) em fatores primos.

Corolário 2.76 (Teorema Fundamental da Aritmética)**.** *Se n é um número inteiro positivo e*

$$n = p_1 p_2 \dots p_m = q_1 q_2 \dots q_n,$$

com p_i e q_j primos, então $m = n$ e existe uma permutação $i \leftrightarrow j$, tal que, $p_i = q_j$ para todo $1 \leq i \leq m$.

Prova. Fazer isto ... □

Capítulo 3

Anéis

3.1 Anéis e subanéis

Definição 3.1. Seja $A \neq \emptyset$ um conjunto munido de duas operações, $*$ e $\circ$. Dizemos que A é um *anel* com as operações $*$ e $\circ$, se (e somente se)

i) $*$ é associativa, isto é, $a * (b * c) = (a * b) * c$ para todos $a, b, c \in A$,

ii) $*$ admite um elemento neutro 0_A, isto é, $a * 0_A = 0_A * a = a$ para todo $a \in A$,

iii) para todo $a \in A$, existe $(-a) \in A$, tal que, $a * (-a) = (-a) * a = 0_A$,

iv) $*$ é comutativa, isto é, $a * b = b * a$ para todos $a, b \in A$,

v) $\circ$ é associativa, isto é, $a \circ (b \circ c) = (a \circ b) \circ c$ para todos $a, b, c \in A$,

vi) $\circ$ é distributiva com relação a $*$, isto é, $a \circ (b * c) = (a \circ b) * (a \circ c)$ e $(a * b) \circ c = (a \circ c) * (b \circ c)$ para todos $a, b, c \in A$.

Como no caso dos grupos, o fato de A ser um anel é devido às propriedades das duas operações, isto significa que o mesmo conjunto A com outras operações pode não tornar-se anel. Por este motivo, dizemos que A é um anel sobre as operações $*$ e $\circ$ ou ainda que estas operações definem em A uma estrutura de anel.

É comum usar a representação na forma de terna ordenada $(A, *, \circ)$ e a expressão "anel $(A, *, \circ)$" para dizer que o conjunto não vazio A é um anel com as operações $*$ e $\circ$. É importante não confundir as ternas ordenadas $(A, *, \circ)$ e $(A, \circ, *)$.

Note que os quatro primeiros axiomas da definição nos dizem que dado o anel $(A, *, \circ)$, o par $(A, *)$ é grupo abeliano. Nestes termos, o leitor deveria esperar que o elemento neutro e o elemento simétrico de $a \in A$ pela operação $*$ fosse representados respectivamente por e e a' como no capítulo anterior. Esta mudança é necessária pois estamos trabalhando agora com duas operações. Cada uma delas pode possuir elemento neutro e um dado elemento $a \in A$ pode ser simetrizável por qualquer uma destas operações. Precisamos então de notações diferentes para designar estes dois elementos neutros e os simétricos de a por $*$ e por $\circ$.

Definição 3.2. Um anel $(A, *, \circ)$ é dito um *anel comutativo* se a operação $\circ$ for comutativa, isto é, $a \circ b = b \circ a$ para todos $a, b \in A$.

Definição 3.3. Dado um anel $(A, *, \circ)$, A é dito um *anel com unidade* se existir um elemento

em A, indicado por 1_A, tal que $1_A \circ a = a \circ 1_A = a$ para todo $a \in A$. Neste caso, o elemento $1_A \in A$, é o elemento neutro para a operação $\circ$, denominado *unidade* do anel A.

Cuidado para não confundir a unidade de um anel com o número 1. Escrever 1_A não significa que o número 1 está no anel A. 1_A é apenas um símbolo que representa qualquer elemento em A que satisfaz $1_A \circ a = a \circ 1_A = a$ para todo $a \in A$.

Definição 3.4. Seja $(A, *, \circ)$ um anel com unidade 1_A. Dizemos que $a \in A$ é invertível se a admite simétrico para a operação $\circ$, isto é, se existe um elemento $b \in A$ tal que

$$a \circ b = b \circ a = 1_A.$$

Neste caso, o elemento b é comumente denotado por a^{-1} e chamado de *inverso* de a.

Proposição 3.5. *Se $(A, *, \circ)$ é um anel com unidade 1_A e $a \in A$ é um elemento invertível, então o inverso de a é único.*

Prova. Suponha $a \in A$ invertível e sejam $a_1, a_2 \in A$ dois inversos de $a \in A$. Então, da definição de inverso, temos que

$$a \circ a_1 = a_1 \circ a = 1_A, \qquad \text{e} \qquad a \circ a_2 = a_2 \circ a = 1_A.$$

Desta forma,

$$a_1 = a_1 \circ 1_A = a_1 \circ (a \circ a_2) = (a_1 \circ a) \circ a_2 = 1_A \circ a_2 = a_2,$$

como desejado. □

É imediato da definição, se a é invertível, então a própria igualdade $a \circ a^{-1} = a^{-1} \circ a = 1_A$ garante que a^{-1} é também invertível sendo a o seu inverso. Isto é, $(a^{-1})^{-1} = a$. Podemos também verificar que, se a e b são invertíveis, então $a \circ b$ é invertível sendo o seu inverso $(b^{-1} \circ a^{-1})$. Simbolicamente $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$. Deixamos a prova disto como exercício.

Proposição 3.6. *Se um anel $(A, *, \circ)$ possui unidade então esta unidade é única.*

Prova. Suponha que existam duas unidades no anel $(A, *, \circ)$, que representaremos por 1_1 e 1_2. Como 1_1 é unidade então $1_1 \circ 1_2 = 1_2$. Da mesma forma, sendo 1_2 uma unidade de A, temos $1_1 \circ 1_2 = 1_1$. Temos então

$$1_1 = 1_1 \circ 1_2 = 1_2,$$

mostrando que a unidade é única. □

Exemplo 3.1. Os conjuntos $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ com as operações usuais de soma e produto de números são anéis. Todos são comutativos, e todos possuem unidade, sendo a unidade de $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$, o número 1, e a unidade de $\mathbb{C}$ é $(1 + 0i)$. ■

Exemplo 3.2. O conjunto das matrizes quadradas de ordem n com coeficientes reais, $(M_n(\mathbb{R}), +, \cdot)$ com a soma e o produto usuais de matrizes, é um anel. Tem unidade

$$1_{M_n(\mathbb{R})} = I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

que é a matriz identidade de ordem n. Não é comutativo. ■

Exemplo 3.3. Considere o conjunto das funções de $\mathbb{R}$ em $\mathbb{R}$, $\mathcal{F} = \{f : \mathbb{R} \to \mathbb{R}\}$, com a soma e a composição de funções,

$$(f+g)(x) = f(x) + g(x),$$
$$(f \circ g)(x) = f(g(x)).$$

$(\mathcal{F}, +, \circ)$ não é anel, pois pode-se observar que a composição de funções não é distributiva com relação a soma de funções. Para ser mais preciso, vale a distributividade à direita, e não vale a distributividade à esquerda. De fato, dadas f, g e h, em $\mathcal{F}$ temos para todo $x \in \mathbb{R}$,

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

donde $(f+g)\circ h = (f\circ h) + (g\circ h)$. No entanto,

$$(f \circ (g+h))(x) = f((g+h)(x)) = f\left(g(x) + h(x)\right)$$

e em geral, o último membro não pode ser desmembrado em $f(g(x)) + f(h(x)) = (f\circ g)(x) + (f \circ h)(x)$. Não há garantias portanto que $f \circ (g+h) = (f\circ g) + (f\circ h)$. Entretanto, estas operações definem no conjunto das funções lineares $\mathcal{L} = \{f : \mathbb{R} \to \mathbb{R}; \quad f(x) = ax; \quad a \in \mathbb{R}^*\}$ é um anel com estas operações, já que a linearidade dos elementos de f permitem a distributividade à esquerda. ■

Proposição 3.7. *Seja $(A, *, \circ)$ um anel. Então $a \circ 0_A = 0_A \circ a = 0_A$, para todo $a \in A$.*

Prova. Para qualquer $a \in A$, temos

$$a \circ 0_A = a \circ (0_A * 0_A) = a \circ 0_A * a \circ 0_A,$$

e da regularidade do elemento $a \circ 0_A$ temos $0_A = a \circ 0_A$. A igualdade $0_A \circ a = 0_A$, é análoga. □

Como consequência desta última proposição podemos provar que em um anel com unidade que possui pelo menos dois elementos, sempre temos $1_A \neq 0_A$. De fato, procedendo contrapositivamente, se $0_A = 1_A$ então para qualquer $a \in A$, temos $a = a \circ 1_A = a \circ 0_A = 0_A$ e portanto $A = \{0_A\}$. Também é consequência da última proposição que 0_A não é invertível, mesmo que A possua unidade. Isto porque não há elemento $a \in A$ tal que $0_A \circ a = 1_A$. Nestes termos, se a é invertível, devemos obrigatoriamente ter $a \neq 0_A$, e além disso, como a^{-1} é também invertível, $a^{-1} \neq 0_A$ também.

Com o intuito de simplificar a notação $a*(-a)$ vamos definir a operação diferença entre elementos de A.

Definição 3.8. Se $(A, *, \circ)$ é um anel, então para cada $a, b \in A$ definimos a *diferença* entre a e b, como sendo o elemento de A, representado por $a - b$ e determinado por $a - b = a * (-b)$.

Se $(A, *, \circ)$ é um anel, então são válidas as seguintes propriedades em A, decorrentes imediatamente das propriedades de grupos

i) 0_A é único,

ii) para todo $a \in A$, $-a \in A$ é único,

iii) para todo $a \in A$, $-(-a) = a$,

iv) para todo $a \in A$, $a - a = 0_A$,

v) para todos $a_1, a_2, \ldots, a_n \in A$, tem-se $-(a_1 * a_2 * \cdots * a_n) = -a_1 - a_2 - \cdots - a_n$,

vi) todo $a \in A$ é regular para a operação $*$, isto é, se $a * x = a * y$ ou $x * a = y * a$ para quaisquer $x, y \in A$, então $x = y$.

Estas propriedades não necessitam de demonstração pois já foram todas demonstradas no capítulo anterior, quando foram enunciadas para os grupos. Apenas citamos aqui para evidenciar que elas continuam valendo para anéis, sobretudo com a notação $(-a)$ no lugar de (a').

Proposição 3.9. *Para quaisquer a, b e c em um anel $(A, *, \circ)$ tem-se*

i) $-(a \circ b) = a \circ (-b) = (-a) \circ b$,

ii) $(-a) \circ (-b) = a \circ b$,

iii) $a \circ (b - c) = (a \circ b) - (a \circ c)$ *e também* $(b - c) \circ a = (b \circ a) - (c \circ a)$.

Prova. Para o item (i) temos

$$(a \circ b) * (a \circ (-b)) = a \circ (b * (-b)) = a \circ 0_A = 0_A,$$

e também,

$$(a \circ (-b)) * (a \circ b) = a \circ ((-b) * b) = a \circ 0_A = 0_A,$$

e então o elemento $(a \circ (-b))$ é o simétrico de $(a \circ b)$ para a operação $*$, isto é, $(a \circ (-b)) = -(a \circ b)$. Analogamente

$$(a \circ b) * ((-a) \circ b) = (a * (-a)) \circ b = 0_A \circ b = 0_A,$$

e então $((-a) \circ b)$ é o elemento simétrico de $(a \circ b)$, isto é, $((-a) \circ b) = -(a \circ b)$.

Para provar o item (ii), usando o item (i), temos que

$$(-a) \circ (-b) = -(a \circ (-b)) = -(-(a \circ b)) = (a \circ b).$$

Para mostrar (iii) usaremos novamente o item (i). Então

$$\begin{aligned} a \circ (b - c) = a \circ (b * (-c)) &= (a \circ b) * (a \circ (-c)) \\ &= (a \circ b) * (-(a \circ c)) = (a \circ b) - (a \circ c). \end{aligned}$$

Também,

$$\begin{aligned} (b - c) \circ a = (b * (-c)) \circ a &= (b \circ a) * ((-c) \circ a) \\ &= (b \circ a) * (-(c \circ a)) = (b \circ a) - (c \circ a), \end{aligned}$$

e isto encerra a demonstração. □

No capítulo anterior usamos a notação a^n para designar um elemento a (de um grupo) operado consigo mesmo n vezes. Como agora temos duas operações envolvidas, precisamos de duas notações diferentes que designarão um elemento a operado consigo mesmo pela operação $*$ e pela operação $\circ$. Iremos manter a notação a^n para a operação $\circ$.

Definição 3.10. Dados um anel $(A, *, \circ)$, e um número inteiro m, definimos o múltiplo inteiro ma, do elemento $a \in A$, como sendo o elemento dado por

$$ma = \begin{cases} 0_A, & \text{se} \quad m = 0, \\ (m-1)a * a, & \text{se} \quad 0 < m, \\ (-m)(-a), & \text{se} \quad m < 0. \end{cases}$$

Definição 3.11. Dado um anel $(A, *, \circ)$, e um número natural não nulo n, definimos a potência natural não nula a^n do elemento $a \in A$, por

$$a^n = \begin{cases} a, & \text{se} \quad n = 1, \\ a^{n-1} \circ a, & \text{se} \quad n > 1. \end{cases}$$

Se o anel possuir unidade 1_A, então definiremos ainda $a^0 = 1_A$ desde que $a \neq 0_A$. Se além disso, a for invertível, então para $n \in \mathbb{Z}$ com $n < 0$, definiremos a potência inteira negativa de a como sendo $a^n = (a^{-1})^{-n}$.

A definição de múltiplo envolve apenas a operação $*$, que torna o conjunto A um grupo comutativo. Por este motivo, as propriedades envolvendo esta definição são as mesmas da Proposição (2.27). Adequando a notação estabelecida agora, temos que para todo elemento a do anel A e para quaisquer $m, n \in \mathbb{Z}$ tem-se:

i) $1a = a$,
ii) $ma * mb = m(a * b)$,
iii) $ma * na = (m + n)a$,
iv) $n(ma) = (mn)a$,

que não necessitam de demonstração (pois já foram mostradas). As propriedades envolvendo a segunda operação do anel A necessitam de demonstração.

Proposição 3.12. *Se $(A, *, \circ)$ é um anel e $a, b \in A$ são dois elementos quaisquer, então*

$$m(a \circ b) = (ma) \circ b = a \circ (mb),$$

para todo $m \in \mathbb{Z}$.

Prova. Suponha inicialmente $m \in \mathbb{N}^*$ e provaremos que $m(a \circ b) = (ma) \circ b$ usando indução sobre m. Para $m = 1$,

$$1(a \circ b) = a \circ b = (1a) \circ b.$$

Suponhamos agora (por indução) que a igualdade seja válida para $m = k$. Então,

$$\begin{aligned} (k+1)(a \circ b) &= k(a \circ b) * (a \circ b) \\ &= ((ka) \circ b) * (a \circ b) \\ &= (ka * a) \circ b = ((k+1)a) \circ b, \end{aligned}$$

mostrando a validade da igualdade para todo $m > 0$. Para $m = 0$ trivialmente

$$0(a \circ b) = 0_A = 0_A \circ b = (0a) \circ b.$$

Finalmente, para $m < 0$, então

$$m(a \circ b) = (-m)(-(a \circ b)) = (-m)((-a) \circ b) = ((-m)(-a)) \circ b = (ma) \circ b.$$

Segue que $m(a \circ b) = (ma) \circ b$ para todo $m \in \mathbb{Z}$. A igualdade $m(a \circ b) = a \circ (mb)$ é provada de maneira análoga. □

Proposição 3.13. *Para todo elemento a de um anel $(A, *, \circ)$, tem-se*

i) $a^n = a^{n-1} \circ a = a \circ a^{n-1}$,

ii) $a^m \circ a^n = a^{m+n}$,

iii) $(a^m)^n = a^{mn}$,

para quaisquer $m, n \in \mathbb{N}^*$.

Prova. Nos dois casos usaremos indução sobre n para qualquer $m \in \mathbb{N}^*$. Para o item (i), suponha $n = 1$, então temos diretamente da definição que

$$a^{m+1} = a^{(m+1)-1} \circ a = a^m \circ a = a^m \circ a^1.$$

Suponha agora, o resultado válido para k. Então,

$$\begin{aligned} a^m \circ a^{k+1} &= a^m \circ (a^k \circ a) \\ &= (a^m \circ a^k) \circ a \\ &= a^{m+k} \circ a = a^{(m+k)+1} = a^{m+(k+1)}, \end{aligned}$$

e assim o resultado vale para todo $n \in \mathbb{N}^*$. Para o item (ii), se $n = 1$, então o resultado é trivialmente satisfeito, pois

$$(a^m)^1 = a^m = a^{m \circ 1}.$$

Supondo (por indução) que o resultado seja válido para $n = k$, temos então que,

$$(a^m)^{k+1} = (a^m)^k \circ a^m = a^{mk} \circ a^m = a^{mk+m} = a^{m(k+1)},$$

mostrando o resultado para todo $n \in \mathbb{N}^*$. □

No caso em que $(A, *, \circ)$ é um anel com unidade, podemos definir a potência a^0, colocando $a^0 = 1_A$ para qualquer $a \in A$ com $a \neq 0_A$. Definido desta forma a proposição anterior fica válida para $m, n \in \mathbb{N}$. A exigência de que $a \neq 0_A$ ficará clara no futuro quando definirmos potência negativa.

Ainda não definimos a potência negativa de um elemento porque potências negativas, em geral, são definidas sobre os simétricos dos elementos. Então para definirmos adequadamente potências negativas, precisamos que os elementos do anel sejam simetrizáveis para a operação $\circ$. Para o momento não temos esta garantia, e portanto, definiremos as potências negativas

mais tarde quando tivermos a garantia de que todos os elementos (não nulos) do anel forem simetrizáveis em relação à operação $\circ$.

Dado um anel A estamos agora interessados em determinar subconjuntos $S \subset A$ não vazios de forma que S sejam eles próprios anéis.

Definição 3.14. Seja $(A, *, \circ)$ um anel. Um subconjunto não vazio $S \subset A$ é um subanel de A, se S é fechado para as operações $*$ e $\circ$, isto é, para quaisquer $a, b \in S$, temos $(a * b) \in S$ e $(a \circ b) \in S$, e além disso, $(S, *, \circ)$ também é anel.

Sabemos que em um subanel (subgrupo), o elemento neutro é o mesmo elemento neutro do anel (grupo). Este fato não acontece necessariamente para a unidade. É possível encontrar anéis com unidade de forma que os subanéis tenham unidade diferente da unidade do anel.

Definição 3.15. Sejam A um anel com unidade 1_A, e S um subanel de A com unidade 1_S. Dizemos que S é subanel *unitário* de A, se $1_A = 1_S$.

Exemplo 3.4. Consideremos o anel $A = (\mathbb{Z}_4 \times \mathbb{Z}_4, \oplus, \odot)$, onde $\oplus$ e $\odot$ são as operações de soma e produto induzidas pelo produto cartesiano. É claro que este anel possui elemento unidade $1_A = (\overline{1}, \overline{1})$. Consideremos $S = (\mathbb{Z}_4 \times \{\overline{0}\}, \oplus, \odot)$, que claramente é um subanel de A. S também tem unidade $1_S = (\overline{1}, \overline{0}) \neq (\overline{1}, \overline{1}) = 1_A$, e assim S não é subanel unitário de A. ■

Exemplo 3.5. Considere o anel $A = (\mathbb{Z}_{20}, +, \cdot)$ e o subanel $S = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}\}$. É fácil ver que $1_A = \overline{1}$ é a unidade de $\mathbb{Z}_{20}$, e no entanto,

$$\begin{aligned}
\overline{5} \cdot \overline{0} &= \overline{5 \cdot 0} = \overline{0} \\
\overline{5} \cdot \overline{5} &= \overline{5 \cdot 5} = \overline{25} = \overline{5} \\
\overline{5} \cdot \overline{10} &= \overline{5 \cdot 10} = \overline{50} = \overline{10} \\
\overline{5} \cdot \overline{15} &= \overline{5 \cdot 15} = \overline{75} = \overline{15},
\end{aligned}$$

o que mostra que a unidade de S é o elemento $\overline{5}$. Assim, $1_S = \overline{5} \neq \overline{1} = 1_A$. ■

Proposição 3.16. *Sejam $(A, *, \circ)$ um anel e $S \neq \emptyset$ um subconjunto de A. A fim de que S seja subanel de A é necessário e suficiente que*

$$(a - b) \in S \quad e \quad (a \circ b) \in S, \quad \textit{para todos} \quad a, b \in S,$$

isto é, S é fechado para as operações $-$ e $\circ$.

Prova. Se S é subanel de A, então S é um anel também, e desta forma, para quaisquer $a, b \in S$, tem-se $(-b) \in S$ e do fechamento de $*$ e $\circ$ em S, segue que

$$(a * (-b)) = (a - b) \in S \quad \text{e} \quad (a \circ b) \in S.$$

Suponha agora que para quaisquer $a, b \in S$, tem-se $(a - b), (a \circ b) \in S$. Da proposição (2.7), o conjunto $(S, *)$ é subgrupo do grupo $(A, *)$, e como a operação $*$ é comutativa em A, será também em S. Como $\circ$ é associativa e distributiva em relação a $*$ em A, será também em S, e desta forma, S é também um anel, e portanto S é subanel de A. □

3.2 Anéis de integridade

Vimos na proposição 3.7 que em um anel $(A, *, \circ)$ quando $a = 0_A$ ou $b = 0_A$, então temos também $a \circ b = 0_A$. O recíproco é que em geral é falso. Em outras palavras, existem anéis em que $a \circ b = 0_A$ mesmo para $a \neq 0_A$ e $b \neq 0_A$.

Definição 3.17. Um anel $(A, *, \circ)$, comutativo com unidade é dito um *anel de integridade* ou um *domínio de integridade* se, e somente se dados quaisquer $a, b \in A$ com $a \circ b = 0_A$, tem-se $a = 0_A$ ou $b = 0_A$.

Isto significa que no anel A não há divisores próprios de zero. Equivalentemente, poderíamos usar a contrapositiva da implicação acima e dizer que um anel $(A, *, \circ)$ é um anel de integridade se para quaisquer $a \neq 0_A$ e $b \neq 0_A$ tem-se que $a \circ b \neq 0_A$, e portanto para que $(A, *, \circ)$ não seja anel de integridade, basta encontrar $a \neq 0_A$ e $b \neq 0_A$ de forma que $a \circ b = 0_A$.

Exemplo 3.6. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, *, \cdot)$, com as operações usuais de soma e produto de números, são anéis de integridade. ■

Exemplo 3.7. O conjunto das matrizes diagonais, quadradas de ordem 2,

$$M = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}; \quad a, b \in \mathbb{R} \right\},$$

com as operações de soma e produto de matrizes usuais, é um anel comutativo com unidade. Entretanto, não é anel de integridade. De fato, considerando

$$A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{e} \qquad B = \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix},$$

temos claramente $A \neq 0_M$ e $B \neq 0_M$ e no entanto

$$A \cdot B = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_M.$$

■

Exemplo 3.8. O conjunto $(\mathbb{Z}_6, +, \cdot)$ com as operações de soma e produto usual nas classes de equivalência módulo 6 é um anel comutativo e com unidade. Não é domínio de integridade pois escolhendo $a = \overline{2} \neq \overline{0}$ e $b = \overline{3} \neq \overline{0}$ temos $a \cdot b = \overline{2} \cdot \overline{3} = \overline{2 \cdot 3} = \overline{6} = \overline{0}$. ■

Exemplo 3.9. O conjunto $(\mathbb{Z}_p, +, \cdot)$, p um número primo, com as operações de soma e produto de classes equivalência módulo p é um anel comutativo e com unidade. Mostraremos que é um domínio (anel) de integridade. Sejam $\overline{a}, \overline{b} \in \mathbb{Z}_p$ tais que $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{0}$. Para mostrar que pelo menos um dos elementos $\overline{a}$ ou $\overline{b}$ é igual a $\overline{0}$, vamos supor que um deles não é $\overline{0}$, e provar que neste caso obrigatoriamente o outro será. Suponha então que $\overline{a} \neq \overline{0}$. Como $\overline{ab} = \overline{a} \cdot \overline{b} = \overline{0}$ então temos que ab está relacionado com 0, ou ainda, $(ab - 0) = ab$ é múltiplo de p. Equivalentemente $p|ab$. Agora como $\overline{a} \neq \overline{0}$, então a não é múltiplo de p. Desta forma $\text{mdc}(a, p) = 1$. Como $a|ab$, e $\text{mdc}(a, p) = 1$, então segue do lema 1.10 que $ap|ab$. Agora do item (iv) da proposição 1.3, temos que $p|b$. Equivalentemente, b é múltiplo de p. Desta forma, $b - 0$ é múltiplo de p, donde b está relacionado com 0, e portanto $\overline{b} = \overline{0}$. ■

Proposição 3.18. *Seja $(A, *, \circ)$ um anel comutativo com unidade. A é um anel de integridade se e somente se, todo elemento não nulo de A é regular para a operação $\circ$.*

Prova. Suponhamos que A seja anel de integridade, e $a, b, c \in A$, tais que $a \circ b = a \circ c$, com $a \neq 0_A$. Então,

$$a \circ (b - c) = a \circ b - a \circ c = 0_A.$$

Como A é anel de integridade, então, ou $a = 0_A$ ou $(b - c) = 0_A$, e como por hipótese, $a \neq 0_A$ temos que $b - c = 0_A$, o que implica em $b = c$.

Reciprocamente, suponha que todo elemento não nulo de A é regular para a operação $\circ$. Sejam $a, b \in A$, satisfazendo $a \circ b = 0_A$, e ainda $a \neq 0_A$. Então

$$a \circ b = 0_A = a \circ 0_A,$$

e pela hipótese de regularidade de a, segue que $b = 0_A$, o que mostra que A é anel de integridade. □

3.3 Homomorfismos e isomorfismos

Consideremos dois anéis A e B. Estamos interessados nas aplicações de A em B que preservam as leis de composição entre esses dois anéis.

Definição 3.19. Sejam $(A, *, \circ)$ e $(B, +, \cdot)$ dois anéis, e $\varphi : A \to B$ uma aplicação. Dizemos que φ é um *homomorfismo* entre os anéis A e B, se

$$\varphi(a * b) = \varphi(a) + \varphi(b) \qquad \text{e} \qquad \varphi(a \circ b) = \varphi(a) \cdot \varphi(b),$$

para quaisquer $a, b \in A$.

O núcleo de um homomorfismo de anéis, ainda será denotado por $Ker(\varphi)$ e ainda é o conjunto dos elementos de A que são levados no elemento neutro do anel B. Continuaremos portanto escrevendo $Ker(\varphi) = \{a \in A;\ \varphi(a) = 0_B\}$.

Definição 3.20. Uma aplicação φ entre os anéis A e B é dita um *isomorfismo* se φ for homomorfismo e for uma aplicação bijetora. Neste caso dizemos que A e B são anéis isomorfos (ou simplesmente isomorfos) e escrevemos $A \approx B$.

Se A e B forem anéis e $\varphi : A \to B$ um homomorfismo, então se φ for sobrejetor dizemos que φ é um *epimorfismo*. Se φ for injetor, φ é dito um *monomorfismo*. Se A e B forem o mesmo anel, então φ é chamado de *endomorfismo*.

Exemplo 3.10. Considerando $\mathbb{C}$ e $\mathbb{R}$ com as operações usuais de soma e produto, a aplicação $\varphi : \mathbb{C} \to \mathbb{R}$ dada por $\varphi(z) = |z|$ não é homomorfismo. Embora $\varphi(z \cdot w) = |z \cdot w| = |z| \cdot |w| = \varphi(z) \cdot \varphi(w)$, para quaisquer complexos z e w, temos $\varphi(z+w) = |z+w| \leq |z| + |w| = \varphi(z) + \varphi(w)$. Note que algumas vezes a igualdade se verifica, mas não sempre. ■

Exemplo 3.11. Seja $\mathbb{C}$ com as operações usuais de soma e produto de números complexos. A aplicação $\varphi : \mathbb{C} \to \mathbb{C}$ dada por $\varphi(z) = \overline{z}$, que a cada complexo z associa o seu conjugado, é

homomorfismo. De fato, para quaisquer complexos z e w, temos $\varphi(z+w) = \overline{z+w} = \overline{z} + \overline{w} = \varphi(z) + \varphi(w)$, e também, $\varphi(z \cdot w) = \overline{z \cdot w} = \overline{z} \cdot \overline{w} = \varphi(z) \cdot \varphi(w)$. É também claro que neste caso, $Ker(\varphi) = \{0_{\mathbb{C}} = 0 + 0i\}$. ■

Exemplo 3.12. Dados dois anéis $(A, *, \circ)$ e $(B, +, \cdot)$ quaisquer e a aplicação $\eta : A \to B$ dada por $\eta(a) = 0_B$ para todo $a \in A$, é claramente um homomorfismo. De fato, para quaisquer $a, b \in A$, temos $\eta(a * b) = 0_B = 0_B + 0_B = \eta(a) + \eta(b)$, e também, $\eta(a \circ b) = 0_B = 0_B \cdot 0_B = \eta(a) \cdot \eta(b)$. Neste caso, η é chamado de homomorfismo nulo, ou homomorfismo trivial. Além disso, temos $Ker(\eta) = A$. ■

Algumas propriedades dos homomorfismos de grupos continuam valendo para anéis, principalmente porque em um anel $(A, *, \circ)$, o par $(A, *)$ ainda é um grupo. Desta forma, as propriedades que continuam valendo, são as propriedades a respeito da operação $*$. A próxima proposição irá apenas reunir estas propriedades, uma vez que já demonstramos todas elas na seção (2.2).

Proposição 3.21. *Dados dois anéis $(A, *, \circ)$ e $(B, +, \cdot)$, e $\varphi : A \to B$ um homomorfismo entre A e B, então*

i) $\varphi(0_A) = 0_B$,
ii) $\varphi(-a) = -\varphi(a)$ *para qualquer* $a \in A$,
iii) $\varphi(a - b) = \varphi(a) - \varphi(b)$ *para todos* $a, b \in A$,
iv) φ *é injetor, se e somente se,* $Ker(\varphi) = \{0_A\}$.

Os resultados que serão enunciados a seguir, envolvem a segunda operação do anel, e portanto necessitam de demonstração.

Proposição 3.22. *Seja $\varphi : A \to B$ um homomorfismo sobrejetor entre os anéis $(A, *, \circ)$ e $(B, +, \cdot)$. Então,*

i) Se A tem unidade, então B também tem unidade, e mais ainda, $1_B = \varphi(1_A)$.

ii) Se A possui unidade e $a \in A$ é invertível, então $\varphi(a) \in B$ também será invertível, e mais ainda, $(\varphi(a))^{-1} = \varphi(a^{-1})$.

iii) Se A é comutativo, então B também será comutativo.

Prova. Suponha 1_A a unidade do anel A. Dado $y \in B$ arbitrário, como φ é sobrejetor, existe $x \in A$ tal que $\varphi(x) = y$. Desta forma

$$\varphi(1_A) \cdot y = \varphi(1_A) \cdot \varphi(x) = \varphi(1_A \circ x) = \varphi(x) = y,$$

e

$$y \cdot \varphi(1_A) = \varphi(x) \cdot \varphi(1_A) = \varphi(x \circ 1_A) = \varphi(x) = y.$$

Logo, B possui unidade, e a unidade de B é o elemento $\varphi(1_A)$, isto é, $1_B = \varphi(1_A)$.

Suponha agora A com unidade 1_A, e $a \in A$ invertível. Então existe $a^{-1} \in A$ tal que $(a \circ a^{-1}) = 1_A$. Do item anterior B também tem unidade $1_B = \varphi(1_A)$ e assim,

$$\varphi(a^{-1}) \cdot \varphi(a) = \varphi(a^{-1} \circ a) = \varphi(1_A) = 1_B,$$

e

$$\varphi(a) \cdot \varphi(a^{-1}) = \varphi(a \circ a^{-1}) = \varphi(1_A) = 1_B,$$

e da definição de elemento invertível, o elemento $\varphi(a) \in B$ possui inverso e o seu inverso é precisamente o elemento $\varphi(a^{-1})$, isto é, $(\varphi(a))^{-1} = \varphi(a^{-1})$.

Considere $x, y \in B$ arbitrários. Como φ é sobrejetivo, existem $a, b \in A$ tais que $x = \varphi(a)$ e $y = \varphi(b)$. Desta forma,

$$x \cdot y = \varphi(a) \cdot \varphi(b) = \varphi(a \circ b) = \varphi(b \circ a) = \varphi(b) \cdot \varphi(a) = y \cdot x,$$

mostrando a comutatividade de $\cdot$ em B. □

O item (i) desta última proposição pode ser garantido em anéis de integridade, mesmo que o homomorfismo não seja sobrejetor. Mais precisamente, podemos garantir que $\varphi(1_A) = 1_B$, se A e B forem anéis de integridade, desde que o homomorfismo não seja o homomorfismo nulo.

Proposição 3.23. *Sejam $(A, *, \circ)$ e $(B, +, \cdot)$ dois anéis com unidade, sendo B um anel de integridade, e $\varphi : A \to B$ um homomorfismo. Então $\varphi(1_A) = 1_B$ ou φ é o homomorfismo nulo.*

Prova. Como $1_A \circ 1_A = 1_A$, então $\varphi(1_A \circ 1_A) = \varphi(1_A)$, e disto temos

$$\begin{aligned}\varphi(1_A) \cdot (\varphi(1_A) - 1_B) &= (\varphi(1_A) \cdot \varphi(1_A)) - \varphi(1_A) \\ &= \varphi(1_A \circ 1_A) - \varphi(1_A) = \varphi(1_A) - \varphi(1_A) = 0_B.\end{aligned}$$

Como B é anel de integridade, segue que $\varphi(1_A) = 0_B$ ou $(\varphi(1_A) - 1_B) = 0_B$. Se $(\varphi(1_A) - 1_B) = 0_B$ então temos $\varphi(1_A) = 1_B$. Mas se $\varphi(1_A) = 0_B$, então para cada $x \in A$ teremos

$$\varphi(x) = \varphi(x \circ 1_A) = \varphi(x) \cdot \varphi(1_A) = \varphi(x) \cdot 0_B = 0_B,$$

o que mostra que φ é o homomorfismo nulo. Isto posto, ou $\varphi(1_A) = 1_B$, ou φ é o homomorfismo nulo. □

Proposição 3.24. *Sejam $(A, *, \circ)$ e $(B, +, \cdot)$ dois anéis e φ um homomorfismo de A em B. Então,*

i) Se S é subanel de A, $\varphi(S)$ é subanel de B.

ii) Se S é subanel de B, $\varphi^{-1}(S)$ é subanel de A.

Prova. Suponha primeiramente S subanel de A. Para mostrar que $\varphi(S)$ é subanel, sejam $x, y \in \varphi(S)$, então existem $a, b \in S$, tais que $\varphi(a) = x$ e $\varphi(b) = y$. Assim,

$$x - y = \varphi(a) - \varphi(b) = \varphi(a - b), \qquad \text{e} \qquad x \cdot y = \varphi(a) \cdot \varphi(b) = \varphi(a \circ b),$$

Como S é subanel, então $(a - b) \in S$ e $(a \circ b) \in S$, então $\varphi(a - b) \in \varphi(S)$ e $\varphi(a \circ b) \in \varphi(S)$, e assim, $(x - y) \in \varphi(S)$ e $(x \cdot y) \in \varphi(S)$, mostrando que $\varphi(S)$ é subanel de B.

Para a segunda parte, suponha S subanel de B. Para mostrar que $\varphi^{-1}(S)$ é subanel, sejam $x, y \in \varphi^{-1}(S)$ e então, $\varphi(x) \in S$ e $\varphi(y) \in S$. Como S é subanel, temos que $\varphi(x) - \varphi(y) = \varphi(x - y) \in S$ e também $\varphi(x) \cdot \varphi(y) = \varphi(x \circ y) \in S$. Desta forma $(x - y), (x \circ y) \in \varphi^{-1}(S)$, mostrando que $\varphi^{-1}(S)$ é subanel de A. □

3.4 Ideais e anéis quociente

Definição 3.25. Seja $(A, *, \circ)$ um anel. Dizemos que um subconjunto não vazio $I \subset A$ é um ideal em A, se (e somente se)

$i)$ $(x - y) \in I$, para todos $x, y \in I$,

$ii)$ $x \circ a \in I$ e $a \circ x \in I$, para quaisquer $x \in I$ e $a \in A$.

Observação: As definições de ideal em um anel costumam ser diferentes entre os autores. Alguns autores exigem que o conjunto I seja um subanel de A e portanto a condição (i) não é necessária, pois já fica cumprida pelo fato de I ser subanel. Também a condição (ii) é em alguns casos separada. Se $x \circ a \in I$ para $x \in I$ e $a \in A$ então I é dito ideal à direita em A. Se $a \circ x \in I$ para $x \in I$ e $a \in A$ então I é dito ideal à esquerda em A. Nestes casos o conjunto I é dito ideal em A, se for ideal à direita e ideal à esquerda em A. Alguns autores exigem na definição que o anel seja comutativo e neste caso as noções de ideal à esquerda, ideal à direita e ideal em A coincidem. Assim, se A é anel comutativo, a condição (ii) fica resumida a $x \circ a \in I$ se $x \in I$ e $a \in A$.

Exemplo 3.13. Consideremos $A = (\mathbb{Z}, +, \cdot)$ com as operações usuais de soma e produto de inteiros, e $m \in \mathbb{N}$ um natural fixado com $m \geq 2$. O conjunto $I = m\mathbb{Z} = \{mk; \quad k \in \mathbb{Z}\}$, formado pelos múltiplos inteiros de m é um ideal de A. De fato, a diferença entre dois múltiplos de m é múltiplo de m, e o produto de um inteiro qualquer com um múltiplo de m é múltiplo de m. De outra forma, se $x, y \in I$ e $a \in \mathbb{Z}$ então $x = mk_1$ e $y = mk_2$ para $k_1, k_2 \in \mathbb{Z}$. Então $(x - y) = mk_1 - mk_2 = m(k_1 - k_2) \in I$ já que $(k_1 - k_2) \in \mathbb{Z}$ e $ax = a(mk_1) = m(ak_1) \in I$ já que $(ak_1) \in \mathbb{Z}$. ■

Exemplo 3.14. Tomemos o anel $A = (\mathbb{Z}_6, +, \cdot)$ o com as operações usuais de soma e produto de classes de equivalência módulo 6 nos inteiros, e o subconjunto $I = \{\overline{0}, \overline{3}\} \subset A$. I é um ideal de A, como pode ser observado nas tábuas

$-$	$\overline{0}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$

■

Exemplo 3.15. Considere o anel das funções $\mathcal{F} = \{f : \mathbb{R} \to \mathbb{R}\}$ dotado das operações de soma e produto usual de funções. O subconjunto $I = \{f : \mathbb{R} \to \mathbb{R}; f(1) = 0\}$ é um ideal de $\mathcal{F}$, pois se $f, g \in I$ e $h \in \mathcal{F}$ então

$$\begin{aligned} (f - g)(1) &= f(1) - g(1) = 0 - 0 = 0, \quad \text{e} \\ (f \cdot h)(1) &= f(1) \cdot h(1) = 0 \cdot h(1) = 0. \end{aligned}$$

■

Exemplo 3.16. No anel $(\mathbb{Q}, +, \cdot)$ dos racionais, com a soma e o produto usuais, considere o conjunto dos inteiros $\mathbb{Z}$ que é claramente um subanel de $\mathbb{Q}$. Entretanto $\mathbb{Z}$ não é ideal de $\mathbb{Q}$, pois

embora a diferença entre inteiros seja inteiro, não é verdade que o produto de um número inteiro por qualquer outro número racional, seja inteiro. ■

Observe que em qualquer anel A, os subconjuntos $\{0_A\}$ e A são ideais em A, chamados ideais triviais do anel A.

Proposição 3.26. *Dado um anel $(A, *, \circ)$ e um ideal I de A, então I é um subanel de A.*

A demonstração desta proposição é imediata, pois as definições de conjunto ideal cumprem as condições de (3.16). Cuidado com a recíproca, nem todo subanel de A é ideal de A. Veja o último exemplo acima.

Vamos verificar agora que é possível construir ideais em um anel comutativo A, a partir de um conjunto selecionado de elementos deste anel. Seja $(A, *, \circ)$ um anel comutativo. Escolhemos um elemento $a \in A$ e consideremos o conjunto

$$[a] = \{a \circ x; \quad \text{para todo} \quad x \in A\}.$$

Afirmamos que o conjunto $[a]$ é um ideal de A. De fato, para quaisquer $m, n \in [a]$ e $k \in A$, temos $m = a \circ x$ e $n = a \circ y$ para algum $x, y \in A$. Desta forma $m - n = (a \circ x) - (a \circ y) = a \circ (x - y)$ que pertence a $[a]$ pois $(x - y) \in A$. Também, dado qualquer $k \in A$, temos que $m \circ k = (a \circ x) \circ k = a \circ (x \circ k)$ que pertence a $[a]$ pois $(x \circ k) \in A$. Observe que sendo A comutativo, $(k \circ m) = (m \circ k) \in [a]$ também.

Segue que $[a]$ é um ideal de A, chamado de ideal gerado por $a \in A$. Observe a exigência de que A seja comutativo. O conjunto $[a]$ é formado por elementos $a \circ x$ com $x \in A$. Para que o conjunto $[a]$ seja ideal, deve também ocorrer que $x \circ a \in [a]$. Isto nem sempre é conseguido e então nesta construção exigimos que o anel seja comutativo para garantir que $x \circ a \in [a]$ também.

De forma geral, escolhendo $a_1, a_2, \ldots, a_n \in A$, o conjunto

$$[a_1, a_2, \ldots, a_n] = \{a_1 \circ x_1 * a_2 \circ x_2 * \cdots * a_n \circ x_n; \quad x_i \in A \text{ para } 1 \leq i \leq n\},$$

é um ideal de A, chamado de ideal gerado pelos elementos $a_1, a_2, \ldots, a_n$.

Definição 3.27. Se um ideal gerado for gerado por apenas um elemento, dizemos que este ideal é um ideal principal de A. Um anel de integridade onde todos os ideais são principais é chamado de anel principal, ou domínio de ideais principais.

Proposição 3.28. *O anel de integridade $(\mathbb{Z}, +, \cdot)$ é um domínio de ideais principais. De outra forma, todo ideal de $\mathbb{Z}$ é ideal principal.*

Prova. Seja I ideal de $\mathbb{Z}$. Se $I = \{0\}$ então não há o que mostrar, pois $I = \{0\} = [0]$. Se $I \neq \{0\}$, então existe um elemento $a \in I$ não nulo, e neste caso, a e $-a$ estão em I, e um deles é positivo. Seja n o menor elemento positivo não nulo de I. Mostraremos então que $I = [n] = \{nz; z \in \mathbb{Z}\} = n\mathbb{Z}$. Seja $b \in I \subset \mathbb{Z}$ um elemento arbitrário. Temos então que existem $q, r \in \mathbb{Z}$ tais que

$$b = qn + r \quad \text{com} \quad 0 \leq r < n.$$

Então, $r = b - qn$, donde $r \in I$ pois $b, qn \in I$. Como n é o menor elemento positivo em I devemos ter $r = 0$, e assim, $b = qn$ ou seja, $b \in [n]$. Isto mostra que $I \subset [n]$. A outra inclusão é imediata, uma vez que $n \in I$ então $kn \in I$, e portanto $[n] \subset I$. □

Definição 3.29. Um ideal I de um anel $(A, *, \circ)$ é dito um ideal maximal se, $I \neq A$ e o único ideal em A que contém I e é diferente de I for o próprio A. Isto é, se J é ideal de A, com $I \subsetneq J \subset A$ então $J = A$.

Nossa última proposição garante que todo ideal de $\mathbb{Z}$ é ideal principal. Isto é, se I é ideal de $\mathbb{Z}$ então obrigatoriamente $I = [n]$ para alguma $n \in \mathbb{Z}$ com $n > 0$. O próximo resultado determina as condições para que os ideais de $\mathbb{Z}$ sejam ideais maximais.

