Notas da disciplina MAT0264 - Anéis e Corpos

Prof. Vinicius Rodrigues

10 de abril de 2025, 17:27

Sumário

Prefácio

Estas notas começaram a ser escritas durante o primeiro semestre de 2025, enquanto lecionada a disciplina MAT0264 - Anéis e Corpos, no Instituto de Matemática e Estatística da Universidade de São Paulo (IME-USP). No presente estado, elas estão em um formato de rascunho, e não são um material completo, nem revisado. O objetivo é que, ao longo do semestre, as notas sejam revisadas e completadas, de modo a se tornarem um material didático mais completo e acessível aos alunos da disciplina.

Capítulo 1

Pré-Requisitos Conjuntistas

Durante o texto, precisamos de algumas definições e resultados envolvendo noções básicas sobre conjuntos e funções.

Não é objetivo deste texto desenvolver a parte inicial da Teoria dos Conjuntos. Também não é o objetivo desta seção explicar toda a notação de conjuntos utilizada. Assumimos familiaridade do leitor com funções e com manipulação de conjuntos a nível básico. Apenas apresentaremos algumas definições, notações e resultados básicos que utilizaremos ao longo do texto.

1.1 Famílias e produtos cartesianos

Famílias são funções com notação especial. Muitas vezes, ao pensar em funções, pensamos em um "dispositivo de entrada/saída". Quando, ao invés disso, estamos pensando apenas em um "conjunto indexado de valores", a notação de família pode ser mais conveniente.

No quadro abaixo, apresentamos uma comparação entre as duas notações. Enfatizamos que, matemáticamente, funções e famílias podem ser vistas como o mesmo objeto.

Conceito	**Função**	**Família**
Mapa	$u : I \to A$	$(u_i)_{i\in I} = (u_i : i \in I)$
Valor	$u(i)$	u_i
Imagem	$\operatorname{ran} u$	$\{u_i : i \in I\}$
Intuição	objeto dinâmico	objeto estático
Inputs	domínio I	conjunto de índices I

Tabela 1.1: Comparativo de família e função

Como exemplos, consideremos sequências infinitas e finitas:

Exemplo 1.1 (Sequências)**.** Uma sequência é uma família cujo conjunto de índices é $\mathbb{N}$. Compare a intuição que passa as notações:

- Considere a sequência $u = (\frac{1}{2^n}))_{n\in\mathbb{N}}$...
- Considere a função $u : \mathbb{N} \to \mathbb{R}$ dada por $u(n) = \frac{1}{2^n}$...

Exemplo 1.2 (Sequências finitas)**.** Se $n \geq 1$, identificamos $n = \{0, 1, \ldots, n-1\}$. Assim:

- Uma família com n elementos é uma família $(a_i)_{i<n} = (a_i)_{i\in n} = (a_0, \ldots, a_{n-1})$.

Essa notação é bastante funcional no sentido de que dá significado como conjunto aos números naturais, e corresponde à construção usual dos números naturais na Teoria dos Conjuntos. Como desvantagem, seus contadores se iniciam no 0, e não no 1, o que pode ser pouco intuitivo e não coincidir com a notação da maioria dos textos de matemática, apesar de ser muito adotada em textos mais próximos de Teoria dos Conjuntos.

Agora vamos seguir para a definição de produto cartesiano. Primeiro, vamos lembrar a definição de produto cartesiano de dois conjuntos.

Definição 1.3 (Produto cartesiano de dois conjuntos)**.** Sejam A, B conjuntos. Então $A \times B = \{(a, b) : a \in A, b \in B\}$ é o *produto cartesiano de A e B*. Ou seja, o conjunto de todos os pares ordenados (a, b) tais que $a \in A$ e $b \in B$. □

Pares ordenados são conjuntos especiais que carregam duas coordenadas de modo a permitem distinguir a ordem dos elementos. Sua propriedade principal é a de se a, b, c, d são conjuntos,então $(a, b) = (c, d)$ se, e somente se $a = c$ e $b = d$. Uma construção usual, chamada de par de Kuratowski, para a qual não é difícil provar que vale essa propriedade, é dada por $(a, b) = \{\{a\}, \{a, b\}\}$. Porém, isso não será importante neste texto.