Proposição 3.30. *Seja $I = [p]$ um ideal de $(\mathbb{Z}, +, \cdot)$. Então I é ideal maximal de $\mathbb{Z}$, se e somente se, p é primo.*

Prova. Suponha que $[p]$ é ideal maximal de $\mathbb{Z}$. Para provar que p é primo suponha que $p = ab$. Podemos supor sem perda de generalidade que $a \neq p$ e provaremos que obrigatoriamente $a = 1$. Consideremos o ideal $[a]$. Então temos que

$$[p] = \{pn; \quad n \in \mathbb{Z}\} = \{abn; \quad n \in \mathbb{Z}\} \subset [a].$$

Como também temos que $a \neq p$ então $0 < a < p$ e portanto $a \notin [p]$. Segue que $[p] \subsetneq [a] \subset \mathbb{Z}$, e sendo $[p]$ ideal maximal, segue que $[a] = \mathbb{Z}$. Então $1 \in [a]$ e assim existe $z \in \mathbb{Z}$ de forma que $1 = az$. Esta igualdade só é satisfeita no conjunto dos números inteiros colocando $a = z = 1$, e portanto

$$[a] = [1] = \{1 \cdot n; \quad n \in \mathbb{Z}\} = \mathbb{Z}.$$

Suponha agora que p é primo e provaremos que $[p]$ é ieal maximal. Para isto, seja J um ideal de $\mathbb{Z}$ de forma que $[p] \subsetneq J \subset \mathbb{Z}$. Então $J = [n]$ para algum $n \in \mathbb{Z}$ com $n > 0$. Como $p \in [p]$ então $p \in J = [n]$ e portanto $p = na$ para algum $a \in \mathbb{Z}$. Mas como p é primo, então $n = 1$ ou $n = p$. Claramente não pode ocorrer que $n = p$ pois caso contrário teríamos $[p] = [n] = J$ contrariando a hipótese. Resta que $n = 1$ e desta forma

$$J = [n] = [1] = \{1 \cdot n; \quad n \in \mathbb{Z}\} = \mathbb{Z},$$

provando que $[p]$ é maximal. □

Definição 3.31. Seja I um ideal de um anel $(A, *, \circ)$. Dizemos que I é ideal primo se, $I \neq A$ e,

$$a \circ b \in I \quad \Rightarrow \quad a \in I \quad \text{ou} \quad b \in I.$$

Proposição 3.32. *Seja $(A, *, \circ)$ um anel comutativo com unidade. Todo ideal maximal em A é um ideal primo.*

Prova. Seja I ideal maximal em A. Suponha $(a \circ b) \in I$ e $a \notin I$. Mostraremos que $b \in I$.

Consideremos o ideal $[a] * I = \{(x \circ a) * i; \quad x \in A, i \in I\}$. Temos que $I = 0_A * I = (0_A \circ a) * I \subset [a] * I$. Mas como $a = (1_A \circ a) * 0_A \in [a] * I$ e $a \notin I$ então $I \subsetneq [a] * I$. Sendo I maximal, tem-se $[a] * I = A$, então todo elemento de A é também escrito na forma

$$(x \circ a) * i \quad \text{com} \quad x \in A \quad \text{e} \quad i \in I,$$

em particular $1_A = (x \circ a) * i$, com $x \in A$ e $i \in I$, e então

$$b = 1_A \circ b = ((x \circ a) * i) \circ b = (x \circ (a \circ b)) * (i \circ b),$$

e como $(a \circ b) \in I$, segue que $(x \circ (a \circ b)) \in I$ e também $i \in I$ segue que $(i \circ b) \in I$ e do fechamento em I, segue que $b \in I$, provando que I é ideal primo. □

Vamos agora introduzir o conceito de anel quociente. Consideremos um anel $(A, *, \circ)$, e um ideal I de A. Definimos sobre A a relação $\sim$ dada por

$$x \sim y \quad \Leftrightarrow \quad (x - y) \in I.$$

Vejamos as propriedades desta relação. Primeiramente, sendo I ideal de A, então $0_A \in I$ e assim, $(x - x) \in I$ para qualquer $x \in A$, e isto mostra a reflexividade da relação $\sim$. Sejam agora $x, y \in A$ tais que $x \sim y$. Sendo assim, $(x - y) \in I$ e como I é subanel, $-(x - y) \in I$, ou ainda, $(y - x) \in I$, e então $y \sim x$ mostrando a simetria de $\sim$. Sejam agora $x, y, z \in A$ tais que $x \sim y$ e $y \sim z$. Então $(x - y) \in I$, e também $(y - z) \in I$. Novamente, sendo I subanel, temos $(x - y) * (y - z) \in I$ ou seja, $(x - z) \in I$ mostrando que $x \sim z$ e a transitividade de $\sim$. Do exposto, $\sim$ é uma relação de equivalência, e podemos portanto falar em classes de equivalência definidas pela relação $\sim$.

Dado então um elemento arbitrário $a \in A$, a classe de equivalência de a, será o conjunto de todos os elementos de A que se relacionam com a por $\sim$. Isto é,

$$\overline{a} = \{x \in A; \quad x \sim a\} = \{x \in A; \quad (x - a) \in I\}.$$

Observe que, como já comentamos antes, qualquer uma destas classes de equivalência nunca é vazia, pois para todo $a \in A$, $a \sim a$ e portanto $a \in \overline{a}$.

O conjunto de todas as distintas classes de equivalência determinadas pelos elementos de A, é chamado de conjunto quociente de A pelo ideal I e indicado por $\frac{A}{I}$, ou A/I. Temos então,

$$A/I = \frac{A}{I} = \{\overline{a}; \quad a \in I\}.$$

A próxima proposição nos fornece um meio mais rápido para determinar exatamente quem são os elementos de uma determinada classe $\overline{a}$ para $a \in A$.

Proposição 3.33. *De acordo com a construção acima, para qualquer elemento arbitrário $a \in A$, temos*

$$\overline{a} = a * I = \{a * h; \quad h \in I\}.$$

Prova. Considerando a definição de classe de equivalência de a, e a definição da relação $\sim$, temos que, se $x \in \overline{a}$, então $x \sim a$, e então $(x - a) \in I$. Desta forma $x = a * (x - a) \in a * I$. Isto mostra que $\overline{a} \subset a * I$. Reciprocamente, se $x \in a * I$ então $x = a * h$ para algum $h \in I$. Segue que $(x - a) = h$ e então $(x - a) \in I$, donde $x \sim a$ ou ainda $x \in \overline{a}$. Segue que $a * I \subset \overline{a}$ o que completa esta demonstração. □

Em virtude da igualdade que acabamos de mostrar, $\overline{a} = a * I$, a classe $\overline{a}$ é também chamada de classe de equivalência módulo I. É comum então a representação $x \equiv a (\text{mod } I)$ para indicar que $x \sim a$. Agora, o conjunto quociente de A pelo ideal I pode ser reescrito como

$$A/I = \frac{A}{I} = \{\overline{a}; \quad a \in I\} = \{a * I; \quad a \in A\}.$$

Proposição 3.34. *Dois elementos $(a * I)$ e $(b * I)$ do conjunto quociente $\frac{A}{I}$, são iguais, se e somente se, $(a - b) \in I$.*

Prova. Considerando as propriedades da relação de equivalência e a igualdade mostrada na proposição anterior,

$$(a * I) = (b * I) \quad \Leftrightarrow \quad \overline{a} = \overline{b} \quad \Leftrightarrow \quad a \sim b \quad \Leftrightarrow \quad (a - b) \in I.$$

□

Vamos agora definir no conjunto $\frac{A}{I}$, duas operações (uma adição e uma multiplicação) que definirão neste conjunto uma estrutura de anel. Definimos então em $\frac{A}{I}$ as operações $*$ e $\circ$, dadas por

$$(a * I) * (b * I) = (a * b) * I,$$
$$(a * I) \circ (b * I) = (a \circ b) * I$$

para quaisquer $a * I$ e $b * I$ em $\frac{A}{I}$.

Como estamos operando com classes de equivalência, precisamos saber se as operações estão bem definidas, isto é, se escolhermos dois representantes diferentes de uma mesma classe, os resultados das operações continuam equivalentes.

Sejam então $a * I, x * I, b * I, y * I \in \frac{A}{I}$, tais que $a * I = x * I$ e $b * I = y * I$. Temos então que $(a - x) \in I$ e também $(b - y) \in I$. Assim, como I é subanel, $(a - x) * (b - y) \in I$, ou ainda $(a * b) - (x * y) \in I$ e da igualdade de classes $(a * b) * I = (x * y) * I$, donde $(a * I) * (b * I) = (a * b) * I = (x * y) * I = (x * I) * (y * I)$ e a operação $*$ está bem definida em $\frac{A}{I}$.

Também como $(a-x) \in I$ e $(b-y) \in I$. Da condição (ii) de ideal, temos que $(a-x) \circ b \in I$ e também $x \circ (b - y) \in I$. Como I é subanel, temos que $((a - x) \circ b) * (x \circ (b - y)) \in I$ ou ainda $(a \circ b) - (x \circ b) * (x \circ b) - (x \circ y) \in I$. Então temos $(a \circ b) - (x \circ y) \in I$, e da igualdade de classes $(a \circ b) * I = (x \circ y) * I$ donde $(a * I) \circ (b * I) = (a \circ b) * I = (x \circ y) * I = (x * I) \circ (y * I)$ mostrando que a multiplicação de classes também está bem definida em $\frac{A}{I}$.

Proposição 3.35. *O conjunto quociente $\frac{A}{I}$, de um anel $(A, *, \circ)$ por um ideal I, é um anel sob as operações $*$ e $\circ$ definidas como acima.*

Prova. Em primeiro lugar, $\frac{A}{I}$ é não vazio, pois A e I são não vazios. Mostraremos as propriedades da definição de anel para $\frac{A}{I}$.

Sejam $(a * I)$, $(b * I)$ e $(c * I)$ elementos arbitrários de $\frac{A}{I}$. Então

$$\begin{aligned}[(a * I) * (b * I)] * (c * I) &= [(a * b) * I] * (c * I) \\ &= ((a * b) * c) * I = (a * (b * c)) * I \\ &= (a * I) * [(b * c) * I] = (a * I) * [(b * I) * (c * I)],\end{aligned}$$

mostrando que $*$ é associativa. Também,

$$(a * I) * (b * I) = (a * b) * I = (b * a) * I = (b * I) * (a * I),$$

mostrando que $*$ é comutativa.

Procuramos agora $0_{\frac{A}{I}} = x * I \in \frac{A}{I}$ tal que $(x * I) * (a * I) = a * I$ para qualquer $a * I \in \frac{A}{I}$. Um tal elemento $x \in A$ deve então satisfazer $(x * a) * I = a * I$, e da igualdade destas classes,

$x*a-a \in I$, ou ainda $x \in I$. O elemento neutro $0_{\frac{A}{I}} = x*I$ é então uma classe determinada por qualquer elemento $x \in I$. O representante mais simples desta classe é 0_A*I já que $0_A \in I$. Além disso, lembremos que para qualquer $x \in I$, como $0_A \in I$, temos que $x - 0_A \in I$, e da proposição 3.34, $x*I = 0_A*I$. Sendo assim, $0_{\frac{A}{I}} = 0_A*I$. Também podemos denotar simplesmente $0_{\frac{A}{I}} = I$.

Dado $(a*I) \in \frac{A}{I}$ arbitrário, queremos obter um elemento $-(a*I) = (x*I) \in \frac{A}{I}$, dito elemento simétrico de $a*I$ em $\frac{A}{I}$ para a operação $*$. Um tal elemento $(x*I) \in \frac{A}{I}$ deve então satisfazer $(x*I)*(a*I) = 0_A*I$. O elemento $x \in A$ deve então satisfazer $(x*a)*I = 0_A*I$, e da igualdade de classes módulo I, devemos ter $(x*a-0_A) \in I$, isto é, $(x*a) \in I$, ou ainda $(x-(-a)) \in I$, donde $x*I = (-a)*I$. Desta forma, $-(a*I) = x*I = (-a)*I$, isto é, o simétrico da classe $a*I$ em $\frac{A}{I}$ é a classe do simétrico $(-a)$ em A, para qualquer elemento $a*I \in \frac{A}{I}$.

Para quaisquer $(a*I)$, $(b*I)$ e $(c*I)$ em $\frac{A}{I}$, temos

$$\begin{aligned}[(a*I)\circ(b*I)]\circ(c*I) &= [(a\circ b)*I]\circ(c*I)\\ &= ((a\circ b)\circ c)*I = (a\circ(b\circ c))*I\\ &= (a*I)\circ[(b\circ c)*I] = (a*I)\circ[(b*I)\circ(c*I)],\end{aligned}$$

que mostra que $\circ$ é associativa.

Sejam $(a*I)$, $(b*I)$ e $(c*I)$ arbitrários em $\frac{A}{I}$. Então,

$$\begin{aligned}(a*I)\circ[(b*I)*(c*I)] &= (a*I)\circ((b*c)*I)\\ &= ((a\circ(b*c))*I = ((a\circ b)*(a\circ c))*I\\ &= ((a\circ b)*I)*((a\circ c)*I)\\ &= [(a*I)\circ(b*I)]*[(a*I)\circ(c*I)],\end{aligned}$$

e a operação $\circ$ é distributiva pela esquerda em relação à $*$. A distributividade pela direita é análoga. Do exposto, temos que $(\frac{A}{I}, *, \circ)$, é um anel. □

Proposição 3.36. *Se $(A, *, \circ)$ é um anel comutativo, o anel quociente $\frac{A}{I}$, de A por um ideal $I \subset A$, é também comutativo.*

Prova. Se $(a*I), (b*I) \in \frac{A}{I}$, então

$$(a*I)\circ(b*I) = (a\circ b)*I = (b\circ a)*I = (b*I)\circ(a*I),$$

mostrando que $\circ$ é comutativa. □

Proposição 3.37. *Se o anel $(A, *, \circ)$ possuir unidade 1_A, então o anel quociente também possui unidade, e mais ainda, $1_{\frac{A}{I}} = (1_A*I)$.*

Prova. Seja $(a*I) \in \frac{A}{I}$ arbitrário, e consideremos o elemento (1_A*I) que também está no anel quociente. Temos que

$$(a*I)\circ(1_A*I) = (a\circ 1_A)*I = (a*I) = (1_A\circ a)*I = (1_A*I)\circ(a*I).$$

Assim, o elemento (1_A*I) é a unidade do anel $\frac{A}{I}$, isto é, $1_{\frac{A}{I}} = 1_A*I$. □

Proposição 3.38. *Dado um homomorfismo $f : A \to B$ entre os anéis $(A, *, \circ)$ e $(B, +, \cdot)$, então $Ker(f)$ é ideal de A.*

Prova. Primeiramente, já sabemos que $0_A \in Ker(f)$ e portanto $Ker(f) \neq \emptyset$. Sejam $x, y \in Ker(f)$ arbitrários. Então $f(x) = f(y) = 0_B$. Assim,

$$f(x-y) = f(x) - f(y) = 0_B - 0_B = 0_B,$$

mostrando que $(x-y) \in Ker(f)$. Sejam agora $x \in Ker(f)$ e $a \in A$ arbitrários. Então $f(x) = 0_B$. Assim,

$$f(a \circ x) = f(a) \cdot f(x) = f(a) \cdot 0_B = 0_B,$$

e também

$$f(x \circ a) = f(x) \cdot f(a) = 0_B \cdot f(a) = 0_B,$$

mostrando que $(a \circ x) \in Ker(f)$ e também $(x \circ a) \in Ker(f)$. Da definição de ideal, $Ker(f)$ é ideal de A. □

Já que $Ker(f)$ é um ideal de A, podemos então falar no quociente $\frac{A}{Ker(f)}$, e com isto temos um importante resultado.

Teorema 3.39 (Teorema Fundamental do Homomorfismo)**.** *Seja $f : A \to B$ um homomorfismo entre os anéis $(A, *, \circ)$ e $(B, +, \cdot)$. Então $\frac{A}{Ker(f)}$ é isomorfo a $Im(f) \subset B$. Simbolicamente,*

$$\frac{A}{Ker(f)} \approx Im(f).$$

Prova. Para facilitar as notações, chamemos $I = Ker(f)$. Consideremos a aplicação φ dada por

$$\begin{array}{rcl} \varphi : \dfrac{A}{I} & \to & Im(f) \\ (a * I) & \mapsto & \varphi(a * I) = f(a). \end{array}$$

Em primeiro lugar, precisamos mostrar que φ está bem definida. Sejam então $(a * I) = (b * I)$, representantes da mesma classe. Da igualdade das classes, temos $(a - b) \in I = Ker(f)$ e então $f(a - b) = 0_B$. Como $f(a - b) = f(a) - f(b)$, então $f(a) - f(b) = 0_B$ ou ainda $f(a) = f(b)$ o que garante que $\varphi(a * I) = \varphi(b * I)$ e φ está bem definida.

Mostraremos agora que φ é homomorfismo. Dados $(a * I), (b * I) \in \frac{A}{I}$, temos que

$$\varphi((a * I) * (b * I)) = \varphi((a * b) * I) = f(a * b) = f(a) + f(b) = \varphi(a * I) + \varphi(b * I),$$

e também que

$$\varphi((a * I) \circ (b * I)) = \varphi((a \circ b) * I) = f(a \circ b) = f(a) \cdot f(b) = \varphi(a * I) \cdot \varphi(b * I),$$

e portanto φ é um homomorfismo.

Resta mostrar a bijetividade de φ. Sejam $(a*I), (b*I) \in \frac{A}{I}$ tais que $\varphi(a*I) = \varphi(b*I)$, então, $f(a) = f(b)$ ou ainda $f(a - b) = 0_B$, e assim, $(a - b) \in Ker(f) = I$ e da igualdade das classes, $(a*I) = (b*I)$, mostrando a injetividade. Para a sobrejetividade, seja $y \in Im(f)$, então da definição de imagem, existe $x \in A$ tal que $f(x) = y$. Sendo $x \in A$, temos que $(x * I) \in \frac{A}{I}$, e também, $\varphi(x*I) = f(x) = y$, o que mostra a sobrejetividade de φ. Portanto, φ é homomorfismo bijetor, e então um isomorfismo entre $\frac{A}{I}$ e $Im(f)$, resultando que $\frac{A}{I} \approx Im(f)$. □

Corolário 3.40. *Seja $f : A \to B$ um homomorfismo sobrejetor entre os anéis $(A, *, \circ)$ e $(B, +, \cdot)$. Então,*

$$\frac{A}{Ker(f)} \approx B.$$

Corolário 3.41. *Sejam $(\mathbb{Z}, +, \cdot)$ o anel dos inteiros, $m \geq 2$ um número inteiro fixado, e $[m] = \{mk; \quad k \in \mathbb{Z}\} = m\mathbb{Z}$ o ideal gerado por m. Então*

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \approx \mathbb{Z}_m.$$

Prova. Consideremos a aplicação

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Z}_m \\ z &\mapsto \varphi(z) = \overline{z}. \end{aligned}$$

Claramente φ é homomorfismo, pois

$$\varphi(x + y) = \overline{x + y} = \overline{x} + \overline{y} = \varphi(x) + \varphi(y)$$

e

$$\varphi(x \cdot y) = \overline{x \cdot y} = \overline{x} \cdot \overline{y} = \varphi(x) \cdot \varphi(y).$$

Segue do Teorema Fundamental do Homomorfismo que

$$\frac{\mathbb{Z}}{Ker(\varphi)} \approx Im(\varphi).$$

Mas agora, dado qualquer $\overline{z} \in \mathbb{Z}_m$ temos que $z \in \mathbb{Z}$ cumpre $\varphi(z) = \overline{z}$ donde φ é sobrejetora, isto é, $Im(\varphi) = \mathbb{Z}_m$. Também

$$\begin{aligned} Ker(\varphi) &= \{z \in \mathbb{Z}, \quad \varphi(z) = \overline{0}\} \\ &= \{z \in \mathbb{Z}, \quad \overline{z} = \overline{0}\} = \{z \in \mathbb{Z}, \quad z = mk; \, k \in \mathbb{Z}\} = m\mathbb{Z}. \end{aligned}$$

Portanto segue que

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \approx \mathbb{Z}_m.$$

□

3.5 Característica de um anel

Considere $(A, *, \circ)$ um anel. Já sabemos (ver definição 3.10) que $0a = 0_A$ para qualquer $a \in A$. Nosso interesse agora é saber se existem outros números inteiros n, tais que $na = 0_A$ para todo $a \in A$. Consideremos o subconjunto S de $\mathbb{N}^*$ dado por

$$S = \{n \in \mathbb{N}^*; \quad na = 0_A, \quad \text{para todo} \quad a \in A\}.$$

Neste caso, existem duas possibilidades para S.

i) $S = \emptyset$. Neste caso, 0 é o único inteiro que satisfaz $na = 0_A$, e dizemos então que a característica do anel A é 0.

ii) $S \neq \emptyset$. Neste caso, existe um elemento em S que é o mínimo de S. Se k é este mínimo em S, então dizemos que a característica de A é k. Isto motiva a próxima definição.

Definição 3.42. Seja $(A, *, \cdot)$ um anel. O menor número natural k não nulo, tal que,

$$ka = 0_A \qquad \text{para todo} \quad a \in A,$$

é chamado de característica do anel A, e representado por $Car(A)$. Se não existir tal número, então a característica de A é zero.

Observe que, nestes termos, $Car(A) = k$ se e somente se, $ka = 0_A$ para todo $a \in A$ e se $na = 0_A$ para todo $a \in A$ com $0 \leq n < k$ então $n = 0$.

Exemplo 3.17. No anel dos inteiros $(\mathbb{Z}, +, \cdot)$ o único natural k que satisfaz

$$kz = 0, \quad \text{para todos} \quad z \in \mathbb{Z},$$

é $k = 0$. Logo a característica deste anel é zero. ■

Exemplo 3.18. Considere o anel $(\mathbb{Z}_8, +, \cdot)$. Queremos determinar

$$S = \{n \in \mathbb{N}^*; \quad n\overline{a} = \overline{0}, \quad \text{para todo} \quad \overline{a} \in \mathbb{Z}_8\}.$$

Nestes termos, os números n devem satisfazer

$$\overline{0} = n\overline{a} = \underbrace{\overline{a} + \overline{a} + \overline{a} + \cdots + \overline{a}}_{n \text{ vezes}} = \underbrace{\overline{a + a + \cdots + a}}_{n \text{ vezes}} = \overline{na},$$

e então $\overline{na} = \overline{0}$, o que significa que 8 divide na. Como a é arbitrário, não há como garantir que $8|a$ e mais ainda existem $\overline{a} \in \mathbb{Z}_8$ de forma que $\text{mdc}\{a, 8\} = 1$. Então 8 deve dividir n, ou que n deve ser múltiplo de 8. Segue que $S = \{8, 16, 24, 32, 40, \dots\} \subset \mathbb{N}$. O conjunto S é portanto não vazio, e o menor elemento é a característica do anel, isto é, $Car(\mathbb{Z}_8) = \min\{S\} = 8$. ■

É bastante claro para nós que não poderemos ter um anel com característica 1, pois se isto acontecer, devemos ter $A = \{0_A\}$. De fato, se a característica de A for igual a 1, então da definição de característica, devemos ter $1a = 0_A$, para todo $a \in A$. Mas da definição de múltiplo inteiro, $1a = a$ para qualquer $a \in A$, e desta forma, temos que $a = 1a = 0_A$, e portanto $A = \{0_A\}$. Equivalentemente, se $A \neq \{0_A\}$ então $Car(A) \neq 1$.

Proposição 3.43. *Seja $(A, *, \circ)$ um anel com unidade. Se m e n são inteiros quaisquer, então*

$$(mn)1_A = (m1_A) \circ (n1_A).$$

Prova. Usaremos primeiramente indução sobre $n \geq 0$, para qualquer $m \in \mathbb{Z}$. Se $n = 0$, então

$$(m0)1_A = 01_A = 0_A = (m1_A) \circ 0_A = (m1_A) \circ (01_A).$$

Suponha agora (por indução) que o resultado seja válido para $n = k$, isto é,

$$(mk)1_A = (m1_A) \circ (k1_A),$$

então,

$$\begin{aligned}(m(k+1))1_A &= (mk + m)1_A \\ &= ((mk)1_A) * (m1_A)\end{aligned}$$

$$= (m1_A) \circ (k1_A) * (m1_A) \circ 1_A$$
$$= (m1_A) \circ ((k1_A) * 1_A) = (m1_A) \circ ((k+1)1_A)$$

e o resultado vale então para $n = k + 1$ ficando assim provado a validade da igualdade para $n \geq 0$. Consideremos agora $n < 0$. Temos então

$$(mn)1_A = (-(m(-n)))1_A = -((m(-n))1_A)$$
$$= -((m1_A) \circ ((-n)1_A))$$
$$= (m1_A) \circ (-((-n)1_A)) = (m1_A) \circ (n1_A),$$

o que conclui a demonstração para todo $n \in \mathbb{Z}$. □

Proposição 3.44. *Se $(A, *, \circ)$ é um anel com unidade, então a característica de A é igual ao período (ordem) da unidade.*

Prova. Suponhamos que $o(1_A) = k > 0$. Então $k1_A = 0_A$, e se $0 \leq n < k$ satisfaz $n1_A = 0_A$ então $n = 0$. Assim, para qualquer $a \in A$, temos

$$ka = k(1_A \circ a) = (k1_A) \circ a = 0_A \circ a = 0_A.$$

Além disso, se houvesse outro número natural n com $0 \leq n < k$, tal que $na = 0_A$ para todo $a \in A$, então especificamente para $a = 1_A$ deveria acontecer que $n1_A = 0_A$, o que traria $n = 0$. Segue que $Car(A) = k = o(1_A)$.

O caso $o(1_A) = 0$ é trivialmente válido, já que neste caso, sendo $o(1_A) = 0$, não pode haver número positivo k, tal que $k1_A = 0_A$ e portanto não há um número positivo k tal que $ka = 0_A$ para todo $a \in A$. Segue que $Car(A) = 0$. □

Corolário 3.45. *Seja $(A, *, \circ)$ um anel com unidade 1_A. Então $Car(A) = k$ se, e somente se, $k\mathbb{Z}$ é o núcleo do homomorfismo*

$$\begin{aligned} \varphi : \mathbb{Z} &\to A \\ n &\mapsto \varphi(n) = n1_A \end{aligned}$$

Prova. Suponha $Car(A) = k$ então da proposição anterior, k é o período da unidade. Seja agora

$$Ker(\varphi) = \{m \in \mathbb{Z}; \quad \varphi(m) = 0_A\} = \{m \in \mathbb{Z}; \quad m1_A = 0_A\},$$

e vamos provar que $Ker(\varphi) = k\mathbb{Z}$. Seja $m \in Ker(\varphi)$, isto é, $\varphi(m) = 0_A$. Do algoritmo da divisão de Euclides, $m = qk + r$, com $0 \leq r < k$, e como $m1_A = \varphi(m) = 0_A$ temos $(qk + r)1_A = 0_A$ donde $r1_A = 0_A$. Como k é o período da unidade e $0 \leq r < k$ devemos ter $r = 0$, donde $m = qk \in k\mathbb{Z}$. Para a inclusão contrária, seja $m \in k\mathbb{Z}$. Então $m = kq$ para algum $q \in \mathbb{Z}$, e $\varphi(m) = m1_A = (kq)1_A = (k1_A) \circ (q1_A) = 0_A \circ (q1_A) = 0_A$. Segue que $m \in Ker(\varphi)$.

Suponha agora que $k\mathbb{Z} = Ker(\varphi)$, e vamos provar que $o(1_A) = k$. Primeiro, como $k \in k\mathbb{Z}$ então $k \in ker(\varphi)$ e assim, $k1_A = \varphi(k) = 0_A$. Suponha agora que existe $0 \leq r < k$ tal que $r1_A = 0_A$ também. Então, $(k+r)1_A = (k1_A) * (r1_A) = 0_A * 0_A = 0_A$ e assim $\varphi(k+r) = 0_A$. Desta forma $(k+r) \in Ker(\varphi) = k\mathbb{Z}$, donde $(k+r)$ é um múltiplo de k, isto é, $(k+r) = qk$ para algum $q \in \mathbb{Z}$. Então $r = (q-1)k$ é um múltiplo de k, e como $0 \leq r < k$, então $r = 0$, mostrando que k é o menor número inteiro não nulo tal que $k1_A = 0_A$ e sendo assim, k é o período da unidade, e portanto (da proposição anterior) a característica de A. □

Corolário 3.46. *Se $(A, *, \circ)$ é anel de integridade, então a característica de A é zero ou um número primo.*

Prova. Vamos provar a contrapositiva equivalente, isto é, se a característica de A não é nula e não é um número primo, então A não é anel de integridade. Seja então $Car(A) = k > 0$ e k não é primo. Devem existir então números m e n em $\mathbb{N}^*$ tais que $k = mn$ com $0 < m, n < k$. Da proposição anterior, o período da unidade é k, e assim, é o menor natural não nulo tal que $k1_A = 0_A$. Logo, $(m1_A) \neq 0_A$ e também $(n1_A) \neq 0_A$, e no entanto,

$$(m1_A) \circ (n1_A) = (mn)1_A = k1_A = 0_A,$$

donde A não é anel de integridade. □

Consideremos agora um anel com unidade $(A, *, \circ)$ e o subconjunto de $S \subset A$, dado por

$$S = \mathbb{Z}1_A = \{m1_A; \quad m \in \mathbb{Z}\}.$$

Mostraremos primeiramente que este conjunto é um anel. Para tanto, é suficiente mostrar que é um subanel de A. É claro que S é um conjunto não vazio. Também, dados $a, b \in S$, temos que $a = m1_A$ e $b = n1_A$ para algum $m, n \in \mathbb{Z}$. Então

$$a - b = (m1_A) - (n1_A) = (m - n)1_A \in \mathbb{Z}1_A$$
$$a \circ b = (m1_A) \circ (n1_A) = (mn)1_A \in \mathbb{Z}1_A,$$

garantindo que $S = \mathbb{Z}1_A$ é de fato um subanel de A e portanto é um anel. Mais ainda, $S = \mathbb{Z}1_A$ é comutativo (mesmo que A não seja comutativo) e possui unidade $1_S = (1)1_A = 1_A$. De fato, para todos $a = m1_A, b = n1_A \in S$,

$$a \circ b = (m1_A) \circ (n1_A) = (mn)1_A = (nm)1_A = (n1_A) \circ (m1_A) = b \circ a,$$

e também

$$a \circ 1_S = (m1_A) \circ ((1)1_A) = (m1)1_A = m1_A = a.$$

Proposição 3.47. *Seja $(A, *, \circ)$ um anel com unidade e com característica $Car(A) = k$. Então, o subanel $\mathbb{Z}1_A$ é isomorfo a um anel com característica k. Mais precisamente,*

i) $\mathbb{Z}1_A \approx \mathbb{Z}$ se $k = 0$, e

ii) $\mathbb{Z}1_A \approx \mathbb{Z}_k$ se $k > 0$.

Prova. Consideremos primeiramente que $Car(A) = 0$, e a aplicação

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Z}1_A \\ m &\mapsto \varphi(m) = m1_A. \end{aligned}$$

Temos então que para cada $m, n \in \mathbb{Z}$,

$$\varphi(m + n) = (m + n)1_A = (m1_A) * (n1_A) = \varphi(m) * \varphi(n)$$
$$\varphi(mn) = (mn)1_A = (m1_A) \circ (n1_A) = \varphi(m) \circ \varphi(n),$$

mostrando que φ é um homomorfismo. Além disso, seja $y \in \mathbb{Z}1_A$, então $y = m1_A$ para algum $m \in \mathbb{Z}$ e então escolhendo $x = m$ temos $\varphi(x) = \varphi(m) = (m1_A) = y$ mostrando a sobrejetividade de φ. Sejam agora $m, n \in \mathbb{Z}$ com $\varphi(m) = \varphi(n)$. Então

$$(m-n)1_A = (m1_A) - (n1_A) = \varphi(m1_A) - \varphi(n1_A) = 0_A.$$

Mas o período da unidade, que é igual à característica de A, é 0. Portanto o único $(m-n)$ que satisfaz a última igualdade é 0, isto é, $(m-n) = 0$ donde $m = n$, mostrando a injetividade de φ. Segue que φ é um isomorfismo, e $\mathbb{Z} \approx \mathbb{Z}1_A$.

Para a segunda parte, suponha $Car(A) = k > 0$, e a aplicação

$$\begin{aligned} \varphi : \mathbb{Z}_k &\to \mathbb{Z}1_A \\ \overline{m} &\mapsto \varphi(\overline{m}) = m1_A. \end{aligned}$$

Lembremos que $o(1_A) = k$, isto é, k é o menor inteiro positivo tal que $k1_A = 0_A$. Primeiramente, já que estamos trabalhando com classes de equivalência, mostraremos que φ está bem definida. Sejam $\overline{m} = \overline{n}$, então da igualdade de classes de equivalência módulo k, temos $(m-n) = kq$ para algum $q \in \mathbb{Z}$. Assim,

$$(m1_A) - (n1_A) = (m-n)1_A = (qk)1_A = (q1_A) \circ (k1_A) = (q1_A) \circ 0_A = 0_A,$$

e então, $(m1_A) = (n1_A)$ donde $\varphi(\overline{m}) = \varphi(\overline{n})$, o que mostra que φ não depende do representante escolhido para cada classe. Sejam agora $\overline{m}, \overline{n} \in \mathbb{Z}_k$, então,

$$\begin{aligned} \varphi(\overline{m} + \overline{n}) &= \varphi(\overline{m+n}) = (m+n)1_A = (m1_A) * (n1_A) = \varphi(\overline{m}) * \varphi(\overline{n}), \\ \varphi(\overline{m} \cdot \overline{n}) &= \varphi(\overline{mn}) = (mn)1_A = (m1_A) \circ (n1_A) = \varphi(\overline{m}) \circ \varphi(\overline{n}), \end{aligned}$$

mostrando que φ é um homomorfismo. Além disso, se $y \in \mathbb{Z}1_A$, então $y = n1_A$ para algum $n \in \mathbb{Z}$. Tomemos $\varphi(x) = \overline{n}$, e temos

$$\varphi(x) = \varphi(\overline{n}) = (n1_A) = y,$$

provando a sobrejetividade de φ. Sejam agora $\overline{m}, \overline{n} \in \mathbb{Z}_k$ tais que $\varphi(\overline{m}) = \varphi(\overline{n})$. Então $m1_A = n1_A$ ou ainda $(m-n)1_A = 0_A$. Do algoritmo da divisão de Euclides existem $q, r \in \mathbb{Z}$ tais que $(m-n) = qk + r$, com $0 \leq r < k$. Então,

$$0_A = (m-n)1_A = (qk+r)1_A = ((q1_A) \circ (k1_A)) * (r1_A) = ((q1_A) \circ 0_A) * (r1_A) = r1_A.$$

Como k é o menor inteiro positivo tal que $k1_A = 0_A$, resulta então $r = 0$, e então $(m-n) = qk$. Isto garante que $\overline{m} = \overline{n}$ concluindo a injetividade de φ. Assim $\mathbb{Z}_k \approx \mathbb{Z}1_A$. □

3.6 Anéis de polinômios

Definição 3.48. Uma sequência de elementos de um anel $(A, *, \circ)$ é uma aplicação $f : \mathbb{N} \to A$, que a cada $n \in \mathbb{N}$ associa um elemento $a_n \in A$. Indicaremos uma sequência f pelos seus valores funcionais, sob a forma $(a_0, a_1, a_2, \ldots, a_n, \ldots)$, ou mais economicamente, (a_n), sendo que para cada $k \in \mathbb{N}$, $a_k \in A$. Cada um dos elementos $a_k \in A$ é chamado de termo da sequência.

Definição 3.49. Dadas duas sequências $(a_n), (b_n) \in A$, dizemos que a sequência (a_n) é igual à sequência (b_n), e escrevemos $(a_n) = (b_n)$, se (e somente se)

$$a_k = b_k \qquad \text{para todo} \qquad k \in \mathbb{N},$$

isto é, se os termos correspondentes das duas sequências forem iguais.

Vamos agora estabelecer duas operações, uma adição e uma multiplicação, para o conjunto das sequências de um anel A, e verificar que propriedades possuem estas operações.

Definição 3.50. Dadas (a_n) e (b_n) sequências sobre o anel $(A, *, \circ)$, definimos a soma de (a_n) com (b_n), como sendo a sequência denotada por $(c_n) = (a_n) + (b_n)$ e determinada por

$$c_k = a_k * b_k, \qquad \text{para todo} \qquad k \in \mathbb{N}.$$

Desta forma, a soma de (a_n) com (b_n) consiste em "somar" os termos correspondentes de (a_n) e (b_n).

Definição 3.51. Dadas (a_n) e (b_n) duas sequências sobre o anel $(A, *, \circ)$, definimos o produto de (a_n) com (b_n), como sendo a sequência denotada por $(c_n) = (a_n) \cdot (b_n)$ e determinada por

$$c_k = \sum_{j=0}^{k} a_j \circ b_{k-j} = \sum_{i+j=k} a_i \circ b_j, \qquad \text{para todo} \qquad k \in \mathbb{N}.$$

Observe que se $(a_n) \cdot (b_n) = (c_n)$, então

$$\begin{aligned}
c_0 &= (a_0 \circ b_0),\\
c_1 &= (a_0 \circ b_1) * (a_1 \circ b_0),\\
c_2 &= (a_0 \circ b_2) * (a_1 \circ b_1) * (a_2 \circ b_0),\\
c_3 &= (a_0 \circ b_3) * (a_1 \circ b_2) * (a_2 \circ b_1) * (a_3 \circ b_0),\\
&\vdots\\
c_k &= (a_0 \circ b_k) * (a_1 \circ b_{k-1}) * (a_2 \circ b_{k-2}) * \cdots * (a_k \circ b_0).
\end{aligned}$$

Definição 3.52. Sejam $(A, *, \circ)$ um anel, (a_n) uma sequência de A e $w \in A$ um elemento fixo. Definimos o produto de w com (a_n), como sendo a sequência denotada por $(c_n) = w \cdot (a_n)$ e determinada por

$$c_k = w \circ a_k, \qquad \text{para todo} \qquad k \in \mathbb{N}.$$

De outra forma, o produto de (a_n) por w consiste no "produto" de cada termo da sequência de (a_n) por w.

Definição 3.53. Dado o anel $(A, *, \circ)$ a sequência $(a_n) = (a_0, a_1, a_2, \ldots, a_n, \ldots)$ de elementos de A, recebe o nome de polinômio sobre o anel A, ou simplesmente polinômio sobre A, se existe $n_0 \in \mathbb{N}$, tal que,

$$a_n = 0_A \qquad \text{para todo} \qquad n \geq n_0.$$

Isto significa que um polinômio é uma sequência que possui apenas um número finito de termos não nulos.

Exemplo 3.19. A sequência $(1, 2, 3, 4, 0, 0, 0, 0, \dots)$ é uma sequência em $(\mathbb{R}, +, \cdot)$. Como a partir do índice 4, todos os termos são nulos, então este é um polinômio em $\mathbb{R}$. ■

Exemplo 3.20. No anel $(\mathbb{Z}_{10}, +, \cdot)$ com soma e produto usual de classes de equivalência módulo 10, a sequência $(\overline{0}, \overline{3}, \overline{1}, \overline{9}, \overline{7}, \overline{0}, \overline{0}, \dots)$, é um polinômio. A partir do índice 5, todos os elementos da sequência são iguais ao elemento neutro $\overline{0} \in \mathbb{Z}_{10}$. ■

Exemplo 3.21. A sequência $(0_A, 0_A, 0_A, 0_A, \dots)$ é um polinômio em qualquer anel $(A, *, \circ)$. Este polinômio é chamado de polinômio nulo do anel A. ■

Exemplo 3.22. Considerando o anel $\mathcal{M} = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}; \quad a, b \in \mathbb{R} \right\}$, das matrizes diagonais de ordem 2. A sequência

$$\left(\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \dots \right)$$

é um polinômio, pois a partir do índice 3 todos os elementos da sequência são iguais ao elemento neutro do anel, que é a matriz nula. ■

O conjunto de todos os polinômios com coeficientes no anel A, será indicado por $A[X]$. Desta forma um elemento do conjunto $A[X]$ será sempre uma sequência de elementos de A, sendo que a partir de um certo índice finito, todos os elementos desta sequência serão iguais a 0_A, elemento neutro de A.

Observe ainda, que para cada anel A, temos $A \neq \emptyset$ por definição, e então existe pelo memos um elemento em A, na pior das hipóteses $0_A \in A$. Então o polinômio $f = (0_A, 0_A, 0_A, \dots, 0_A, \dots)$ é um polinômio sobre A, o que assegura que $A[X]$ é não vazio para qualquer anel A.

Proposição 3.54. *Seja $(A, *, \circ)$ um anel. O conjunto $A[X]$ é fechado para as operações de adição e multiplicação de polinômios definidas acima.*

Prova. Sejam $(a_n), (b_n) \in A[X]$ e denotemos $(c_n) = (a_n) + (b_n)$ e $(d_n) = (a_n) \cdot (b_n)$. Queremos mostrar que $(c_n), (d_n) \in A[X]$, isto é, existem índices a partir dos quais os coeficientes de (c_n) e de (d_n) são todos nulos. Como $(a_n), (b_n) \in A[X]$, então existem $n_1, n_2 \in \mathbb{N}$, tais que $a_k = 0$ para todo $k > n_1$, e $b_k = 0$ para todo $k > n_2$. Escolhemos $n_0 = \max\{n_1, n_2\}$. Nestes termos temos que $a_k = 0_A$ para todo $k > n_0 \geq n_1$, e também que $b_k = 0_A$ para todo $k > n_0 \geq n_2$. Logo,

$$c_k = a_k * b_k = 0_A, \qquad \text{para todo} \qquad k > n_0.$$

e portanto (c_n) é um polinômio, isto é, $(c_n) = (a_n) + (b_n) \in A[X]$. Para a segunda parte, escolhemos o índice $n_0 = n_1 + n_2$ e temos que para todo $k \in \mathbb{N}^*$,

$$\begin{aligned} d_{n_1+n_2+k} &= \sum_{j=0}^{n_1+n_2+k} a_j \circ b_{n_1+n_2+k-j} \\ &= (a_0 \circ b_{n_1+n_2+k}) * (a_1 \circ b_{n_1+n_2+k-1}) * \cdots * (a_{n_1} \circ b_{n_2+k}) * \end{aligned}$$

$$(a_{n_1+1} \circ b_{n_1+n_2-1}) * \cdots * (a_{n_1+n_2+k} \circ b_0).$$

Como $a_j = 0_A$ para todo $j > n_1$, então

$$d_{n_1+n_2+k} = (a_0 \circ b_{n_1+n_2+k}) * (a_1 \circ b_{n_1+n_2+k-1}) * \cdots * (a_{n_1} \circ b_{n_2+k}) * (0_A \circ b_{n_2+k-1}) * \cdots * (0_A \circ b_0),$$

e como $b_j = 0_A$ para todo $j > n_2$, temos

$$d_{n_1+n_2+k} = (a_0 \circ 0_A) * (a_1 \circ 0_A) * \cdots * (a_{n_1} \circ 0_A) * (0_A \circ b_{n_2+k-1}) * \cdots * (0_A \circ b_0),$$

e assim $b_{n_1+n_2+k} = 0_A$ para todo $k \in \mathbb{N}$, e isto significa que a partir do índice $n_1 + n_2$ todos os elementos de (d_n) são nulos, isto é, $(d_n) = (a_n) \cdot (b_n) \in A[X]$. □

Proposição 3.55. *Se $(A, *, \circ)$ é um anel, então o conjunto $(A[X], +, \cdot)$, com a soma e o produto de polinômios definidos acima, é um anel.*

Prova. Como já mostramos que as operações de soma e produto são fechadas em $A[X]$ então resta mostrar que estas duas operações satisfazem as propriedades da definição de anel. Em toda esta demonstração (a_n), (b_n) e (c_n) são polinômios arbitrários em A.

Associatividade da adição: Denotando $(d_n) = (b_n) + (c_n)$, $(e_n) = (a_n) + (b_n)$, e também $(x_n) = (a_n) + (d_n)$ e $(y_n) = (e_n) + (c_n)$ mostraremos que $(x_n) = (y_n)$. De fato, para todo $k \in \mathbb{N}$,

$$x_k = a_k * d_k = a_k * (b_k * c_k) = (a_k * b_k) * c_k = e_k * c_k = y_k.$$

Comutatividade da adição: Denotando $(x_n) = (a_n) + (b_n)$, $(y_n) = (b_n) + (a_n)$, temos para todo $k \in \mathbb{N}$,

$$x_k = a_k * b_k = b_k * a_k = y_k.$$

Existência do elemento neutro: Queremos encontrar um elemento $e = 0_{A[X]} \in A[X]$ tal que $(a_n) + e = e + (a_n) = (a_n)$ para todo $(a_n) \in A[X]$. Nestes termos $e = (x_n)$ deve satisfazer $(a_n) + (x_n) = (a_n)$, e portanto $a_k * x_k = a_k$ para todo $k \in \mathbb{N}$. Segue que $x_k = 0_A$ para todo $k \in \mathbb{N}$. Desta forma,

$$0_{A[X]} = (x_n) = (0_A) = (0_A, 0_A, 0_A, 0_A, 0_A, \dots),$$

é o elemento neutro para a adição de polinômios. Este elemento é chamado de polinômio nulo de A.