Definição 1.4 (Produto cartesiano de conjuntos)**.** Seja $(A_i)_{i\in I}$ uma família de conjuntos. O produto cartesiano de conjuntos é o conjunto $\prod_{i\in I} A_i$ definido como o conjunto de todas as famílias $(a_i : i \in I)$ tais que para cada $i \in I$, $a_i \in A_i$.

$$\prod_{i\in I} A_i = \{(a_i)_{i\in I} : \forall i \in I \, a_i \in A_i\}.$$

□

Definição 1.5 (Exponenciação de conjuntos)**.** Sejam A, I conjuntos. O conjunto A^I é o conjunto de todas as funções de I em A. Ou seja, $A^I = \{f : I \to A\}$. Note que:

$$A^I = \prod_{i\in I} A = \{(a_i)_{i\in I} : \forall i \in I \, a_i \in A\}.$$

□

Na notação anterior, se $n \geq 1$, então:

$$A^n = \{(a_i)_{i<n} : \forall i < n \, a_i \in A\} = \{(a_0, \ldots, a_{n-1}) : a_0, \ldots, a_{n-1} \in A\} \approx A \times \cdots \times A \, (n \text{ vezes}).$$

1.2 Operações

Ao trabalharmos com estruturas algébricas necessitaremos da noção de operação, que se define como a seguir:

Definição 1.6 (Operações n-árias)**.** Se X é um conjunto e $n \in \mathbb{N}$, uma operação n-ária em X é uma função $f : X^n \to X$. □

Operações 2-árias e 1-árias são frequentemente chamadas de *binárias* e *unárias*, respectivamente.

Caso $*$ seja uma operação binária, a notação $x * y$ é frequentemente utilizada para denotar $x * y$.

Caso $*$ seja uma operação unária, a notação $*x$ é frequentemente utilizada para denotar $*(x)$.

Capítulo 2

Noções de Grupos

2.1 Definição e Propriedades Básicas

O principal objetivo deste texto é servir como texto para um estudo introdutório sobre anéis e corpos. A noção de grupo é mais simples do que ambas essas estruturas, porém, necessita de ferramentas especiais para seu tratamento completo que fogem do escopo deste texto. Assim, não é objetivo deste capítulo apresentar uma introdução ao estudo de grupos, mas sim apenas enunciar as principais definições e propriedades que utilizaremos ao longo do texto.

Definição 2.1. Um grupo é uma quadrupla $(G, \cdot, e)$, tal que G é um conjunto, $\cdot$ é uma operação binária em G e $0 \in G$, e satisfazem:

- (**Propriedade associativa**) $\forall a, b, c \in G\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- (**Elemento neutro**) $\forall a \in G\ e \cdot a = a \cdot e = a$.
- (**Elemento inverso**) $\forall a \in G\ \exists b \in G\ a \cdot b = b \cdot a = e$.

Se, adicionalmente, a seguinte propriedade é satisfeita, o grupo é chamado de *comutativo*, ou, mais comunmente, *Abeliano*:

- (**Comutatividade**) $\forall a, b \in G\, a \cdot b = b \cdot a$.

□

Algumas observações importantes sobre a notação utilizada no estudo de grupos:

- Ao discursar sobre grupos, é comum omitir a operação e o elemento neutro, referindo-se apenas ao conjunto G.
- Caso o grupo seja Abeliano, é comum que sua operação binária seja denotada por $+$ ou outro símbolo similar. Nesse contexto, o elemento neutro é frequentemente denotado por 0.
- Caso o grupo não seja Abeliano, é comum que sua operação binária seja denotada por $\cdot$ ou outro símbolo similar. Nesse contexto, o elemento neutro é frequentemente denotado por e, e a operação é frequentemente omitida, ou seja, $a \cdot b$ é frequentemente escrito como ab.

Alguns exemplos:

- Com a soma usual, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ são grupos Abelianos.
- Com a multiplicação usual, o círculo unitário complexo $\mathbb{T} = \{x \in \mathbb{C} : |x| = 1\}$ é um grupo Abeliano com elemento neutro 1. De fato, o produto de complexos é comutativo, associativo e tem 1 como elemento neutro. Note que $1 \in \mathbb{T}$ e $0 \notin \mathbb{T}$. Se $x \in \mathbb{T}$, o inverso multiplicativo de x é dado por $\frac{\bar{x}}{|x|^2}$, onde $\bar{x}$ denota o conjugado de x. Como $|\bar{x}| = |x| = 1$, segue que $\mathbb{T}$ tem todos os inversos de todos seus elementos.
- Os inteiros módulo n ($n \geq 1$), dados por $\mathbb{Z}_n = \{0, \ldots, n-1\}$ com a soma dada pela aritmética módulo n, são grupos.