Elementos simetrizáveis: Para $(a_n) \in A[X]$, queremos mostrar a existência de um polinômio $(x_n) \in A[X]$, tal que $(a_n) + (x_n) = 0_{A[X]} = (0_A)$. Nestes termos $a_k * x_k = 0_A$ para todo $k \in \mathbb{N}$. Temos portanto que $x_k = -a_k$ para todo $k \in \mathbb{N}$. Desta forma, o elemento simétrico de (a_n) em $A[X]$ para a operação de adição de polinômios, é

$$-(a_n) = (x_n) = (-a_0, -a_1, -a_2, -a_3, \dots, -a_n, \dots) = (-a_n).$$

Associatividade da multiplicação: Denotemos $(d_n) = (b_n)\cdot(c_n)$, $(e_n) = (a_n)\cdot(b_n)$, e também $(x_n) = (a_n)\cdot(d_n)$ e $(y_n) = (e_n)\cdot(c_n)$. Mostraremos que $(x_n) = (y_n)$. De fato, para todo $k \in \mathbb{N}$,

$$\begin{aligned} x_k &= \sum_{m+n=k} a_m \circ d_n \\ &= \sum_{m+n=k} a_m \circ \left(\sum_{l+j=n} b_l \circ c_j \right) \\ &= \sum_{m+l+j=k} a_m \circ (b_l \circ c_j) = \sum_{m+l+j=k} (a_m \circ b_l) \circ c_j \\ &= \sum_{t+j=k} \left(\sum_{m+l=t} a_m \circ b_l \right) \circ c_j = \sum_{t+j=k} e_t \circ c_j = y_k. \end{aligned}$$

Distributividade da multiplicação em relação à adição: Sejam $(u_n) = (b_n) + (c_n)$, $(v_n) = (a_n)\cdot(b_n)$ e $(w_n) = (a_n)\cdot(c_n)$, e também $(x_n) = (a_n)\cdot(u_n)$ e $(y_n) = (v_n) + (w_n)$. Mostraremos que $(x_n) = (y_n)$. Para todo $k \in \mathbb{N}$, temos que

$$\begin{aligned} x_k &= \sum_{m+n=k} a_m \circ u_n = \sum_{m+n=k} a_m \circ (b_n * c_n) \\ &= \sum_{m+n=k} (a_m \circ b_n) * (a_m \circ c_n) \\ &= \sum_{m+n=k} (a_m \circ b_n) * \sum_{m+n=k} (a_m \circ c_n) = v_k * w_k = y_k \end{aligned}$$

e então está provada a distributividade à esquerda. A distributividade à direita é análoga. Desta forma, o conjunto $A[X]$ é de fato um anel. □

Proposição 3.56. *Seja $(A, *, \circ)$ um anel, e $(A[X], +, \cdot)$ o seu anel de polinômios. Então*

i) Se A for comutativo, $A[X]$ também será comutativo,

ii) Se A possuir unidade 1_A, $A[X]$ também terá unidade, e

iii) Se A for anel de integridade então $A[X]$ também será anel de integridade.

Prova. Primeiramente, mostraremos (i). Sejam (a_n) e (b_n) polinômios em $A[X]$. Se $(x_n) = (a_n)\cdot(b_n)$ e $(y_n) = (b_n)\cdot(a_n)$, temos então que para cada $k \in \mathbb{N}$,

$$x_k = \sum_{m+n=k} a_m \circ b_n = \sum_{n+m=k} b_n \circ a_m = y_k,$$

o que mostra que $(x_n) = (y_n)$ e então $A[X]$ é anel comutativo.

Para mostrar (ii), seja (a_n) um polinômio em $A[X]$. Queremos encontrar um elemento $1_{A[X]} = (x_n)$ tal que $(a_n)\cdot(x_n) = (x_n)\cdot(a_n) = (a_n)$ para qualquer que seja $(a_n) \in A[X]$. Desta forma, os termos x_i devem satisfazer

$$a_k = \sum_{i=0}^{k} a_i \circ x_{k-i}.$$

para todos $k \in \mathbb{N}$. Para $k = 0$ temos

$$a_0 = a_0 \circ x_0,$$

e como a_0 é arbitrário em A, isto obriga $x_0 = 1_A$.

Usaremos indução para provar que $x_k = 0_A$ para $k \geq 1$. Para $k = 1$, temos que

$$a_1 = (a_0 \circ x_1) * (a_1 \circ x_0) = (a_0 \circ x_1) * a_1,$$

donde segue que $0_A = a_0 \circ x_1$ e como a_0 é arbitrário em A, devemos ter que $x_1 = 0_A$. Suponha que $x_i = 0_A$ para todo $1 \leq i < k$. Então, como

$$\begin{aligned} a_k &= \sum_{i=0}^{k} a_i \circ x_{k-i} \\ &= (a_0 \circ x_k) * (a_1 \circ x_{k-1}) * \cdots * (a_{k-1} \circ x_1) * (a_k \circ x_0), \end{aligned}$$

só há dois termos não nulos no segundo membro. Assim,

$$a_k = (a_k \circ x_0) * (a_0 \circ x_k) = a_k * (a_0 \circ x_k),$$

donde segue que $0_A = a_0 \circ x_k$ e sendo a_0 arbitrário em A, então obrigatoriamente $x_k = 0_A$. Assim $1_{A[X]} = (x_n) = (1_A, 0_A, 0_A, 0_A, \dots) \in A[X]$, é a unidade de $A[X]$.

Para (iii), mostraremos que $(a_n) \cdot (b_n) = 0_{A[X]}$ implica $(a_n) = 0_{A[X]}$ ou $(b_n) = 0_{A[X]}$, ou equivalentemente $(a_n) \neq 0_{A[X]}$ e $(b_n) \neq 0_{A[X]}$ implica $(a_n) \cdot (b_n) \neq 0_{A[X]}$. Com efeito, sejam (a_n) e (b_n) não nulos em $A[X]$, então, existem $m, n \in \mathbb{N}$ tais que $a_m \neq 0_A$, e $b_n \neq 0_A$ e também $a_k = 0_A$ para todo $k > m$ e $b_k = 0_A$ para todo $k > n$. Denotando $(c_n) = (a_n) \cdot (b_n)$, calculemos c_{m+n}, obtendo

$$\begin{aligned} c_{m+n} &= \sum_{i=0}^{m+n} a_i \circ b_{m+n-i} \\ &= (a_0 \circ b_{m+n}) * (a_1 \circ b_{m+n-1}) * \cdots * (a_{m-1} \circ b_{n+1}) * (a_m \circ b_n) * (a_{m+1} \circ b_{n-1}) * \cdots * (a_{m+n} \circ b_0) \\ &= \sum_{i=0}^{m-1} a_i \circ b_{m+n-i} * (a_m \circ b_n) * \sum_{i=m+1}^{m+n} a_i \circ b_{m+n-i}, \end{aligned}$$

e como cada $a_{m+i} = b_{n+i} = 0_A$ para qualquer $i > 0$, temos

$$c_{m+n} = a_m \circ b_n,$$

e como ambos a_m e b_n são não nulos, em um anel de integridade o produto será não nulo também, isto é, c_{m+n} é não nulo. Isto prova que $(a_n) \cdot (b_n) \neq 0_{A[X]}$, pois possui pelo menos um termo não nulo. Isto completa esta prova. □

No caso do anel A ter unidade, então podemos fazer uso de uma notação mais comum e útil para os polinômios. Consideramos o polinômio

$$X = (0_A, 1_A, 0_A, 0_A, \dots) \in A[X].$$

Note que

$$\begin{aligned} X^0 &= 1_{A[X]} = (1_A, 0_A, 0_A, 0_A, \dots) \\ X^1 &= X = (0_A, 1_A, 0_A, 0_A, \dots) \\ X^2 &= X \cdot X = (0_A, 0_A, 1_A, 0_A, 0_A, \dots) \end{aligned}$$

$$\begin{aligned} X^3 &= X^2 \cdot X = (0_A, 0_A, 0_A, 1_A, 0_A, 0_A, \dots) \\ &\vdots \\ X^n &= (\underbrace{0_A, \dots, 0_A}_{n \text{ vezes}}, 1_A, 0_A, 0_A, \dots). \end{aligned}$$

Desta forma, dado um polinômio $(a_n) \in A[X]$, podemos escrever

$$\begin{aligned} (a_n) =& (a_0, a_1, a_2, \dots, a_n, 0_A, 0_A, \dots) \\ =& (a_0, 0_A, 0_A, \dots) + (0_A, a_1, 0_A, 0_A, \dots) + \\ &+ (0_A, 0_A, a_2, 0_A, \dots) + \cdots + (0_A, \dots, 0_A, a_n, 0_A, 0_A, \dots) \\ =& a_0 \cdot (1_A, 0_A, 0_A, \dots) + a_1 \cdot (0_A, 1_A, 0_A, 0_A, \dots) \\ &+ a_2 \cdot (0_A, 0_A, 1_A, 0_A, \dots) + \cdots + a_n \cdot (0_A, \dots, 0_A, 1_A, 0_A, 0_A, \dots) \\ =& a_0 + a_1 \cdot X + a_2 \cdot X^2 + a_3 \cdot X^3 + \cdots + a_n \cdot X^n, \end{aligned}$$

que para simplificar ainda mais, omitiremos o símbolo da operação "$\cdot$", e também escreveremos $a(X)$ no lugar de (a_n), ou simplesmente $a \in A[X]$ para designar que $a(X) = (a_n) \in A[X]$. Mas cuidado para não confundir $a \in A$ com $a \in A[X]$. Desta forma,

$$(a_n) = a(X) = (a_0, a_1, a_2, \dots, a_n, 0_A, \dots) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n.$$

Para construir esta notação partimos do pressuposto que A possui unidade. Entretanto, com o intuito de facilitar a escrita, assumiremos que

$$(a_n) = a(X) = (a_0, a_1, a_2, \dots, a_n, 0_A, \dots) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n,$$

mesmo que A não possua unidade.

Observe também que se $a \in A$ e $a(X) \in A[X]$ a notação desenvolvida acima nos permite escrever $a(X) = a$ e esta igualdade só pode ser entendida no sentido que

$$a(X) = a + 0_AX + 0_AX^2 + 0_Ax^3 + \cdots = (a, 0_A, 0_A, 0_A, \dots).$$

Notemos então que, dados $a(X), b(X) \in A[X]$ e $w \in A$, podemos escrever $(a + b), (a \cdot b), (w \cdot a) \in A[X]$, sendo

$$\begin{aligned} (a+b)(X) &= a(X) + b(X) = (a_0 * b_0) + (a_1 * b_1)X + (a_2 * b_2)X^2 + \cdots + (a_n * b_n)X^n, \\ (w \cdot a)(X) &= w \cdot a(X) = (w \circ a_0) + (w \circ a_1)X + (w \circ a_2)X^2 + \cdots + (w \circ a_n)X^n, \\ (a \cdot b)(X) &= a(X) \cdot b(X) = (a_0 \circ b_0) + \left(\sum_{i+j=1} a_i \circ b_j \right) X \\ &\quad + \left(\sum_{i+j=2} a_i \circ b_j \right) X^2 + \cdots + \left(\sum_{i+j=n} a_i \circ b_j \right) X^n. \end{aligned}$$

Vamos agora mostrar a imersão do anel A no seu anel de polinômios $A[X]$. Consideremos o subconjunto S de $A[X]$ dado por

$$S = \{(a, 0_A, 0_A, 0_A, \dots); \quad a \in A\}.$$

É fácil ver que este conjunto S é um subanel de $A[X]$. De fato, se $a(X) = (a, 0_A, \dots), b(X) = (b, 0_A, \dots) \in S$ são elementos arbitrários, temos que

$$(a-b)(X) = a(X) - b(X) = (a-b, 0_A, 0_A, 0_A, \dots),$$
$$(a \cdot b)(X) = a(X) \cdot b(X) = (a \circ b, 0_A, 0_A, 0_A, \dots),$$

e como $(a-b)$ e $(a \circ b)$ ainda pertencem a A, segue que $a(X) - b(X)$ e $a(X) \cdot b(X)$ estão em S.

Proposição 3.57. *O anel $(A, *, \circ)$ é isomorfo ao subanel $S = \{(a, 0_A, 0_A, 0_A, \dots); a \in A\} \subset A[X]$.*

Prova. Consideremos a aplicação

$$\begin{array}{rcl} \varphi : A & \to & S \\ a & \mapsto & \varphi(a) = (a, 0_A, 0_A, 0_A, 0_A, \dots) \end{array}$$

que satisfaz

$$\begin{aligned} \varphi(a * b) &= (a * b, 0_A, 0_A, 0_A, \dots) \\ &= (a, 0_A, 0_A, 0_A, \dots) + (b, 0_A, 0_A, 0_A, \dots) = \varphi(a) + \varphi(b), \\ \varphi(a \circ b) &= (a \circ b, 0_A, 0_A, 0_A, \dots) \\ &= (a, 0_A, 0_A, 0_A, \dots) \cdot (b, 0_A, 0_A, 0_A, \dots) = \varphi(a) \cdot \varphi(b), \end{aligned}$$

para todos $a, b \in A$, e então φ é um homomorfismo.

A sobrejetividade é imediata, pois para qualquer $y \in S$, tem-se $y = (a, 0_A, 0_A, 0_A, \dots)$ e escolhendo $x = a \in A$, tem-se $\varphi(x) = \varphi(a) = (a, 0_A, 0_A, 0_A, \dots) = y$. A injetividade também é imediata. Sejam $a, b \in A$ com $\varphi(a) = \varphi(b)$, isto é,

$$(a, 0_A, 0_A, 0_A, \dots) = (b, 0_A, 0_A, 0_A, \dots),$$

e da igualdade de polinômios, segue que $a = b$ e segue que φ é injetiva, e portanto, um isomorfismo. □

O fato de termos um subanel de $A[X]$ isomorfo ao anel A, significa que temos uma "cópia" do anel A dentro de $A[X]$. Este fato é matematicamente expresso dizendo que A está *imerso* ou *mergulhado* em $A[X]$. A aplicação φ neste caso é dita uma *imersão*.

Definição 3.58. Seja $a(X)$ um polinômio não nulo em um anel $(A, *, \cdot)$. Dizemos que o *grau* de $a(X)$, indicado por $gr(a)$, ou por ∂a, é o número natural n, se $a_n \neq 0_A$ e $a_k = 0_A$ para qualquer $k > n$.

Não definiremos o grau de um polinômio nulo. Desta forma, sempre que falarmos em grau de um polinômio, estaremos supondo implicitamente que este polinômio é não nulo. Para nós, zero será o grau de um polinômio com o termo $a_0 \neq 0_A$ e todos os demais termos a_k iguais a 0_A (o zero do anel A). Tal polinômio será chamado de polinômio *constante*. Em qualquer caso, se o grau de $a(X)$ for n, então o termo a_n será dito *termo dominante* do polinômio, mais ainda, se este termo dominante for igual a 1_A então o polinômio será dito *polinômio unitário* ou ainda *polinômio mônico*.

Proposição 3.59. *Sejam $a(X)$ e $b(X)$ dois polinômios não nulos em $A[X]$, de forma que $(a+b)(X) \neq 0_{A[X]}$, então $gr(a+b) \leq \max\{gr(a), gr(b)\}$.*

Prova. Denotemos $c(X) = a(X) + b(X)$ e suponha $m = gr(a)$ e $n = gr(b)$. Então

$$\begin{aligned} a_m \neq 0_A \quad \text{e} \quad a_k = 0_A, \quad \text{para todo} \quad k > m, \\ b_n \neq 0_A \quad \text{e} \quad b_k = 0_A, \quad \text{para todo} \quad k > n. \end{aligned}$$

Escolhemos $k_0 = \max\{m, n\}$. Assim

$$\begin{aligned} a_k = 0_A \quad \text{para todo} \quad k > k_0 \geq m, \\ b_k = 0_A \quad \text{para todo} \quad k > k_0 \geq n, \end{aligned}$$

logo $c_k = a_k * b_k = 0_A * 0_A = 0_A$ para todo $k > k_0$. Não sabemos o que acontece no termo c_{k_0}, mas a partir do índice k_0 todos os termos da soma, serão nulos, e portanto $gr(a+b) = gr(c) \leq k_0 = \max\{m, n\} = \max\{gr(a), gr(b)\}$. □

Proposição 3.60. *Sejam $a(X)$ e $b(X)$ dois polinômios não nulos em $A[X]$, de forma que $(a \cdot b)(X) \neq 0_{A[X]}$, então*

$$gr(a \cdot b) \leq gr(a) + gr(b),$$

mais ainda, se A for um anel de integridade, então a igualdade acontece.

Prova. Denotando $c(X) = (a \cdot b)(X)$, e $m = gr(a)$ e $n = gr(b)$, então para todo $k \in \mathbb{N}^*$, temos

$$c_{m+n+k} = \sum_{j=0}^{m+n+k} a_j \circ b_{m+n+k-j} = \sum_{j=0}^{m} a_j \circ b_{m+n+k-j} * \sum_{j=m+1}^{m+n+k} a_j \circ b_{m+n+k-j},$$

e como todos os a_{m+k} e todos os b_{n+k} são nulos, temos que $c_{m+n+k} = 0_A$ para qualquer $k \in \mathbb{N}^*$, e então todos os termos c_j com índice a partir de $m+n$ são nulos. Como não podemos garantir nada sobre o elemento $c_{m+n} = a_m \circ b_n$ então o grau de $(a \cdot b)$ é no máximo $m+n$, isto é,

$$gr(a \cdot b) \leq m + n = gr(a) + gr(b).$$

Mas, se A for um anel de integridade, então como $c_{m+n} = a_m \circ b_n$ com $a_m \neq 0_A$ e $b_n \neq 0_A$, temos que c_{m+n} é não nulo, e então o grau de $(a \cdot b)$ é exatamente $m+n$, isto é,

$$gr(a \cdot b) = m + n = gr(a) + gr(b).$$

□

Teorema 3.61 (Algoritmo da divisão)**.** *Seja $(A, *, \circ)$ um anel com unidade 1_A. Dados dois polinômios $a(X)$ e $b(X) \neq 0_{A[X]}$ em $A[X]$, com $gr(b) = n$ e b_n invertível em A, então existem $q(X), r(X) \in A[X]$ chamados respectivamente de quociente e resto da divisão, de modo que*

$$a(X) = q(X) \cdot b(X) + r(X),$$

com $r = 0_{A[X]}$ ou $gr(r) < gr(b)$.

Prova. Se $a(X) = 0_{A[X]}$ então o teorema é imediato com $q(X) = r(X) = 0_{A[X]}$. Se $a(X) \neq 0_{A[X]}$ e $m = gr(a) < gr(b) = n$ o teorema também é imediato com $q(X) = 0_{A[X]}$ e $r(X) = a(X)$.

Se $a(X) \neq 0_{A[X]}$ e $gr(a) \geq gr(b)$ então usaremos indução sobre o grau de a. Se $gr(a) = 0$ então $gr(b) = 0$ e $a(X) = a_0$ e $b(X) = b_0$. O teorema se verifica com $q(X) = b_0^{-1} \circ a_0$ e $r(X) = 0_{A[X]}$. Suponha agora (hipótese de indução) que o resultado seja verdadeiro para todo polinômio com grau menor que m, e que $gr(a) = m$. Considere

$$w(X) = a(X) - ((a_m \circ b_n^{-1})X^{m-n}) \cdot b(X).$$

Se $w(X) = 0_{A[X]}$ então o teorema se verifica com $q(X) = ((a_n \circ b_m^{-1})X^{n-m})$ e $r(X) = 0_{A[X]}$. Se $w(X) \neq 0_{A[X]}$, então temos $gr(w) \leq m - 1 < m$ e pela hipótese de indução existem, $q_1(X), r_1(X) \in A[X]$ tais que

$$w(X) = q_1(X) \cdot b(X) + r_1(X),$$

com $r_1(X) = 0_{A[X]}$ ou $gr(r_1) < gr(b)$. Então

$$a(X) - (a_m \circ b_n^{-1})X^{m-n} \cdot b(X) = q_1(X) \cdot b(X) + r_1(X),$$

isto é,

$$a(X) = \big(q_1(X) + (a_m \circ b_n^{-1})X^{m-n}\big) \cdot b(X) + r_1(X),$$

e o teorema fica satisfeito com $q(X) = q_1(X) + (a_m \circ b_n^{-1})X^{m-n}$ e $r(X) = r_1(X)$. □

Nas mesmas hipóteses do teorema anterior, com algumas modificações na demonstração, podemos mostrar que também existem $p(X), s(X) \in A[X]$ de modo que

$$a(X) = b(X) \cdot p(X) + s(X),$$

com $s(X) = 0_{A[X]}$ ou $gr(s) < gr(b)$. O leitor desatento pode achar isto estranho mas sem a hipótese de comutatividade no anel A, podem existir diferentes quocientes pela direita e pela esquerda da divisão. O próximo exemplo ilustra isso.

Exemplo 3.23. Consideremos o anel (não comutativo) dos quatérnios $(\mathbb{H}, +, \cdot)$ e os polinômios $a(X) = kX^2 + 2jX + k$ e $b(X) = iX + 1$. Como $gr(b) = 1$ com $b_1 = i$ invertível em $\mathbb{H}$, podemos garantir a existência de $q(X), p(X), r(X), s(X) \in \mathbb{H}[X]$ de forma que

$$a(X) = q(X) \cdot b(X) + r(X) = b(X) \cdot p(X) + s(X),$$

com $r(X), s(X) = 0_{\mathbb{H}[X]}$ ou $gr(r), gr(s) < gr(b) = 1$. Entretanto não teremos $q(X) = p(X)$ e $r(X) = s(X)$. De fato,

$$kX^2 + 2jX + k = (iX + 1)(jX - k) + 2k = (-jX + 3k)(iX + 1) + (-2k).$$

■

Teorema 3.62. *Se A é um anel de integridade, então é único o par $q(X)$ e $r(X)$ que satisfaz o algoritmo da divisão.*

Prova. Suponha $a(X) = q(X) \cdot b(X) + r(X) = q_1(X) \cdot b(X) + r_1(X)$, com $r = 0_{A[X]}$ ou $gr(r) < gr(b)$ e $r_1 = 0_{A[X]}$ ou $gr(r_1) < gr(b)$. Assim

$$(q - q_1)(X) \cdot b(X) = (r_1 - r)(X).$$

Suponha (por absurdo) que tivéssemos $r_1(X) \neq r(X)$, isto é, $(r_1 - r)(X) \neq 0_{A[X]}$, então $gr(r_1 - r) = gr(b \cdot (q - q_1))$ e como $A[X]$ é anel de integridade, temos que

$$gr(r_1 - r) = gr(b \cdot (q_1 - q)) = gr(b) + gr(q_1 - q),$$

e então $gr(r_1 - r) \geq gr(b)$, que é uma contradição, pois o grau de qualquer um dos restos r ou r_1, deve ser menor que o grau de b. Segue que devemos obrigatoriamente ter $(r_1 - r)(X) = 0_{A[X]}$ ou seja, $r_1(X) = r(X)$. Além disso,

$$(q - q_1)(X) \cdot b(X) = (r_1 - r)(X) = 0_{A[X]},$$

e como b é não nulo e $A[X]$ é anel de integridade segue que $(q_1 - q)(X) = 0_{A[X]}$ ou seja $q_1(X) = q(X)$, donde segue a unicidade do quociente e do resto da divisão de polinômios. □

Exemplo 3.24. Se $gr(b) = n$ com b_n não invertível então não é possível garantir a existência de $q(X)$ e $r(X)$. Considere o anel de integridade $(\mathbb{Z}, +, \cdot)$ e $a(X) = 5X^2$ e $b(X) = 2X$ dois polinômios em $\mathbb{Z}[X]$. É fácil ver que não existem $q(X)$ e $r(X)$ tais que

$$5X^2 = q(X) \cdot (2X) + r(X)$$

satisfazendo as condições do algoritmo da divisão. De fato, se existissem tais quociente e resto, então deveríamos ter $gr(r) = 0$ e $gr(q) = 1$, donde $r(X) = r_0$ e $q(X) = q_1X + q_0$ e desta forma, deveria ocorrer que

$$5X^2 = (q_1X + q_0) \cdot (2X) + r_0 = (2 \cdot q_1)X^2 + (2 \cdot q_0)X + r_0,$$

e portanto

$$5 = 2 \cdot q_1, \qquad 0 = 2 \cdot q_0 \qquad \text{e} \qquad 0 = r_0.$$

Mas não há coeficiente $q_1 \in \mathbb{Z}$ que faça com que $q_1 \cdot 2 = 5$. ■

Exemplo 3.25. Se A não for anel de integridade não é possível garantir a unicidade do quociente e do resto. Tomemos o anel $(\mathbb{Z}_{12}, +, \cdot)$ que não é anel de integridade, e $a(X) = \overline{8}X^2 + \overline{4}X + \overline{4}$ e $b(X) = \overline{2}X + \overline{1}$ em $\mathbb{Z}_{12}[X]$. Note que

$$\begin{aligned} \overline{8}X^2 + \overline{4}X + \overline{4} &= (\overline{4}X) \cdot (\overline{2}X + \overline{1}) + \overline{4} \\ \overline{8}X^2 + \overline{4}X + \overline{4} &= (\overline{10}X + \overline{3}) \cdot (\overline{2}X + \overline{1}) + \overline{1} \end{aligned}$$

e portanto a divisão de $a(X)$ por $b(X)$ admite (pelo menios) dois quocientes com seus dois respectivos restos. ■

Definição 3.63. Dado o anel $(A, *, \circ)$ e $a(X)$ e $b(X)$ dois polinômios em $A[X]$ com $b(X) \neq 0_{A[X]}$, dizemos que $b(X)$ *divide* $a(X)$, ou que $a(X)$ é *divisível* por $b(X)$, se (e somente se) existe $q(X) \in A[X]$ tal que

$$a(X) = b(X) \cdot q(X) = q(X) \cdot b(X),$$

e escrevemos $b(X)|a(X)$, ou simplesmente $b|a$ para dizer que $b(X)$ divide $a(X)$.

Note que, escrever $b|a$, ou dizer que $b(X)$ divide $a(X)$, significa que o resto $r(X)$ da divisão de $a(X)$ por $b(X)$ é igual a $0_{A[X]}$. No caso de não existir um polinômio $q(X) \in A[X]$ que cumpre a definição anterior, então dizemos que $b(X)$ não divide $a(X)$, e expressamos este fato escrevendo $b \nmid a$. Assim como no caso de números inteiros, valem certas propriedades para a divisibilidade de polinômios. Mostraremos as principais.

Proposição 3.64. *Sejam $(A, *, \circ)$ um anel e $a(X)$, $b(X)$ e $c(X)$ polinômios em $A[X]$. Então*

i) Se A possui unidade, $a|a$ (reflexividade),

ii) Se A for comutativo, $a|b$ e $b|c$, então $a|c$ (transitividade),

iii) Se A for comutativo e $a|b$, então $a|(w \cdot b)$ para qualquer $w \in A[X]$,

iv) Se A for comutativo, $a|b$ e $a|c$, então $a|(u \cdot b + v \cdot c)$ para quaisquer $u, v \in A[X]$.

Prova. Para (i), notemos que $a(X) = a(X) \cdot 1_{A[X]} = 1_{A[X]} \cdot a(X)$ e a definição (de divisibilidade) fica satisfeita com $q(X) = 1_{A[X]}$.

Para (ii), como $a|b$ então existe $q_1(X) \in A[X]$ tal que $b(X) = a(X) \cdot q_1(X) = q_1(X) \cdot a(X)$. Também como $b|c$ então existe $q_2 \in A[X]$ tal que $c(X) = b(X) \cdot q_2(X) = q_2(X) \cdot b(X)$. Desta forma,

$$c(X) = q_2(X) \cdot b(X) = q_2(X) \cdot (q_1(X) \cdot a(X)) = (q_2(X) \cdot q_1(X)) \cdot a(X),$$

e também

$$c(X) = b(X) \cdot q_2(X) = (a(X) \cdot q_1(X)) \cdot q_2(X) = a(X) \cdot (q_1(X) \cdot q_2(X)).$$

Segue da comutatividade de $A[X]$ que $(q_1(X) \cdot q_2(X)) = (q_2(X) \cdot q_1(X))$ e da definição de divisibilidade que $a|c$.

Para mostrar (iii) notemos primeiro que para qualquer $w(X) \in A[X]$, temos $b|(w \cdot b)$, pois a definição de divisibilidade fica satisfeita com $q(X) = w(X)$. Assim, como $a|b$ e $b|(w \cdot b)$ então pelo item (ii), $a|(w \cdot b)$ para qualquer $w \in A[X]$.

Para mostrar (iv), suponha $a|b$ e $a|c$. Da definição de divisibilidade, existem $q_1, q_2 \in A[X]$, de forma que $b(X) = q_1(X) \cdot a(X) = a(X) \cdot q_1(X)$ e $c(X) = q_2(X) \cdot a(X) = a(X) \cdot q_2(X)$. Assim, para quaisquer $u, v \in A[X]$ temos

$$\begin{aligned} u(X) \cdot b(X) + v(X) \cdot c(X) &= u(X) \cdot (q_1(X) \cdot a(X)) + v(X) \cdot (q_2(X) \cdot a(X)) \\ &= (u(X) \cdot q_1(X) + q_2(X) \cdot v(X)) \cdot a(X), \end{aligned}$$

e da comutatividade de $A[X]$ segue também que $(u \cdot b) + (v \cdot c) = a \cdot ((u \cdot q_1) + (q_2 \cdot v))$. Da definição de divisibilidade temos que $a|(u \cdot b + v \cdot c)$. Isto encerra esta demonstração. □

Cuidado! No caso da divisibilidade de números naturais é também válida a propriedade antissimétrica, mas esta propriedade não vale na divisibilidade de polinômios, bem como não vale na divisibilidade de números inteiros. Veja o próximo exemplo.

Exemplo 3.26. Considere o anel dos racionais $(\mathbb{Q}, +, \cdot)$, e os polinômios $a(X) = 4 + 2X$ e $b(X) = 2 + X$ em $\mathbb{Q}[X]$. Então

$$a(X) = 4 + 2X = 2 \cdot (2 + X) = 2 \cdot b(X), \quad \text{e}$$
$$b(X) = 2 + X = \frac{1}{2} \cdot (4 + 2X) = \frac{1}{2} \cdot a(X),$$

e então, da definição de divisibilidade, $a|b$ com $q(X) = \frac{1}{2} = (\frac{1}{2}, 0, 0, \dots)$ e $b|a$ com $q(X) = 2 = (2, 0, 0, \dots)$, e no entanto $a(X) \neq b(X)$. ■

Exemplo 3.27. Considerando o anel comutativo, com unidade, $A = M_2(\mathbb{R})$ das matrizes quadradas diagonais, com coeficientes reais, e

$$a(X) = \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix} + \begin{bmatrix} -5 & 0 \\ 0 & 1 \end{bmatrix} X + \begin{bmatrix} 2 & 0 \\ 0 & 6 \end{bmatrix} X^2,$$
$$b(X) = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} + \begin{bmatrix} -2 & 0 \\ 0 & 3 \end{bmatrix} X$$

polinômios em $A[X]$, temos que $a|b$ pois,

$$a(X) = \left(\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} + \begin{bmatrix} -2 & 0 \\ 0 & 3 \end{bmatrix} X \right) \cdot \left(\begin{bmatrix} 2 & 0 \\ 0 & -1 \end{bmatrix} + \begin{bmatrix} -1 & 0 \\ 0 & 2 \end{bmatrix} X \right),$$

e a definição de divisibilidade fica cumprida com $q(X) = \begin{bmatrix} 2 & 0 \\ 0 & -1 \end{bmatrix} + \begin{bmatrix} -1 & 0 \\ 0 & 2 \end{bmatrix} X$. ■

Definição 3.65. Seja $(A, *, \circ)$ um anel comutativo e

$$a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots + a_nX^n,$$

um polinômio em $A[X]$. Para qualquer $u \in A$, chama-se valor de a em u, ao elemento de A, denotado por $a(u)$ e dado por

$$a(u) = a_0 * (a_1 \circ u) * (a_2 \circ u^2) * (a_3 \circ u^3) * \cdots * (a_n \circ u^n).$$

Mais ainda, se $a(u) = 0_A$, dizemos que u é *raiz* de a em A.

Proposição 3.66. *Se a e b são polinômios sobre um anel $(A, *, \circ)$, e $u \in A$ então*

i) $(a + b)(u) = a(u) * b(u)$,

ii) $(a \cdot b)(u) = a(u) \circ b(u)$.

Prova. Dados $a(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, e $b(X) = b_0 + b_1X + b_2X^2 + \cdots + b_mX^m$, dois polinômios em $A[X]$, temos que

$$(a + b)(X) = (a_0 * b_0) + (a_1 * b_1)X + (a_2 * b_2)X^2 + \cdots + (a_n * b_n)X^n,$$

donde

$$\begin{aligned}(a + b)(u) &= (a_0 * b_0) * (a_1 * b_1) \cdot u * (a_2 * b_2) \cdot u^2 * \cdots * (a_n * b_n) \cdot u^n = \\ &= a_0 * b_0 * a_1 \cdot u * b_1 \cdot u * a_2 \cdot u^2 * b_2 \cdot u^2 * \cdots * a_n \cdot u^n * b_n \cdot u^n \\ &= (a_0 * a_1 \cdot u * a_2 \cdot u^2 * \cdots * a_n \cdot u^n) * (b_0 * b_1 \cdot u * b_2 \cdot u^2 * \cdots * b_n \cdot u^n)\end{aligned}$$

$$= a(u) * b(u).$$

Para o produto, temos que

$$(a \cdot b)(X) = (a_0 \circ b_0) + \left(\sum_{i+j=1} a_i \circ b_j\right) X + \left(\sum_{i+j=2} a_i \circ b_j\right) X^2 + \cdots + \left(\sum_{i+j=m+n} a_i \circ b_j\right) X^{m+n},$$

e assim,

$$\begin{aligned}(a \cdot b)(u) &= (a_0 \circ b_0) + \left(\sum_{i+j=1} a_i \circ b_j\right) u + \left(\sum_{i+j=2} a_i \circ b_j\right) u^2 + \cdots + \left(\sum_{i+j=m+n} a_i \circ b_j\right) u^{m+n} \\ &= (a_0 + a_1 u + a_2 u^2 + \cdots + a_n u^n) \circ (b_0 + b_1 u + b_2 u^2 + \cdots + b_m u^m) \\ &= a(u) \circ b(u).\end{aligned}$$

□

Proposição 3.67. *Seja $(A, *, \circ)$ um anel com unidade, $u \in A$ e $a(X) \in A[X]$. Então o resto $r(X)$, da divisão de $a(X)$ por $(X-u)$, é igual a $a(u)$, sendo esta igualdade entendida no sentido $r(X) = a(u) + 0_A X + 0_A X^2 + \cdots$.*

Prova. Tomando $b(X) = (X - u) = (1_A X - u)$, que é não nulo e o coeficiente dominante é invertível, podemos aplicar o algoritmo da divisão em $a(X)$ e $b(X)$, isto é, existem $q(X), r(X) \in A[X]$ tais que

$$a(X) = q(X) \cdot (X - u) + r(X),$$

com $r(X) = 0_{A[X]}$ ou $gr(r) < gr(b) = 1$.

Se $r(X) = 0_{A[X]}$ então temos que $a(X) = q(X) \cdot (X-u)$, e também $a(u) = q(u) \cdot (u-u) = q(u) \cdot 0_A = 0_A = r(X)$.

Se por outro lado, $r(X) \neq 0_{A[X]}$, então o grau de $r(X)$ é zero, e assim $r(X) = r_0$. Nestes termos

$$a(u) = q(u) \circ (u - u) + r(u) = q(u) \circ 0_A * r_0 = r_0,$$

e então $r(X) = r_0 = a(u)$. □

Corolário 3.68. *Um polinômio $a(X) \in A[X]$ é divisível por $(X - u) \in A[X]$ se e somente se $a(u) = 0_A$, isto é, se e somente se u é raiz de a.*

Teorema 3.69. *Seja $(A, *, \cdot)$ um domínio de integridade e $a(X) \in A[X]$ um polinômio não nulo. Então o número de raízes de a em A é no máximo $gr(a)$.*

Prova. Usaremos indução sobre o grau de a. Se $gr(a) = 0$ então a não admite raízes em A, já que $a(X)$ é não nulo. Logo o teorema fica verificado.

Suponha agora que o teorema seja verdadeiro para todo polinômio com grau $k - 1$, e suponha $gr(a) = k > 0$. Se a não tiver raízes em A, então novamente o teorema se verifica. Se a tiver ao menos uma raiz u em A, então existe $q(X) \in A[X]$ tal que

$$a(X) = q(X) \cdot (X - u).$$

Além disso, qualquer outra raiz u_0 de $a(X)$ será também raiz de $q(X)$, pois

$$0_A = a(u_0) = q(u_0) \circ (u_0 - u),$$

e sendo A um anel de integridade, como $(u_0 - u) \neq 0_A$, resulta que $q(u_0) = 0_A$ donde u_0 será também raiz de $q(X)$, e então $a(X)$ não tem outras raízes além de u e das raízes de $q(X)$. Como A é anel de integridade, então $gr(a) = gr(q) + gr(X - u)$, isto é, $gr(q) = k - 1$. Pela hipótese de indução, o teorema se verifica para $q(X)$, isto é, $q(X)$ tem no máximo $k-1$ raízes em A, e então $a(X)$ tem no máximo as $k - 1$ raízes de $q(X)$ e ainda a raiz u, ou seja, no máximo $k = gr(a)$ raízes. Segue do princípio de indução finita, que o resultado vale para todo polinômio de grau n. □

Exemplo 3.28. Consideremos o polinômio $a(X) = 2X^3 - X^2 - 2X + 1$ sobre o anel dos inteiros $\mathbb{Z}$. Como $\mathbb{Z}$ é anel de integridade, então $a(X)$ tem no máximo $gr(a) = 3$ raízes em $\mathbb{Z}$. De fato, as raízes de $a(X)$ são 1, -1 e $\frac{1}{2}$, e portanto duas raízes em $\mathbb{Z}$. ■

Exemplo 3.29. Seja $a(X) = \overline{1}X^3 + \overline{5}X$ um polinômio sobre o anel $A = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Como A não é anel de integridade, não podemos garantir que $a(X)$ tenha no máximo $gr(a) = 3$ raízes em A. De fato,

$$\begin{aligned}
a(\overline{0}) &= \overline{1} \cdot (\overline{0})^3 + \overline{5} \cdot \overline{0} = \overline{0} + \overline{0} = \overline{0} \\
a(\overline{1}) &= \overline{1} \cdot (\overline{1})^3 + \overline{5} \cdot \overline{1} = \overline{1} + \overline{5} = \overline{0} \\
a(\overline{2}) &= \overline{1} \cdot (\overline{2})^3 + \overline{5} \cdot \overline{2} = \overline{2} + \overline{4} = \overline{0} \\
a(\overline{3}) &= \overline{1} \cdot (\overline{3})^3 + \overline{5} \cdot \overline{3} = \overline{3} + \overline{3} = \overline{0} \\
a(\overline{4}) &= \overline{1} \cdot (\overline{4})^3 + \overline{5} \cdot \overline{4} = \overline{4} + \overline{2} = \overline{0} \\
a(\overline{5}) &= \overline{1} \cdot (\overline{5})^3 + \overline{5} \cdot \overline{5} = \overline{5} + \overline{1} = \overline{0}
\end{aligned}$$

e desta forma todos os elementos de $A = \mathbb{Z}_6$ são raízes de $a(X)$, e portanto o número de raízes de $a(X)$ é maior que o grau de $a(X)$. ■

No caso em que A é um anel de integridade, então $A[X]$ é também um anel de integridade, e assim, podemos então falar de ideais neste anel.

Se J é um subconjunto de A, o subconjunto $J[X]$ de $A[X]$ é o conjunto de todos os polinômios com coeficientes em J. É fácil verificar que se I é um ideal de A, então $I[X]$ é um ideal de $A[X]$. Deixaremos a prova deste fato como exercício.

Podemos também construir ideais gerados por subconjuntos de $A[X]$. Escolhendo um conjunto de polinômios, $S = \{a_1, a_2, a_3, \cdots, a_n\}$, todos em $A[X]$, o subconjunto de $A[X]$ dado por

$$\langle a_1, \cdots, a_n \rangle = \{h_1 \cdot a_1 + h_2 \cdot a_2 + \cdots + h_n \cdot a_n; \quad h_i \in A[X]\},$$

é um ideal de $A[X]$, chamado de ideal gerado pelo conjunto S, ou ideal gerado pelos polinômios a_i.

Um ideal gerado por um único polinômio, é dito ideal principal, de $A[X]$. Desta forma, todo ideal principal é da forma,

$$J = \langle a \rangle = \{h \cdot a; \quad h \in A[X]\} = A[X] \cdot a = a \cdot A[X].$$

3.7 Aneis fatoriais e anéis Euclidianos

Escrever esta seção....

Capítulo 4

Corpos

O objetivo deste capítulo é o estudo dos corpos. Como veremos, um corpo obrigatoriamente possui uma unidade. Já comentamos anteriormente que em um anel com unidade, se a unidade for igual ao elemento neutro, então este anel se reduz a um único elemento, o próprio elemento neutro. Para evitar confusões deixamos então claro aqui que durante todo este capítulo, vamos admitir que os conjuntos envolvidos, anéis ou corpos, possuem pelo menos dois elementos distintos. Isto será apenas para garantir que $1_A \neq 0_A$.

4.1 Corpos e subcorpos

Definição 4.1. Um anel comutativo com unidade $(\mathbb{K}, *, \circ)$ é dito um corpo, se e somente se, todo elemento não nulo de $\mathbb{K}$ admite inverso, isto é, dado qualquer $b \in \mathbb{K}$ com $b \neq 0_{\mathbb{K}}$, existe $b^{-1} \in \mathbb{K}$ tal que $(b \circ b^{-1}) = (b^{-1} \circ b) = 1_{\mathbb{K}}$.

Exemplo 4.1. Os conjuntos $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ com as operações usuais de soma e produto são corpos, pois são domínios de integridade e quaisquer elementos não nulos admitem inverso multiplicativo no próprio conjunto. ■

Exemplo 4.2. $(\mathbb{Z}, +, \cdot)$ não é corpo, pois apesar de ser um domínio de integridade, nem todos os elementos de $\mathbb{Z}$ admitem inverso em $\mathbb{Z}$. ■

Proposição 4.2. *Se $(\mathbb{K}, *, \circ)$ é um corpo, então, $(\mathbb{K}, *, \circ)$ é anel de integridade.*

Prova. Sejam $a, b \in \mathbb{K}$ tais que $(a \circ b) = 0_{\mathbb{K}}$, e $a \neq 0_{\mathbb{K}}$. Então, existe $a^{-1} \in \mathbb{K}$ tal que $(a \circ a^{-1}) = (a^{-1} \circ a) = 1_{\mathbb{K}}$. Desta forma,

$$b = (1_{\mathbb{K}} \circ b) = (a^{-1} \circ a) \circ b = a^{-1} \circ (a \circ b) = a^{-1} \circ 0_{\mathbb{K}} = 0_{\mathbb{K}},$$

que prova que $\mathbb{K}$ é um anel de integridade. □

Nestes termos, todo corpo é anel de integridade. Mas a recíproca não é verdadeira. Como já sabemos $\mathbb{Z}$ é anel de integridade e não é corpo. Entretanto com hipóteses adicionais pode-se conseguir este resultado.

Proposição 4.3. *Todo anel de integridade finito é um corpo.*

Prova. Seja $(A, *, \circ)$ um anel de integridade finito, isto é,

$$A = \{0_A, a_1, a_2, \ldots, a_n\}.$$

Tomemos $a \neq 0_A \in A$ arbitrário e mostraremos que a é invertível. Seja

$$\begin{array}{rcl} \varphi : A & \to & a \circ A = \{0_A, a \circ a_1, a \circ a_2, \ldots, a \circ a_n\} \\ a_i & \mapsto & \varphi(a_i) = a \circ a_i \qquad 1 \leq i \leq n. \end{array}$$

Trata-se claramente de uma aplicação sobrejetiva. Também, se $\varphi(a_i) = \varphi(a_j)$ então $a \circ a_i = a \circ a_j$ e assim, $a \circ (a_i - a_j) = (a \circ a_i) - (a \circ a_j) = 0_A$, e sendo $a \neq 0_A$, decorre que $(a_i - a_j) = 0_A$, donde $a_i = a_j$ e φ é injetora. Segue que A e $a \circ A$, possuem a mesma quantidade de elementos. Como $a \circ A \subset A$ e $a \circ A$ possui a mesma quantidade de elementos de A então $A = a \circ A$, e também como $1_A \in A$, temos $1_A \in a \circ A$, isto é, existe $a_k \in A$, tal que

$$1_A = a \circ a_k,$$

mas isto significa que a é invertível com a_k o seu inverso, concluindo esta demonstração. □

Corolário 4.4. *Se p é um número inteiro primo, então $(\mathbb{Z}_p, +, \cdot)$ é corpo.*

Definição 4.5. Se $(\mathbb{K}, *, \circ)$ é um corpo e $\mathbb{S} \neq \emptyset$ é um subconjunto de $\mathbb{K}$, dizemos que $\mathbb{S}$ é subcorpo de $\mathbb{K}$ se

i) $\mathbb{S}$ é fechado para as operações $*$ e $\circ$, e
ii) $(\mathbb{S}, *, \circ)$ é também um corpo.

Já sabemos que em um anel com unidade, qualquer subanel pode ou não possuir unidade. Mesmo o subanel possuindo unidade, sabemos que esta unidade pode ser diferente da unidade do anel. Isto pode não ocorrer com corpos e seus subcorpos. Um subcorpo possui obrigatoriamente unidade e esta unidade deve coincidir com a unidade do corpo. Este fato será demonstrado na próxima proposição.

Proposição 4.6. *Se $(\mathbb{K}, *, \circ)$ é um corpo e $\mathbb{S}$ é um subcorpo de $\mathbb{K}$ então $1_{\mathbb{S}} = 1_{\mathbb{K}}$.*

Prova. Como $\mathbb{S}$ é subcorpo, então $\mathbb{S}$ é também corpo, e assim $\mathbb{S}$ possui unidade $1_{\mathbb{S}}$. Além disso, de acordo com a definição de unidade, esta unidade deve satisfazer $1_{\mathbb{S}} \circ 1_{\mathbb{S}} = 1_{\mathbb{S}}$. Por outro lado $1_{\mathbb{S}} \in \mathbb{S} \subset \mathbb{K}$ e portanto, de acordo com a definição de unidade em $\mathbb{K}$, temos $1_{\mathbb{S}} \circ 1_{\mathbb{K}} = 1_{\mathbb{S}}$.

Logo

$$1_{\mathbb{S}} \circ 1_{\mathbb{K}} - 1_{\mathbb{S}} \circ 1_{\mathbb{S}} = 0_{\mathbb{K}} = 0_{\mathbb{S}},$$

ou ainda

$$1_{\mathbb{S}} \circ (1_{\mathbb{K}} - 1_{\mathbb{S}}) = 0_{\mathbb{K}},$$

e como $\mathbb{K}$ é anel de integridade e $1_{\mathbb{S}} \neq 0_{\mathbb{K}}$, segue que $1_{\mathbb{K}} - 1_{\mathbb{S}} = 0_{\mathbb{K}}$, donde $1_{\mathbb{S}} = 1_{\mathbb{K}}$. □

Corolário 4.7. *Se $(\mathbb{K}, *, \circ)$ é um corpo e $\mathbb{S}$ é um subcorpo de $\mathbb{K}$ então para qualquer $a \in \mathbb{S}$ com $a \neq 0_{\mathbb{S}}$ temos que $(a^{-1})_{\mathbb{S}} = (a^{-1})_{\mathbb{K}}$.*

Prova. Como $0_{\mathbb{S}} = 0_{\mathbb{K}}$ então dado $a \neq 0_{\mathbb{S}}$, temos que $a \neq 0_{\mathbb{K}}$ também. Assim existem $(a^{-1})_{\mathbb{S}}$ e $(a^{-1})_{\mathbb{K}}$, de forma que

$$(a^{-1})_{\mathbb{S}} \circ a = a \circ (a^{-1})_{\mathbb{S}} = 1_{\mathbb{S}},$$

e também

$$(a^{-1})_{\mathbb{K}} \circ a = a \circ (a^{-1})_{\mathbb{K}} = 1_{\mathbb{K}}.$$

Logo

$$a \circ (a^{-1})_{\mathbb{S}} - a \circ (a^{-1})_{\mathbb{K}} = 1_{\mathbb{S}} - 1_{\mathbb{K}} = 0_{\mathbb{K}},$$

ou ainda

$$a \circ ((a^{-1})_{\mathbb{S}} - (a^{-1})_{\mathbb{K}}) = 0_{\mathbb{K}},$$

e como $\mathbb{K}$ é anel de integridade e $a \neq 0_{\mathbb{K}}$, segue que $(a^{-1})_{\mathbb{S}} - (a^{-1})_{\mathbb{K}} = 0_{\mathbb{K}}$, donde $(a^{-1})_{\mathbb{S}} = (a^{-1})_{\mathbb{K}}$. □

O trabalho de identificar subcorpos pode ser simplificado. A próxima proposição nos oferece um método seguro e mais simples para garantir quando um subconjunto não vazio de um corpo é um subcorpo.

Proposição 4.8. *Se $(\mathbb{K}, *, \circ)$ é um corpo, um subconjunto não vazio $\mathbb{S} \subset \mathbb{K}$ é um subcorpo de $\mathbb{K}$, se e somente se*

i) $1_{\mathbb{K}} \in \mathbb{S}$,
ii) $a - b \in \mathbb{S}$ *para todos* $a, b \in \mathbb{S}$,
iii) $a \circ b^{-1} \in \mathbb{S}$ *para todos* $a, b \neq 0_{\mathbb{K}} \in \mathbb{S}$.

Prova. Supondo inicialmente que $\mathbb{S}$ é subcorpo de $\mathbb{K}$ então $(\mathbb{S}, *, \circ)$ é também corpo. Portanto, as condições (i), (ii) e (iii) são trivialmente satisfeitas.

Reciprocamente, suponha que (i)-(iii) acontecem. Provaremos que $*$ e $\circ$ são fechadas em $\mathbb{S}$ e também que $(\mathbb{S}, *, \circ)$ é um corpo. Por (i), $\mathbb{S} \neq \emptyset$. Certamente, a operação $*$ é associativa e também comutativa em $\mathbb{S}$, pois o é em todo $\mathbb{K}$. Como $1_{\mathbb{K}} \in \mathbb{S}$, da condição (ii) temos que $(1_{\mathbb{K}} - 1_{\mathbb{K}}) \in \mathbb{S}$, isto é, $0_{\mathbb{K}} \in \mathbb{S}$. Da mesma condição (ii) decorre que dado qualquer $a \in \mathbb{S}$, então $(0_{\mathbb{K}} - a) \in \mathbb{S}$ e assim $(-a) \in \mathbb{S}$. Segue que $\mathbb{S}$ possui elemento neutro para $*$ e todo $a \in \mathbb{S}$ e simetrizável, logo $(\mathbb{S}, *)$ é subgrupo abeliano do grupo $(\mathbb{K}, *)$.

A operação $\circ$ é associativa, comutativa e também é distributiva com relação a $*$ pois estas propriedades ocorrem em todo o corpo $\mathbb{K}$. Além disso, por (i), $\mathbb{S}$ possui unidade, e assim $\mathbb{S}$ é subanel comutativo com unidade (a mesma unidade de $\mathbb{K}$). Para finalizar, dado $b \in \mathbb{S}$ não nulo, como $1_{\mathbb{K}} \in \mathbb{S}$ pela condição (iii) temos que $(1_{\mathbb{K}} \circ b^{-1}) \in \mathbb{S}$, donde $b^{-1} \in \mathbb{S}$ e assim, todo elemento não nulo em $\mathbb{S}$ é invertível.

Resta provar que as operações são fechadas em $\mathbb{S}$. Dados $a, b \in \mathbb{S}$ temos que $(-b) \in \mathbb{S}$ e pela condição (ii) temos que $(a - (-b)) \in \mathbb{S}$, isto é, $(a * b) \in \mathbb{S}$. Também se $b = 0_{\mathbb{S}}$ então $a \circ b = 0_{\mathbb{S}} \in \mathbb{S}$ e se por outro lado $b \neq 0_{\mathbb{S}}$ então b é invertível isto é, $b^{-1} \in \mathbb{S}$ e da condição (iii) temos que $(a \circ (b^{-1})^{-1}) \in \mathbb{S}$, isto é, $(a \circ b) \in \mathbb{S}$. Segue que as operações $*$ e $\circ$ são fechadas em $\mathbb{S}$. Fica assim concluído que $(\mathbb{S}, *, \circ)$ é também um corpo, e portanto, um subcorpo de $(\mathbb{K}, *, \circ)$. □

Observe que, $\{0_G\}$ é subgrupo (trivial) de um grupo $(G, *)$, $\{0_A\}$ é subanel (trivial) de um anel $(A, *, \circ)$, entretanto $\{0_{\mathbb{K}}\}$ não é subcorpo de um corpo $(\mathbb{K}, *, \circ)$. Sendo assim, $\mathbb{K}$ possui um único subcorpo trivial que é o próprio $\mathbb{K}$. Vamos provar agora o comentário que segue a definição de corpo.

Já que um corpo é um anel de integridade, podemos nos referir a ideais em um corpo, e neste caso, obtemos alguns resultados importantíssimos.

Teorema 4.9. *Seja $(\mathbb{K}, *, \circ)$ um corpo. Então os únicos ideais de $\mathbb{K}$ são os ideais triviais.*

Prova. Seja J um ideal de $\mathbb{K}$, com

$$\{0_{\mathbb{K}}\} \subsetneq J \subset \mathbb{K}.$$

Então existe $a \in J$ com $a \neq 0_{\mathbb{K}}$. Sendo $\mathbb{K}$ um corpo, então existe $a^{-1} \in \mathbb{K}$ tal que $a \circ a^{-1} = 1_{\mathbb{K}}$. Mas da definição de ideal, como $a \in J$, então $a \circ a^{-1} \in J$, isto é, $1_{\mathbb{K}} \in J$ e segue agora que $J = \mathbb{K}$, pois dado qualquer $a \in \mathbb{K}$ deve ocorrer que $a = a \circ 1_{\mathbb{K}} \in J$. □

Note que este último teorema afirma que $\{0_{\mathbb{K}}\}$ é um ideal maximal em $\mathbb{K}$, uma vez que não existe outro ideal J com $\{0_{\mathbb{K}}\} \subsetneq J \subset \mathbb{K}$ exceto o próprio $\mathbb{K}$.

Teorema 4.10. *Seja $(A, *, \circ)$ um anel comutativo com unidade 1_A, e I um ideal de A. Então I é ideal maximal, se e somente se, $\frac{A}{I}$ é corpo.*

Prova. Suponha I ideal maximal de A. Já sabemos que $(\frac{A}{I}, *, \circ)$ é um anel comutativo com unidade sob as operações definidas no conjunto quociente. Seja $(a * I) \in \frac{A}{I}$ com $(a * I) \neq 0_{\frac{A}{I}} = (0_A * I)$. De outra forma, $a \notin I$. Seja

$$J = [a] = \{a \circ x; \quad x \in A\},$$

e também

$$I * J = \{m * n; \quad m \in I, n \in J\}.$$

Sabemos que J e $I * J$ são ideais de A. Além disso, $I \subset I * J$ mas como $a = (0_A * a) \in I * J$ e $a \notin I$ então $I \subsetneq I * J \subset A$. Como I é ideal maximal, segue que $I * J = A$, e então $1_A \in I * J$. Existem portanto $m \in I$ e $n = a \circ x \in J$ tais que

$$1_A = m * a \circ x.$$

Sendo assim, $1_A * I = (m * a \circ x) * I = (m * I) * ((a * I) \circ (x * I))$. Como $m \in I$ então $m * I = I = 0_A * I$ e então

$$1_{\frac{A}{I}} = 1_A * I = (a * I) \circ (x * I),$$

e segue que $(a * I)$ é invertível em $\frac{A}{I}$ e portanto $\frac{A}{I}$ é corpo.

Reciprocamente, suponha que $\frac{A}{I}$ seja corpo. Então existem $0_{\frac{A}{I}}$ e $1_{\frac{A}{I}}$ elementos distintos em $\frac{A}{I}$. De outra forma $(0_A * I) \neq (1_A * I)$, e isto significa que $1_A = (1_A - 0_A) \notin I$ e portanto $I \subsetneq A$. Tomemos J, um ideal de A, satisfazendo

$$I \subsetneq J \subset A.$$

Existe portanto $a \in J$ com $a \notin I$. Como $a = (a - 0_A) \notin I$, então $(a * I) \neq (0_A * I) = 0_{\frac{A}{I}}$. Como $\frac{A}{I}$ é corpo existe $(x * I) \in \frac{A}{I}$ tal que

$$(a * I) \circ (x * I) = 1_A * I,$$

ou ainda

$$(a \circ x) * I = 1_A * I.$$

Da igualdade entre classes, segue que $(a \circ x) - 1_A \in I$, e como $I \subset J$, então $((a \circ x) - 1_A) \in J$. Mas como $a \in J$ e J é ideal de A, então $(a \circ x) \in J$. Segue que $(a \circ x) - ((a \circ x) - 1_A) \in J$, ou ainda $1_A \in J$. Segue disto que $J = A$ e então I é ideal maximal de A. □

Corolário 4.11. *Se p é um número inteiro primo, então $(\mathbb{Z}_p, +, \cdot)$ é corpo.*

Prova. No anel de integridade $(\mathbb{Z}, +, \cdot)$ consideremos o ideal $p\mathbb{Z} = [p] = \{pk; k \in \mathbb{Z}\}$. Vamos provar que $p\mathbb{Z}$ é ideal maximal. De fato, seja J um ideal tal que $p\mathbb{Z} \subsetneq J \subset \mathbb{Z}$. Pela proposição 3.28, J também é ideal principal, e assim $J = [m] = \{mz; z \in \mathbb{Z}\} = m\mathbb{Z}$. Segue que $p\mathbb{Z} \subsetneq m\mathbb{Z} \subset \mathbb{Z}$ e como $p \in p\mathbb{Z}$ então $p \in m\mathbb{Z}$ e desta forma, $p = mz$ para algum $z \in \mathbb{Z}$. Como p é primo, segue que $m = \pm p$ ou $m = \pm 1$. Mas se $m = \pm p$ então $p\mathbb{Z} = m\mathbb{Z} = J$ o que contradiz a hipótese de que $p\mathbb{Z} \subsetneq J$. Segue que $m = \pm 1$ e desta forma $J = m\mathbb{Z} = \mathbb{Z}$. Segue que $p\mathbb{Z}$ é ideal maximal.

Do teorema anterior, $\frac{\mathbb{Z}}{p\mathbb{Z}}$ é corpo. Como também do corolário 3.41, $\frac{\mathbb{Z}}{p\mathbb{Z}}$ é isomorfo a $\mathbb{Z}_p$, segue que $\mathbb{Z}_p$ é corpo. □

Definição 4.12. Um corpo $\mathbb{K}$ é dito um corpo primo se $\mathbb{K}$ não admite subcorpos além dos triviais, isto é, o único subcorpo de $\mathbb{K}$ é o próprio $\mathbb{K}$. Um subcorpo $\mathbb{S}$ de um corpo $\mathbb{K}$, é dito um subcorpo primo, se $\mathbb{S}$ é um corpo primo.

Teorema 4.13. *Se $\mathbb{K}$ é um corpo primo com característica p, então*

i) $\mathbb{K}$ é isomorfo a $\mathbb{Q}$, se $p = 0$,

ii) $\mathbb{K}$ é isomorfo a $\mathbb{Z}_p$, se $p > 0$.

Prova. Ver esta demonstração... □

4.2 Corpo das frações de um anel de integridade

O que faremos nesta seção é construir um corpo a partir de um anel de integridade. Para tal tarefa, necessitamos não somente construir um conjunto, mas também definir adequadamente operações neste conjunto, que o tornem um corpo.

Consideremos então, um anel de integridade $(A, *, \circ)$, e tomemos o conjunto $A \times A^*$ dos pares ordenados cuja segunda coordenada é um elemento não nulo de A. Isto é,

$$A \times A^* = \{(a, b); \quad a, b \in A, \quad b \neq 0_A\}.$$

Neste conjunto definimos a relação, denotada por $\simeq$, e definida por

$$(a, b) \simeq (c, d) \qquad \Leftrightarrow \qquad a \circ d = b \circ c.$$

Notemos que:

i) para qualquer $(a,b) \in A \times A^*$, como A é anel de integridade, A é comutativo para a operação $\circ$, e desta forma tem-se $a \circ b = b \circ a$ e da definição da relação, segue que $(a,b) \simeq (a,b)$, para todo $(a,b) \in A \times A^*$, mostrando que $\simeq$ é reflexiva.

ii) Dados (a,b) e (c,d) em $A \times A^*$ com $(a,b) \simeq (c,d)$, temos da definição que $a \circ d = b \circ c$ e como A é comutativo, temos que $c \circ b = d \circ a$, o que significa que $(c,d) \simeq (a,b)$, mostrando que $\simeq$ é simétrica.

iii) Se $(a,b),(c,d),(e,f) \in A \times A^*$ satisfazem $(a,b) \simeq (c,d)$ e $(c,d) \simeq (e,f)$, então $a \circ d = b \circ d$ e $c \circ f = d \circ e$. Assim,

$$a \circ f \circ d = a \circ d \circ f = b \circ c \circ f = b \circ d \circ e = b \circ e \circ d,$$

e como $d \neq 0_A$ então d é regular para a operação $\circ$, concluindo que $a \circ f = b \circ e$ e da definição da relação, tem-se que $(a,b) \simeq (e,f)$, mostrando que $\simeq$ é transitiva.

Dos fatos *i*), *ii*) e *iii*) temos que $\simeq$ é uma relação de equivalência em $A \times A^*$, e portanto estabelece uma forma de estimar quando dois elementos deste conjunto são equivalentes.

Desta forma, $\overline{(a,b)}$ representa a classe de equivalência do elemento $(a,b) \in A \times A^*$. Isto é, $\overline{(a,b)} = \{(x,y) \in A \times A^*; \quad (x,y) \simeq (a,b)\}$. Note que a expressão $\overline{(a,b)}$ denota um conjunto, e não um só elemento. $\overline{(a,b)}$ é o conjunto de todos os elementos que são equivalentes ao par (a,b), pela relação de equivalência $\simeq$.

Consideremos $\frac{A \times A^*}{\simeq}$, o conjunto de todas as classes de equivalência determinadas por $\simeq$, e denotemos este conjunto por $\mathbb{F}$. Então

$$\mathbb{F} = \left\{ \overline{(a,b)}; \quad a \in A, b \in A^* \right\}.$$

Este conjunto é denominado conjunto das frações de um anel de integridade. Esta nomenclatura, é natural no sentido de que podemos representar estes pares ordenados como frações da forma $(a,b) \equiv \frac{a}{b}$, com $b \neq 0_A$. Além disso, observe que a relação de equivalência definida acima, é a que estabelece a igualdade entre duas frações,

$$\frac{a}{b} = \frac{c}{d} \qquad \Leftrightarrow \qquad ad = cb.$$

Vamos agora dotar este conjunto de duas operações e mostraremos que com estas operações este conjunto tem estrutura de corpo. Observe que estas operações serão definidas exatamente como as operações usuais de soma e produto de frações no conjunto dos números reais.

Definimos em $\mathbb{F}$ as operações $+$ e $\cdot$, dadas por

$$\overline{(a,b)} + \overline{(x,y)} = \overline{(a \circ y * b \circ x, b \circ y)} \qquad \text{e} \qquad \overline{(a,b)} \cdot \overline{(x,y)} = \overline{(a \circ x, b \circ y)},$$

para quaisquer $\overline{(a,b)}, \overline{(x,y)} \in \mathbb{F}$. Observe que as operações envolvidas no segundo membro de cada igualdade, são as operações definidas no anel A.

Nosso primeiro trabalho é verificar que estas operações estão bem definidas. Como estamos fazendo operações com classes de equivalência, poderíamos perguntar se ao operarmos um elemento $\overline{(a,b)}$ podemos escolher qualquer um dos representantes desta classe, isto é, se $(a,b) \simeq (x,y)$ então $\overline{(a,b)} + \overline{(c,d)} = \overline{(x,y)} + \overline{(c,d)}$, qualquer que seja $\overline{(c,d)} \in \mathbb{F}$.

Proposição 4.14. *As operações $+$ e $\cdot$ definidas como acima, não dependem da escolha do representante das classes.*

Prova. Sejam $\overline{(a,b)}, \overline{(c,d)}, \overline{(x,y)}, \overline{(z,w)} \in \mathbb{F}$, tais que $(a,b) \simeq (x,y)$ e $(c,d) \simeq (z,w)$. Então, da definição de $\simeq$ temos $a \circ y = b \circ x$ e $c \circ w = d \circ z$. Assim, temos

$$\begin{aligned}(a \circ d * b \circ c) \circ (y \circ w) &= (a \circ d \circ y \circ w) * (b \circ c \circ y \circ w) \\ &= (a \circ y \circ d \circ w) * (b \circ y \circ c \circ w) \\ &= (b \circ x \circ d \circ w) * (b \circ y \circ d \circ z) \\ &= (x \circ w \circ b \circ d) * (y \circ z \circ b \circ d) = (x \circ w * y \circ z) \circ (b \circ d)\end{aligned}$$

e portanto $(a \circ d * b \circ c) \circ (y \circ w) = (x \circ w * y \circ z) \circ (b \circ d)$ e da definição da relação $(a \circ d * b \circ c, b \circ d) \simeq (x \circ w * y \circ z, y \circ w)$, isto é, $\overline{(a,b)} + \overline{(c,d)} = \overline{(x,y)} + \overline{(z,w)}$.

Para a multiplicação, temos então,

$$a \circ c \circ y \circ w = a \circ y \circ c \circ w = b \circ x \circ d \circ z = b \circ d \circ x \circ z,$$

donde segue da definição da relação, que $(a \circ c, b \circ d) \simeq (x \circ z, y \circ w)$, e então, $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(x,y)} \cdot \overline{(z,w)}$. Portanto as operações $+$ e $\cdot$ não dependem do representante escolhido para cada uma das classes envolvidas. □

Observe atentamente a definição do conjunto $\mathbb{F}$ e das operações $+$ e $\cdot$. Poderíamos perguntar, porque exigimos inicialmente que o anel A seja anel de integridade? Poderíamos construir corpo de frações de um anel qualquer? Da maneira que definimos o conjunto $\mathbb{F} = \{\overline{(a,b)} \in A \times A^*\}$, e suas operações, $+$ e $\cdot$, poderíamos ter problemas com o fechamento das duas operações em um anel qualquer. De fato, em $\overline{(a,b)} + \overline{(x,y)}$ e em $\overline{(a,b)} \cdot \overline{(x,y)}$ temos que $b \neq 0_A$ e também $y \neq 0_A$. Mas em um anel qualquer, não há garantias que $b \circ y \neq 0_A$ e então não há garantias de que a soma e o produto estejam em $A \times A^*$, ou seja, em um anel qualquer, a soma e o produto definidos como acima, podem não ser fechadas em $\mathbb{F}$.

Proposição 4.15. *O conjunto $(\mathbb{F}, +, \cdot)$, construído acima, é um corpo.*

Prova. Vamos mostrar que os axiomas da definição de corpo são todos satisfeitos. Dados quaisquer $\overline{(a,b)}, \overline{(x,y)}, \overline{(m,n)} \in \mathbb{F}$, temos

$$\begin{aligned}(\overline{(a,b)} + \overline{(x,y)}) + \overline{(m,n)} &= \overline{(a \circ y * b \circ x, b \circ y)} + \overline{(m,n)} \\ &= \overline{((a \circ y * b \circ x) \circ n * b \circ y \circ m, b \circ y \circ n)} \\ &= \overline{(a \circ y \circ n * b \circ x \circ n * b \circ y \circ m, b \circ y \circ n)} \\ &= \overline{(a \circ y \circ n * b \circ (x \circ n * y \circ m), b \circ y \circ n)} \\ &= \overline{(a,b)} \cdot \overline{(x \circ n * y \circ m, y \circ n)} = \overline{(a,b)} \cdot (\overline{(x,y)} \cdot \overline{(m,n)}),\end{aligned}$$

e também,

$$\begin{aligned}\overline{(a,b)} + \overline{(x,y)} &= \overline{(a \circ y * b \circ x, b \circ y)} \\ &= \overline{(x \circ b * y \circ a, y \circ b)} = \overline{(x,y)} + \overline{(a,b)},\end{aligned}$$

o que mostra que $+$ é associativa e comutativa.

Queremos agora obter $0_{\mathbb{F}} = \overline{(x,y)}$, tal que

$$\overline{(a,b)} + \overline{(x,y)} = \overline{(x,y)} + \overline{(a,b)} = \overline{(a,b)},$$

para todos $\overline{(a,b)} \in \mathbb{F}$. Nestes termos $x, y \in A$ devem satisfazer

$$\overline{(a \circ y * b \circ x, b \circ y)} = \overline{(a,b)},$$

ou equivalentemente

$$(a \circ y * b \circ x, b \circ y) \simeq (a,b).$$

Da definição da relação deve então ocorrer que

$$(a \circ y * b \circ x) \circ b = b \circ y \circ a,$$

e assim,

$$a \circ y \circ b * b \circ x \circ b = b \circ y \circ a,$$

donde

$$b \circ x \circ b = 0_A.$$

Mas como $b \neq 0_A$ e A é anel de integridade, então segue que $x = 0_A$. Deta forma, o elemento $\overline{(x,y)}$ procurado é precisamente $\overline{(x,y)} = \overline{(0_A,y)}$. A escolha de $y \in A^*$ é irrelevante, já que dados $y_1, y_2 \in A^*$, temos que $(0_A, y_1) \simeq (0_A, y_2)$ e portanto $\overline{(0_A,y_1)} = \overline{(0_A,y_2)}$.

Notemos então que dado qualquer $\overline{(a,b)} \in \mathbb{F}$ e $y \in A^*$, temos que

$$\begin{aligned} \overline{(a,b)} + \overline{(0_A,y)} &= \overline{(a \circ y * b \circ 0_A, b \circ y)} \\ &= \overline{(a \circ y, b \circ y)} = \overline{(a,b)}, \end{aligned}$$

já que $(a \circ y, b \circ y) \simeq (a,b)$. Sendo a adição comutativa, vale também que $\overline{(a,b)} + \overline{(0_A,y)} = \overline{(0_A,y)} + \overline{(a,b)} = \overline{(a,b)}$. Segue portanto que $0_{\mathbb{F}} = \overline{(0_A,y)}$ é o elemento neutro para a adição em $\mathbb{F}$, qualquer que seja $y \in A^*$. Observe ainda que

$$\overline{(x,y)} = 0_{\mathbb{F}} \qquad \text{se e somente se} \qquad x = 0_A.$$

Dado $\overline{(a,b)} \in \mathbb{F}$ arbitrário, queremos agora obter $-\overline{(a,b)} = \overline{(x,y)} \in \mathbb{F}$, de forma que

$$\overline{(a,b)} + \overline{(x,y)} = \overline{(x,y)} + \overline{(a,b)} = \overline{(0_A,m)},$$

sendo que $m \in A^*$. Os elementos $x, y \in A$ devem então satisfazer

$$\overline{(a \circ y * b \circ x, b \circ y)} = \overline{(0_A,m)},$$

ou ainda,

$$(a \circ y * b \circ x, b \circ y) \simeq (0_A, m),$$

e da definição da relação,

$$(a \circ y * b \circ x) \circ m = b \circ y \circ 0_A = 0_A.$$

Como $m \neq 0_A$ e A é anel de integridade, então temos que $a \circ y * b \circ x = 0_A$ ou ainda

$$x \circ b = b \circ x = -(a \circ y) = (-a) \circ y,$$

e da definição da relação $(x, y) \simeq (-a, b)$ e portanto $\overline{(x, y)} = \overline{(-a, b)} \in \mathbb{F}$.

O elemento $\overline{(-a, b)}$ cumpre portanto a igualdade

$$\overline{(a, b)} + \overline{(-a, b)} = \overline{(-a, b)} + \overline{(a, b)} = \overline{(0_A, b \circ b)} = 0_{\mathbb{F}},$$

donde todo $\overline{(a, b)} \in \mathbb{F}$ é simetrizável sendo o seu simétrico o elemento $-\overline{(a, b)} = \overline{(-a, b)}$. Podemos ver também que $\overline{(-a, b)} = \overline{(a, -b)}$, já que $(-a, b) \simeq (a, -b)$ e portanto

$$-\overline{(a, b)} = \overline{(-a, b)} = \overline{(a, -b)},$$

qualquer que seja $\overline{(a, b)} \in \mathbb{F}$.

Para a operação $\cdot$, sejam novamente $\overline{(a, b)}, \overline{(x, y)}, \overline{(m, n)} \in \mathbb{F}$ arbitrários. Então

$$\begin{aligned}
\Big(\overline{(a, b)} \cdot \overline{(x, y)}\Big) \cdot \overline{(m, n)} &= \overline{(a \circ x, b \circ y)} \cdot \overline{(m, n)} \\
&= \overline{((a \circ x) \circ m, (b \circ y) \circ n)} \\
&= \overline{(a \circ (x \circ m), b \circ (y \circ n))} \\
&= \overline{(a, b)} \cdot \overline{(x \circ m, y \circ n)} = \overline{(a, b)} \cdot \Big(\overline{(x, y)} \cdot \overline{(m, n)}\Big),
\end{aligned}$$

e também,

$$\overline{(a, b)} \cdot \overline{(x, y)} = \overline{(a \circ x, b \circ y)} = \overline{(x \circ a, y \circ b)} = \overline{(x, y)} \cdot \overline{(a, b)},$$

mostrando que $\cdot$ é também associativa e comutativa. Também,

$$\begin{aligned}
\overline{(a, b)} \cdot \Big(\overline{(x, y)} + \overline{(m, n)}\Big) &= \overline{(a, b)} \cdot \overline{(x \circ n * y \circ m, y \circ n)} \\
&= \overline{(a \circ (x \circ n * y \circ m), b \circ (y \circ n))} \\
&= \overline{(a \circ x \circ n * a \circ y \circ m, b \circ y \circ n)} \\
&= \overline{(b \circ (a \circ x \circ n * a \circ y \circ m), b \circ b \circ y \circ n)} \\
&= \overline{(a \circ x \circ b \circ n * b \circ y \circ a \circ m, b \circ y \circ b \circ n)} \\
&= \overline{(a \circ x, b \circ y)} + \overline{(a \circ m, b \circ n)} \\
&= \Big(\overline{(a, b)} \cdot \overline{(x, y)}\Big) + \Big(\overline{(a, b)} \cdot \overline{(m, n)}\Big),
\end{aligned}$$

donde a multiplicação é distributiva em relação à adição pela esquerda. Também vale a distributividade pela direita em virtude da comutatividade da multiplicação. Segue que $\cdot$ é distributiva em relação a $+$.

Para mostrar que $\mathbb{F}$ possui unidade, queremos obter $1_{\mathbb{F}} = \overline{(x, y)} \in \mathbb{F}$ de forma que

$$\overline{(a, b)} \cdot \overline{(x, y)} = \overline{(x, y)} \cdot \overline{(a, b)} = \overline{(a, b)},$$

para todo $\overline{(a, b)} \in \mathbb{F}$. Os elementos $x, y \in A$ devem então satisfzer

$$\overline{(a \circ x, b \circ y)} = \overline{(a, b)},$$

e portanto

$$(a \circ x, b \circ y) \simeq (a, b),$$

e da definição da relação segue que $a \circ x \circ b = b \circ y \circ a$. Como $b \neq 0_A$ e A é anel de integridade então segue que $a \circ x = y \circ a$, e novamente da definição da relação $(x, y) \simeq (a, a)$ donde $\overline{(x, y)} = \overline{(a, a)}$. Evidentemente esta escolha para $\overline{(x, y)}$ só pode ser feita quando $a \neq 0_A$. O caso em que $a = 0_A$ não afeta a procura por $\overline{(x, y)}$ já que no caso em que $a = 0_A$, então $\overline{(0_A, b \circ y)} = \overline{(0_A, y)}$, já que $(0_A, b \circ y) \simeq (0_A, y)$, e desta forma é imediato que

$$\overline{(0_A, b)} \cdot \overline{(x, y)} = \overline{(0_A \circ x, b \circ y)} = \overline{(0_A, b \circ y)} = \overline{(0_A, y)},$$

para qualquer escolha de $\overline{(x, y)}$.

Desta forma, para qualquer $n \in A^*$ podemos verificar que $\overline{(n, n)} \in \mathbb{F}$ cumpre

$$(a \circ n, b \circ n) \simeq (a, b),$$

e portanto

$$\overline{(a, b)} \cdot \overline{(n, n)} = \overline{(a \circ n, b \circ n)} = \overline{(a, b)},$$

para todo $\overline{(a, b)} \in \mathbb{F}$. Da comutatividade da multiplicação, segue também que $\overline{(n, n)} \cdot \overline{(a, b)} = \overline{(a, b)}$. Portanto a unidade em $\mathbb{F}$ é o elemento $1_{\mathbb{F}} = \overline{(n, n)}$ qualquer que seja $n \in A^*$.

Resta mostrar que todo elemento não nulo de $\mathbb{F}$ é invertível. Consideremos então $\overline{(a, b)} \in \mathbb{F}$ com $\overline{(a, b)} \neq 0_{\mathbb{F}}$ e portanto $a \neq 0_A$. Queremos obter $\overline{(a, b)}^{-1} = \overline{(x, y)} \in \mathbb{F}$ de forma que

$$\overline{(a, b)} \cdot \overline{(x, y)} = \overline{(x, y)} \cdot \overline{(a, b)} = 1_{\mathbb{F}} = \overline{(n, n)}.$$

Os elementos $x, y \in A$ devem então satisfazer

$$\overline{(a \circ x, b \circ y)} = \overline{(n, n)},$$

ou ainda

$$(a \circ x, b \circ y) \simeq (n, n),$$

e da definição da relação temos que $a \circ x \circ n = b \circ y \circ n$. Como $n \neq 0_A$ e A é anel de integridade, então segue que $a \circ x = b \circ y$, e da definição da relação $(x, y) \simeq (b, a)$. Desta forma,

$$\overline{(x, y)} = \overline{(b, a)},$$

e como $a \neq 0_A$, então $\overline{(b, a)} \in \mathbb{F}$. Podemos então ver que dado $\overline{(a, b)} \in \mathbb{F}$ com $a \neq 0_A$, então $\overline{(b, a)} \in \mathbb{F}$ cumpre

$$\overline{(a, b)} \cdot \overline{(b, a)} = \overline{(a \circ b, b \circ a)} = \overline{(a \circ b, a \circ b)} = 1_{\mathbb{F}}.$$

Da comutatividade da operação $\cdot$ temos também que $\overline{(b, a)} \cdot \overline{(a, b)} = 1_{\mathbb{F}}$. Segue que todo elemento não nulo $\overline{(a, b)} \in \mathbb{F}$ é invertível sendo $\overline{(b, a)} \in \mathbb{F}$ o seu inverso, isto é, $\overline{(a, b)}^{-1} = \overline{(b, a)}$. □

Decorre portanto, que $(\mathbb{F}, +, \cdot)$ tem estrutura de corpo. O corpo $\mathbb{F}$ é então chamado de corpo das frações do anel de integridade A. Por este motivo, é comum representar os elementos

de $\mathbb{F}$ como frações, e não como pares ordenados. De qualquer forma, é só a notação que muda, isto é,

$$\frac{a}{b} \equiv (a,b) \qquad \text{para quaisquer} \quad a \in A, b \in A^*.$$

Como complemento desta seção, mostraremos que A é isomorfo um subconjunto de $\mathbb{F}$. Consideremos o subconjunto $\mathbb{S}$ de $\mathbb{F}$, dado por

$$\mathbb{S} = \left\{ \overline{(a,1_A)}; \quad a \in A \right\} \subset \mathbb{F}.$$

O conjunto $\mathbb{S}$ é não vazio, e além disso para quaisquer $\overline{(a,1_A)}, \overline{(b,1_A)} \in \mathbb{S}$, temos

$$\overline{(a,1_A)} - \overline{(b,1_A)} = \overline{(a,1_A)} + \overline{(-b,1_A)} = \overline{(a \circ 1_A * (-b) \circ 1_A, 1_A \circ 1_A)} = \overline{(a-b,1_A)} \in \mathbb{S},$$

e também,

$$\overline{(a,1_A)} \cdot \overline{(b,1_A)} = \overline{(a \circ b, 1_A \circ 1_A)} = \overline{(a \circ b, 1_A)} \in \mathbb{S},$$

e portanto o conjunto $\mathbb{S}$ é subanel do anel $\mathbb{F}$. Logo $\mathbb{S}$ é também um anel (de integridade pois é subanel de um corpo). O subanel $\mathbb{S}$ é unitário, pois $1_{\mathbb{S}} = \overline{(1_A,1_A)} = 1_{\mathbb{F}}$.

Consideremos a aplicação $\varphi : A \to \mathbb{S}$, dada por

$$\begin{array}{rcl} \varphi : A & \to & \mathbb{S} \\ a & \mapsto & \varphi(a) = \overline{(a,1_A)}. \end{array}$$

Vamos verificar que trata-se de um isomorfismo entre anéis. Sejam $a, b \in A$, então

$$\varphi(a*b) = \overline{(a*b,1_A)} = \overline{(a \circ 1_A * b \circ 1_A, 1_A \circ 1_A)} = \overline{(a,1_A)} + \overline{(b,1_A)} = \varphi(a) + \varphi(b)$$
$$\varphi(a \circ b) = \overline{(a \circ b,1_A)} = \overline{(a \circ b, 1_A \circ 1_A)} = \overline{(a,1_A)} \cdot \overline{(b,1_A)} = \varphi(a) \cdot \varphi(b)$$

e assim φ é homomorfismo entre anéis. Também, φ é claramente uma aplicação sobrejetora, pois para todo $y = \overline{(a,1_A)} \in \mathbb{S}$, tome $x = a \in A$ e segue que $\varphi(x) = \varphi(a) = \overline{(a,1_A)} = y$. Para finalizar, suponha $a, b \in A$ com $\varphi(a) = \varphi(b)$. Então $\overline{(a,1_A)} = \overline{(b,1_A)}$ e da igualdade das classes $(a,1_A) \simeq (b,1_A)$, e da definição da relação $a \circ 1_A = 1_A \circ b$, isto é, $a = b$, o que mostra a injetividade de φ, e portanto $A \approx \mathbb{S}$. Neste caso, dizemos que existe uma cópia de A em $\mathbb{F}$, ou que A está imerso (mergulhado) em $\mathbb{F}$.

O processo que acabamos de fazer é exatamente o processo utilizado para a construção do corpo dos racionais. Se considerarmos o anel $\mathbb{Z}$ dos inteiros, definimos os elementos (frações) do conjunto dos racionais $\mathbb{Q}$ e também operações entre tais frações, que possuem as propriedades que tornam o conjunto $\mathbb{Q}$ um corpo. Além disso como já é sabido, o conjunto dos racionais contém o conjunto dos inteiros, e é o que mostramos na segunda parte, que um subconjunto dos racionais, é isomorfo ao anel dos inteiros. São exatamente os racionais com denominador igual a 1.

4.3 Polinômios em um corpo

Na seção 3.6 já estudamos alguns resultados sobre polinômios com coeficientes em um anel, ou até mesmo, em anéis de integridade. Nesta seção vamos considerar polinômios com

coeficientes em um corpo $\mathbb{K}$. Já que um corpo é um anel de integridade, os resultados da seção 3.6 continuam válidos. Todavia, certos resultados podem ser melhorados e outros ainda podem ser obtidos quando consideramos os coeficientes do polinômio em um corpo.

Seja então $(\mathbb{K}, *, \circ)$ um corpo. O conjunto dos polinômios com coeficientes em $\mathbb{K}$ será denotado por $\mathbb{K}[X]$ e assim

$$f = a_0 + a_1 \cdot X + a_2 \cdot X^2 + \cdots + a_n \cdot X^n \in \mathbb{K}[X]$$

se e somente se $a_i \in \mathbb{K}$ para todos $0 \leq i \leq n$. Também $X = (0_{\mathbb{K}}, 1_{\mathbb{K}}, 0_{\mathbb{K}}, 0_{\mathbb{K}}, \dots)$.

Do que já vimos até agora, $\mathbb{K}[X]$ é anel de integridade. Cuidado! Embora $\mathbb{K}$ seja corpo, $\mathbb{K}[X]$ não é corpo. Isto é fácil de ser verificado. Também em $\mathbb{K}[X]$ vale o algoritmo da divisão, com quociente e resto unicamente determinados. Dados dois polinômios f e g em $\mathbb{K}[X]$, dizemos que f divide g, ou que f é um divisor de g, ou ainda que g é um múltiplo de f, se existe um $h \in \mathbb{K}[X]$ tal que

$$g = f \cdot h = h \cdot f.$$

Note que neste caso, o resto da divisão de g por f é $0_{\mathbb{K}[X]}$. Escrevemos ainda $f|g$ para dizer que f divide g.

Definição 4.16. Dados f e g polinômios ambos não nulos em $\mathbb{K}[X]$, então dizemos que $d \in \mathbb{K}[X]$ é um máximo divisor comum de f e g, se

i) $d|f$ e $d|g$, e

ii) Se $d_0 \in \mathbb{K}[X]$ satisfaz $d_0|f$ e $d_0|g$ então $d_0|d$.

Observe atentamente a expressão "d é **um** máximo divisor". Um fato importantíssimo, é que se existe um máximo divisor comum de f e g ele não é único. Para qualquer $k \in \mathbb{K}^*$, teremos que $k \cdot d \in \mathbb{K}[X]$ também será máximo divisor comum de f e g. De fato, suponha d um máximo divisor de f e g, e $k \in \mathbb{K}^*$ arbitrário. Então, k é invertível, e

$$d|f \quad \Rightarrow \quad f = h \cdot d \quad \Rightarrow \quad f = (k^{-1} \cdot h) \cdot (k \cdot d),$$

donde $(k \cdot d)|f$. Da mesma forma, mostra-se que $(k \cdot d)|g$. Suponha agora, $d_0|f$ e $d_0|g$. Então do item *ii*) da definição de máximo divisor comum, $d_0|d$ e assim,

$$d_0|d \quad \Rightarrow \quad d = h \cdot d_0 \quad \Rightarrow \quad (k \cdot d) = (k \cdot h) \cdot d_0,$$

ou seja, $d_0|(k \cdot d)$, e então $(k \cdot d)$ satisfaz também os dois axiomas que o definem como um máximo divisor comum entre f e g.

Como vimos então, existem muitos "máximos divisores" entre dois polinômios f e g. Outro fato importantíssimo, é que se d_0 e d_1 são dois máximos divisores comuns a f e g, então d_0 e d_1 diferem apenas por alguma constante não nula em $\mathbb{K}$, isto é, $d_0 = k \cdot d_1$ para $k \in \mathbb{K}^*$. De fato, do item *ii*) da definição de máximo divisor comum, temos que $d_0|d_1$, e então $d_1 = h_1 \cdot d_0$, com $gr(d_0) \leq gr(d_1)$. Por outro lado, pelo mesmo item *ii*) da definição, temos que $d_1|d_0$, e da mesma forma, $d_0 = h_2 \cdot d_1$, com $gr(d_1) \leq gr(d_0)$. Segue que $gr(d_0) = gr(d_1)$ e por conseguinte $gr(h_2) = gr(h_1) = 0$ e então h_1 e h_2 são polinômios constantes (e não nulos). Segue a nossa afirmação. Existe $k \in \mathbb{K}^*$, tal que, $d_0 = k \cdot d_1$.

Definição 4.17. Dado um polinômio f em $\mathbb{K}[X]$, com $gr(f) \geq 1$, dizemos que f é redutível sobre o corpo $\mathbb{K}$, ou redutível em $\mathbb{K}[X]$, se existem dois polinômios g e h, ambos em $\mathbb{K}[X]$ e não nulos, com $gr(h) \geq 1$ e $gr(g) \geq 1$ e satisfazendo

$$f = g \cdot h = h \cdot g.$$

Se a igualdade só puder ser cumprida com polinômios g ou h constantes, isto é, onde $gr(g) = 0$ ou $gr(h) = 0$, então f é dito irredutível sobre $\mathbb{K}$.

O produto $g \cdot h$ é dito uma decomposição para f, e os termos g e h são ditos fatores da decomposição. Observe que esta ideia é semelhante à ideia de decomposição de números inteiros em fatores. Além disso os polinômios irredutíveis fazem o papel dos números primos, que só aceitam decomposição se um dos fatores for igual a ± 1. A ideia de irredutibilidade de polinômios pode ser formulada também para polinômios com coeficientes em um anel. Mas foi só agora enunciada, pois sua maior importância se dará deste ponto em diante.

Notemos também que se um polinômio $f \in \mathbb{K}[X]$, com $gr(f) \geq 2$, possui uma raiz $u \in \mathbb{K}$ então f é redutível em $\mathbb{K}[X]$. De fato, como provamos em (3.68) f é divisível por $(X - u)$ que por sua vez é um polinômio em $\mathbb{K}[X]$ também. Da divisibilidade decorre que $f = h \cdot (X - u)$. Como $gr(f) \geq 2$ e $gr(X - u) = 1$ temos que $gr(h) \geq 1$. E portanto f é redutível em $\mathbb{K}[X]$.