Agora iniciaremos a provar algumas propriedades básicas sobre grupos.

Proposição 2.2 (Unicidade do elemento neutro)**.** Seja $(G, \cdot, e)$ um grupo. Então, o elemento neutro e é único. Isto é, se $h \in G$ é tal que $\forall a \in G\ h \cdot a = a \cdot h = a$, então $h = e$.

Demonstração. Note que $h = he$, pois e é elemento neutro. Por outro lado, $e = he$, pois h é elemento neutro. Assim, $h = he = e$. □

Proposição 2.3 (Unicidade dos inversos)**.** Seja $(G, \cdot, e)$ um grupo. Então todo $a \in G$ possui um único elemento inverso, ou seja, para todo $g \in G$, é único. Isto é $\forall a \in G\ \exists!\, b \in G\ a \cdot b = b \cdot a = e$.

Demonstração. A existência do inverso é garantida pela definição de grupo. Para provar a unicidade, suponha que b, c são inversos de a, ou seja, $a \cdot b = b \cdot a = e$ e $a \cdot c = c \cdot a = e$. Então, temos:

$$b = be = b(ac) = (ba)c = ec = c.$$

□

A unicidade do elemento neutro e dos inversos nos permite definir a notação a^{-1} para o inverso de a em um grupo $(G, \cdot, e)$. Caso $(G, +, 0)$ seja um grupo Abeliano, a notação $-a$ é frequentemente utilizada para denotar o inverso de a, e, nesse caso, $-a$ é chamado de *oposto* de a.

Note que assim, ficam definidos operadores unários $(\,)^{-1} : G \to G$ (ou $- : G \to G$). Para o segundo caso, define-se também que $a - b = a + (-b)$.

Proposição 2.4 (Cancelamento)**.** Seja $(G, \cdot, e)$ um grupo. Então, se $a, b, c \in G$ e $a \cdot b = a \cdot c$, então $b = c$. Analogamente, se$b \cdot a = c \cdot a$, então $b = c$.

Demonstração. Provaremos a primeira afirmação. A segunda é análoga e fica como exercício. Suponha que $ba = ca$. Então $b = be = b(aa^{-1}) = (ba)a^{-1} = (ca)a^{-1} = c(aa^{-1}) = ce = c$. Assim, $b = c$. □

Corolário 2.5 (Cancelamento II)**.** Seja $(G, \cdot, e)$ um grupo. Para todos $a, b \in G$, se $ab = a$, então $b = e$. Analogamente, se $ba = a$, então $b = e$.

Demonstração. Para a primeira afirmação, note que $ab = ae$, logo, pela proposição anterior, $b = e$. A segunda afirmação é análoga. □

Proposição 2.6 (Regras de sinal)**.** Seja G um grupo e $a, b \in G$. Então:

a) $((a)^{-1})^{-1} = a$ [na notação aditiva, $-(-a) = a$].

b) $(ab)^{-1} = b^{-1}a^{-1}$ [na notação aditiva, $-(a+b) = (-b) + (-a)$].

c) $e^{-1} = e$ [na notação aditiva, $-0 = 0$].

Demonstração. a): Temos que $(a^{-1})^{-1}a^{-1} = e = aa^{-1}$. Cancelando a^{-1}, segue.

b): Temos que $(ab)^{-1}(ab) = e = (b^{-1}a^{-1})ab$. Cancelando ab, segue que $(ab)^{-1} = b^{-1}a^{-1}$. Analogamente, $(ba)^{-1} = a^{-1}b^{-1}$.

c): Temos que $(e^{-1})e = e = ee$. Cancelando e à direita, segue.

□

2.2 Somatórios

Nessa seção, formalizaremos a noção de somatório. É desejável que o leitor já possua familiaridade com alguma notação de somatório, mas aqui apresentaremos a notação e as técnicas de "substituição de variáveis" que serão utilizadas.