Exemplo 4.3. O polinômio $f(X) = 2 - X + 5X^2 + 3X^3$, é redutível em $\mathbb{Z}[X]$, pois

$$f(X) = 2 - X + 5X^2 + 3X^3 = (2 + X) \cdot (1 - X + 3X^2) = g(X) \cdot h(X),$$

com $gr(g) = 1 > 0$ e $gr(h) = 2 > 0$. ■

Exemplo 4.4. O polinômio $f = 1 + X^2$ em $\mathbb{R}[X]$ é irredutível. De fato, se f fosse redutível, deveriam existir dois polinômios g e h ambos de grau 1, tais que $f = g \cdot h$, isto é, $X^2 + 1 = (X + a) \cdot (X + b)$ onde $a, b \in \mathbb{R}$. Uma multiplicação simples no segundo membro mostrará que $(a + b) = 0$ e $a \cdot b = 1$. Ou ainda $a = -b$ e depois $-b^2 = 1$. Tal número b não existe em $\mathbb{R}$. ■

Exemplo 4.5. O polinômio $f = -2 + X^2$, em $\mathbb{Q}[X]$, é também irredutível, pois se $f = g \cdot h$ for uma decomposição de f, devemos ter $gr(g) = gr(h) = 1$. Desta forma, $-2+X^2 = (X+a)\cdot(X+b)$ onde $a, b \in \mathbb{Q}$. Multiplicando o segundo membro, e igualando com o primeiro, devemos ter $(a + b) = 0$ e também $a \cdot b = -2$. Decorre que $a = -b$ e depois $-b^2 = -2$, donde $b = -a = \sqrt{2}$. Então $f = X^2 - 2 = (X + \sqrt{2}) \cdot (X - \sqrt{2})$. O problema é que $\sqrt{2} \notin \mathbb{Q}$. ■

Um fato que tem bastante importância, é saber quando um polinômio é irredutível sobre um determinado corpo $\mathbb{K}$. Vários são os métodos para determinar isto. Apresentaremos alguns métodos que podem decidir sobre a irredutibilidade de um polinômio. Alguns destes métodos podem ser de aplicação não tão imediatas.

Teorema 4.18 (Critério de Eisenstein)**.** *Seja $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, um polinômio de grau n em $\mathbb{Z}[X]$. Se existir um número primo p, tal que*

i) $p \nmid a_n$,

ii) $p | a_i$, para todos $0 \leq i < n$, e

iii) $p^2 \nmid a_0$,

então f é irredutível sobre $\mathbb{Z}$.

Prova. Seja p, um número primo, satisfazendo $(i) - (iii)$. Suponha que f seja decomposto no produto

$$f = g \cdot h = (b_0 + b_1X + b_2X^2 + \cdots + b_rX^r) \cdot (c_0 + c_1X + c_2X^2 + \cdots + c_sX^s),$$

com $r + s = n$, e g e h não nulos. Mostraremos que $s = 0$ ou que $r = 0$.

Temos então que $a_0 = b_0 \cdot c_0$. Como $p|a_0$, então $p|b_0$ ou $p|c_0$ mas não ambos simultaneamente, pois $p^2 \nmid a_0$. Suponhamos sem perda de generalidade que $p|b_0$ e $p \nmid c_0$. Por outro lado, $p \nmid a_n = b_r \cdot c_s$ e assim, $p \nmid b_r$ e também $p \nmid c_s$. Considere j o menor índice tal que $p \nmid b_j$ e $p|b_{j-1}, b_{j-2}, \ldots, b_0$. Observe que tal índice j existe, e $1 \leq j \leq r$. Sendo assim, para este índice j, teremos

$$a_j = b_0 \cdot c_j + b_1 \cdot c_{j-1} + \cdots + b_{j-1} \cdot c_1 + b_j \cdot c_0.$$

O número p divide todos os termos da soma acima, pois $p|b_{j-1}, b_{j-2}, \ldots, b_0$, com exceção do último, pois p é primo, e $p \nmid b_j$ e $p \nmid c_0$. Por consequência disto, $p \nmid a_j$. Mas pelo item $ii)$, temos que $j = n$. Mas como $j \leq r \leq n$, temos que obrigatoriamente $r = n$. Segue que $s = 0$, e então pela definição, f é irredutível. □

Apesar de ser um importante critério de irredutibilidade, estamos interessados em irredutibilidade sobre corpos, e $\mathbb{Z}$ não é corpo. O Critério de Eisenstein, e o próximo resultado, formam um dupla incrível.

Teorema 4.19 (Teorema de Gauss)**.** *Se um polinômio $f \in \mathbb{Z}[X]$ é irredutível sobre $\mathbb{Z}$, então f será também irredutível sobre $\mathbb{Q}$.*

Prova. Ver isto depois... □

Colocar alguns exemplos....

Já mencionamo que a ideia de decomposição de polinômios está associada à ideia de decomposição de números inteiros, sendo que os polinômios irredutíveis fazem o papel de números primos. Lembremos que já mostramos anteriormente que todo ideal de $\mathbb{Z}$ é principal, e se p é um número primo então $[p]$ é ideal maximal, e também $\frac{\mathbb{Z}}{[p]} = \frac{\mathbb{Z}}{p\mathbb{Z}}$ é corpo. Vamos agora mostrar resultados similares para ideais em $\mathbb{K}[X]$. Lembremos primeiro que um ideal I de $\mathbb{K}[X]$ será ideal principal se for gerado por apenas um elemento de $\mathbb{K}[X]$, isto é, existe $p(X) \in \mathbb{K}[X]$ de forma, que

$$I = [p] = \{p(X) \cdot f(X); \quad f(X) \in \mathbb{K}[X]\}.$$

Lema 4.20. *Se $(\mathbb{K}, *, \circ)$ é um corpo, todo ideal de $\mathbb{K}[X]$ é principal.*

Prova. Seja $I \subset K[X]$ um ideal. Se $I = \{0_{\mathbb{K}[X]}\}$ então é imediato que I é principal pois será gerado pelo elemento neutro $0_{\mathbb{K}[X]}$, isto é,

$$I = \{0_{\mathbb{K}[X]}\} = \{0_{\mathbb{K}[X]} \cdot q(X);\ q(X) \in \mathbb{K}[X]\} = [0_{\mathbb{K}[X]}].$$

Se por outro lado, $I \neq \{0_{\mathbb{K}[X]}\}$ então existem polinômios não nulos em I. Seja $p(X)$ o polinômio de menor grau em I. Mostraremos que $I = [p]$.

Seja $f(X) \in I$. Então do algoritmo da divisão temos que existem $q(X), r(X) \in \mathbb{K}[X]$ de forma que

$$f(X) = p(X) \cdot q(X) + r(X),$$

com $r(X) = 0_{\mathbb{K}[X]}$ ou $gr(r) < gr(p)$. Mas desta forma, $r(X) = f(X) - p(X) \cdot q(X)$ e como $p(X) \in I$ então $p(X) \cdot q(X) \in I$ já que I é ideal. Como também $f(X) \in I$ então $r(X) \in I$. Então não podemos ter $gr(r) < gr(p)$ pois $p(X)$ é o polinômio de menor grau em I. Segue que $r(X) = 0_{\mathbb{K}[X]}$ e assim segue que $f(X) = p(X) \cdot q(X) \in [p]$.

Suponha agora $f(X) \in [p]$. Então temos imediatamente que $f(X) = p(X) \cdot q(X) \in I$ já que $p(X) \in I$ e I é ideal. Isto termina esta prova. □

Teorema 4.21. *Seja* $(\mathbb{K}, *, \circ)$ *um corpo e* $p(X) \in \mathbb{K}[X]$ *não nulo.* p *é irredutível sobre* $\mathbb{K}$*, se e somente se,* $I = [p]$ *for ideal maximal em* $\mathbb{K}[X]$*.*

Prova. Suponha inicialmente p irredutível sobre $\mathbb{K}$, e o ideal $I = [p]$. Suponha que J é outro ideal de $\mathbb{K}[X]$, com $I \subset J \subset \mathbb{K}[X]$. Mostraremos que $J = I$, ou $J = \mathbb{K}[X]$.

Do lema anterior, J é ideal principal, e então $J = [h]$, para algum $h \in \mathbb{K}[X]$. Sabemos que

$$p \in [p] = I \subset J = [h].$$

Desta forma, $p(X) = h(X) \cdot g(X)$, para algum $g \in \mathbb{K}[X]$. Como p é irredutível, então $g(X)$ ou $h(X)$ é um polinômio constante não nulo de $\mathbb{K}[X]$. Isto é, $g(X) = a$ com $a \in \mathbb{K}^*$ ou $h(X) = b$ com $b \in \mathbb{K}^*$. Se $g(X) = a$ com $a \neq 0_{\mathbb{K}}$, então teremos $I = J$. De fato $p(X) = h(X) \cdot a$, e então, $h(X) = (a^{-1}) \cdot p(X)$, donde $[h] \subset [p]$, isto é, $J \subset I$ e portanto $I = J$. Se por outro lado, $h(X) = b$ com $b \neq 0_{\mathbb{K}}$, então teremos $\mathbb{K}[X] = J$. De fato dado qualquer $f(X) \in \mathbb{K}[X]$ temos que $f(X) = b \cdot (b^{-1}) \cdot f(X) = h(X) \cdot (b^{-1} \cdot f(X)) \in [h]$, isto é, $\mathbb{K}[X] \subset [h] = J$ e portanto $\mathbb{K}[X] = J$. Isto prova a maximalidade de I.

Reciprocamente, suponha que $I = p \cdot \mathbb{K}[X]$ é ideal maximal de $\mathbb{K}[X]$. Sejam $h(X)$ e $g(X)$ polinômios não nulos em $\mathbb{K}[X]$ tais que $p(X) = h(X) \cdot g(X)$. Mostraremos que $g(X)$ ou $h(X)$ é constante.

Primeiramente, observemos que como $p(X) = h(X) \cdot g(X)$, então $I = [p] \subset [h] \subset \mathbb{K}[X]$. Como I é maximal, teremos $[h] = I$, ou $[h] = \mathbb{K}[X]$.

Se $[h] = I$, então $h \in [h] = I = [p]$, e então $h(X) = p(X) \cdot k(X)$ para algum $k \in \mathbb{K}[X]$. Desta forma, $p(X) = g(X) \cdot h(X) = g(X) \cdot p(X) \cdot k(X)$, e como $p(X)$ é não nulo, segue que $1_{\mathbb{K}[X]} = g(X) \cdot k(X)$, pois $\mathbb{K}[X]$ é anel de integridade. Mais ainda, como $gr(1_{\mathbb{K}[X]}) = 0$ decorre que $gr(g) = gr(k) = 0$. Disto, temos que $g(X)$ é constante, e não nulo.

Se por outro lado, $[h] = \mathbb{K}[X]$, então todo $k \in \mathbb{K}[X] = [h]$ é da forma $k(X) = h(X) \cdot g(X)$ com $g(X)$ ainda em $\mathbb{K}[X]$. Em particular, isto deve valer para $k(X)$ constante (não nulo). Desta forma a igualdade só será possível se $h(X)$ for constante também, e não nulo.

Segue que se $p(X) = h(X) \cdot g(X)$ então h ou g é constante. Portanto $p(X)$ é irredutível, em $\mathbb{K}[X]$. □

O próximo corolário é consequência imediata deste último teorema e do teorema 4.10. É o corolário similar do corolário 4.11 em $\mathbb{K}[X]$.

Corolário 4.22. *Seja* $(\mathbb{K}, *, \circ)$ *um corpo e* $p \in \mathbb{K}[X]$ *não nulo.* p *é irredutível sobre* $\mathbb{K}$ *se e somente se* $\frac{\mathbb{K}[X]}{[p]}$ *for corpo.*

Teorema 4.23 (Princípio da Fatoração Única)**.** *Seja* $\mathbb{K}$ *um corpo e* f *um polinômio em* $\mathbb{K}[X]$*. Então* f *pode ser decomposto da forma*

$$f = a \cdot h_1 \cdot h_2 \cdot \cdots \cdot h_n,$$

sendo $a \in \mathbb{K}$ *uma constante e* $h_i \in \mathbb{K}[X]$ *fatores irredutíveis, unitários e não constantes em* $\mathbb{K}[X]$*. Mais ainda, esta decomposição é única, a menos de uma constante ou de permutações nos fatores* h_i*.*

Prova. Ver isto depois... Adilson pg 79. □

4.4 Extensão de corpos

Nesta seção, estamos interessados, em construir corpos, a partir de corpos já conhecidos, pela adjunção de elementos. Este é um método interessante para construirmos novos corpos, e estamos particularmente interessados em obter corpos $\mathbb{K}$, de forma que, $\mathbb{Q} \subsetneq \mathbb{K} \subsetneq \mathbb{R}$, isto é, corpos que estão entre os racionais e os reais. O corpo dos complexos é igualmente interessante, mas como veremos mais adiante, não existem outros corpos entre os reais e os complexos. Entenda-se que não existem corpos $\mathbb{K}$, tais que, $\mathbb{R} \subsetneq \mathbb{K} \subsetneq \mathbb{C}$.

Definição 4.24. Dado um corpo $\mathbb{K}$, qualquer corpo $\mathbb{L}$, que contém um subcorpo isomorfo a $\mathbb{K}$, é chamado de extensão do corpo $\mathbb{K}$. Neste caso, escrevemos $\mathbb{L} : \mathbb{K}$ para denotar que $\mathbb{L}$ é extensão de $\mathbb{K}$.

É claro que se $\mathbb{K} \subset \mathbb{L}$ então é imediato que $\mathbb{L}$ possui um subcorpo isomorfo a $\mathbb{K}$, que é o próprio $\mathbb{K}$. Portanto, se $\mathbb{K} \subset \mathbb{L}$ então $\mathbb{L}$ é imediatamente uma extensão de $\mathbb{K}$. Com o intuito de facilitar a notação, só para não precisarmos trabalhar com o isomorfismo entre $\mathbb{K}$ e o subcorpo de $\mathbb{L}$ isomorfo a $\mathbb{K}$ a que se refere a última definição, vamos considerar deste ponto em diante que $\mathbb{K} \subset \mathbb{L}$.

Definição 4.25. Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos com $\mathbb{K} \subset \mathbb{L}$, isto é, $\mathbb{L} : \mathbb{K}$. Um elemento $u \in \mathbb{L}$, é dito algébrico sobre $\mathbb{K}$ se, e somente se, existe um polinômio não nulo em $f \in \mathbb{K}[X]$ de forma que $f(u) = 0_{\mathbb{K}} = 0_{\mathbb{L}}$, isto é, u é raiz de f. Se u não é algébrico sobre $\mathbb{K}$, então dizemos que u é transcendente sobre $\mathbb{K}$.

Observe que se u é transcendente sobre $\mathbb{K}$, ou equivalentemente u não é algébrico sobre $\mathbb{K}$, então de acordo com a definição anterior, não existem polinômios não nulos em $\mathbb{K}[X]$, tais que $f(u) = 0_{\mathbb{K}} = 0_{\mathbb{L}}$. Portanto, quando u é transcendente sobre $\mathbb{K}$, então $f(u) = 0_{\mathbb{K}} = 0_{\mathbb{L}}$, se e somente se, $f = 0_{\mathbb{K}[X]}$ é o polinômio nulo.

É imediato também da definição que todo $u \in \mathbb{K} \subset \mathbb{L}$ é algébrico sobre $\mathbb{K}$.

Definição 4.26. Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos com $\mathbb{K} \subset \mathbb{L}$ e $u \in \mathbb{L}$. Definimos $\mathbb{K}[u]$ como sendo o conjunto dos valores $f(u)$ para quaisquer polinômios f em $\mathbb{K}[X]$, isto é,

$$\mathbb{K}[u] = \{f(u); \quad f \in \mathbb{K}[X]\} \subset \mathbb{L}.$$

É fácil verificar que $\mathbb{K} \subset \mathbb{K}[u] \subset \mathbb{L}$. Além disso, se $u \in \mathbb{K}$ então $\mathbb{K}[u] = \mathbb{K}$. Nossa preocupação agora é estabelecer quando $\mathbb{K}[u]$ é corpo. Isto está diretamente ligado ao nosso objetivo de encontrar corpos $\mathbb{S}$ tais que $\mathbb{Q} \subset \mathbb{S} \subset \mathbb{R}$. O que podemos garantir é que o conjunto $\mathbb{K}[u]$ é anel de integridade, e só será corpo quando u for algébrico sobre $\mathbb{K}$. Os próximos dois teoremas garantem isto.

Teorema 4.27. *Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos com $\mathbb{K} \subset \mathbb{L}$, e $u \in \mathbb{L}$. Se u é algébrico sobre $\mathbb{K}$ então $\mathbb{K}[u]$ é corpo.*

Prova. Consideremos a aplicação

$$\begin{aligned} \varphi : \mathbb{K}[X] &\to \mathbb{L} \\ f &\mapsto \varphi(f) = f(u). \end{aligned}$$

Nestes termos dados $f, g \in \mathbb{K}[X]$ arbitrários, temos

$$\varphi(f+g) = (f+g)(u) = f(u) * g(u) = \varphi(f) * \varphi(g),$$

e também

$$\varphi(f \cdot g) = (f \cdot g)(u) = f(u) \circ g(u) = \varphi(f) \circ \varphi(g),$$

e assim, φ é um homomorfismo. Segue do Teorema Fundamental do Homomorfismo (de anéis) que

$$\frac{\mathbb{K}[X]}{Ker(\varphi)} \approx Im(\varphi).$$

O que precisamos agora é determinar $Ker(\varphi)$ e $Im(\varphi)$. Primeiro temos que

$$Ker(\varphi) = \{f \in \mathbb{K}[X]; \quad \varphi(f) = 0_{\mathbb{L}}\} = \{f \in \mathbb{K}[X]; \quad f(u) = 0_{\mathbb{L}}\}.$$

Seja p o polinômio em $\mathbb{K}[X]$ de menor grau tal que $p(u) = 0_{\mathbb{L}}$. Tal polinômio existe pois u é algébrico sobre $\mathbb{K}$. Mostraremos que $Ker(\varphi) = [p]$.

Para a primeira inclusão, seja $f \in Ker(\varphi)$, isto é, $\varphi(f) = 0_{\mathbb{L}}$ e então $f(u) = 0_{\mathbb{L}}$. Do algoritmo da divisão, existem $q(X), r(X) \in \mathbb{K}[X]$ tais que $f(X) = q(X) \cdot p(X) + r(X)$, com $r(X) = 0_{\mathbb{K}[X]}$ ou $gr(r) < gr(p)$. Mas notemos que $r(u) = f(u) - q(u) \cdot p(u) = 0_{\mathbb{L}}$, pois $f(u) = p(u) = 0_{\mathbb{L}}$. Desta forma, não podemos ter $gr(r) < gr(p)$ pois p é o polinômio de menor grau tal que $p(u) = 0_{\mathbb{L}}$. Segue que $r(X) = 0_{\mathbb{K}[X]}$ e sendo assim, $f(X) = p(X) \cdot q(X) \in [p]$.

Para a segunda inclusão, seja $f \in [p]$, isto é, $f(X) = p(X) \cdot h(X)$ para algum $h(X) \in \mathbb{K}[X]$. Então, $\varphi(f) = f(u) = (p \cdot h)(u) = p(u) \circ h(u) = 0_{\mathbb{L}} \circ h(u) = 0_{\mathbb{L}}$, e portanto $f \in Ker(\varphi)$. Segue que $Ker(\varphi) = [p]$.

Observemos ainda que o fato de p ser o polinômio de menor grau tal que $p(u) = 0_{\mathbb{L}}$ significa que p é irredutível sobre $\mathbb{K}$. De fato, procedendo contrapositivamente, se p for redutível sobre $\mathbb{K}$, então $p(X) = g(X) \cdot h(X)$ com $g(X), h(X) \in \mathbb{K}[X]$ e $1 \leq gr(g), gr(h) < gr(p)$. Desta

forma, $0_{\mathbb{L}} = p(u) = g(u) \circ h(u)$ e sendo $\mathbb{K}$ um anel de integridade segue que $g(u) = 0_{\mathbb{L}}$ ou $h(u) = 0_{\mathbb{L}}$ e portanto p não é o polinômio de menor grau tal que $p(u) = 0_{\mathbb{L}}$.

Também temos que

$$Im(\varphi) = \{\varphi(f); \quad f \in \mathbb{K}[X]\} = \{f(u); \quad f \in \mathbb{K}[X]\} = \mathbb{K}[u].$$

Segue que

$$\frac{\mathbb{K}[X]}{[p]} = \frac{\mathbb{K}[X]}{Ker(\varphi)} \approx Im(\varphi) = \mathbb{K}[u],$$

e como p é irredutível sobre $\mathbb{K}$, segue do teorema (4.22) que o primeiro quociente da igualdade acima é corpo. Portanto $\mathbb{K}[u]$ é também corpo. □

Teorema 4.28. *Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos com $\mathbb{K} \subset \mathbb{L}$ e $u \in \mathbb{L}$. Se u é transcendente sobre $\mathbb{K}$ então $\mathbb{K}[u]$ é um anel de integridade (isomorfo a $\mathbb{K}[X]$).*

Prova. Esta demonstração é feita como no teorema anterior. Consideremos a mesma aplicação $\varphi(f) = f(u)$, e como já vimos, φ é homomorfismo e também $Im(\varphi) = \mathbb{K}[u]$. Mas agora, como u é transcendente sobre $\mathbb{K}$, então $f(u) = 0_{\mathbb{L}}$, se e somente se, f é o polinômio nulo. Segue que

$$\begin{aligned} Ker(\varphi) &= \{f \in \mathbb{K}[X]; \quad \varphi(f) = 0_{\mathbb{L}}\} \\ &= \{f \in \mathbb{K}[X]; \quad f(u) = 0_{\mathbb{L}}\} = \{0_{\mathbb{K}[X]}\}, \end{aligned}$$

E assim, do Teorema Fundamental do Homomorfismo de anéis, temos que,

$$\mathbb{K}[X] \approx \frac{\mathbb{K}[X]}{\{0_{\mathbb{K}[X]}\}} = \frac{\mathbb{K}[X]}{Ker(\varphi)} \approx Im(\varphi) = \mathbb{K}[u].$$

Portanto $\mathbb{K}[X] \approx \mathbb{K}[u]$, e além disso, como $\mathbb{K}[X]$ é anel de integridade então $\mathbb{K}[u]$ também o é. □

Definição 4.29. Se $\mathbb{L}$ é uma extensão de $\mathbb{K}$ e todos os elementos do corpo $\mathbb{L}$ são algébricos sobre o corpo $\mathbb{K}$, então $\mathbb{L}$ se diz extensão algébrica de $\mathbb{K}$.

Observe então que, se $\mathbb{K}$ é corpo e u é algébrico sobre $\mathbb{K}$, então $\mathbb{K}[u]$ um corpo, e como $\mathbb{K} \subset \mathbb{K}[u]$ então também $\mathbb{K}[u]$ é uma extensão de $\mathbb{K}$, e mais ainda, é uma extensão algébrica de $\mathbb{K}$, pois u é algébrico sobre $\mathbb{K}$.

Exemplo 4.6. Consideremos os corpos $\mathbb{Q} \subset \mathbb{R}$, e tomemos $u = \sqrt{2} \in \mathbb{R}$. Queremos determinar $\mathbb{Q}[u] = \mathbb{Q}[\sqrt{2}]$. Como sabemos, $\sqrt{2} \notin \mathbb{Q}$, mas $\sqrt{2}$ é algébrico sobre $\mathbb{Q}$, pois $\sqrt{2}$ é raiz do polinômio não nulo $(X^2 - 2) \in \mathbb{Q}[X]$. Do que vimos anteriormente $\mathbb{Q}[\sqrt{2}]$ é corpo e também,

$$\mathbb{Q}[\sqrt{2}] = \{f(\sqrt{2}); \quad f \in \mathbb{Q}[X]\}.$$

Além disso, considerando também o polinômio $(X^2 - 2) \in \mathbb{Q}[X]$, do algoritmo da divisão temos que existem q e r (unicamente determinados) tais que $f(X) = q(X) \cdot (X^2 - 2) + r(X)$, onde $gr(r) < gr(X^2 - 2) = 2$. Devemos ter então $r(X) = a + bX$ com $a, b \in \mathbb{Q}$. Segue que

$$f(\sqrt{2}) = g(\sqrt{2}) \cdot 0 + r(\sqrt{2}) = a + b \cdot \sqrt{2},$$

e então

$$\mathbb{Q}[\sqrt{2}] = \left\{ f(\sqrt{2}); \quad f \in \mathbb{Q}[X] \right\} = \{a + b\sqrt{2}; \quad a, b \in \mathbb{Q}\}.$$

■

Exemplo 4.7. Consideremos os corpos $\mathbb{Q} \subset \mathbb{R}$ e $u = \sqrt[4]{3} \in \mathbb{R}$. Vamos determinar $\mathbb{Q}[\sqrt[4]{3}]$. Em primeiro lugar $\sqrt[4]{3}$ é algébrico sobre $\mathbb{Q}$ pois $\sqrt[4]{3}$ é raiz do polinômio não nulo $(X^4 - 3) \in \mathbb{Q}[X]$. Temos então que $\mathbb{Q}[\sqrt[4]{3}]$ é corpo e

$$\mathbb{Q}[\sqrt[4]{3}] = \left\{ f(\sqrt[4]{3}); \quad f \in \mathbb{Q}[X] \right\}.$$

Mas, dado qualquer $f \in \mathbb{Q}[X]$, temos que existem únicos $q, r \in \mathbb{Q}[X]$ tais que $f(X) = q(X) \cdot (X^4 - 3) + r(X)$, com $gr(r) < gr(X^4 - 3) = 4$. Então $r = a + bX + cX^2 + dX^3$ com $a, b, c, d \in \mathbb{Q}$. E além disso,

$$\begin{aligned} f(\sqrt[4]{3}) &= q(\sqrt[4]{3}) \cdot 0 + r(\sqrt[4]{3}) \\ &= r(\sqrt[4]{3}) \\ &= a + b\sqrt[4]{3} + c(\sqrt[4]{3})^2 + d(\sqrt[4]{3})^3 \\ &= a + b\sqrt[4]{3} + c\sqrt[4]{9} + d\sqrt[4]{27}. \end{aligned}$$

Desta forma,

$$\mathbb{Q}[\sqrt[4]{3}] = \{f(\sqrt[4]{3}); \quad f \in \mathbb{Q}[X]\} = \{a + b\sqrt[4]{3} + c\sqrt[4]{9} + d\sqrt[4]{27}; \quad a, b, c, d \in \mathbb{Q}\}.$$

■

Exemplo 4.8. Considerando os corpos $\mathbb{Q} \subset \mathbb{R}$ e $u = \sqrt{2} + \sqrt{5} \in \mathbb{R}$, queremos determinar $\mathbb{Q}[\sqrt{2} + \sqrt{5}]$. Podemos ver que $(\sqrt{2} + \sqrt{5})$ é algébrico sobre $\mathbb{Q}$, pois é raiz do polinômio não nulo $p(X) = (X^4 - 14X^2 + 9) \in \mathbb{Q}[X]$. Então, $\mathbb{Q}[\sqrt{2} + \sqrt{5}]$ é corpo com

$$\mathbb{Q}[\sqrt{2} + \sqrt{5}] = \{f(\sqrt{2} + \sqrt{5}); \quad f \in \mathbb{Q}[X]\}.$$

Mas, dado f arbitrário em $\mathbb{Q}[X]$, existem $q(X), r(X) \in \mathbb{Q}[X]$, tais que

$$f(X) = q(X) \cdot (X^4 - 14X^2 + 9) + r(X),$$

com $gr(r) < gr(X^4 - 14X^2 + 9) = 4$. Devemos ter portanto $r = a + bX + cX^2 + dX^3$, com $a, b, c, d \in \mathbb{Q}$. Além disso,

$$\begin{aligned} f(\sqrt{2} + \sqrt{5}) &= q(\sqrt{2} + \sqrt{5}) \cdot 0 + r(\sqrt{2} + \sqrt{5}) \\ &= r(\sqrt{2} + \sqrt{5}) = a + b(\sqrt{2} + \sqrt{5}) + c(\sqrt{2} + \sqrt{5})^2 + d(\sqrt{2} + \sqrt{5})^3 \\ &= (a + 7c) + (b + 17d)\sqrt{2} + (b + 11d)\sqrt{5} + 2c\sqrt{10}. \end{aligned}$$

Com o ajuste adequado das constantes e sabendo que $a, b, c, d \in \mathbb{Q}$, podemos reescrever

$$\begin{aligned} \mathbb{Q}[\sqrt{2} + \sqrt{5}] &= \{f(\sqrt{2} + \sqrt{5}); \quad f \in \mathbb{Q}[X]\} \\ &= \{a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}, \quad a, b, c, d \in \mathbb{Q}\}. \end{aligned}$$

■

Exemplo 4.9. Neste exemplo, vamos construir o corpo dos números complexos a partir do corpo dos números reais, com a adjunção do número (não real) i que satisfaz $i^2 = -1$. Primeiramente, i é algébrico sobre $\mathbb{R}$, pois $p(X) = X^2 + 1$ é um polinômio não nulo em $\mathbb{R}[X]$, que cumpre $p(i) = 0$. Então temos,

$$\mathbb{R}[i] = \{f(i); \quad f \in \mathbb{R}[X]\}.$$

Entretanto, dado f arbitrário em $\mathbb{R}[X]$, pelo algoritmo da divisão, existem polinômios q e r em $\mathbb{R}[X]$ tais que $f(X) = q(X) \cdot (X^2 + 1) + r(X)$, onde $gr(r) < gr(X^2 + 1) = 2$. Segue que $r = a + bX$, com $a, b \in \mathbb{R}$, e assim,

$$f(i) = q(i) \cdot (i^2 + 1) + r(i) = q(i) \cdot 0 + r(i) = r(i) = a + bi.$$

Isto mostra que,

$$\mathbb{R}[i] = \{f(i); \quad f \in \mathbb{R}[X]\} = \{a + bi; \quad a, b \in \mathbb{R}\} = \mathbb{C}.$$

■

Se observarmos atentamente estes últimos exemplos, eles nos dão uma ideia para formular precisamente como são os elementos dos conjuntos $\mathbb{K}[u]$, no caso em que u é algébrico sobre $\mathbb{K}$. Estes exemplos inspiram o próximo resultado.

Teorema 4.30. *Seja $\mathbb{L}$ um corpo extensão de $\mathbb{K}$ e $u \in \mathbb{L}$ algébrico sobre $\mathbb{K}$. Seja f o polinômio irredutível, tal que $f(u) = 0_{\mathbb{K}}$. Então, se $n = gr(f)$, temos*

$$\mathbb{K}[u] = \{a_0 + a_1u + a_2u^2 + \cdots + a_{n-1}u^{n-1}; \quad a_i \in \mathbb{K}\},$$

para todos $0 \leq i \leq n - 1$.

Prova. Suponha então f o polinômio irredutível em $\mathbb{K}[X]$, tal que $f(u) = 0_{\mathbb{K}}$. Suponha ainda $gr(f) = n$. Mostraremos a dupla inclusão dos conjuntos. Dado então

$$w \in \{a_0 + a_1u + a_2u^2 + \cdots + a_{n-1}u^{n-1}; \quad a_i \in \mathbb{K}\},$$

temos que $w = b_0 + b_1u + b_2u^2 + \cdots + b_{n-1}u^{n-1}$, para certos elementos $b_i \in \mathbb{K}$. Tomando o polinômio $h = b_0 + b_1X + b_2X^2 + \cdots + b_{n-1}X^{n-1}$, em $\mathbb{K}[X]$, temos que

$$w = b_0 + b_1u + b_2u^2 + \cdots + b_{n-1}u^{n-1} = h(u) \in \mathbb{K}[u].$$

Para a segunda inclusão, seja $w \in \mathbb{K}[u]$. Então $w = h(u)$ para algum polinômio h de $\mathbb{K}[X]$. Pelo algoritmo da divisão existem polinômios q e r, em $\mathbb{K}[X]$, unicamente determinados, de forma que $h = q \cdot f + r$ com $gr(r) < gr(f) = n$. Então

$$r = a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1},$$

sendo que $a_i \in \mathbb{K}$, para todos $0 \leq i \leq n - 1$. Desta forma,

$$w = h(u) = q(u) \cdot f(u) + r(u) = q(u) \cdot 0_{\mathbb{K}} + r(u) = r(u) = a_0 + a_1u + a_2u^2 + \cdots + a_{n-1}u^{n-1},$$

mostrando a segunda inclusão. Mais ainda, para cada elemento $w \in \mathbb{K}[u]$, os $a_i \in \mathbb{K}$ são unicamente determinados. De fato, se $w = h(u)$ admite

$$h(u) = a_0 + a_1u + a_2u^2 + \cdots + a_{n-1}u^{n-1} = b_0 + b_1u + b_2u^2 + \cdots + b_{n-1}u^{n-1},$$

então

$$(a_0 - b_0) + (a_1 - b_1)u + (a_2 - b_2)u^2 + \cdots + (a_{n-1} - b_{n-1})u^{n-1} = 0_{\mathbb{K}}.$$

Como f é o polinômio não nulo de menor grau (irredutível) tal que $f(u) = 0_{\mathbb{K}}$ então o polinômio do primeiro membro na última igualdade deve ser o polinômio nulo, isto é, $(a_i - b_i) = 0_{\mathbb{K}}$ donde $a_i = b_i$ para todo $0 \leq i \leq n-1$. □

O conjunto $S = \{1_{\mathbb{K}}, u, u^2, \ldots, u^{n-1}\}$ é chamado de conjunto gerador (base) da extensão $\mathbb{K}[u]$. Esta é uma ideia adotada da Álgebra Linear. Além disso, na Álgebra Linear, o número de vetores de S, no caso n, é dito dimensão de $\mathbb{K}[u]$ sobre $\mathbb{K}$. A extensão $\mathbb{K}[u]$ também é dita extensão finita de $\mathbb{K}$. Se u é transcendente sobre $\mathbb{K}$ então o número de geradores é infinito, isto é,

$$S = \{1_{\mathbb{K}}, u, u^2, u^3, \ldots, u^n, \ldots\},$$

e então a dimensão de $\mathbb{K}[u]$ sobre $\mathbb{K}$ é dita infinita, e neste caso, a extensão $\mathbb{K}[u]$ sobre $\mathbb{K}$ é dita infinita.

Corolário 4.31. *Sejam p um número primo, u algébrico sobre $\mathbb{Z}_p$, e f o polinômio irredutível em $\mathbb{Z}_p$, tal que $f(u) = 0_{\mathbb{L}}$, tem grau n. Então $\mathbb{Z}_p[u]$ é um corpo e tem exatamente p^n elementos.*

Prova. Do fato de u ser algébrico sobre $\mathbb{Z}_p$, temos que $\mathbb{Z}_p[u]$ é corpo. Mais ainda, pelo teorema anterior,

$$\mathbb{Z}_p[u] = \{a_0 + a_1u + a_2u^2 + \cdots + a_{n-1}u^{n-1}\},$$

com $a_i \in \mathbb{Z}_p$, para todos $0 \leq i \leq n-1$. A aplicação

$$\begin{array}{rcl} \eta : \mathbb{Z}_p[u] & \to & (\mathbb{Z}_p)^n = \overbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}^{\text{n vezes}} \\ a_0 + a_1u + \cdots + a_{n-1}u^{n-1} & \mapsto & \eta(a_0 + a_1u + \cdots + a_{n-1}u^{n-1}) = (a_0, a_1, \ldots, a_{n-1}) \end{array}$$

é claramente uma aplicação bijetora, e como $(\mathbb{Z}_p)^n$ tem exatamente p^n elementos, também o corpo $\mathbb{Z}_p[u]$ terá p^n elementos. □

Este corolário nos permite construir corpos com k elementos desde que k seja uma potência natural de um primo qualquer, isto é, $k = p^n$ para algum $n \in \mathbb{N}$. Logicamente, para n igual a 1 isto não tem relevância, pois $\mathbb{Z}_p$ já é corpo e tem p elementos. Vejamos um exemplo.

Exemplo 4.10. Vamos construir um corpo com 27 elementos. Note que $27 = 3^3 = p^n$. Basta então tomar o corpo $\mathbb{Z}_3$ e u um elemento tal que $u^3 = \overline{1}$. Então teremos

$$\mathbb{Z}_3[u] = \{a + b \cdot u + c \cdot u^2; \quad a, b, c \in \mathbb{Z}_3\}.$$

tem exatamente 27 elementos e é um corpo. Deixaremos para o leitor verificar que de fato os axiomas de corpo são satisfeitos em $\mathbb{Z}_3[u]$. ■

Exemplo 4.11. Para construir um corpo com 1331 elementos, basta observar que $1331 = 11^3 = p^n$, e então consideremos $\mathbb{Z}_p = \mathbb{Z}_{11}$ e u um elemento tal que $u^3 = \overline{1}$. Temos então que,

$$\mathbb{Z}_{11}[u] = \{a + b \cdot u + c \cdot u^2; \quad a, b, c \in \mathbb{Z}_{11}\},$$

é um corpo com 1331 elementos. ■

Definição 4.32. Seja $\mathbb{K}$ um corpo, e $\mathbb{K}[u]$ a extensão de $\mathbb{K}$, pela adjunção de u. Se u é algébrico sobre $\mathbb{K}$, definimos o grau da extensão $\mathbb{K}[u]$ sobre $\mathbb{K}$, como sendo o grau do polinômio f, não nulo e irredutível sobre $\mathbb{K}$, tal que $f(u) = 0_{\mathbb{K}}$, e se u é transcendente sobre $\mathbb{K}$, definimos então o grau da extensão como infinito. Denotamos o grau da extensão por $[\mathbb{K}[u] : \mathbb{K}]$.

Observe que do que expomos até agora, são equivalentes as afirmações:
i) u é algébrico sobre $\mathbb{K}$,
ii) $\mathbb{K}[u]$ é extensão algébrica de $\mathbb{K}$,
iii) $\mathbb{K}[u]$ possui dimensão finita sobre $\mathbb{K}$,
iv) $\mathbb{K}[u]$ é extensão finita de $\mathbb{K}$,
v) $[\mathbb{K}[u] : \mathbb{K}]$ é finito.

Exemplo 4.12. O grau da extensão do corpo $\mathbb{Q}[\sqrt{2}]$ sobre $\mathbb{Q}$ é igual a 2, pois o polinômio irredutível sobre $\mathbb{Q}$ com raiz igual a $\sqrt{2}$ é $p(X) = X^2 - 2$, de grau 2. Desta forma $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$. Deixamos para o leitor verificar que p é irredutível sobre $\mathbb{Q}$. ■

Exemplo 4.13. O grau da extensão do corpo $\mathbb{Q}[\sqrt[4]{3}]$ sobre $\mathbb{Q}$ é igual a 4, pois o polinômio irredutível sobre $\mathbb{Q}$, com raiz igual a $\sqrt[4]{3}$, é $p(X) = X^4 - 3$, de grau 4. Escrevemos então $[\mathbb{Q}[\sqrt[4]{3}] : \mathbb{Q}] = 4$. Deixamos para o leitor verificar que p é irredutível sobre $\mathbb{Q}$. ■

Exemplo 4.14. O grau da extensão do corpo $\mathbb{Q}[\sqrt{2} + \sqrt{5}]$ sobre $\mathbb{Q}$, pode ser obtido observando que o polinômio $p(X) = X^4 - 14X^2 + 9$ é irredutível sobre $\mathbb{Q}$, e satisfaz $p(\sqrt{2} + \sqrt{5}) = 0$, donde imediatamente, $[\mathbb{Q}[\sqrt{2} + \sqrt{5}] : \mathbb{Q}] = gr(p) = 4$. ■

Exemplo 4.15. O grau da extensão de $\mathbb{C}$ sobre $\mathbb{R}$ é 2. Lembremos que $\mathbb{C} = \mathbb{R}[i]$, e também $p(X) = X^2 + 1$ é o polinômio irredutível sobre $\mathbb{R}$, tal que, $p(i) = 0$. Assim, $[\mathbb{C} : \mathbb{R}] = [\mathbb{R}[i] : \mathbb{R}] = gr(p) = 2$. ■

Podemos generalizar a adjunção de elementos a um corpo $\mathbb{K}$. Se u é algébrico sobre $\mathbb{K}$ então já vimos que $\mathbb{K}[u]$ é corpo. Seja agora v algébrico sobre $\mathbb{K}$. Então v será também algébrico sobre o corpo $\mathbb{K}[u]$. Da mesma forma, $(\mathbb{K}[u])[v]$ será corpo, e será uma extensão algébrica de $\mathbb{K}[u]$. Neste caso, $\mathbb{K}[u, v] = \mathbb{K}[u][v] = (\mathbb{K}[u])[v]$ denotará a extensão de $\mathbb{K}[u]$ pela adjunção de v, e portanto a extensão de $\mathbb{K}$ pela adjunção de u e v. O próximo resultado nos garantirá que, neste caso, $\mathbb{K}[u, v]$ é algébrico sobre $\mathbb{K}$.

Proposição 4.33. *Sejam $\mathbb{L}$, $\mathbb{S}$ e $\mathbb{K}$, três corpos, tais que $\mathbb{L} : \mathbb{S} : \mathbb{K}$. Então, $\mathbb{L}$ é algébrico sobre $\mathbb{K}$, se e somente se, $\mathbb{L}$ é algébrico sobre $\mathbb{S}$ e $\mathbb{S}$ é algébrico sobre $\mathbb{K}$. Mais ainda,*

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{S}] \cdot [\mathbb{S} : \mathbb{K}].$$

Prova. Fazer esta demonstração... □

Por indução, podemos então afirmar que se $u_0, u_1, \ldots, u_k$ forem elementos algébricos sobre o corpo $\mathbb{K}$, então $\mathbb{K}[u_0, u_1, \ldots, u_k]$ será uma extensão algébrica de $\mathbb{K}$. Mais ainda, denotando $\mathbb{K}_i = \mathbb{K}[u_0, u_1, \ldots, u_i]$, temos

$$[\mathbb{K}_k : \mathbb{K}] = [\mathbb{K}_k : \mathbb{K}_{k-1}] \cdot [\mathbb{K}_{k-1} : \mathbb{K}_{k-2}] \cdot \cdots \cdot [\mathbb{K}_1 : \mathbb{K}_0] \cdot [\mathbb{K}_0 : \mathbb{K}].$$

Corolário 4.34. *Se $\mathbb{L}$ é uma extensão algébrica sobre $\mathbb{K}$, tais que $[\mathbb{L}:\mathbb{K}]=p$, com p um número primo, então não existem corpos entre $\mathbb{K}$ e $\mathbb{L}$, isto é, não existe um corpo $\mathbb{S}$, tal que, $\mathbb{K}\subsetneq\mathbb{S}\subsetneq\mathbb{L}$.*

Corolário 4.35. *Não existem subcorpos próprios de $\mathbb{C}$, que contém $\mathbb{R}$ como subcorpo próprio. Em outras palavras, não existe um corpo $\mathbb{K}$, tal que, $\mathbb{R}\subsetneq\mathbb{K}\subsetneq\mathbb{C}$.*

Prova. Imediato do corolário anterior, já que, $[\mathbb{C}:\mathbb{R}]=2$, é um número primo. □

Teorema 4.36. *O grau da extensão de $\mathbb{R}$ sobre $\mathbb{Q}$ é infinito. Simbolicamente, $[\mathbb{R}:\mathbb{Q}]=\infty$.*

Prova. Suponha, por contradição, que o grau da extensão em questão seja finito. Isto é, $[\mathbb{R}:\mathbb{Q}]=k<\infty$. Consideremos $u=\sqrt[k]{2}$, e o polinômio $p=X^k-2$, que é polinômio irredutível em $\mathbb{Q}[X]$, e satisfaz $p(u)=p(\sqrt[k]{2})=0$. Sendo assim, $\mathbb{Q}[\sqrt[k]{2}]$ é um corpo e portanto uma extensão algébrica de $\mathbb{Q}$ sendo o grau desta extensão igual a k, isto é, $[\mathbb{Q}[\sqrt[k]{2}]:\mathbb{Q}]=k$. Mais ainda, $\mathbb{Q}[\sqrt[k]{2}]$ é um subcorpo de $\mathbb{R}$. Do teorema (4.33), temos que,

$$[\mathbb{R}:\mathbb{Q}]=[\mathbb{R}:\mathbb{Q}[\sqrt[k]{2}]]\cdot[\mathbb{Q}[\sqrt[k]{2}]:\mathbb{Q}]=[\mathbb{R}:\mathbb{Q}[\sqrt[k]{2}]]\cdot k.$$

Mas como $[\mathbb{R}:\mathbb{Q}[\sqrt[k]{2}]]>1$, então $[\mathbb{R}:\mathbb{Q}]>k$. Contradição com a suposição $[\mathbb{R}:\mathbb{Q}]=k$. □

Definição 4.37. Seja $\mathbb{L}$ uma extensão de $\mathbb{K}$. Se existir $\alpha\in\mathbb{L}$, tal que, $\mathbb{L}=\mathbb{K}[\alpha]$, então o corpo $\mathbb{L}$ é dito uma extensão simples de $\mathbb{K}$.

Observe que uma extensão simples não é sempre evidente. O corpo $\mathbb{Q}[\sqrt{2},\sqrt{5}]$ é uma extensão simples sobre $\mathbb{Q}$. De fato, $\mathbb{Q}[\sqrt{2},\sqrt{5}]=\mathbb{Q}[\sqrt{2}+\sqrt{5}]$. Para ver isto, lembremos que $\mathbb{Q}[\sqrt{2},\sqrt{5}]=(\mathbb{Q}[\sqrt{2}])[\sqrt{5}]$. Já mostramos que

$$\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2};\quad a,b\in\mathbb{Q}\},$$

e sabemos que

$$\mathbb{Q}[\sqrt{2}][\sqrt{5}]=(\mathbb{Q}[\sqrt{2}])[\sqrt{5}]=\{f(\sqrt{5});\quad f\in(\mathbb{Q}[\sqrt{2}])[X]\}.$$

Mas dado qualquer $f\in(\mathbb{Q}[\sqrt{2}])[X]$ existem polinômios $q(X)$ e $r(X)$ em $(\mathbb{Q}[\sqrt{2}])(X)$, tais que $f(X)=(x^2-5)q(X)+r(X)$ com $r(X)=0$ ou $gr(r)<2$. Desta forma $r(X)=mX+n$ com $m,n\in\mathbb{Q}[\sqrt{2}]$. Segue que

$$f(X)=(x^2-5)q(X)+r(X)=(x^2-5)q(X)+(mX+n),$$

e portanto

$$f(\sqrt{5})=((\sqrt{5})^2-5)q(\sqrt{5})+(m\sqrt{5}+n)=(m\sqrt{5}+n),$$

donde segue que

$$\begin{aligned}\mathbb{Q}[\sqrt{2}][\sqrt{5}]&=\{m\sqrt{5}+n;\quad m,n\in\mathbb{Q}[\sqrt{2}]\}\\&=\{(a+b\sqrt{2})\sqrt{5}+(c+d\sqrt{2});\quad a,b,c,d\in\mathbb{Q}\}\\&=\{a\sqrt{5}+b\sqrt{10}+c+d\sqrt{2};\quad a,b,c,d\in\mathbb{Q}\}=\mathbb{Q}[\sqrt{2}+\sqrt{5}].\end{aligned}$$

Definição 4.38. Um corpo $\mathbb{K}$ é dito algebricamente fechado, se todo polinômio $f\in\mathbb{K}[X]$, com $gr(f)\geq 1$, tem pelo menos uma raiz u em $\mathbb{K}$.

Esta definição equivale a dizer que todo polinômio $f \in \mathbb{K}[X]$ tem todas as suas raízes em $\mathbb{K}$. De fato, se f tem uma raiz $u_0 \in \mathbb{K}$, então já sabemos que, f é divisível por $(X - u_0)$, isto é, $f = q_0 \cdot (X - u_0)$. Mas q_0 é também um polinômio em $\mathbb{K}[X]$, que por sua vez, de acordo com a definição, também tem uma raiz em $u_1 \in \mathbb{K}$. Isto é, $q_0 = q_1 \cdot (X - u_1)$. Procedendo desta forma, até que $q_{k+1} = a$ um polinômio constante, teremos

$$f = q_0 \cdot q_1 \cdot q_2 \cdot \cdots \cdot q_k \cdot a = (X - u_0) \cdot (X - u_1) \cdot (X - u_2) \cdot \cdots \cdot (X - u_k) \cdot a,$$

onde vemos que f tem todas as suas raízes $u_0, \ldots, u_k$ em $\mathbb{K}$.

Lema 4.39. *Seja $\mathbb{K}$ um corpo. $\mathbb{K}$ é algebricamente fechado, se e somente se, todo polinômio irredutível, unitário, e não constante de $\mathbb{K}[X]$, é da forma $(X - a)$, onde $a \in \mathbb{K}$.*

Prova. Suponha então $\mathbb{K}$ algebricamente fechado. Seja f um polinômio arbitrário, irredutível, unitário e não constante, em $\mathbb{K}[X]$. Então da definição de corpo algebricamente fechado, existe um $u \in \mathbb{K}$ tal que $f(u) = 0_{\mathbb{K}}$. Logo do corolário (3.68) temos que f é divisível por $(X - u)$, isto é, $f = q \cdot (X - u)$. Mas como f é irredutível sobre $\mathbb{K}$, então segue da definição de irredutibilidade que q é constante. Como f também é unitário, segue que $f = (X - u)$.

Suponha agora que todo polinômio não constante, irredutível e unitário, seja da forma $(X - a)$. Dado $f \in \mathbb{K}[X]$ arbitrário, então pelo princípio da fatoração única,

$$f = k \cdot q_1 \cdot q_2 \cdot \cdots \cdot q_n,$$

onde $k \in \mathbb{K}$ é constante, e os fatores $q_i \in \mathbb{K}[X]$, para $1 \leq i \leq n$, são irredutíveis e unitários. Pela nossa hipótese, $q_i = (X - a_i)$, com $a_i \in \mathbb{K}$ para cada i. Então,

$$f = k \cdot (X - a_1) \cdot (X - a_2) \cdot \cdots \cdot (X - a_n),$$

donde vemos claramente que f tem pelo menos uma raiz (um dos a_i) em $\mathbb{K}$. Logo $\mathbb{K}$ é algebricamente fechado. □

Definição 4.40. Um corpo $\mathbb{L}$ é dito um corpo de decomposição de um polinômio $f \in \mathbb{K}[X]$ se $\mathbb{L}$ é o menor corpo que contém todas as raízes de f. O corpo de decomposição do polinômio $f \in \mathbb{K}[X]$ é denotado por $Gal(f, \mathbb{K})$[1].

O corpo de decomposição de um polinômio $f \in \mathbb{K}[X]$ pode ser construído. Se f é um polinômio de grau n, com coeficientes em $\mathbb{K}$, e $u_1, u_2, \cdots, u_k$ são as k raízes de f que não estão em $\mathbb{K}$, por um processo repetitivo, fazemos a adjunção de cada um dos elementos u_i, para $i = 1, 2, \ldots, k$, ao corpo $\mathbb{K}$. Obtemos assim o corpo $\mathbb{K}[u_1, u_2, \ldots, u_k]$, que é um corpo que contém todas as raízes de f. Entretanto este processo pode nos levar à adjunção de elementos "repetidos" ao corpo $\mathbb{K}$. Como exemplo, citamos o caso de encontrar o corpo de decomposição do polinômio $f(X) = X^2 - 2 \in \mathbb{Q}[X]$. As raízes de f são $\sqrt{2}$ e $-\sqrt{2}$, entretanto, $\mathbb{Q}[\sqrt{2}, -\sqrt{2}] = \mathbb{Q}[\sqrt{2}]$.

Terminar esta seção

[1] Esta notação é devida a Galois. Veja apêndice A, nota A.3.

Capítulo 5

Construção com régua e compasso

Desde os tempos antigos, sempre houve problemas que intrigaram os matemáticos. Alguns destes problemas, mantiveram os estudiosos de sua época, e às vezes de épocas vindouras, trabalhando por muito tempo para conseguirem soluções. Certos problemas foram resolvidos, e outros foram ditos (e provados) impossíveis de serem resolvidos.

Dentre estes problemas figuram três em que os gregos da antiguidade desejavam solução. São eles: a quadratura do círculo, que consiste em obter um quadrado com área igual à área de um círculo dado; a duplicação do cubo, que consiste em dado um cubo qualquer, construir um segundo cubo com volume igual ao dobro do primeiro; e a trissecção do ângulo, que consiste em dividir um ângulo qualquer em três ângulos de igual medida.

O detalhe para a solução destes três problemas, é que os gregos da época, só usavam a régua não graduada (sem marcas) e o compasso, como instrumentos de construção da geometria. Eles acreditavam que somente a reta e o círculo eram figuras geométricas perfeitas. Parecem três problemas simples. Entretanto, hoje é sabido que tratam-se de problemas impossíveis de serem resolvidos apenas com régua e compasso.

Apesar disto, a construção geométrica com régua e compasso, está longe de ser inútil. Muitas construções geométricas são possíveis apenas com régua e compasso, entre eles, podemos citar a obtenção de um triângulo com área igual a área de um polígono dado, a construção de retas paralelas ou perpendiculares a uma reta dada, passando por um ponto dado, a bissecção de um ângulo qualquer, a construção do ponto médio de dois pontos dados, divisão de um segmento de reta em partes iguais, a construção de certos polígonos convexos regulares.

O objetivo desta seção é mostrar como a álgebra garante a impossibilidade de solução para os três problemas citados acima. Claro que antes disto, precisamos conhecer alguns outros fatos.

5.1 Pontos, retas e circunferências construtíveis

Definição 5.1. Consideremos E um subconjunto do plano $\mathbb{R}^2$ e suponhamos que E possui pelo menos 2 pontos. Dizemos que é construtível a partir de E,

i) Toda reta que passa por 2 pontos de E.

ii) Toda circunferência que tem como centro um ponto de E e que passa outro ponto de E.

iii) Todo ponto de $\mathbb{R}^2$ que é a intersecção de duas retas distintas, ou de uma reta e uma circunferência, ou de duas circunferências distintas, construtíveis a partir de E.

Um ponto obtido como descrito no item (*iii*) da definição anterior, é chamado de ponto construtível a partir de E. É comum também dizer que um tal ponto é construtível por meio de régua e compasso a partir de E. Isto se deve ao fato de que as intersecções são obtidas somente com retas ou circunferências que somente podem ser traçadas com régua e compasso respectivamente. O conjunto dos pontos construtíveis a partir de E será denotado por $S(E)$.

Proposição 5.2. *Seja $E \subset \mathbb{R}^2$ com pelo menos dois pontos. Então $E \subseteq S(E)$.*

Prova. Seja $P \in E$. Como E possui pelo menos dois elementos, existe $Q \in E$ com $Q \neq P$. Neste caso, a reta r determinada por P e Q é construtível a partir de E. A circunferência α de centro Q passando por P é construtível a partir de E. Como $P \in r \cap \alpha$, concluímos que P é construtível a partir de E, logo $P \in S(E)$. □

Definição 5.3. Dados dois pontos $P, Q \in \mathbb{R}^2$, definimos $d(P;Q)$ como sendo a distância (Euclidiana) entre P e Q. De outra forma, se $P = (x, y)$ e $Q = (a, b)$, então

$$d(P;Q) = \sqrt{(x-a)^2 + (y-b)^2}.$$

Proposição 5.4. *Se E é finito então $E \neq S(E)$.*

Prova. Seja P um ponto de E e seja $Q \in E$ tal que $d(P;X) \leq d(P;Q)$ para todo $X \in E$. Em outras palavras tomamos Q como sendo o ponto de E que possui a maior distância Euclidiana de P. A reta r que passa por P e Q é construtível a partir de E e a circunferência α de centro Q e que passa por P também é construtível a partir de E. A reta r e a circunferência α se interseptam em dois pontos sendo um deles o próprio P. Assim $r \cap \alpha = \{P, P_0\}$, com $P_0 \in \mathbb{R}^2$. Então, P_0 é construtível a partir de E. Como $d(P;P_0) = 2d(Q;P) > d(Q;P)$, concluímos que P_0 não pertence a E, mas evidentemente temos $P_0 \in S(E)$. □

Consideremos agora o conjunto $E_0 = \{(0,0),(1,0)\} \subset \mathbb{R}^2$ e para todo natural n consideremos $E_{n+1} = S(E_n)$. Temos então que $E_n \subset S(E_n) = E_{n+1}$ e $E_n \neq E_{n+1}$. Designemos $H = \bigcup_{n\in\mathbb{N}} E_n$, e

i) todo ponto do conjunto H será denominado ponto construtível;

ii) toda reta construtível a partir de H será denominada reta construtível;

iii) toda circunferência construtível a partir de H será denominada circunferência construtível.

Podemos afirmar que todo ponto construtível (a partir de H) ainda pertence a H, ou seja, $S(H) \subset H$. De fato, suponha que $P \in S(H)$, isto é,

i) P é a insersecção entre duas retas construtíveis;

ii) P é a intersecção entre uma reta e uma circunferência construtíveis;

iii) P é a intersecção entre duas circunferências construtíveis.

Abordaremos apenas o caso (i) pois os outros dois casos serão análogos. Supondo que ocorre (i), temos que existem r e s duas retas construtíveis tais que $P \in r \cap s$. Mas como r é uma reta construtível, existem pontos $Q_1, Q_2 \in H$ que determinam r. Da mesma forma, existem pontos $M_1, M_2 \in H$ que determinam s. Mas $Q_1, Q_2, M_1, M_2 \in H$ e H sendo a união de todos os conjuntos E_n, existem então $n_1, n_2, n_3, n_4 \in \mathbb{N}$ de forma que $Q_1 \in E_{n_1}$, $Q_2 \in E_{n_2}$, $M1 \in E_{n_3}$ e $M_2 \in E_{n_4}$. Como $E_n \subset S(E_n) = E_{n+1}$ para qualquer n, então $Q_1, Q_2, M_1, M_2 \in E_k$ sendo $k = \max\{n_1, n_2, n_3, n_4\}$. Isto significa que r e s são duas retas construtíveis a partir de E_k. Como P é o ponto de intersecção de 2 retas construtíveis a partir de E_k, então $P \in S(E_k) = E_{k+1}$ e portanto ainda um ponto de H já que $E_{k+1} \subset H$. Segue que $S(H) \subset H$. Procedimento análogo se considerarmos (ii) ou (iii).

Note que como já havíamos provado que $H \subset S(H)$, então temos precisamente a igualdade entre estes dois conjuntos. De outra forma, $S(H) = H$. Naturalmente, em virtude da proposição 5.4, temos que H é um conjunto infinito.

Chamaremos a interseção de duas retas construtíveis, a interseção de uma reta construtível com uma circunferência construtível e a interseção de duas circunferências construtíveis de operações elementares em H. Podemos dizer também que um ponto $P \in \mathbb{R}^2$ é construtível a partir de H se pudermos obter P através de alguma dessas operações elementares em H.

Proposição 5.5. *Os eixos coordenados Ox e Oy são retas construtíveis.*

Prova. O eixo Ox é construtível pois é a reta determinada pelos pontos $(0,0)$ e $(1,0)$ pertencentes a E_0. O ponto $(-1,0)$ pertence à intersecção do eixo Ox com a circunferência α de centro $(0,0)$ e que passa pelo ponto $(1,0)$. Logo $(-1,0)$ é construtível. Considerando α_1, a circunferência de centro $(-1,0)$ que passa por $(1,0)$ e α_2, a circunferência de centro $(1,0)$ que passa por $(-1,0)$, os pontos de interseção eentre α_1 e α_2 são construtíveis e esses pontos pertencem ao eixo Oy. Assim o eixo Oy é construtível. □

Proposição 5.6. *Sejam $a \in \mathbb{R}$ e $A = (a,0)$, $B = (0,a)$, $C = (-a,0)$ e $D = (0,-a)$ pontos de $\mathbb{R}^2$. Se qualquer um destes pontos for construtível, então os outros três pontos são construtíveis.*

Prova. Se $a = 0$ então o resultado é óbvio já que os quatro pontos coincidem. Consideremos então $a \neq 0$ e que qualquer um destes quatro pontos seja construtível. Note que a circunferência construtível α de centro $(0,0)$ e que passa por este ponto construtível, passa pelos outros três pontos e que estes outros três pontos são as intersecções de α com os eixos coordenados Ox e Oy. Sendo estes eixos construtíveis, os outros três pontos são construtíveis. □

Proposição 5.7. *Se $A = (a,0) \in \mathbb{R}^2$ é construtível, então (a,a) também é construtível.*

Prova. Se $a = 0$ não há o que provar, já que neste caso $(a,0)$ e (a,a) coincidem. Suponha então $a \neq 0$. O ponto $B = (0,a)$ é também construtível, logo a circunferência α_1 de centro $A = (a,0)$ e a circunferência α_2 de centro $B = (0,a)$ que passam por $(0,0)$ são construtíveis. Além disso α_1 e α_2 se interceptam nos pontos $(0,0)$ e (a,a). Segue que (a,a) é construtível. □

5.2 Números reais construtíveis

Definição 5.8. Um número real a é construtível se, e somente se, o ponto $(a, 0) \in \mathbb{R}^2$ for construtível.

Note que em decorrência da proposição 5.6 um número real é construtível se e somente se qualquer um dos pontos $A = (a, 0)$, $B = (0, a)$, $C = (-a, 0)$ ou $D = (0, -a)$ for construtível. É comum também dizer neste caso que o número real a é construtível por meio de régua e compasso.

Exemplo 5.1. Lembrando que $E_0 = \{(0, 0), (1, 0)\}$ temos claramente que os pontos $(0, 0)$ e $(1, 0)$ pertencem a H. Logo pela definição anterior, os número 0 e 1 são construtíveis. A circunferência de dentro $(0, 0)$ que passa pelo ponto $(1, 0)$ intercepta o eixo Ox no ponto $(-1, 0)$. Segue que o ponto $(-1, 0)$ é construtível e portanto o número -1 também é construtível. Por indução, a circunferência de centro em $(\pm n, 0)$ que passa pelo ponto $(\pm(n-1), 0)$ intercepta o eixo Ox no ponto $(\pm(n+1), 0)$. Segue que os pontos $(n+1, 0)$ e $(-(n+1), 0)$ são construtíveis e portanto os números $n+1$ e $-(n+1)$ também são construtíveis. Desta forma todos os números inteiros são construtíveis. ■

Proposição 5.9. *Se A e B são pontos construtíveis distintos, então o ponto médio M do segmento AB é construtível e as retas perpendiculares a AB passando pelos pontos A, B e M também são construtíveis.*

Prova. Consideremos duas circunferências, α_1 e α_2, construtíveis centradas em cada um dos pontos A e B respectivamente, e passando pelo outro. Estas duas circunferências se interceptam em dois pontos M_1 e M_2. Seja r a reta que contém estes pontos M_1 e M_2. Esta reta r intercepta o segmento AB em M o ponto médio de AB. Segue que o ponto M, ponto médio do segumento AB é construtível. Além disso a reta r perpendicular a AB passando por M é construtível. Agora consideremos s a reta que contém A e B. A reta s intercepta a circunferência α_1 em B e outro ponto que chamaremos de C. O ponto A é o ponto médio do segmento CB e portanto, pelo passo anterior, a reta perpendicular a AB que passa por A é construtível. Também a reta s intercepta a circunferência α_2 em A e outro ponto que chamaremos de D. O ponto B é o ponto médio do segmento AD e pelo primeiro passo, a reta perpendicular a AB passando pelo ponto B é construtível. □

Corolário 5.10. *Se A e B são pontos construtíveis distintos, e M é um ponto construtível qualquer do segmento AB então a reta perpendicular a AB passando pelo ponto M também é construtível.*

Prova. Consideremos a reta r que passa por A e B e a circunferência α construtível centradas em M e que passa por A. Esta circunferência intercepta r em dois pontos sendo um deles o próprio ponto A, e um outro ponto que chamaremos C. O ponto C é construtível e o ponto M é agora o ponto médio do segmento AC. Pela proposição anterior, a reta perpendicular ao ponto M é construtível. □

Proposição 5.11. *Sejam A e r, respectivamente um ponto construtível e uma reta construtível com $A \in r$. Se B é outro ponto construtível qualquer, então existe uma reta s construtível que contém B e é paralela a r.*

Prova. Se B está sobre a reta r então não há o que mostrar, pois neste caso, a reta s procurada é a própria reta r. Se B não pertence a r então seja α a circunferência construtível centrada em A que passa por B. Esta circunferência intercepta a reta r em dois pontos construtíveis. Escolhemos um destes pontos e o chamaremos de C. Sejam β_1 e β_2 as circunferências construíveis centradas respectivamente em B e C que passam por A. As duas circunferências β_1 e β_2 se interceptam em dois pontos sendo um deles o próprio ponto A e um outro ponto que chamaremos de D. A reta s que passa por B e D é uma reta construtível, paralela a s, e que contém B. □

Proposição 5.12. *Sejam A e r respectivamente um ponto construtível e uma reta construtível com $A \in r$. Se C e D são pontos construtíveis então existe um ponto construtível B tal que $B \in r$ e os segmentos AB e CD possuem o mesmo comprimento.*

Prova. Seja s a reta construtível que passa por A e C. Seja α a circunferência construtível de centro em C e que passa por D. Tomemos P um ponto construtível qualquer desta circunferência α, que não percence a s. Este ponto pode ser o próprio ponto D caso D não pertença a s. Independentemente de D pertencer ou não à reta s, um tal ponto P sempre existe. Pode-se tomar P como sendo a intersecção entre α e a reta construtível perpendicular a s que passa pelo ponto construtível C. Pelo ponto construtível P, tomamos a reta construtível t, paralela a s que passa por P, e tomamos também a reta construtível u, que passa por A e é paralela à reta construtível que contém o segmento CP. Seja R o ponto construtível, intersecção entre as retas u e t. O segmento AR possui o mesmo comprimento que o segmento CP que por sua vez possui o mesmo comprimento do segmento CD. Basta agora tomar a circunferência construtível β centrada em A que passa por R. Esta circunferência intercepta a reta r em dois pontos. Qualquer um destes dois pontos pode ser o ponto B procurado. □

Proposição 5.13. *(i) Sejam A, B e C 3 pontos construtíveis não alinhados. Então existe um ponto construtível D tal que A, B, C e D formam um paralelogramo. Em particular a reta passando por C e paralela ao segmento AB é construtível. (ii) Um ponto A = (a; b) 2 R2 é construtível se e somente se as suas coordenadas a; b 2 R são números construtíveis.*

Prova. Demonstração. Figura 2.11: Construção de um paralelogramo e retas paralelas construtíveis. (i) Sejam r e s as retas suportes, respectivamente, dos segmentos AB e CA. Aplicando o item (ii) da proposição anterior para B 2 r encontramos um ponto construtível Z 2 r tal que j BZ j=j AC j e aplicando o mesmo resultado para C 2 s encontramos um ponto construtível Y 2 s tal que j CY j=j AB j. Agora o ponto D é encontrado, como na figura acima, interceptando as circunferências α1 de centro B e passando por Z e α2 de centro C e passando por Y . (ii)): Seja A = (a; b) um ponto construtível e sejaM o ponto médio do segmento OA. Segue da geometria elementar que o ponto A0 = (a; 0) é interseção a reta OU e da circunferência C de centro M passando por A como na figura 2:12. 15 Achando o ponto A0 = (a; 0) pertencente à reta OU, pelo intem (ii) da proposição anterior encontra-se o ponto B0 = (b; 0) traçando a partir de O a circunferência de raio j A0A j. Figura 2.12: Pontos construtíveis e coordenadas de pontos com números construtíveis. (: Reciprocamente suponhamos a e b construtíveis, isto é, (a; 0) e (b; 0) 2 H. É fácil ver que a reta determinada por 0 e por (0; 1) é construtível. Assim constrói-se (0; b) a partir de (b; 0). Como podemos traçar paralelas ou perpendiculares, segue a construção de (a; b) a partir de (a; 0) e (0; b). Isto prova a proposição 2.9. □

Observe que por esta proposição, os números construtíveis são exatamente as coordenadas dos pontos construtíveis.

Teorema 5.14. *S = f u 2 R : u construtível g é um subcorpo de R contendo Q.*

Prova. Demonstração. Sabemos que Z ⊂ S, pois foi mostrado no exemplo 2.7. Agora precisamos mostrar que: (a) x; y 2 S) y.. x 2 S (b) x; y 2 S) x fi 2 S. (c) 0 6= 2 S) 1 2 S. 16 Figura 2.13: O conjunto dos números construtíveis é subcorpo. Assumindo sem perda de generalidade, fi >> 0. Seja A = (; 0) e B = (fi; 0). Pelo item (ii) da proposição 2.8 segue que podemos construir Z à direita de O sobre a reta OU tal que j OZ j=j AB j e isto quer dizer que Z = (fi .. ; 0). Isto demonstra (a). Observe que existem retas construtíveis contendo O além das retas OU e OT onde T = (0,1). Seja r uma reta construtível como na figura 2:12 e sejam A1;B1 2 r construídos de modo que j OA1 j=j OA j= , e BB1 seja paralela a UA1. Por semelhança de triângulos temos que 1 = jOB1j fi e isto nos diz que j OB1 j= fi e daí segue que fi é construtível. Considere a figura 2:13, seja U1 2 r tal que j OU1 j = 1 e Z 2 OU tal que ZU1 seja paralela a UA1. Segue da semelhança de triângulos que j OZ j= 1 e portanto 1 é construtível e isto demonstra o teorema 2.10. □

Proposição 5.15. *Se r α 0 é um número construtível então p r também é construtível. Em particular 2i p m é construtível, para todo i;m 2 N.*

Prova. Seja R = (r; 0) e seja R1 = (1 + r; 0) como na figura 2:14. 17 Figura 2.14: p r é construtível. Assim, como r é construtível segue que R e R1 são construtíveis. Seja s a reta construtível perpendicular a OU passando por U e seja M o ponto médio do segmento OR1. Seja α a circunferência de centro M e seja Z 2 s α. Pela geometria elementar, o ponto Z 2 H, como na figura 2:14, é tal que j UZ j= p r. Assim pelo item (ii) da proposição 2.9 segue que p r é construtível. □

Proposição 5.16. *Seja S o corpo dos números construtíveis. Se L é um subcorpo de S, M é subcorpo de R e L ⊂ M e [M : L] 2, então M ⊂ S.*

Prova. Demonstração. Supondo que $[M : L] = 2$. Se x 2 M e x não pertence a L, então $M = L[x]$ e o polinômio mínimo de x sobre L tem grau 2, logo x é construtível e portanto x 2 S, então $M = L[x] \subset S$. □

Definição 5.17. definição 2.13. Diremos que toda sequência de subcorpos de R que satisfaz (i), (ii) e (iii) é uma sequência admissível para u. (i) S0 = Q ⊂ S1 ⊂ S2 ⊂ ::: ⊂ Sm..1 ⊂ Sm, (ii) $[Sj : Sj..1]$ 2 para j = 1; 2; :::;m, (iii) u 2 Sm.

Lema 5.18. *lema 2.14. Afirmaremos que se u e v são dois números reais e se existem sequências admissíveis para u e para v, então existe uma mesma sequência admissível tanto para u como para v.*

Prova. Demonstração. Suponha (Sj), j=0,1,...,m; sequência admissível para u e (Li), i=0,1,...,n; sequência admissível para v, temos que Li = Li..1(ci); i = 1; 2; :::; n onde ci é algébrico de grau menor ou igual a 2 sobre Li. Consideremos a sequência (Mr)0rm de subcorpos de R definidas por: Mr = Sr para r = 0; 1; :::;m. Mm+s = Mm+s..1(cs) para s = 1; 2; :::; n. Temos que Mm+1 = Mm(c1) = Sm(c1) S0(c1) = L1. E como c1 é algébrico de grau 2 sobre Mm = Sm, logo

$[Mm+1 : Mm]$ 2. Analogamente Mm+2 = Mm+1(c2) L1(c2) = L2 e como c2 é algébrico de grau 2 sobre Mm+1 L1, logo $[Mm+2 : Mm+1]$ 2. Por indução obtemos $[Mm+s : Mm+s..1]$ 2 para s = 1; 2; :::; n. Portanto, a sequência (Mr) para 0 r m + n satisfaz as condições (i) e (ii) e assim u; v 2 Mm+n, logo esta sequência é admissível tanto para u como para v. □

Por indução completa, demonstra-se que se V é um subconjunto finito e não vazio de $\mathbb{R}$ e se existe uma sequência admissível para cada elemento de V, então existe uma sequência admissível simultaneamente para todos os elementos de V.

Teorema 5.19. *Um número u é construtível, se e somente se, existe uma sequência admissível para u.*

Prova. Demonstração. Supondo (i), (ii) e (iii) da definição de sequência admissível satisfeitas e considerando o conjunto N de todos os números naturais i 2 $[0; m]$ tais que Si $\subset$ S, onde S é o conjunto dos números construtíveis. Temos que 0 2 N pois S0 = Q. Vamos supor que t 2 N e t ¡ m. De t 2 N segue que St $\subset$ S e como $[St+1 : St]$ 2, segue por 2.12 que St+1 $\subset$ S, então t + 1 2 N. Logo N = $[0; m]$, de onde vem que Sm $\subset$ S. Como u 2 Sm, segue que u 2 S e portanto u é construtível. Vamos demonstrar a recíproca. Suponha que o número real u seja construtível, logo (u; 0) é construtível, isto é, (u; 0) 2 H = S1 n=0 En. 19 Podemos supor que u 6= 1 e u 6= 0, senão bastaria escolher m = 0 e S0 = Q. Portanto existe um número natural n α 1 tal que (u; 0) 2 En e (u; 0) não pertence a En..1. Demonstrando por indução completa sobre n α 1 que se (a; b) 2 En, então pelo lema 2.14 existe uma sequência admissível para a e b. Assim: Para n = 1 temos: E1 = f(0; 0); (1; 0); (..1; 0); (2; 0); (1 2 ; p 3 2); (1 2 ; .. p 3 2)g, logo basta tomar S0 = Q; S1 = Q(p 3). Vamos supor $n > 1$ e que o teorema acima seja verdadeiro para n..1, isto é, que para todo (c; d) 2 En..1, existe uma sequência admissível para todas as coordenadas dos elementos de En..1(En..1 é um conjunto finito). Por hipótese temos: Figura 2.15: Operações elementares. onde Pi = (ci; di) 2 En..1 para i = (1; 2; 3; 4), logo ci; di 2 Sm para i = 1; 2; 3; 4. Consideremos agora cada um dos três casos acima separadamente. 20 1) As retas r e s são distintas e se cortam no ponto (a; b). As equações de r e s são: r : (d1 .. d2)x + (c2 .. c1)y + (c1d2 .. c2d1) = 0, s : (d3 .. d4)x + (c4 .. c3)y + (c3d4 .. c4d3) = 0, onde os coeficientes são elementos do corpo Sm e o determinante dos coeficientes das incógnitas é não nulo pois as retas r e s se cortam no ponto (a; b). Como (a; b) é a única solução desse sistema, resulta imediatamente que a e b pertencem a Sm e então (Sj)0jm é a única sequência admissível para a e b. 2) O ponto (a; b) pertence à intersecção da reta r de equação (d1 .. d2)x + (c2 .. c1)y + (c1d2 .. c2d1) = 0 com a circunferência α de equação (x .. c3)2 + (y .. d3)2 = (c4 .. c3)2 + (d4 .. d3)2. Calculando y em função de x a partir da primeira equação supondo c1 6= c2 e substituindo esse valor resultante na segunda equação obtemos uma equação da forma x2 + Ax + B = 0 onde A:B 2 Sm. Então x2 + Ax + B = 0) (x + A=2)2 = A2 4 .. B. Como (x + A=2)2 α 0) A2..4B 4 α 0) A2 .. 4B α 0. Daí resulta que x 2 Sm+1 = Sm(p A2 .. 4B), logo y 2 Sm+1. Como $[Sm+1 : Sm]$ 2, concluímos que (Sj); 0 j m + 1 é uma sequência admissível para a e b. 3) Este caso pode ser reduzido ao anterior, pois o ponto (a; b) pertence à intersec ção de circunferência α de equação (x .. c1)2 + (y .. d1)2 = (c2 .. c1)2 + (d2 .. d1)2 = r2 com a reta de equação 2(c2 .. c1)x + 2(d2 .. d1)y = r2 1 .. r2 2 .. c21 .. d21 + c22 + d22 onde r2 é o raio da circunferência d com os coeficientes pertencentes a Sm. □

Teorema 5.20. *teorema 2.16. Todo número real construtível u é algébrico sobre Q e o grau de u sobre Q é uma potência de 2.*

Prova. Demonstração. Se u é construtível, então existe uma sequência (Sj)0jm de subcorpos de R que satisfaz as condições (i), (ii) e (iii) da definição 2.13. Temos que Sm é uma extensão finita de Q e $[Sm : Q0]$ 2, logo u 2 Sm é algébrico sobre Q e o grau de u sobre Q é divisor de 2m pois $[Sm : S0] = [Sm : Sm..1][Sm..1 : Sm..2]$ ::: $[S1 : Q]$ 2m de onde resulta que o grau de u sobre Q é uma potência de 2. □

Revisar esta seção...

5.3 Duplicação do cubo

Fazer esta seção...

5.4 Quadratura do círculo

Fazer esta seção...

5.5 Trissecção do ângulo

Iniciar esta seção...

Apesar do que vimos aqui, é devido a Arquimedes um processo para trissectar qualquer ângulo usando régua **graduada** e compasso. Mais precisamente, basta que a régua tenha dois pontos marcados. Apresentaremos a seguir a construção de Arquimedes.

Dado um ângulo $A\widehat{O}B$, marque B' sobre o segmento $\overline{OB}$, de tal forma que a distância de O a B' seja igual à distância entre dois dos pontos marcados na régua. Em seguida, construa a circunferência de centro O e que passa por B'.

Colocar figura ...

Considere a reta r determinada pelo segmento $\overline{OA}$. Coloque um dos pontos marcados na régua (digamos M) sobre a reta r, e o outro ponto da régua (digamos N) sobre a circunferência e de forma que a régua ainda passe por B'. Trace o segmento $\overline{MB'}$.

Colocar figura ...

Com esta construção, o ângulo $O\widehat{M}B'$ tem medida igual a um terço da medida do ângulo dado $A\widehat{O}B = A\widehat{O}B'$. Vamos fazer esta verificação.

No que se segue, usaremos a mesma inscrição para designar um ângulo ou sua medida, e também a mesma inscrição para designar um segmento e a medida deste segmento, e usaremos o sistema de medida de ângulo em graus. Acompanhe a demonstração com a figura abaixo.

Colocar figura ...

Designemos o ângulo dado $A\widehat{O}B$ por α, e o ângulo $O\widehat{M}B'$, por β. Notemos primeiro que $\overline{OB'} = \overline{ON} = \overline{MN}$, pois são segmentos com medidas iguais à distância entre as marcas da régua. Sendo assim, o triângulo MNO é isósceles, e então $M\widehat{O}N = \beta$, e portanto $M\widehat{N}O = 180^\circ - 2\beta$. Segue que $O\widehat{N}B' = 2\beta$. Além disso, o triângulo $O\widehat{N}B'$ é isósceles também, e por isso, $O\widehat{B'}N = 2\beta$. Por outro lado, temos que $N\widehat{O}B' = 180^\circ - \alpha - \beta$. Com estas informações, temos que,

$$N\widehat{O}B' + O\widehat{N}B' + N\widehat{B'}O = 180^\circ,$$

ou equivalentemente

$$180^\circ - \alpha - \beta + 2\beta + 2\beta = 180^\circ.$$

Segue que $-\alpha + 3\beta = 0$ e portanto $\beta = \frac{\alpha}{3}$.

Capítulo 6

Construção do corpo ordenado dos números reais

Neste capítulo.... Fazer uma introdução do capítulo...

6.1 Construção axiomática dos números naturais

Começamos esta seção postulando a existência de um conjunto que satisfaz certas propriedades axiomáticas. Tais axiomas são conhecidos como axiomas de Peano.

Postulado 6.1. Postulamos a existência de um conjunto $\mathcal{P}$ não vazio e de uma aplicação $s : \mathcal{P} \to \mathcal{P}$, que a cada $x \in \mathcal{P}$ associa o elemento $s(x) \in \mathcal{P}$, satisfazendo os seguintes axiomas:

$\mathbf{P_i}$ (axioma da infinidade) A aplicação s é injetiva mas não sobrejetiva.

$\mathbf{P_{ii}}$ (axioma da indução) Se $S \subset \mathcal{P}$ com $S \not\subset s(\mathcal{P})$ e $s(S) \subset S$, então $S = \mathcal{P}$.

Observe que da não sobrejetividade de s segue que existe (pelo menos) um elemento em $\mathcal{P}$ que não está na imagem $Im(s) = s(\mathcal{P})$. Também, da injetividade de s, temos uma bijeção entre $\mathcal{P}$ e $s(\mathcal{P}) \subsetneq \mathcal{P}$. Mas não é possível bijeção entre um conjunto finito X e um subconjunto próprio de X. Segue que $\mathcal{P}$ não é finito, e daí o fato de o axioma $\mathbf{P_i}$ ser conhecido como axioma da infinidade.

A aplicação s associada a $\mathcal{P}$ é chamada aplicação sucessor, e o elemento $s(x) \in \mathcal{P}$ é dito elemento sucessor do elemento $x \in \mathcal{P}$. Como $\mathcal{P} - s(\mathcal{P})$ é não vazio existe $x \in \mathcal{P}$ de forma que $x \notin s(\mathcal{P})$, isto é, existe um elemento de $\mathcal{P}$ que não é sucessor de elemento algum de $\mathcal{P}$. Vamos mostrar que tal elemento é único.

Proposição 6.2. *O conjunto $\mathcal{P} - s(\mathcal{P})$ possui um único elemento.*

Prova. Seja $e \in \mathcal{P} - s(\mathcal{P})$, isto é, $e \in \mathcal{P}$ e $e \notin s(\mathcal{P})$, e consideremos o conjunto

$$X = \{e\} \cup s(\mathcal{P}).$$

Assim, como $e \in \mathcal{P}$ e $s(\mathcal{P}) \subset \mathcal{P}$, temos que $X \subset \mathcal{P}$. Por outro lado, $X \not\subset s(\mathcal{P})$ já que $e \in X$ e $e \notin s(\mathcal{P})$. Também, como $X \subset \mathcal{P}$, então $s(X) \subset s(\mathcal{P}) \subset \{e\} \cup s(\mathcal{P}) \subset X$. Segue do

axioma $\mathbf{P_{ii}}$ que $X = \mathcal{P}$, isto é, $\mathcal{P} = \{e\} \cup s(\mathcal{P})$ e portanto existe um único elemento que pertence a $\mathcal{P}$ e não pertence a $s(\mathcal{P})$. □

Deste ponto em diante, o elemento e da proposição anterior, será chamado de zero de $\mathcal{P}$, e denotado por $0_{\mathcal{P}}$, ou simplesmente 0. É o único elemento que não é sucessor de nenhum elemento de $\mathcal{P}$, isto é, o único elemento que pertence ao conjunto $\mathcal{P} - s(\mathcal{P})$.

Os axiomas $\mathbf{P_i}$ e $\mathbf{P_{ii}}$ podem ser substituídos por axiomas alternativos, para agora contemplar a existência (e unicidade) do elemento $0 \in \mathcal{P} - s(\mathcal{P})$.

Postulado 6.3. Postulamos a existência de um conjunto $\mathcal{P}$, com um elemento $0 \in \mathcal{P}$, e uma aplicação $s : \mathcal{P} \to \mathcal{P}$, satisfazendo

$\mathbf{P_1}$) $0 \notin s(\mathcal{P})$.

$\mathbf{P_2}$) s é injetiva.

$\mathbf{P_3}$) Se $X \subset \mathcal{P}$ com $0 \in X$ e $s(X) \subset X$, então $X = \mathcal{P}$.

Vamos mostrar que os dois postulados são equivalentes.

Proposição 6.4. *Os postulados 6.1 e 6.3 são equivalentes.*

Prova. Suponha então válidos $\mathbf{P_i}$ e $\mathbf{P_{ii}}$. $\mathbf{P_2}$ é consequência imediata de $\mathbf{P_i}$. A proposição 6.2 garante $\mathbf{P_1}$. Para mostrar $\mathbf{P_3}$, seja $X \subset \mathcal{P}$ tal que $0 \in X$ e $s(X) \subset X$. Então como $0 \in S$ e $0 \notin s(\mathcal{P})$ então $X \not\subset s(\mathcal{P})$. Então temos $X \subset \mathcal{P}$ com $X \not\subset s(\mathcal{P})$ e $s(X) \subset X$, e do axioma $\mathbf{P_{ii}}$ temos que $X = \mathcal{P}$, o que prova $\mathbf{P_3}$.

Suponha agora $\mathbf{P_1}$, $\mathbf{P_2}$ e $\mathbf{P_3}$ válidos. De $\mathbf{P_2}$, s é injetiva e como $0 \in \mathcal{P}$ com $0 \notin s(\mathcal{P})$ temos que $\mathcal{P} \not\subset s(\mathcal{P})$ donde s não é sobrejetiva, e isto garante $\mathbf{P_i}$. Para mostrar $\mathbf{P_{ii}}$, seja $X \subset \mathcal{P}$ com $X \not\subset s(\mathcal{P})$ e $s(X) \subset X$. Como $X \not\subset s(\mathcal{P})$ então existe $x \in X \subset \mathcal{P}$ com $x \notin s(\mathcal{P})$ e assim, $x \in \mathcal{P} - s(\mathcal{P})$. Mas o único elemento de $\mathcal{P}$ que não está em $s(\mathcal{P})$ é 0, donde $x = 0$. Assim, $X \subset \mathcal{P}$, com $x = 0 \in X$ e $s(X) \subset X$. De $\mathbf{P_3}$ temos que $X = \mathcal{P}$, o que prova $\mathbf{P_{ii}}$. □

Dentre todos os conjuntos e aplicações que satisfazem os axiomas de Peano, escolhemos um destes conjuntos e uma destas aplicações e deste ponto em diante os citaremos como o conjunto $\mathbb{N}$ e a aplicação s. O conjunto $\mathbb{N}$ escolhido é chamado conjunto dos números naturais e os seus elementos são chamados de números naturais. O conjunto $\mathbb{N}^* = s(\mathbb{N})$ é chamado de conjunto dos números naturais positivos. O número 0 é o (único) número natural que satisfaz $0 \in \mathbb{N} - s(\mathbb{N})$.

Vamos dotar este conjunto de operações e mostrar que estas operações satisfazem propriedades importantes. Primeiro vamos definir uma adição em $\mathbb{N}$. Como $\mathbb{N} = \{0\} \cup s(\mathbb{N})$ então vamos definir a adição sobre $\mathbb{N}$ definindo indutivamente, primeiro sobre $\{0\}$ e depois sobre elementos de $s(\mathbb{N})$.

Definição 6.5. A adição em $\mathbb{N}$ é a operação que a cada par de números naturais n e m, associa o número natural representado por $n + m$, chamado de soma de n com m e dado por

i) $n + 0 = n$, se $m = 0 \notin s(\mathbb{N})$, e

ii) $n + s(p) = s(n + p)$, se $m = s(p) \in s(\mathbb{N})$.

No que se segue vamos provar que a adição em $\mathbb{N}$ possui elemento neutro, é comutativa, associativa e vale a lei do cancelamento.

Teorema 6.6. *A adição em $\mathbb{N}$ admite elemento neutro, isto é, existe $e \in \mathbb{N}$, tal que $e+a = a = a+e$ para qualquer $a \in \mathbb{N}$.*

Prova. O elemento neutro e da adição, se existir deve ser único, e deve satisfazer $e+a = a+e = a$ para qualquer $a \in \mathbb{N}$. Desta forma, o item (i) da definição da adição, nos diz que se algum elemento neutro existir, este elemento deve ser 0. Vamos então mostrar que 0 satisfaz as duas igualdades.

Claramente o próprio item (i) da definição da adição garante que $0 + a = a$, para todo $a \in \mathbb{N}$, e então vamos mostrar a segunda igualdade. Seja

$$S = \{m \in \mathbb{N}; \quad m = m + 0\}.$$

Naturalmente $S \subset \mathbb{N}$ com $0 \in S$. Seja agora $y = s(x) \in s(S)$ para algum $x \in S$. Como $x \in S$, temos $x + 0 = x$ e disto decorre que $y + 0 = s(x) + 0 = s(x + 0) = s(x) = y$, donde $y \in S$ também. Assim $s(S) \subset S$, e do axioma $\mathbf{P_3}$ segue que $S = \mathbb{N}$. Logo, $0 + m = m = m + 0$ para todo $m \in \mathbb{N}$, e então 0 é o elemento neutro da adição em $\mathbb{N}$. □

Observe que tradicionalmente seríamos levados a provar primeiro a comutatividade da adição para não precisar provar as duas igualdades no teorema anterior. Entretanto como veremos adiante, para provar a comutatividade da adição, precisaremos da existência do elemento neutro bem como da associatividade da adição.

Teorema 6.7. *A adição em $\mathbb{N}$ é associativa, isto é, $(x + y) + z = x + (y + z)$, para quaisquer $x, y, z \in \mathbb{N}$.*

Prova. Seja

$$S = \{m \in \mathbb{N}; \quad m + (a + b) = (m + a) + b \quad \text{para todos} \quad a, b \in \mathbb{N}\}.$$

Temos que $S \subset \mathbb{N}$ e $0 \in S$ já que $0 + (a + b) = a + b = (0 + a) + b$ para quaisquer $a, b \in \mathbb{N}$. Seja agora $y = s(x) \in s(S)$ para algum $x \in S$. Então para quaisquer $a, b \in \mathbb{N}$ temos $x + (a + b) = (x + a) + b$ e também

$$\begin{aligned} y + (a + b) &= s(x) + (a + b) \\ &= s(x + (a + b)) = s((x + a) + b) \\ &= s(x + a) + b = (s(x) + a) + b = (y + a) + b. \end{aligned}$$

Segue que $y \in S$, o que mostra que $s(S) \subset S$. Do axioma $\mathbf{P_3}$ temos que $S = \mathbb{N}$ e portanto todo $m \in \mathbb{N}$ satisfaz $m + (a + b) = (m + a) + b$ para quaisquer $a, b \in \mathbb{N}$. Fica mostrada a associatividade da adição. □

Sendo válida a associatividade da adição em $\mathbb{N}$, a partir de agora escreveremos simplesmente $m + a + b$, para indicar $m + (a + b)$ ou $(m + a) + b$. A comutatividade também exigirá um lema auxiliar.

Lema 6.8. *Para qualquer $n \in \mathbb{N}$ tem-se $s(n) = n + s(0)$.*

Prova. Seja

$$S = \{n \in \mathbb{N}; \quad s(n) = n + s(0)\}.$$

Então $S \subset \mathbb{N}$ e do item (i) da definição da adição, $0 \in S$. Também, seja $y = s(x) \in s(S)$, para algum $x \in S$. Desta forma $s(x) = x + s(0)$. Usando isto e o item (ii) da definição da adição, obtemos

$$s(y) = s(s(x)) = s(x + s(0)) = s(x) + s(0) = y + s(0),$$

e assim, $y = s(x) \in S$, donde $s(S) \subset S$. Segue de $\mathbf{P_3}$ que $S = \mathbb{N}$, e portanto $s(n) = n + s(0)$ para qualquer $n \in \mathbb{N}$. □

Teorema 6.9. *A adição em $\mathbb{N}$ é comutativa, isto é, $m + n = n + m$ para quaisquer $m, n \in \mathbb{N}$.*

Prova. Seja

$$S = \{m \in \mathbb{N}; \quad m + a = a + m \quad \text{para todo} \quad a \in \mathbb{N}\}.$$

Claramente $S \subset \mathbb{N}$ e pelo teorema 6.6 temos $0 + a = a = a + 0$, isto é, $0 \in S$. Dado $y = s(x) \in s(S)$ para algum $x \in S$, então para todo $a \in \mathbb{N}$ temos $x + a = a + x$ e usando o lema 6.8 e a definição de adição, temos

$$\begin{aligned} y + a &= s(x) + a = s(x + a) \\ &= s(a + x) = s(a) + x \\ &= a + s(0) + x = a + s(0 + x) = a + s(x) = a + y. \end{aligned}$$

Então $y \in S$ o que mostra que $s(S) \subset S$ e pelo axioma $\mathbf{P_3}$ temos que $S = \mathbb{N}$. Segue a comutatividade da adição. □

Mostraremos agora a validade da lei do cancelamento para a adição em $\mathbb{N}$.

Teorema 6.10. *Para quaisquer $x, y, m \in \mathbb{N}$, se $x + m = y + m$ então $x = y$.*

Prova. Consideremos o conjunto

$$S = \{m \in \mathbb{N}; \quad a + m = b + m \quad \Rightarrow \quad a = b, \quad \text{para quaisquer} \quad a, b \in \mathbb{N}\}.$$

Temos $S \subset \mathbb{N}$ com $0 \in S$ já que, se $a + 0 = b + 0$ então $a = b$ para quaisquer $a, b \in \mathbb{N}$. Agora, tomemos $y = s(x) \in s(S)$ para $x \in S$. Queremos mostrar que $y = s(x) \in S$ e para isto suponhamos que $a + s(x) = b + s(x)$ para $a, b \in \mathbb{N}$ arbitrários. Então disto decorre que

$$s(x + a) = s(x) + a = s(x) + b = s(x + b).$$

Da injetividade de s segue que $x + a = x + b$ e como $x \in S$ então segue que $a = b$. Desta forma $y = s(x) \in S$, e do axioma $\mathbf{P_3}$ temos que $S = \mathbb{N}$, o que significa que para qualquer $m \in \mathbb{N}$, se $a + m = b + m$ então $a = b$, quaisquer que sejam $a, b \in \mathbb{N}$. □

Vamos agora dotar o conjunto $\mathbb{N}$ de uma relação de ordem (total). Definimos em $\mathbb{N}$, a relação $\leq$ dada por,

$$a \leq b, \quad \text{se e somente se,} \quad \text{existe} \quad n \in \mathbb{N} \quad \text{tal que} \quad a + n = b.$$

Escrevemos também $a < b$ para designar que $a \leq b$ com $a \neq b$. Observe que se $a < b$ então $a \neq b$ e assim, o número $n \in \mathbb{N}$ tal que $a + n = b$ é obrigatoriamente diferente de 0. Resumindo,

$$a < b, \quad \text{se e somente se,} \quad \text{existe} \quad n \in \mathbb{N}^* \quad \text{tal que} \quad a + n = b.$$

Vamos verificar primeiro que $\leq$ é de fato uma relação de ordem.

Proposição 6.11. *A relação $\leq$ é uma relação de ordem (parcial) em $\mathbb{N}$.*

Prova. Dado qualquer $a \in \mathbb{N}$, temos $a \leq a$, uma vez que $a + 0 = a$. Desta forma $\leq$ é reflexiva.

Dados $a, b \in \mathbb{N}$ tais que $a \leq b$ e $b \leq a$, então temos que existem $m, n \in \mathbb{N}$, que satisfazem $a + m = b$ e $b + n = a$. Assim, $a + m + n = b + n = a = a + 0$, e da lei do cancelamento em $\mathbb{N}$ (teorema 6.10), segue que $m + n = 0$, donde $m + n \notin s(\mathbb{N})$. Vamos mostrar que $m \notin s(\mathbb{N})$. De fato, procedendo contrapositivamente se $m \in s(\mathbb{N})$ então $m = s(x)$ para algum $x \in \mathbb{N}$ e segue que $m + n = s(x) + n = s(x + n) \in s(\mathbb{N})$, o que garante que $m + n \in s(\mathbb{N})$. Isto prova que $m \notin s(\mathbb{N})$ e como o único elemento de $\mathbb{N}$ que não está em $s(\mathbb{N})$ é 0, temos que $m = 0$. Desta forma, $b = a + m = a + 0 = a$, e que a relação é antissimétrica.

Dados agora $a, b, c \in \mathbb{N}$ tais que $a \leq b$ e $b \leq c$, então existem $m, n \in \mathbb{N}$ tais que $a+m = b$ e $b + n = c$. Assim, $a + (m + n) = (a + m) + n = b + n = c$, e então $a \leq c$ já que $m + n \in \mathbb{N}$. Temos portanto a transitividade da relação $\leq$. □

Queremos provar agora que esta ordem é total. Para isto usaremos um lema auxiliar de fácil demonstração.

Lema 6.12. *Para qualquer $n \in \mathbb{N}$ temos que $n \leq s(n)$.*

Prova. Naturalmente, para qualquer $n \in \mathbb{N}$,

$$n + s(0) = s(0) + n = s(0 + n) = s(n),$$

e como $s(0) \in \mathbb{N}$, então $n \leq s(n)$. □

Proposição 6.13. *A relação de ordem $\leq$ é total em $\mathbb{N}$.*

Prova. Seja $a \in \mathbb{N}$ arbitrário, e considere o conjunto

$$S_a = \{n \in \mathbb{N}; \quad a \leq n \quad \text{ou} \quad n \leq a\}.$$

Então $S_a \subset \mathbb{N}$. Como $0 + a = a$ então $0 \leq a$ e com isto $0 \in S_a$. Mostraremos que $s(S_a) \subset S_a$. Seja $y = s(x) \in s(S_a)$ para algum $x \in S_a$. Desta forma, $x \leq a$ ou $a \leq x$.

Se $a \leq x$, como $x \leq s(x)$ então da transitividade de $\leq$ segue que $a \leq s(x)$ donde $s(x) \in S_a$, isto é, $y \in S_a$.

Se $x \leq a$ então $x + k = a$ para algum $k \in \mathbb{N}$. Se $k = 0$ então não há o que mostrar pois daí $a = x$ e podemos utilizar o caso $a \leq x$. Se $k \neq 0$ então $k \in s(\mathbb{N})$, donde $k = s(m)$ para algum $m \in \mathbb{N}$. Então $s(x) + m = s(x + m) = s(m + x) = s(m) + x = k + x = a$. Segue que $s(x) \leq a$ e então $s(x) \in S_a$, ou ainda, $y \in S_a$.

Em qualquer caso, temos $s(S_a) \subset S_a$. Segue do axioma $\mathbf{P_3}$ que $S_a = \mathbb{N}$. Assim, dados $m, n \in \mathbb{N}$ arbitrários, temos que $m \in S_n$ e da definição de S_n, temos que $m \leq n$ ou $n \leq m$, e o conjunto $\mathbb{N}$ é totalmente ordenado. □

Nestes termos, dados $a, b \in \mathbb{N}$, temos $a \leq b$ ou $b \leq a$. Se considerarmos separadamente a possibilidade $a = b$, temos então a propriedade tricotômica da relação de ordem, ou $a = b$, ou $a < b$, ou $b < a$.

Definiremos agora uma multiplicação em $\mathbb{N}$. Novamente, como $\mathbb{N} = \{0\} \cup s(\mathbb{N})$ então definiremos a multiplicação em $\mathbb{N}$ indutivamente, definindo-a primeiro sobre $\{0\}$ e depois sobre os elementos de $s(\mathbb{N})$.

Definição 6.14. Uma aplicação $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, sendo que escrevemos $m \cdot n$ ou simplesmente mn para indicar $\cdot(m, n)$, que satisfaz

i) $0 \cdot a = 0$,

ii) $s(m) \cdot a = (m \cdot a) + a$

para todos $m, a \in \mathbb{N}$, é dita multiplicação em $\mathbb{N}$.

Para o item *(ii)* vamos supor, deste ponto em diante, que a multiplicação tem preferência sobre a adição, e então escreveremos simplesmente $m \cdot a + a$ em vez de $(m \cdot a) + a$. Mostraremos, como no caso da adição, que a multiplicação é única em $\mathbb{N}$.

Proposição 6.15. *Existe uma única aplicação multiplicação em* $\mathbb{N}$.

Prova. Sejam $\cdot$ e $\odot$ duas multiplicações em $\mathbb{N}$. Consideremos

$$S = \{m \in \mathbb{N}; \quad m \cdot a = m \odot a, \quad \text{para todo} \quad a \in \mathbb{N}\}.$$

Temos $S \subset \mathbb{N}$ e também $0 \in S$ já que $0 \cdot a = 0 = 0 \odot a$ para todo $a \in \mathbb{N}$. Seja $y = s(x) \in s(S)$ para algum $x \in S$. Nestes termos, para qualquer $a \in \mathbb{N}$ temos $x \cdot a = x \odot a$ e disto $y \cdot a = s(x) \cdot a = x \cdot a + a = x \odot a + a = s(x) \odot a = y \odot a$, o que garante que $y \in S$ e que $s(S) \subset S$. Do axioma $\mathbf{P_3}$, temos $S = \mathbb{N}$ e então para todos $a, m \in \mathbb{N}$ é válida a igualdade $m \cdot a = m \odot a$, donde segue a igualdade entre $\cdot$ e $\odot$. □

A multiplicação possui propriedades similares às propriedades da adição. Entretanto, as demonstrações destas propriedades são mais extensas para a multiplicação. A multiplicação possui elemento neutro, é comutativa, associativa e vale a lei do cancelamento (com restrições). A prova da existência do elemento neutro precisará de um lema auxiliar.

Lema 6.16. *Dados* $a, b \in \mathbb{N}$, *se* $a \cdot b = 0$, *então* $a = 0$ *ou* $b = 0$.

Prova. Procederemos pela contrapositiva. Suponha que $a \neq 0$ e $b \neq 0$, ou ainda, $a, b \in s(\mathbb{N})$. Existem então $x, y \in \mathbb{N}$ tais que $a = s(x)$ e $b = s(y)$. Assim, das definições de multiplicação e

de adição,

$$a \cdot b = s(x) \cdot s(y) = x \cdot s(y) + s(y) = s(y) + x \cdot s(y) = s(y + x \cdot s(y)),$$

e então, $a \cdot b \in s(\mathbb{N})$ o que garante que $a \cdot b \neq 0$. O resultado fica então demonstrado contrapositivamente. □

Teorema 6.17. *Existe $i \in \mathbb{N}$ tal que $i \cdot a = a = a \cdot i$ para qualquer $a \in \mathbb{N}$;*

Prova. Sabemos que $0 \cdot a = 0$, e portanto na procura por um elemento $i \in \mathbb{N}$ tal que $i \cdot a = a$ para qualquer $a \in \mathbb{N}$, vemos que i não pode ser o elemento 0. Então $i \in s(\mathbb{N})$, e desta forma $i = s(x)$ para algum $x \in \mathbb{N}$. Sendo assim, x deverá satisfazer $s(x) \cdot a = a$, ou ainda $x \cdot a + a = a = 0 + a$. Mas pela lei do cancelamento para a adição, x deve satisfazer $x \cdot a = 0$. Do lema anterior, $x = 0$ ou $a = 0$, e como desejamos a igualdade para $a \in \mathbb{N}$ arbitrário, devemos ter $x = 0$ e desta forma $i = s(x) = s(0)$.

Mostraremos que $s(0)$ satisfaz portanto as duas igualdades desejadas. De fato, $s(0) \cdot a = 0 \cdot a + a = 0 + a = a$ para qualquer $a \in \mathbb{N}$. Agora, para mostrar a segunda igualdade, seja

$$S = \{n \in \mathbb{N}; \quad n \cdot s(0) = n\}.$$

Desta forma, $S \subset \mathbb{N}$ e também $0 \in S$, pois $0 \cdot s(0) = 0$. Dado $y = s(x) \in s(S)$, para algum $x \in S$, temos então $x \cdot s(0) = x$ e usando também o lema 6.8 decorre que,

$$y \cdot s(0) = s(x) \cdot s(0) = x \cdot s(0) + s(0) = x + s(0) = s(x) = y.$$

Então temos que $y \in S$, o que mostra que $s(S) \subset S$ e do axioma $\mathbf{P_3}$, $S = \mathbb{N}$. Temos assim que $a \cdot s(0) = a$ para todo $a \in \mathbb{N}$. □

O elemento $s(0) \in \mathbb{N}$ é então o elemento neutro da multiplicação, e naturalmente este é o elemento sucessor do elemento $0 \in \mathbb{N}$. Chamaremos o elemento $s(0)$ de unidade do conjunto $\mathbb{N}$ e representaremos este elemento de agora em diante por 1. Desta forma, temos $1 = s(0)$ e também $1 \cdot a = a = a \cdot 1$ para qualquer $a \in \mathbb{N}$.

Com a notação $s(0) = 1$ e o lema 6.8 temos imediatamente que $s(x) = x + s(0) = x + 1$, para qualquer $x \in \mathbb{N}$. De outra forma, o sucessor de um número natural x é o número natural $x + 1$.

Queremos agora mostrar que a multiplicação é associativa e comutativa. Para provar isto, precisaremos primeiro da distributividade da multiplicação em relação à adição. Esta por sua vez utilizará um lema auxiliar. Este lema refere-se ao produto por 0 pela esquerda. A definição de multiplicação já garante em seu item (i) que $0 \cdot a = 0$ para qualquer $a \in \mathbb{N}$. Mas como ainda não mostramos a comutatividade da multiplicação, precisaremos provar também que $a \cdot 0 = 0$ para todo $a \in \mathbb{N}$.

Lema 6.18. *Para todo $a \in \mathbb{N}$, temos $a \cdot 0 = 0$.*

Prova. Consideremos o conjunto

$$S = \{m \in \mathbb{N}; \quad m \cdot 0 = 0\}.$$

Temos que $S \subset \mathbb{N}$ e como $0 \cdot 0 = 0$ então $0 \in S$. Também seja $y = s(x) \in s(S)$ para $x \in S$. Então $x \cdot 0 = 0$ e decorre disto que $y \cdot 0 = s(x) \cdot 0 = x \cdot 0 + 0 = x \cdot 0 = 0$. Segue que $y \in S$ e que $s(S) \subset S$. Pelo axioma $\mathbf{P_3}$, $S = \mathbb{N}$, donde $a \cdot 0 = 0$ para todo $a \in \mathbb{N}$. □

Teorema 6.19. *Para quaisquer $x, y, z \in \mathbb{N}$, temos $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ e também $(y+z) \cdot x = (y \cdot x) + (z \cdot x)$, isto é, a operação multiplicação é distributiva com relação à operação adição em $\mathbb{N}$.*

Prova. Consideremos

$$S = \{m \in \mathbb{N}; \quad m \cdot (a + b) = m \cdot a + m \cdot b, \quad \text{para todos} \quad a, b \in \mathbb{N}\}.$$

Claro que $S \subset \mathbb{N}$ e que $0 \in S$ já que $0 \cdot (a + b) = 0 = 0 + 0 = 0 \cdot a + 0 \cdot b$ para quaisquer $a, b \in \mathbb{N}$. Agora suponha $y = s(x) \in s(S)$, para $x \in S$. Então $x \cdot (a + b) = x \cdot a + x \cdot b$ e usando isto temos

$$\begin{aligned} y \cdot (a + b) &= s(x) \cdot (a + b) = x \cdot (a + b) + (a + b) \\ &= x \cdot a + x \cdot b + a + b \\ &= x \cdot a + a + x \cdot b + b \\ &= s(x) \cdot a + s(x) \cdot b = y \cdot a + y \cdot b. \end{aligned}$$

Segue que $y \in S$ e então $s(S) \subset S$. Do axioma $\mathbf{P_3}$ temos $S = \mathbb{N}$ e a distributividade à esquerda da multiplicação em relação à adição. Para provar a distributividade à direita, consideremos o conjunto

$$T = \{m \in \mathbb{N}; \quad (a + b) \cdot m = a \cdot m + b \cdot m, \quad \text{para todos} \quad a, b \in \mathbb{N}\}.$$

Então $T \subset \mathbb{N}$ e usando o lema 6.18 temos que $(a + b) \cdot 0 = 0 = 0 + 0 = a \cdot 0 + b \cdot 0$ para quaisquer $a, b \in \mathbb{N}$, e então $0 \in T$. Agora suponha $y = s(x) \in s(T)$ para $x \in T$. Então $(a + b) \cdot x = a \cdot x + b \cdot x$ e usando o fato que $s(x) = x + 1$, temos

$$\begin{aligned} (a + b) \cdot y &= (a + b) \cdot s(x) = (a + b) \cdot (x + 1) \\ &= (a + b) \cdot x + (a + b) \cdot 1 \\ &= a \cdot x + b \cdot x + a + b \\ &= a \cdot x + a + b \cdot x + b \\ &= a \cdot x + a \cdot 1 + b \cdot x + b \cdot 1 \\ &= a \cdot (x + 1) + b \cdot (x + 1) \\ &= a \cdot s(x) + b \cdot s(x) = a \cdot y + b \cdot y. \end{aligned}$$

Temos então que $y \in T$, e por conseguinte $s(T) \subset T$. Do axioma $\mathbf{P_3}$ temos $T = \mathbb{N}$. A multiplicação é portanto distributiva também à direita em relação à adição. □

Teorema 6.20. *Para quaisquer $x, y, z \in \mathbb{N}$, temos $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.*

Prova. Seja

$$S = \{m \in \mathbb{N}; \quad m \cdot (a \cdot b) = (m \cdot a) \cdot b, \quad \text{para todos} \quad a, b \in \mathbb{N}\}.$$

Temos $S \subset \mathbb{N}$ e também $0 \in S$ pois $0 \cdot (a \cdot b) = 0 = 0 \cdot b = (0 \cdot a) \cdot b$ para quaisquer $a, b \in \mathbb{N}$. Seja agora $y = s(x) \in s(S)$ com $x \in S$. Então para quaisquer $a, b \in \mathbb{N}$ temos $x \cdot (a \cdot b) = (x \cdot a) \cdot b$ e disto temos

$$\begin{aligned} y \cdot (a \cdot b) &= s(x) \cdot (a \cdot b) \\ &= x \cdot (a \cdot b) + a \cdot b \\ &= (x \cdot a) \cdot b + a \cdot b \\ &= (x \cdot a + a) \cdot b = (s(x) \cdot a) \cdot b = (y \cdot a) \cdot b. \end{aligned}$$

Então $y \in S$ e $s(S) \subset S$. Do axioma $\mathbf{P_3}$ temos que $S = \mathbb{N}$ e fica provada a associatividade da multiplicação. □

Teorema 6.21. *Para quaisquer $m, n \in \mathbb{N}$, temos $m \cdot n = n \cdot m$.*

Prova. Considerando

$$S = \{m \in \mathbb{N}; \quad m \cdot a = a \cdot m, \quad \text{para todos} \quad a \in \mathbb{N}\},$$

temos $S \subset \mathbb{N}$. Também, usando a definição da multiplicação e o lema 6.18, temos $a \cdot 0 = 0 = 0 \cdot a$ para todo $a \in \mathbb{N}$, o que garante que $0 \in S$. Suponha agora $y = s(x) \in s(S)$ para $x \in S$. Então para todo $a \in \mathbb{N}$ temos $x \cdot a = a \cdot x$ e também

$$\begin{aligned} y \cdot a = s(x) \cdot a &= x \cdot a + a \\ &= a \cdot x + a \cdot 1 \\ &= a \cdot (x + 1) = a \cdot s(x) = a \cdot y. \end{aligned}$$

Segue que $y \in S$ e então $s(S) \subset S$. O axioma $\mathbf{P_3}$ garante que $S = \mathbb{N}$ e portanto $m \cdot a = a \cdot m$ para todos $a, m \in \mathbb{N}$. □

A lei do cancelamento também é válida para a multiplicação, com uma certa restrição, como dito antes. Como sabemos que $0 \cdot x = 0 = 0 \cdot y$ para quaisquer $x, y \in \mathbb{N}$, isto nos diz que $a \cdot x = a \cdot y$ não pode garantir que $x = y$ no caso em que $a = 0$. Entretanto se $a \neq 0$ então podemos garantir este cancelamento.

Teorema 6.22. *Para quaisquer $a, x, y \in \mathbb{N}$, se $a \neq 0$ e $a \cdot x = a \cdot y$, então $x = y$.*

Prova. Supondo $a \neq 0$, então temos que $a \in s(\mathbb{N})$ e $a = s(m)$ para algum $m \in \mathbb{N}$. Sejam também $x, y \in \mathbb{N}$ tais que $a \cdot x = a \cdot y$. Como a relação de ordem em $\mathbb{N}$ é total, então temos $x \leq y$ ou $y \leq x$. Vamos analisar cada um dos casos.

Se $x \leq y$ então existe $k \in \mathbb{N}$ tal que $x + k = y$. Assim,

$$\begin{aligned} s(m) \cdot x = a \cdot x &= a \cdot y \\ &= a \cdot (x + k) \end{aligned}$$

$$= a \cdot x + a \cdot k = s(m) \cdot x + s(m) \cdot k.$$

Da lei do cancelamento para a adição, temos que $s(m) \cdot k = 0$, e do lema 6.16, temos que obrigatoriamente $k = 0$, uma vez que $s(m) \neq 0$. Sendo assim, $y = x + k = x + 0 = x$.

Analogamente, se $y \leq x$ então existe $l \in \mathbb{N}$ tal que $y + l = x$. Então também

$$s(m) \cdot y = a \cdot y = a \cdot x = a \cdot (y + l) = s(m) \cdot y + s(m) \cdot l,$$

donde segue que $s(m) \cdot l = 0$ e como $s(m) \neq 0$ então $l = 0$. Logo, $x = y + l = y + 0 = y$, e isto encerra esta demonstração. □

Para finalizar, como complemento, mostraremos agora a compatibilidade das operações de adição e multiplicação para com a relação de ordem em $\mathbb{N}$. Isto significa que dados $a, b \in \mathbb{N}$ arbitrários, se $a \leq b$ então $a + m \leq b + m$, e também $a \cdot m \leq b \cdot m$ para qualquer $m \in \mathbb{N}$.

Teorema 6.23. *Dados $a, b \in \mathbb{N}$ com $a \leq b$ então, para qualquer $m \in \mathbb{N}$ temos $a + m \leq b + m$.*

Prova. Sejam então $a, b \in \mathbb{N}$ com $a \leq b$. Então existe $k \in \mathbb{N}$ tal que $a + k = b$. Então usando a comutatividade e a associatividade da adição em $\mathbb{N}$, temos

$$(a + m) + k = (a + k) + m = b + m,$$

para qualquer $m \in N$. Isto garante que $a + m \leq b + m$. □

Teorema 6.24. *Dados $a, b \in \mathbb{N}$ com $a \leq b$ então, para qualquer $m \in \mathbb{N}$ temos $a \cdot m \leq b \cdot m$.*

Prova. Dados $a, b \in \mathbb{N}$ com $a \leq b$, então existe $k \in \mathbb{N}$ tal que $a + k = b$. Então usando a distributividade da multiplicação com relação à adição em $\mathbb{N}$, temos

$$a \cdot m + k \cdot m = (a + k) \cdot m = b \cdot m,$$

para qualquer $m \in \mathbb{N}$. Segue que $a \cdot m \leq b \cdot m$. □

6.2 Construção dos números inteiros

A ideia desta construção é partir do conjunto dos números naturais, e construir um número inteiro como sendo a diferença entre dois números naturais. Isto é, se $z \in \mathbb{Z}$ então $z = a - b$ para $a, b \in \mathbb{N}$. Dois problemas aqui ocorrem. Primeiro a diferença não é uma operação sobre o conjunto dos números naturais, e então para contornar isto, o número inteiro z será associado a um par (a, b). A ideia é que este par seja o número $a - b$. O segundo problema é que um número inteiro z pode ser escrito de muitas maneiras como diferença de dois números naturais, e então temos que trabalhar com classes de equivalência.

Considerando o conjunto $\mathbb{N} \times \mathbb{N}$, definimos a relação $\sim$ dada por

$$(a, b) \sim (x, y) \quad \text{se, e somente se,} \quad a + y = x + b.$$

Aqui, $+$ é a operação de adição de números naturais, sobre a qual incidem as propriedades descritas na seção anterior.

Vamos mostrar que $\sim$ é uma relação de equivalência. Dado qualquer $(a,b) \in \mathbb{N}\times\mathbb{N}$, temos claramente que $a+b=a+b$, donde $(a,b)\sim(a,b)$. A relação é então reflexiva. Seja agora $(a,b),(x,y)\in\mathbb{N}\times\mathbb{N}$, tal que $(a,b)\sim(x,y)$. Da definição da relação temos que $a+y=x+b$, e então $x+b=a+y$ donde $(x,y)\sim(a,b)$. A relação é também simétrica. Finalmente, sejam $(a,b),(x,y),(m,n)\in\mathbb{N}\times\mathbb{N}$ tais que $(a,b)\sim(x,y)$ e $(x,y)\sim(m,n)$, isto é, $a+y=x+b$ e $x+n=m+y$. Das propriedades da adição de números naturais, podemos deduzir que $a+y+n=(a+y)+n=(x+b)+n=(x+n)+b=(m+y)+b=m+y+b$. Pela lei do cancelamento de números naturais pela operação adição, temos $a+n=b+m$, donde $(a,b)\sim(m,n)$ e a relação é transitiva. Segue que $\sim$ é uma relação de equivalência sobre $\mathbb{N}\times\mathbb{N}$.

Consideremos o conjunto quociente de $\mathbb{N}\times\mathbb{N}$ pela relação $\sim$, isto é, o conjunto de todas as classes de equivalência determinadas pela relação $\sim$ em $\mathbb{N}\times\mathbb{N}$. Seja então

$$\mathbb{Z}=\frac{\mathbb{N}\times\mathbb{N}}{\sim}=\{\overline{(a,b)};\quad (a,b)\in\mathbb{N}\times\mathbb{N}\}.$$

O conjunto $\mathbb{Z}$ será, deste ponto em diante, chamado de conjunto dos números inteiros, e um elemento deste conjunto é um número inteiro, ou simplesmente um inteiro. Lembremos ainda que $\overline{(a,b)}=\{(x,y)\in\mathbb{N}\times\mathbb{N};\quad (x,y)\sim(a,b)\}$, e como já mostramos (proposição 1.33),

$$\overline{(a,b)}=\overline{(x,y)}\quad\Leftrightarrow\quad(a,b)\in\overline{(x,y)}\quad\Leftrightarrow\quad(a,b)\sim(x,y)\quad\Leftrightarrow\quad a+y=x+b.$$

Definiremos em $\mathbb{Z}$ duas operações chamadas de adição e multiplicação, representadas respectivamente por $+$ e $\cdot$, e dadas por

$$\overline{(a,b)}+\overline{(x,y)}=\overline{(a+x,b+y)},$$
$$\overline{(a,b)}\cdot\overline{(x,y)}=\overline{(ax+by,ay+bx)}.$$

Aqui, estamos usando no segundo membro destas definições, a notação $+$ para designar a adição de números naturais, e a notação ax para designar a multiplicação $a\cdot x$ de números naturais. Sobre estas duas operações, restritas ao conjunto dos números naturais, incidem as propriedades citadas na seção anterior.

Em primeiro lugar temos que verificar que a adição e a multiplicação de números inteiros estão bem definidas. Isto porque no primeiro membro da definição, temos uma classe $\overline{(a,b)}$ que é na verdade um conjunto de vários elementos relacionados entre si por $\sim$, enquanto no segundo membro temos os elementos a e b. Isto significa que usamos o elemento (a,b) como representante da classe $\overline{(a,b)}$, e precisamos ter certeza que esta escolha não afeta as operações.

Sejam então (a,b) e $(\tilde{a},\tilde{b})$ representantes da mesma classe, bem como (x,y) e $(\tilde{x},\tilde{y})$. Isto é, $(a,b)\sim(\tilde{a},\tilde{b})$ e também $(x,y)\sim(\tilde{x},\tilde{y})$. Da definição da relação, $a+\tilde{b}=\tilde{a}+b$ e também $x+\tilde{y}=y+\tilde{x}$. Segue que

$$(a+x)+(\tilde{b}+\tilde{y})=(a+\tilde{b})+(x+\tilde{y})=(\tilde{a}+b)+(y\tilde{x})=(\tilde{a}+\tilde{x})+(b+y),$$

donde $(a+x,b+y)\sim(\tilde{a}+\tilde{x},\tilde{b}+\tilde{y})$. Então

$$\overline{(a,b)}+\overline{(x,y)}=\overline{(a+x,b+y)}=\overline{(\tilde{a}+\tilde{x},\tilde{b}+\tilde{y})}=\overline{(\tilde{a},\tilde{b})}+\overline{(\tilde{x},\tilde{y})},$$

e a adição está bem definida. Também,

$$(a+\tilde{b})x+(\tilde{a}+b)y+\tilde{a}(x+\tilde{y})+\tilde{b}(y+\tilde{x})=(\tilde{a}+b)x+(a+\tilde{b})y+\tilde{a}(y+\tilde{x})+\tilde{b}(x+\tilde{y})$$

e da lei do cancelamento para a adição de números naturais, resta

$$ax + by + \tilde{a}\tilde{y} + \tilde{b}\tilde{x} = bx + ay + \tilde{a}\tilde{x} + \tilde{b}\tilde{y},$$

ou ainda,

$$(ax + by) + (\tilde{a}\tilde{y} + \tilde{b}\tilde{x}) = (\tilde{a}\tilde{x} + \tilde{b}\tilde{y}) + (ay + bx),$$

e da definição da relação temos que,

$$\overline{(ax + by, ay + bx)} = \overline{(\tilde{a}\tilde{x} + \tilde{b}\tilde{y}, \tilde{a}\tilde{y} + \tilde{b}\tilde{x})},$$

donde segue que,

$$\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(ax + by, ay + bx)} = \overline{(\tilde{a}\tilde{x} + \tilde{b}\tilde{y}, \tilde{a}\tilde{y} + \tilde{b}\tilde{x})} = \overline{(\tilde{a}, \tilde{b})} + \overline{(\tilde{x}, \tilde{y})},$$

e a multiplicação está bem definida.

Vamos agora mostrar que as operações + e $\cdot$ tornam a tripla ordenada $(\mathbb{Z}, +, \cdot)$ um anel de integridade.

Teorema 6.25. *A adição de números inteiros satisfaz as seguintes propriedades:*

1) *Para todos* $\overline{(a,b)}, \overline{(x,y)}, \overline{(m,n)} \in \mathbb{Z}$ *temos*

$$\overline{(a,b)} + (\overline{(x,y)} + \overline{(m,n)}) = (\overline{(a,b)} + \overline{(x,y)}) + \overline{(m,n)}.$$

2) *Para todos* $\overline{(a,b)}, \overline{(x,y)} \in \mathbb{Z}$ *temos*

$$\overline{(a,b)} + \overline{(x,y)} = \overline{(x,y)} + \overline{(a,b)}.$$

3) *Existe* $0_{\mathbb{Z}} \in \mathbb{Z}$ *tal que* $\overline{(a,b)} + 0_{\mathbb{Z}} = 0_{\mathbb{Z}} + \overline{(a,b)} = \overline{(a,b)}$ *para todo* $\overline{(a,b)} \in \mathbb{Z}$*;*

4) *Para todo* $\overline{(a,b)} \in \mathbb{Z}$*, existe um elemento* $-\overline{(a,b)} \in \mathbb{Z}$*, chamado de elemento simétrico de* $\overline{(a,b)}$*, tal que*

$$\overline{(a,b)} + (-\overline{(a,b)}) = (-\overline{(a,b)}) + \overline{(a,b)} = 0_{\mathbb{Z}}.$$

Prova. Dados então $\overline{(a,b)}, \overline{(x,y)}, \overline{(m,n)} \in \mathbb{Z}$ temos que

$$\begin{aligned}
\overline{(a,b)} + (\overline{(x,y)} + \overline{(m,n)}) &= \overline{(a,b)} + \overline{(x+m, y+n)} \\
&= \overline{(a + (x+m), b + (y+n))} = \overline{((a+x) + m, (b+y) + n)} \\
&= \overline{(a+x, b+y)} + \overline{(m,n)} = (\overline{(a,b)} + \overline{(x,y)}) + \overline{(m,n)}.
\end{aligned}$$

Fica mostrada a associatividade da adição. Também,

$$\overline{(a,b)} + \overline{(x,y)} = \overline{(a+x, b+y)} = \overline{(x+a, y+b)} = \overline{(x,y)} + \overline{(a,b)}$$

o que mostra a comutatividade da adição.

Queremos encontrar um elemento $0_{\mathbb{Z}} = \overline{(x,y)} \in \mathbb{Z}$ que satisfaz $\overline{(x,y)} + \overline{(a,b)} = \overline{(a,b)}$, para qualquer $\overline{(a,b)} \in \mathbb{Z}$. De outra forma, desejamos que $\overline{(a+x, b+y)} = \overline{(a,b)}$. Da definição da classe de equivalência temos que $(a + x, b + y) \sim (a, b)$ e da definição da relação, segue que x e y devem satisfazer $a + x + b = b + y + a$. Da lei do cancelamento da adição de números naturais, segue que $x = y$. Ou seja, $0_{\mathbb{Z}}$ é uma classe onde os representantes são os pares

ordenados com coordenadas iguais. De fato, dado qualquer $x \in \mathbb{N}$, e qualquer $\overline{(a,b)} \in \mathbb{Z}$, temos que $(a+x)+b = a+(b+x)$, donde $\overline{(a+x,b+x)} = \overline{(a,b)}$, e disto, temos

$$\overline{(x,x)} + \overline{(a,b)} = \overline{(a+x,b+x)} = \overline{(a,b)}.$$

Segue portanto que $0_{\mathbb{Z}} = \overline{(x,x)}$ para qualquer $x \in \mathbb{N}$. Naturalmente o representante mais simples desta classe é o par $(0,0)$, já que $\overline{(x,x)} = \overline{(0,0)}$. Escolhemos então $0_{\mathbb{Z}} = \overline{(0,0)}$ que é o elemento neutro do conjunto dos números inteiros para a adição.

A segunda igualdade, $\overline{(a,b)} + 0_{\mathbb{Z}} = \overline{(a,b)}$, é consequência imediata da comutatividade da adição.

Dado $\overline{(a,b)} \in \mathbb{Z}$, queremos encontrar $-\overline{(a,b)} = \overline{(x,y)} \in \mathbb{Z}$ que satisfaz $\overline{(x,y)} + \overline{(a,b)} = 0_{\mathbb{Z}} = \overline{(0,0)}$. Mas isto é equivalente a $\overline{(x+a,y+b)} = \overline{(0,0)}$ que pela igualdade de classes de equivalência significa que $x+a = y+b$. Da definição da relação esta última igualdade significa que $(x,y) \sim (b,a)$ e então $\overline{(x,y)} = \overline{(b,a)}$. Assim,

$$(-\overline{(a,b)}) + \overline{(a,b)} = \overline{(b,a)} + \overline{(a,b)} = \overline{(a+b,b+a)} = \overline{(0,0)} = 0_{\mathbb{Z}}.$$

Segue que todo elemento $\overline{(a,b)} \in \mathbb{Z}$ possui elemento simétrico à esquerda para a operação de adição, e da comutatividade da adição, tal elemento também é simétrico à direita. Mais ainda $-\overline{(a,b)} = \overline{(b,a)}$. □

Com os resultados desta proposição, temos que $(\mathbb{Z},+)$ é um grupo abeliano.

Teorema 6.26. *A multiplicação de números inteiros satisfaz as propriedades:*

1) *Para todos* $\overline{(a,b)}, \overline{(x,y)}, \overline{(m,n)} \in \mathbb{Z}$ *temos*

$$\overline{(a,b)} \cdot (\overline{(x,y)} \cdot \overline{(m,n)}) = (\overline{(a,b)} \cdot \overline{(x,y)}) \cdot \overline{(m,n)}.$$

2) *Para todos* $\overline{(a,b)}, \overline{(x,y)}, \overline{(m,n)} \in \mathbb{Z}$ *temos*

$$\overline{(a,b)} \cdot (\overline{(x,y)} + \overline{(m,n)}) = \overline{(a,b)} \cdot \overline{(x,y)} + \overline{(a,b)} \cdot \overline{(m,n)}, \qquad e$$
$$(\overline{(x,y)} + \overline{(m,n)}) \cdot \overline{(a,b)} = \overline{(x,y)} \cdot \overline{(a,b)} + \overline{(m,n)} \cdot \overline{(a,b)}.$$

Prova. Para mostrar a associatividade sejam $\overline{(a,b)}, \overline{(x,y)}, \overline{(m,n)} \in \mathbb{Z}$. Então

$$\begin{aligned}
\overline{(a,b)} \cdot (\overline{(x,y)} \cdot \overline{(m,n)}) &= \overline{(a,b)} \cdot \overline{(xm+yn, xn+ym)} \\
&= \overline{(a(xm+yn)+b(xn+ym), a(xn+ym)+b(xm+yn))} \\
&= \overline{(axm+ayn+bxn+bym, axn+aym+bxm+byn)} \\
&= \overline{((ax+by)m+(ay+bx)n, (ax+by)n+(ay+bx)m)} \\
&= \overline{(ax+by, ay+bx)} \cdot \overline{(m,n)} = (\overline{(a,b)} \cdot \overline{(x,y)}) \cdot \overline{(m,n)}.
\end{aligned}$$

Para mostrar a distributividade à esquerda, da multiplicação em relação à adição, suponha que $\overline{(a,b)}, \overline{(x,y)}, \overline{(m,n)} \in \mathbb{Z}$. Então,

$$\overline{(a,b)} \cdot (\overline{(x,y)} + \overline{(m,n)}) = \overline{(a,b)} \cdot \overline{(x+m, y+n)}$$

$$
\begin{aligned}
&= \overline{(a(x+m)+b(y+n), a(y+n)+b(x+m))} \\
&= \overline{(ax+am+by+bn, ay+an+bx+bm)} \\
&= \overline{(ax+by, ay+bx)} + \overline{(am+bn, an+bm)} \\
&= \overline{(a,b)} \cdot \overline{(x,y)} + \overline{(a,b)} + \overline{(m,n)}.
\end{aligned}
$$

A distributividade à direita é análoga. □

Segue que a terna ordenada $(\mathbb{Z}, +, \cdot)$ é um anel. Vamos ainda mostrar que é comutativo, possui unidade e é um anel de integridade.

Teorema 6.27. *A multiplicação é comutativa em $\mathbb{Z}$.*

Prova. Dados $\overline{(a,b)}, \overline{(x,y)} \in \mathbb{Z}$ arbitrários, temos que

$$\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(ax+by, ay+bx)} = \overline{(xa+yb, ya+xb)} = \overline{(x,y)} \cdot \overline{(a,b)},$$

donde segue a comutatividade da multiplicação em $\mathbb{Z}$. □

Teorema 6.28. *O anel comutativo $(\mathbb{Z}, +, \cdot)$ possui unidade, isto é, elemento neutro para a multiplicação.*

Prova. Queremos encontrar $1_{\mathbb{Z}} = \overline{(x,y)} \in \mathbb{Z}$ tal que

$$\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(x,y)} \cdot \overline{(a,b)} = \overline{(a,b)}$$

para qualquer $\overline{(a,b)} \in \mathbb{Z}$. Da igualdade desejada, $\overline{(x,y)} \cdot \overline{(a,b)} = \overline{(a,b)}$, temos que, $\overline{(xa+yb, xb+ya)} = \overline{(a,b)}$. Da definição de classe de equivalência, $(xa+yb, xb+ya) \sim (a,b)$ e da definição da relação segue que x e y devem satisfazer

$$ax + by + b = a + bx + ay,$$

ou ainda

$$ax + b(y+1) = a(y+1) + bx. \tag{6.1}$$

Esta última igualdade norteia a busca do elemento identidade. Podemos perceber que, quaisquer que sejam $a, b \in \mathbb{N}$, a igualdade (6.1) sempre será satisfeita colocando $x = y + 1$.

Desta forma, o número inteiro $1_{\mathbb{Z}} = \overline{(x,y)} \in \mathbb{Z}$ procurado é $\overline{(y+1, y)}$. De fato, para qualquer $\overline{(a,b)} \in \mathbb{Z}$,

$$\overline{(y+1,y)} \cdot \overline{(a,b)} = \overline{((y+1)a+yb, (y+1)b+ya)} = \overline{(ya+a+yb, yb+b+ya)} = \overline{(a,b)}.$$

A segunda igualdade, $\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(a,b)}$, é garantida pela comutatividade da multiplicação. Naturalmente qualquer representante da classe $\overline{(y+1,y)}$ cumpre o papel de unidade. Como $(y+1, y) \sim (1,0)$, então $\overline{(y+1,y)} = \overline{(1,0)}$. O par $(1,0)$ é o representante mais simples da classe $\overline{(y+1,y)}$, e deste ponto em diante, $1_{\mathbb{Z}} = \overline{(1,0)} \in \mathbb{Z}$ será dito a unidade do anel $\mathbb{Z}$. □

Teorema 6.29. *O anel $(\mathbb{Z}, +, \cdot)$ é um anel de integridade.*

Prova. Sejam $\overline{(a,b)}, \overline{(x,y)} \in \mathbb{Z}$, tais que $\overline{(a,b)} \cdot \overline{(x,y)} = 0_{\mathbb{Z}} = \overline{(0,0)}$, e suponha que $\overline{(a,b)} \neq \overline{(0,0)}$. Consequentemente $a \neq b$. Temos então que $\overline{(ax+by, bx+ay)} = \overline{(0,0)}$, e então $(ax+by, bx+ay) \sim (0,0)$. Da definição da relação, segue que

$$ax + by = bx + ay. \tag{6.2}$$

Como $a \neq b$ restam ainda dois casos exclusivos.

Caso 1 $(a < b)$. Existe então $k \in \mathbb{N}^*$ tal que $a + k = b$, e então substituindo isto em (6.2) temos $ax + (a+k)y = (a+k)z + ay$, e pela lei do cancelamento de números naturais para a adição, $ky = kx$. Esta por sua vez, pela lei do cancelamento de números naturais não nulos para a multiplicação, nos leva a $x = y$.

Caso 2 $(b < a)$. Neste caso $a = b + k$ para algum $k \in \mathbb{N}^*$. Substituindo em (6.2) chegamos a $(b+k)x + by = bx + (b+k)y$ e pelas mesmas leis de cancelamento citadas no caso 1, temos também $x = y$.

Em qualquer caso, segue que $x = y$ o que significa que $\overline{(x,y)} = \overline{(x,x)} = \overline{(0,0)}$. Isto significa que se a multiplicação de dois termos é nula em $\mathbb{Z}$, um dos termos deve obrigatoriamente ser nulo. □

Isto posto, $\mathbb{Z} = \frac{\mathbb{N}\times\mathbb{N}}{\sim}$ é um anel de integridade chamado anel dos inteiros. É fácil ver que este anel de integridade não é corpo. O que precisamos para isto é encontrar um número inteiro não nulo que não admita simétrico para a multiplicação.

Mostraremos que elementos da forma $\overline{(a,0)}$ admitem simétrico multiplicativo somente para $a = 1$. De fato, supondo $\overline{(x,y)} \in \mathbb{Z}$ tal que $\overline{(x,y)} \cdot \overline{(a,0)} = 1_{\mathbb{Z}} = \overline{(1,0)}$, então temos que

$$\overline{(ax, ay)} = \overline{(ax + 0 \cdot y, ya + 0 \cdot x)} = \overline{(x,y)} \cdot \overline{(a,0)} = \overline{(1,0)},$$

e da igualdade entre classes de equivalência, segue que

$$ay + 1 = ax + 0 = ax.$$

Nestes termos o par (x,y) deve obrigatoriamente satisfazer $y \leq x$. Do contrário, se $x \leq y$ então existe $n \in \mathbb{N}$ tal que $x + n = y$ o que nos traz $ax = ay + 1 = ax + an + 1$, e pela lei do cancelamento, $0 = an + 1$, que não é satisfeita para quaisquer $a, n \in \mathbb{N}$, uma vez que $0 \notin s(\mathbb{N})$ e no entanto, $an + 1 = an + s(0) = s(an) \in s(\mathbb{N})$.

Resta que $y \leq x$, e desta forma, $y + n = x$ para algum $n \in \mathbb{N}$. Então

$$ay + 1 = ax = a(y+n) = ay + an,$$

donde segue que $an = 1$ e portanto $a = n = 1$. O único inteiro $\overline{(a,0)}$ que admite simétrico multiplicativo é então $\overline{(1,0)}$, sendo neste caso, $\overline{(x,y)} = \overline{(y+1,y)} = \overline{(1,0)}$ o seu simétrico.

Vamos agora mostrar que o conjunto dos números naturais é isomorfo a um subconjunto do conjunto dos números inteiros. Seja

$$S = \{\overline{(a,0)}; \quad a \in \mathbb{N}\}.$$

Claramente $S \subset \mathbb{Z}$. A aplicação $f : \mathbb{N} \to S$, dada por $f(a) = \overline{(a,0)}$ é bijetora. De fato, a sobrejetividade é consequência imediata da própria definição de S. Para a injetividade, sejam $a, b \in \mathbb{N}$ tais que $f(a) = f(b)$, isto é, $\overline{(a,0)} = \overline{(b,0)}$ e da igualdade de classes de equivalência temos que $a + 0 = b + 0$, donde $a = b$, e isto mostra a injetividade de f.

Para mostrar que é isomorfo, sejam $a, b \in \mathbb{N}$. Então

$$f(a+b) = \overline{(a+b,0)} = \overline{(a,0)} + \overline{(b,0)} = f(a) + f(b),$$

e também

$$f(ab) = \overline{(ab,0)} = \overline{(a,0)} \cdot \overline{(b,0)} = f(a) \cdot f(b).$$

Temos então que $\mathbb{N}$ é isomorfo a S, um subconjunto de $\mathbb{Z}$, o que nos permite olhar para $\mathbb{N}$ como um subconjunto de $\mathbb{Z}$, pois existe uma "cópia" de $\mathbb{N}$ dentro de $\mathbb{Z}$. A aplicação f é dita inclusão de $\mathbb{N}$ em $\mathbb{Z}$.

Vamos agora estabelecer uma relação de ordem (total) sobre o conjunto $\mathbb{Z}$. Definimos a relação $\leq$ dada por

$$\overline{(a,b)} \leq \overline{(x,y)} \quad \Leftrightarrow \quad \text{existe} \quad n \in \mathbb{N} \quad \text{tal que} \quad a + y + n = x + b.$$

Teorema 6.30. *A relação $\leq$ é uma relação de ordem total em $\mathbb{Z}$.*

Prova. Dado qualquer $(a,b) \in \mathbb{Z}$, temos que $a + b + 0 = a + b$, e da definição da relação, $\overline{(a,b)} \leq \overline{(a,b)}$. A relação é então reflexiva.

Sejam agora $\overline{(a,b)}, \overline{(x,y)} \in \mathbb{Z}$ tais que $\overline{(a,b)} \leq \overline{(x,y)}$ e que $\overline{(x,y)} \leq \overline{(a,b)}$. Então existem $m, n \in \mathbb{N}$ tal que $a+y+n = x+b$ e $x+b+m = a+y$. Segue que $a+y = x+b+m = a+y+n+m$ e da lei do cancelamento vem $m + n = 0$. Mas como $m, n \in \mathbb{N}$ esta igualdade somente ocorre se $m = n = 0$. Segue que $x + b = a + y + n = a + y$, o que significa que $(a,b) \sim (x,y)$, e da igualdade de classes que $\overline{(a,b)} = \overline{(x,y)}$. Segue que a relação é antissimétrica.

Dados $\overline{(a,b)}, \overline{(x,y)}, \overline{(p,q)} \in \mathbb{Z}$ tais que $\overline{(a,b)} \leq \overline{(x,y)}$ e $\overline{(x,y)} \leq \overline{(p,q)}$, temos que existem $m, n \in \mathbb{N}$ tais que $a+y+n = x+b$ e $x+p+m = y+q$. Assim, $a+y+n+p+m = x+b+p+m = y + b + q$ e então $a + p + (n + m) = b + q$. Segue da definição da relação que $\overline{(a,b)} \leq \overline{(p,q)}$, e a relação é transitiva.

Resta mostrar que a ordem é total. Dados quaisquer $\overline{(a,b)}, \overline{(x,y)} \in \mathbb{Z}$, temos que $a + y$ e $b + x$ são dois números naturais. Da relação de ordem total dos números naturais, temos que $a + y \leq b + x$ ou $b + x \leq a + y$. Se $a + y \leq b + x$ então da definição da relação de ordem dos naturais, temos que $a+y+n = b+x$ para algum $n \in \mathbb{N}$, e então $\overline{(a,b)} \leq \overline{(x,y)}$. Se $b+x \leq a+y$ então existe $n \in \mathbb{N}$ tal que $b + x + n = a + y$ o que significa que $\overline{(x,y)} \leq \overline{(a,b)}$. A relação de ordem é portanto total. □

Observe que dados $a, x \in \mathbb{N}$, temos que $a \leq x$, se e somente se, existe $n \in \mathbb{N}$ tal que $a + n = x$, se e somente se $\overline{(a,0)} \leq \overline{(x,0)}$, se e somente se $f(a) \leq f(b)$, sendo f o isomorfismo inclusão de $\mathbb{N}$ em $\mathbb{Z}$. Isto significa que a relação $\leq$ dos números inteiros é compatível com a relação $\leq$ dos números naturais.

6.3 Construção dos números racionais

A construção dos números racionais não será aqui desenvolvida pois já foi esquematizada na seção 4.2. Naquela seção construímos, de uma forma geral, o corpo das frações de um anel de integridade. Se este anel de integridade for o conjunto dos números inteiros, então o corpo das frações obtido naquela seção, é o corpo dos números racionais.

6.4 Construção dos números reais

Fazer esta seção... Usar o método dos cortes de Dedekind...

Capítulo 7

Módulos sobre anéis comutativos

Na Álgebra Linear, os conjuntos envolvidos são os espaços vetoriais, que são conjuntos munidos de uma soma interna, e uma multiplicação por escalar, sendo que este escalar é um elemento de um corpo. O conceito de módulo, é uma generalização do conceito de espaço vetorial, quando o conjunto de escalares é um anel. Quando este anel for um corpo, então a definição de módulo, coincidirá com a definição de espaço vetorial da Álgebra Linear.

7.1 Módulos e submódulos

Definição 7.1. Seja $(A, *, \circ)$ um anel com unidade 1_A. Um grupo abeliano $(M, +)$, juntamente com uma operação $\cdot : A \times M \to M$, é dito um *A-módulo*, se

$i)$ $(a * b) \cdot x = a \cdot x + b \cdot x$

$ii)$ $a \cdot (x + y) = a \cdot x + a \cdot y$

$iii)$ $(a \circ b) \cdot x = a \cdot (b \cdot x)$

$iv)$ $1_A \cdot x = x$

para quaisquer $a, b \in A$ e $x, y \in M$.

Na definição, a operação $\cdot$ é denominada *multiplicação por escalar*, e os elementos do conjunto A são denominados *escalares*. A definição sugere que M seja chamado de um A-módulo a esquerda. Podemos estabelecer um A-módulo a direita definindo o produto por escalar como $\cdot : M \times A \to M$, com o anel de escalares a direita. É possível ainda verificar que se A é um anel comutativo, então as definições de módulo a direita e a esquerda coincidem. No que se segue trabalharemos sempre com anéis comutativos.

Proposição 7.2. *Se $(A, *, \circ)$ é um anel, comutativo e com unidade, e $(M, +)$ é um A-módulo, então valem as seguintes propriedades*

$i)$ $0_A \cdot m = a \cdot 0_M = 0_M$,

$ii)$ $a \cdot (m') = (a') \cdot m = (a \cdot m)'$

para todos $a \in A$ e $m \in M$.

Prova. Sejam $a \in A$ e $m \in M$ quaisquer, então para $i)$ notemos que

$$(a \cdot m) + (0_A \cdot m) \quad = \quad (a * 0_A) \cdot m = (a \cdot m), \qquad \text{e}$$

$$(a \cdot m) + (a \cdot 0_M) \quad = \quad a \cdot (m + 0_M) = (a \cdot m).$$

Isto significa que $(0_A \cdot m)$ e $(a \cdot 0_M)$ são elementos neutros para a operação $+$ em M, e da unicidade do elemento neutro, temos $0_M = (0_A \cdot m) = (a \cdot 0_M)$.

Para provar ii), notemos que

$$\begin{aligned} (a \cdot m) + (a' \cdot m) &= (a * a') \cdot m = 0_A \cdot m \overset{(i)}{=} 0_M, \qquad \text{e} \\ (a \cdot m) + (a \cdot m') &= a \cdot (m + m') = a \cdot 0_M \overset{(ii)}{=} 0_M, \end{aligned}$$

e então, $(a' \cdot m)$ e $(a \cdot m')$ são simétricos de $(a \cdot m)$, e da unicidade do simétrico temos que $(a \cdot m)' = (a' \cdot m) = (a \cdot m')$, que encerra esta demonstração. □

Definição 7.3. Um subconjunto $H \neq \emptyset$ de um A-módulo M, é dito um *A-submódulo*, ou simplesmente um submódulo, de M, se

i) H é subgrupo de M (isto é, $(m - n) \in H$ para todos $m, n \in H$),

ii) $a \cdot n \in H$ para todos $a \in A$ e $n \in H$.

Quando o anel A for um corpo, então a definição de submódulo coincide com a definição de subespaço vetorial.

Vejamos agora como é possível construir um submódulo a partir de um subconjunto de elementos de um A-módulo M. Dado um A-módulo $(M, +)$, escolhemos um subconjunto $S = \{m_1, m_2, \ldots, m_k\}$ de $k \geq 1$ elementos de M. Consideremos o subconjunto

$$\langle S \rangle = \{a_1 \cdot m_1 + a_2 \cdot m_2 + \cdots + a_k \cdot m_k; \quad a_i \in A \quad \text{para} \quad 1 \leq i \leq k\}.$$

de M, gerado pelos elementos de S.

Observemos que: O conjunto $\langle S \rangle$ é não vazio, pois $S \subset \langle S \rangle$. $\langle S \rangle$ é um subgrupo de M. De fato, se $x, y \in \langle S \rangle$, então

$$\begin{aligned} x &= a_1 \cdot m_1 + a_2 \cdot m_2 + \cdots + a_k \cdot m_k, \text{ com } a_i \in A, \quad \text{e} \\ y &= b_1 \cdot m_1 + b_2 \cdot m_2 + \cdots + b_k \cdot m_k, \text{ com } b_i \in A, \end{aligned}$$

e desta forma,

$$\begin{aligned} x - y &= x + y' \\ &= (a_1 \cdot m_1 + a_2 \cdot m_2 + \cdots + a_k \cdot m_k) + (b_1 \cdot m_1 + b_2 \cdot m_2 + \cdots + b_k \cdot m_k)' \\ &= (a_1 \cdot m_1) + (a_2 \cdot m_2) + \cdots + (a_k \cdot m_k) + (b_1 \cdot m_1)' + (b_2 \cdot m_2)' + \cdots + (b_k \cdot m_k)' \\ &= (a_1 \cdot m_1) + (a_2 \cdot m_2) + \cdots + (a_k \cdot m_k) + (b'_1 \cdot m_1) + (b'_2 \cdot m_2) + \cdots + (b'_k \cdot m_k) \\ &= (a_1 \cdot m_1) + (b'_1 \cdot m_1) + (a_2 \cdot m_2) + (b'_2 \cdot m_2) + \cdots + (a_k \cdot m_k) + (b'_k \cdot m_k) \\ &\overset{(i)}{=} (a_1 * b'_1) \cdot m_1 + (a_2 * b'_2) \cdot m_2 + \cdots + (a_k * b'_k) \cdot m_k, \end{aligned}$$

que pertence a $\langle S \rangle$ pois cada $(a_i * b'_i) \in A$. Também, se $a \in A$, então

$$\begin{aligned} a \cdot x &= a \cdot (a_1 \cdot m_1 + a_2 \cdot m_2 + \cdots + a_k \cdot m_k) \\ &\overset{(ii)}{=} a \cdot (a_1 \cdot m_1) + a \cdot (a_2 \cdot m_2) + \cdots + a \cdot (a_k \cdot m_k) \end{aligned}$$

$$\stackrel{(iii)}{=} (a \circ a_1) \cdot m_1 + (a \circ a_2) \cdot m_2 + \cdots + (a \circ a_k) \cdot m_k,$$

que pertence a $\langle S \rangle$ pois cada $(a * a_i) \in A$. Os símbolos $\stackrel{(ii)}{=}$ e $\stackrel{(iii)}{=}$ significam que as igualdades são justificadas respectivamente pelos itens (ii) e (iii) da definição de A-módulo.

Estas três observações mostram que $\langle S \rangle$ satisfaz as condições da definição de submódulo, e portanto é um submódulo de M, chamado de *submódulo gerado* pelo conjunto S. O caso particular em que $S = \{m\}$, então $\langle S \rangle = \{a \cdot m; a \in A\}$ e $\langle S \rangle$ é chamado de *submódulo cíclico* gerado por m.

Se $M = \langle S \rangle$ então dizemos que S é um *subconjunto gerador* do módulo M. Os elementos de S são chamados *elementos geradores* de M. Além disso, se S possui um único elemento, $M = \langle S \rangle$ é dito um *módulo cíclico*.

Definição 7.4. Se H_1 e H_2 são submódulos de um A-módulo $(M, +)$, então a soma de H_1 com H_2 é o subconjunto de $(M, +)$, denotado por $H_1 + H_2$, e dado por

$$H_1 + H_2 = \{x + y; \quad x \in H_1, \quad y \in H_2\}.$$

Definição 7.5. Dados dois A-módulos M e N, um homomorfismo de M em N, é uma aplicação $\varphi : M \to N$, tal que

$i)$ $\varphi(x + y) = \varphi(x) + \varphi(y)$, e

$ii)$ $\varphi(a \cdot x) = a \cdot \varphi(x)$,

para todos $x, y \in M$ e $a \in A$.

Note que da condição $i)$ desta definição, um homomorfismo φ entre os módulos M e N é um homomorfismo entre os grupos abelianos M e N, e portanto todas as propriedades vistas na seção (2.2) podem ser utilizadas, bem como a definição de núcleo de um homomorfismo, isto é,

$$Ker(\varphi) = \varphi^{-1}(0_N) = \{x \in M; \quad \varphi(x) = 0_N\}.$$

Da mesma forma que no caso de grupos e anéis, um homomorfismo sobrejetor é chamado de epimorfismo, um homomorfismo injetor é chamado de monomorfismo, um homomorfismo de um módulo M em M é chamado de endomorfismo e finalmente, um homomorfismo bijetor é chamado de isomorfismo. Neste último caso, os módulos M e N são ditos isomorfos e representaremos este fato escrevendo $M \approx N$.

Se o anel A for um corpo, então o conjunto de todos os homomorfismos é precisamente o conjunto das transformações lineares de M em M. Observe que as condições $i)$ e $ii)$ são as condições de linearidade de uma transformação. O conjunto de todos os homomorfismos do A-módulo M no A-módulo N é denotado por $Hom(M, N)$ e este conjunto munido da composição de funções é também um A-módulo. Deixamos este fato como exercício.

Proposição 7.6. *Se $(M, +)$ e $(N, +)$ são A-módulos e $\varphi : M \to N$ é um homomorfismo, então $Ker(\varphi)$ é um A-submódulo de M.*

Prova. Da proposição (2.19) já sabemos que $Ker(\varphi)$ é subgrupo de N. Além disso, dados $a \in A$ e $x \in Ker(\varphi)$, arbitrários, temos que $(a \cdot x) \in M$ e,

$$\varphi(a \cdot x) = a \cdot (\varphi(x)) = a \cdot 0_N = 0_N,$$

desta forma $(a \cdot x) \in Ker(\varphi)$, portanto $Ker(\varphi)$ é submódulo de M. □

Proposição 7.7. *Se $(M,+)$ e $(N,+)$ são A-módulos e $\varphi : M \to N$ é um homomorfismo, então $Im(\varphi)$ é um A-submódulo de N.*

Prova. No corolário (**??**) já mostramos que $Im(\varphi)$ é subgrupo de N. Mostraremos agora o item $ii)$ da definição de submódulo. Sejam então $a \in A$ e $y \in Im(f) \subset N$. Existe então $x \in M$ tal que $\varphi(x) = y$. Assim $(a \cdot x) \in M$, e

$$\varphi(a \cdot x) = a \cdot \varphi(x) = a \cdot y,$$

mostrando que $a \cdot y$ é imagem de alguém de M, logo $(a \cdot y) \in Im(\varphi)$. Segue que $Im(\varphi)$ é de fato submódulo de N. □

7.2 Módulo quociente

Vamos agora construir o conceito de módulo quociente. Seja H um submódulo do A-módulo $(M,+)$, e então como M é abeliano, temos que $H \lhd M$, e podemos falar no grupo $\frac{M}{H}$, quociente de M por H. Lembremos que o grupo quociente é o grupo das classes laterais,

$$\frac{M}{H} = \{x + H; \quad x \in M\} \quad \text{onde} \quad x + H = \{x + h; \quad h \in H\},$$

com a operação dada por

$$(x + H) + (y + H) = (x + y) + H.$$

O elemento neutro desta operação é $0_M + H = H$ e para cada $(x+H) \in \frac{M}{H}$, o simétrico de $(x+H)$ é $(x'+H) \in \frac{M}{H}$ uma vez que $x' \in M$ para todos $x \in M$. Além disso, $x+H = y+H \Leftrightarrow (x-y) \in H$.

Proposição 7.8. *Se $(M,+)$ é um A-módulo e H é um submódulo de M, então o grupo quociente $\frac{M}{H}$ com o produto por escalar*

$$\begin{array}{rcl} \cdot : A \times \dfrac{M}{H} & \to & \dfrac{M}{H} \\ (a, x + H) & \mapsto & a \cdot (x + H) = (a \cdot x) + H \end{array}$$

é um A-módulo, chamado A-módulo quociente de M por H.

Prova. Primeiramente vamos verificar que a operação $\cdot$ está bem definida. Se $x + H = y + H$ então $(x - y) \in H$, e então $a \cdot (x - y) \in H$ para qualquer escalar $a \in A$, pois H é submódulo. Como $(a \cdot x) - (a \cdot y) = a \cdot (x - y)$, temos $(a \cdot x) - (a \cdot y) \in M$, donde $(a \cdot x) + H = (a \cdot y) + H$, que mostra que $\cdot$ não depende do representante escolhido em cada classe de $\frac{M}{H}$.

Vamos agora verificar os axiomas da definição de módulo. Sejam $a, b \in A$ e $m, n \in \frac{M}{H}$, então, $m = x + H$ e $n = y + H$ com $x, y \in M$. Temos assim

$$\begin{array}{rcl} (a * b) \cdot m & = & (a * b) \cdot (x + H) = ((a * b) \cdot x) + H = (a \cdot x * b \cdot x) + H = \\ & & (a \cdot x) + H) + ((b \cdot x) + H) = a \cdot (x + H) + b \cdot (x + H) = a \cdot m + b \cdot m, \\ a \cdot (m + n) & = & a \cdot ((x + H) + (y + H)) = a \cdot ((x + y) + H) = \\ & & (a \cdot (x + y)) + H = (a \cdot x + a \cdot y) + H = \end{array}$$

$$
\begin{aligned}
& ((a\cdot x)+H)+((a\cdot y)+H) = a\cdot(x+H)+a\cdot(y+H) = a\cdot m + a\cdot n,\\
(a\circ b)\cdot m &= (a\circ b)\cdot(x+H) = ((a\circ b)\cdot x)+H) =\\
& (a\cdot(b\cdot x))+H = a\cdot((b\cdot x)+H) = a\cdot(b\cdot(x+H)) = a\cdot(b\cdot m),\\
1_A\cdot m &= 1_A\cdot(x+H) = (1_A\cdot x)+H = x+H = m.
\end{aligned}
$$

Portanto, o produto por escalar dado como acima, define no grupo quociente $\frac{M}{H}$ uma estrutura de A-módulo. □

Como já vimos que o núcleo $Ker(\varphi)$, e a imagem $Im(\varphi)$ de um homomorfismo $\varphi : M \to N$ são submódulos de M e N respectivamente, então podemos escrever os módulos quociente $\frac{M}{Ker(\varphi)}$ e $\frac{N}{Im(\varphi)}$, e estamos prontos para o Teorema Fundamental do Homomorfismo de módulos.

Teorema 7.9 (Teorema Fundamental do Homomorfismo)**.** *Seja $f : M \to N$ um homomorfismo sobrejetor entre os A-módulos M e N. Então*

$$\frac{M}{Ker(f)} \approx Im(f).$$

Prova. Vamos denotar $K = Ker(f)$ e considerar a aplicação

$$
\begin{aligned}
\varphi : \frac{M}{K} &\to Im(f) \subset N\\
(x+K) &\mapsto \varphi(x+K) = f(x),
\end{aligned}
$$

e mostrar que φ é de fato um isomorfismo. Primeiramente, devemos mostrar que φ está bem definida. Para tanto, sejam $x+K = y+K$ representantes da mesma classe. Temos então que $(x-y) \in K = Ker(f)$ e então $f(x-y) = 0_N$, logo $f(x) = f(y)$ em $Im(f)$.

Tomemos agora $a \in A$ e $m, n \in \frac{M}{K}$, e então $m = (x+K)$ e $n = (y+K)$. Desta forma

$$
\begin{aligned}
\varphi(m+n) &= \varphi((x+K)+(y+K)) = \varphi((x+y)+K) =\\
& f(x+y) = f(x)+f(y) = \varphi(x+K)+\varphi(y+K) = \varphi(m)+\varphi(n)\\
\varphi(a\cdot m) &= \varphi(a\cdot(x+K)) = \varphi((a\cdot x)+K) =\\
& f(a\cdot x) = a\cdot f(x) = a\cdot\varphi(x+K) = a\cdot\varphi(m),
\end{aligned}
$$

mostrando que φ é um homomorfismo. Para provar que φ é uma bijeção, seja $y \in Im(f)$. Então existe $a \in M$ com $f(a) = y$. Escolhemos $x = a+K \in \frac{M}{K}$ e temos $\varphi(x) = \varphi(a+K) = f(a) = y$ mostrando a sobrejetividade de φ. Sejam agora $(x+K), (y+K) \in \frac{M}{K}$ com $\varphi(x+K) = \varphi(y+K)$. Segue que

$$\varphi(x+K) = \varphi(y+K) \quad \Rightarrow \quad f(x) = f(y) \quad \Rightarrow \quad f(x)-f(y) = 0_N \quad \Rightarrow \quad f(x-y) = 0_N,$$

donde $(x-y) \in Ker(f) = K$, e então $x+K = y+K$, provando que φ é injetora. Fica então concluído que φ é um isomorfismo e portanto $\frac{M}{Ker(f)} \approx Im(f)$. □

Corolário 7.10. *Seja $f : M \to N$ um homomorfismo sobrejetor entre os A-módulos M e N. Então*

$$\frac{M}{Ker(f)} \approx N.$$

Corolário 7.11. *Seja $f : M \to N$ um homomorfismo sobrejetor entre os A-módulos M e N, então*

i) Se S é submódulo de M, $\frac{M}{S} \approx \frac{N}{f(S)}$,
ii) Se S é submódulo de N, $\frac{M}{f^{-1}(S)} \approx \frac{N}{S}$.

Prova. Fazer esta demonstração (primeiro ver se funciona) ... □

Proposição 7.12. *Todo submódulo H de um A-módulo $(M, +)$ é o núcleo de algum homomorfismo.*

Prova. Vamos construir tal homomorfismo. Seja $\frac{M}{H}$ o A-módulo quociente de M por seu submódulo H. Em $\frac{M}{H}$ estamos considerando a soma de classes $(a + H) + (b + H) = (a * b) + H$ e o produto por escalar definido em (7.8). Considere a aplicação

$$\begin{array}{rcl} \eta : M & \to & \dfrac{M}{H} \\ x & \mapsto & \eta(x) = x + H. \end{array}$$

Primeiro mostremos que η é homomorfismo. De fato, se $x, y \in M$ e $a \in A$, temos,

$$\begin{aligned} \eta(x + y) &= (x + y) + H = (x + H) + (y + H) = \eta(x) + \eta(y), \\ \eta(a \cdot x) &= (a \cdot x) + H = a \cdot (x + H) = a \cdot \eta(x), \end{aligned}$$

e então η é de fato um homomorfismo. Resta mostrar $H = Ker(\eta)$. Para tanto, mostraremos a dupla inclusão. Tomemos $x \in H$ arbitrário. Como $x \in H$, então $x + H = H$, e sabemos que $0_{M/H} = 0_M + H = H$, e desta forma,

$$\eta(x) = x + H = H = 0_{M/H},$$

mostrando que $x \in Ker(\eta)$ e consequentemente $H \subset Ker(\eta)$. Reciprocamente, seja $x \in Ker(\eta)$. Então $\eta(x) = 0_{M/H}$, donde $x+H = 0_{M/H} = 0_M+H$. Mas de $x+H = 0_M+H$ temos $x-0_M \in H$, ou $x \in H$, mostrando que $Ker(\eta) \subset H$, e concluindo que $H = Ker(\eta)$. □

7.3 Módulos livres

Fazer esta seção....

Apêndice A

Notas históricas

Nota A.1. Niels Henrik Abel, de família pobre, nasceu no dia 5 de agosto de 1802 na ilha de Finnöy, Noruega. Abel, assim como seus contemporâneos, queria solucionar as equações algébricas de quinto grau, um dos grandes desafios de sua época, e enquanto estudante secundarista, publicou uma nota sobre a equação geral de quinto grau $x^5+a_1x^4+a_2x^3+a_3x^2+a_4x+a_5 = 0$. O pai de Abel, um ministro protestante, morreu em 1820, e Abel teve que assumir a responsabilidade de cuidar (inclusive financeiramente) da sua mãe e seus seis irmãos. Auxiliado por Holmboe, seu professor, que angariou recursos, Abel ingressou em 1821 na Universidade de Christiania (atual Oslo), e se graduou em 1822. Em 1824, contrariando seus próprios sonhos, Abel provou a impossibilidade de representação de solução de equações de quinto grau por meio de expressões radicais, e afirmou que um grupo finito é solúvel se contém uma cadeia de subgrupos, $G_0, G_1, \ldots, G_n$ em que, para cada i, G_i é normal em G_{i-1} e o grupo quociente G_{i-1}/G_i é cíclico. Gauss, recusou-se a ler o artigo, exclamando: *"aqui está mais uma monstruosidade!"*, provocando uma profunda antipatia por parte de Abel, que dali para frente, sempre que podia, criticava Gauss. Abel também investigou generalizações do teorema binomial, e mostrou que as funções elípticas são generalizações das funções trigonométricas. Em 1825, Abel encontrou August Leopold Crelle (1780-1856) que lhe ajudou a ser reconhecido. Crelle fundou na época o *Journal für die reine und angewandte Mathematik* (Jornal para Matemática pura e aplicada). Os primeiros três números deste jornal, continham vinte e dois artigos de Abel. Há controvérsias sobre quem ajudou quem neste caso. O jornal foi o primeiro periódico no mundo devotado exclusivamente à pesquisa matemática, e só aceitava trabalhos inéditos, verdadeiros e de importância significativa. Em 1826, Abel visitou Legendre e Cauchy em Paris, onde tentou sem êxito mostrar suas descobertas. Numa de suas cartas a um amigo escreveu: *"Todo principiante tem muita dificuldade em se fazer notar aqui. Acabei um extenso tratado sobre certas classes de funções transcendentes mas Cauchy não se dignou a olhá-lo"*. Ainda em 1826, Abel publicou *Memória*, que trata sobre uma propriedade de uma classe de funções transcendentes. Publicou, em 1827, o seu principal trabalho com o título *Recherches sur les fonctions elliptiques*. Este trabalho deveria ser mostrado a Academia de Ciências de Paris, onde Cauchy e Legendre foram designados para referendar o trabalho. Legendre reclamou que o memorial era ilegível, escrito com tinta quase branca e letras mal formadas. Cauchy levou o memorial para casa e jogou-o num canto qualquer esquecendo-o. Em 1829, Jacobi, numa carta para Legendre, pergunta: *"Que descoberta é esta do Sr. Abel? Alguém a viu? Como pode ter acontecido que esta descoberta, talvez a mais im-*

portante feita neste século, comunicada a sua Academia há dois anos, tenha escapado à atenção de seus colegas?". O cônsul norueguês em Paris levantou uma questão diplomática acerca do manuscrito perdido. Cauchy achou-o em 1830. Foi impresso em 1841, lamentavelmente 12 anos depois da morte de Abel. Abel morreu de tuberculose, aos 26 anos, na manhã do dia 6 de abril de 1829. A seu respeito, Charles Hermite disse: *"Abel deixou o suficiente para manter os matemáticos ocupados durante quinhentos anos"*.

Nota A.2. Peter Ludwig Mejdell Sylow, nasceu em 12 de Dezembro de 1832 em Christiania (atual Oslo) na Noruega. Sylow estudou na Universidade de Christiania, onde ganhou um torneio de matemática em 1853, e se graduou em 1856. Devido a falta de vagas para lecionar na universidade, começou ensinar matemática na cidade de Frederikshald em 1858. Trabalhou primeiramente com funções elípticas, inspirado por seu professor de matemática pura, Ole Jacob Broch. Encontrou mais tarde trabalhos de Abel, em solubilidade de equações algébricas por radicais, que achou mais interessante. Em 1861, em Paris, assistiu aulas de Chasles em teoria das cônicas, de Liouville em mecânica racional e de Duhamel em teoria dos limites. Em Berlin, teve proveitosas conversas com Kronecker, mas não conseguiu assistir aulas de Weierstrass, que estava doente na época. Em 1862, substituindo Broch, Sylow conferenciou na Universidade de Christiania, onde explicou trabalhos de Abel e Galois em equações algébricas. Todavia apesar de não provar os Teoremas de Sylow nesta época (ele os publicou 10 anos depois) ele apresentou questões sobre eles. Depois de provado o Teorema de Cauchy, que afirma que um grupo de ordem divisível por um primo p tem um subgrupo de ordem p, Sylow perguntou então se isto poderia ser generalizado para potências de p. Em 1872, Sylow publicou o artigo *Théorèmes sur les groupes de substitutions*, na *Mathematische Annalen*, volume 5 (584 - 594), onde figuram os três Teoremas de Sylow. Quase todos os trabalhos sobre grupos finitos usam os Teoremas de Sylow. Sylow tornou-se um editor da *Acta Mathematica* e em 1894, foi agraciado com o título de doutor honorário da universidade de Copenhagen. Lie criou uma cadeira especial para Sylow na universidade de Christiania e Sylow ensinou lá a partir de 1898. Sylow morreu em 7 de Setembro de 1918 também em Christiania.

Nota A.3. Évariste Galois, nasceu num vilarejo, próximo a Paris, chamado Bourg-l'Egalité, (agora Bourg-la-Reine) no dia 25 de outubro de 1811. Seu pai, Nicholas Gabriel Galois, um homem muito culto foi prefeito de Bourg-l'Egalité, e sua mãe Adelaide Marie Demante, com formação em filosofia, literatura clássica e religião, ensinava grego, latim e religião a Évariste até seus doze anos. Em 1823, Galois ingressa no internato Lycée de Louis-le-Grand. Não era um bom aluno, sendo considerado abaixo do padrão exigido, entretanto, no internato teve a oportunidade de ler trabalhos de Lagrange e Legendre, quando descobriu sua vocação para a matemática. Em 1827, Galois ingressou no seu primeiro curso de matemática. Mas seu sonho era a Écòle Polytechnique de Paris (fundada por Napoleão Bonaparte), e em 1828, se submeteu, sem êxito, ao exame da Écòle Polytechnique. Passou a assistir, como ouvinte, na Écòle Polytechnique, as aulas ministradas por Louis Paul Émile Richard, que reconheceu o gênio precoce, e lhe facilitou o acesso aos trabalhos contemporâneos de Abel, Cauchy, Gauss e Jacobi. Em abril de 1829, Galois publicou o seu primeiro trabalho sobre funções contínuas nos *Annales de Mathématiques* e no mês seguinte, submeteu artigos relacionados com a solução de equações algébricas à Academia de Ciências em que Cauchy fora designado para julgar. Em julho de 1829, abalado pela recente morte de seu pai, Galois apresentou-se mais uma vez para

exame na Écòle Polytechnique, e irritando-se com o examinador Monsieur Dinet, atirou-lhe um apagador na cabeça. Há controvérsias sobre a veracidade deste acontecimento. Galois desejava resolver a equação geral de quinto grau que era um dos desafios de sua época. O trabalho de Abel neste assunto, inspirou Galois que procurou razões mais profundas da insolubilidade das equações algébricas. Galois então enunciou que *Uma equação algébrica pode ser resolvida por meio de radicais se e somente se o seu grupo, em relação ao corpo de seus coeficientes, é solúvel*. Em dezembro de 1829, Galois foi admitido na Écòle Normale Supérieure. Em fevereiro de 1830, Galois enviou a Cauchy trabalhos adicionais sobre as teorias das equações. Cauchy ficou impressionado com os trabalhos, e julgou-o digno de participar da competição do Grande Prêmio de Matemática da Academia. Galois, imediatamente juntou os trabalhos em uma única memória e remeteu-os ao secretário da Academia, Jean Baptiste Fourier, que faleceu logo após receber os papéis, que desta forma se perderam e não foram avaliados para o prêmio. Ainda em 1830, Galois redigiu um manifesto violento, contra o diretor Monsieur Guigniault, e foi expulso da Écòle Normale Supérieure. Depois disso, Galois esteve envolvido em movimentos contra o Rei Louis-Phillipe I, e foi preso duas vezes. Nesse período, ficara sabendo que sua memória fora rejeitada, sob alegação de que a redação era demasiadamente concisa, tornando a leitura incompreensível. Na prisão de Sieur Faultrier conheceu Stéphanie-Félice Poterine du Motel, e se apaixonou. Quando libertado, em abril de 1832, começou a troca de cartas com Stéphanie, que estava comprometida com Pescheux d'Herinville e que, descobrindo a infidelidade da noiva, desafiou Galois para um duelo a fim de lavar a sua honra. Na noite que antecedia o duelo, Galois escreveu uma carta *Lettre à Auguste Chevalier*, solicitando ao amigo Chevalier que submetesse os seus trabalhos à apreciação de Gauss e Jacobi. A carta dizia o seguinte: *"(...) Fiz novas descobertas em análise. (...) Na teoria da equações pesquisei as condições para a solução de equações por radicais. Aprofundei esta teoria e descrevi todas as transformações possíveis em uma equação, mesmo ela não sendo resolvida por radicais. Todas as descobertas estão aqui, nesses três ensaios matemáticos. (...) Por favor, peça a Gauss e a Jacobi para que dêem opiniões, não pela verdade, mas devido a importância desses teoremas. Espero que alguns homens achem valioso analisar esta misturada (...)"*. Na manhã da quarta-feira do dia 30 de maio de 1832, Galois e D'Herbinville se enfrentaram armados com pistolas e Galois foi baleado no estômago. No dia 31 de maio de 1832, Galois não resistiu e faleceu. Após a sua morte, o irmão de Galois, e Auguste Chevalier copiaram os ensaios matemáticos e os enviaram em setembro de 1832 a Gauss, Jacobi e outros matemáticos. Somente em 1846, uma cópia dos trabalhos de Galois chegou às mãos de Joseph Liouville que reconheceu o magnífico trabalho, editou e publicou parte dos manuscritos no *Journal de Mathématiques Pures et Appliquées*. Galois tinha de fato formulado uma completa explicação de como se poderia obter soluções para equações do quinto grau. Estabeleceu as condições sob as quais uma equação algébrica admite uma solução por radicais, e examinou as equações de grau maior do que cinco, identificando as que tinham soluções. Galois foi considerado o verdadeiro iniciador da teoria dos grupos, e a ele deve-se também o termo *grupo*.

Nota A.4. Joseph Louis de Lagrange nasceu em 25 de janeiro de 1736, em Turim, na Itália. Foi educado em Turim e aos dezesseis anos foi nomeado professor de geometria na Real Escola de Artilharia de Turim. Autodidata por natureza, aos dezenove anos de idade enviou a Leonhard Euler um estudo a partir do qual se desenvolveu o cálculo das variações. Em 1758, ajudou a fundar a Academia Real de Ciências. Lagrange explorou todos os ramos da matemática

existentes de sua época. Em 1759 apresentou um modelo teórico de cordas vibrantes, baseado no modelo de massas iguais, uniformemente espaçadas e ligadas entre si por molas com a mesma constante elástica. Lagrange recebeu, nos anos de 1764, 1766, 1772, 1774 e 1778, o prêmio oferecido pela Academia de Ciências de Paris, por seus trabalhos originais. Sucedeu a Euler, em 1766, como diretor da Matemática na Academia da Ciência de Berlim, durante 21 anos. Em Berlim trabalhou em astronomia, teoria das equações, mecânica, entre outros assuntos. Em teoria dos números provou que todo natural é soma de quatro quadrados e o Teorema de Wilson (p é primo, se e só se, p divide $(p-1)!+1$). Em 1787, tornou-se membro da Academia de Ciências de Paris e professor das escolas Normal e Politécnica. Em 1788, Lagrange publicou *Mecânica Analítica* considerada um poema científico pela perfeição e grandeza de sua estrutura. Esta obra continha todo o trabalho e investigações feitas no campo da mecânica desde Newton, e que se tornou notável pelo uso da teoria das equações diferenciais. Em 1790, Lagrange trabalhou no sistema métrico e investigou a base decimal. Em 1797 publicou o livro denominado *Théorie des Fonctions Analytiques*. Lagrange faleceu em 10 de abril de 1813, em Paris.

Nota A.5. Arthur Cayley nasceu em 16 de agosto de 1821, em Richmond, na Inglaterra. Passou parte da infância na Russia, pois seu pai era comerciante em São Petesburgo. Em 1838, começou a graduação no Trinity College, em Cambridge, e enquanto aluno, publicou três artigos no recentemente criado, *Cambridge Mathematical Journal*. Concluiu a graduação 1842. Por mais quatro anos, tendo ganho uma bolsa para pesquisa, Cayley ensinou em Cambridge onde publicou 28 artigos no *Cambridge Mathematical Journal*. Nesta época, inspirado por um trabalho de Boole, Cayley estudou as formas algébricas e seus invariantes por transformações lineares homogêneas. Em 1843 criou a Geometria Analítica no espaço de dimensão n, usando determinantes como instrumento básico. Aliás, Cayley foi pioneiro no estudo de matrizes. Definiu matriz nula, matriz identidade e foi o primeiro a usar a matriz entre duas barras para indicar o determinante. Com o término da bolsa, Cayley foi forçado a procurar outro emprego, e então começou a estudar direito. Enquanto estudante de direito, Cayley assistiu em Dublin (Irlanda) aulas de Hamilton, em quatérnios. Em 1849, publicou um trabalho, onde juntou suas ideias sobre permutações com as ideias de Cauchy. Ainda em 1849, Cayley obteve grau em direito. Cayley trabalharia como advogado pelos próximos 14 anos, fazendo matemática nas suas horas de folga, como hobby. Durante estes 14 anos como advogado, Cayley publicou em torno de 250 artigos matemáticos. Em análise, Cayley estudou as funções elípticas e abelianas, e as funções representadas por integrais definidas. Em mecânica celeste trabalhou a teoria das perturbações e o método de determinação das órbitas planetárias. Em geometria não-Euclidiana, Cayley desenvolveu a álgebra matricial. Pela quantidade de trabalhos produzidos, Cayley só podia ser comparado a Euler e Cauchy. Em 1854 Cayley escreveu dois artigos notáveis em teoria de grupos abstratos. Neles Cayley definiu um grupo abstrato e introduziu a *Tábua de Cayley*, para mostrar a operação de um grupo. Ele exibiu a tábua de operação para grupos especiais de permutação. Além disso, Cayley percebeu que as matrizes e os quatérnios eram grupos. Em 1858, Cayley mostrou que os quatérnios podem ser representados por meio de matrizes quadradas de ordem 2, com coeficientes complexos. Em 1863 Cayley foi indicado para uma cadeira de professor de matemática pura em Cambridge. O salário não era tão bom quanto o de advogado, mas Cayley ficou muito feliz por ter a chance de dedicar todo o seu tempo para a matemática. Em 1881, foi convidado para dar aulas na Universidade Johns Hopkins (Estados Unidos), onde seu amigo Sylvester, era professor de matemática. De janeiro a maio de 1882, Cayley lecionou nesta universidade funções abelianas e funções theta.

No período de 1889 a 1898, Cayley publicou mais de novecentos trabalhos, abrangendo todos os ramos da matemática pura. Suas obras completas foram publicadas em Cambridge, em 13 volumes, com o título *The Collected Mathematical papers of Arthur Cayley.* Cayley faleceu em 26 de janeiro de 1895, em Cambridge, na Inglaterra, antes da publicação total de suas obras.

Notações

$\square$	Fim de uma demonstração;
$\blacksquare$	Fim de um exemplo;
A/I, $\frac{A}{I}$	Anel quociente pelo ideal I;
G/H, $\frac{G}{H}$	Grupo quociente pelo subgrupo normal H;
$A/\sim$, $\frac{A}{\sim}$	Conjunto quociente pela relação de equivalência $\sim$;
$c(g,h)$	Elemento comutador de g e h;
$D(f)$	Conjunto domínio da aplicação f;
$R(f)$, $Im(f)$	*Range* ou conjunto imagem da aplicação f;
$Z(a)$	Centro ou centralizador do elemento a;
$Z(G)$	Centro ou centralizador do grupo G;
$N(a)$	Normalizador do elemento a;
$N(G)$	Normalizador do grupo G;
$Ker(f)$, $N(f)$	*Kernel* ou núcleo da aplicação f;
$o(G)$, $\|G\|$	Ordem ou cardinalidade do grupo G;
	Terminar esta tabela...

Referências

[1] Andrade, Doherty. *Introdução a Álgebra*. Maringá, 1999.

[2] Azevedo, Alberto de. *Módulos sobre domínios principais*. Rio de Janeiro, 1971.

[3] Domingues, Hygino H. & Iezzi, Gelson. *Álgebra Moderna*. 2^a edição. Editora Atual. São Paulo, 1982.

[4] Gonçalves, Adilson. *Introdução à álgebra*. Instituto de Matemática Pura e Aplicada. Rio de Janeiro, 1999.

[5] Hu Sze-Tsen. *Elements of Modern Algebra*. Holden-Day. San Francisco, 1965.

[6] McCoy, Neal Henry. *Rings and Ideals*. The Waverly Press, Baltimore, Maryland, 1948.

[7] Monteiro, L. H. Jacy. *Elementos de Álgebra*. 2^a edição. Livros Técnicos e Científicos. Rio de Janeiro, 1978.

[8] Sah, Chih-Han. *Abstract Algebra*. Academic Press. New York, 1967.

[9] Stewart, Ian. *Galois Theory*. Halsted Press, New York, 1973.

Índice Remissivo