Definição 2.7 (Soma de sequência finita)**.** Seja G um conjunto munido de uma operação $+$ associativa, comutativa e com neutro 0. Define-se, recursivamente para $n \geq 0$, o somatório de famílias $(a_i : i \in F)$, onde F é um conjunto de n índices e $a_i \in G$ para todo $i \in F$, como se segue:

- **Notação:** se $a = (a_i)_{i \in F}$ é uma sequência de elementos de G, então usamos as notações:

$$\sum a = \sum (a_i : i \in F) = \sum_{i \in F} a_i.$$

- Caso base $n = 0$ (soma vazia): só existe uma família com 0 elementos, que é a família vazia $a = () = \emptyset = (a_i : i \in \emptyset)$. Definimos:

$$\sum a = \sum_{i \in \emptyset} a_i = 0$$

.

- Passo recursivo $n \to n+1$: considere uma família $(a_i)_{i \in F}$, onde $|F| = n+1$. Define-se:

$$\sum (a_i : i \in F) = \sum (a_i : i \in F \setminus \{j\}) + a_j,$$

onde $j \in I$ é qualquer elemento.

□

É claro que, para mostrar que a definição acima é consistente, precisamos mostrar que a soma não depende da escolha de j.

Lema 2.8. Qualquer que seja o tamanho (finito) de F, $\sum (a_i)_{i \in F}$ está bem definido.

Demonstração. Seja F um conjunto finito. Se $|F| = 0$, então $F = \emptyset$, e a soma é 0. Se $|F| = 1$, então $F = \{j\}$ – só há uma escolha para j, e a soma é a_j. Se $|F| = n+1$ para $n \geq 1$, tome $j, k \in F$. Devemos ver que $\left(\sum_{i \in F \setminus \{j\}} a_i\right) + a_j = \left(\sum_{i \in F \setminus \{k\}} a_i\right) + a_k$. Com efeito:

$$\left(\sum_{i\in F\setminus\{j\}} a_i\right) + a_j = \left(\left(\sum_{i\in F\setminus\{j,k\}} a_i\right) + a_k\right) + a_j = \left(\sum_{i\in F\setminus\{j,k\}} a_i\right) + (a_k + a_j)$$

$$= \left(\sum_{i\in F\setminus\{j,k\}} a_i\right) + (a_j + a_k) = \left(\left(\sum_{i\in F\setminus\{j,k\}} a_i\right) + a_j\right) + a_k = \left(\sum_{i\in F\setminus\{k\}} a_i\right) + a_k.$$

□

Proposição 2.9. Seja G um conjunto munido de uma operação $+$ associativa, comutativa e com neutro 0. Seja $(a_i : i \in I)$ uma família finita em G e $\phi : J \to I$ uma função bijetora. Então:

$$\sum_{i\in I} a_i = \sum_{j\in J} a_{\phi(j)}.$$

Demonstração. Novamente, procedemos por indução no tamanho de $n = |I|$. A base de tamanho 0 é trivial, já que ambos os lados da igualdade são 0.

Para o passo indutivo em que $|I| = |J| = n+1$, considere $\phi : J \to I$ como no enunciado. Fixe $k \in J$ qualquer e sejam $I' = I \setminus \{\phi(k)\}$, $J' = J \setminus \{k\}$ e $\phi' = \phi|_{J'} : J' \to I'$, que é bijetora. Como $|J'| = |I'| = n$, por hipótese indutiva temos que $\sum_{j\in J'} a_{\phi(j)} = \sum_{i\in I'} a_i$. Segue que:

$$\sum_{j\in J} a_{\phi(j)} = \left(\sum_{j\in J'} a_{\phi(j)}\right) + a_{\phi(k)} = \left(\sum_{i\in I'} a_i\right) + a_{\phi(k)} = \sum_{j\in I} a_i.$$

□

Capítulo 3

Anéis e subanéis

Nesta seção, começaremos a discutir a noção matemática de anel, uma das principais estruturas que serão estudadas.

Definição 3.1 (Anel)**.** Um anel é uma 4-upla $(A, +, \cdot, 0, 1)$ conjunto A com duas operações binárias, adição e multiplicação, denotadas por $+$ e $\cdot$, tais que:

- $(A, +, 0)$ é um grupo abeliano.
- (**Associatividade**) Para todo $a, b \in A$, temos $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- (**Elemento identidade**) $\forall a \in A\ 1 \cdot a = a \cdot 1 = a$.
- (**Propriedades distributivas**) Para todos $a, b, c, \in A$, temos:

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

Se, adicionalmente, a seguinte propriedade é satisfeita, o anel é chamado de *comutativo*.

- (**Comutatividade**) $\forall a, b \in A\ a \cdot b = b \cdot a$.

□

Algumas observações:

- Como em grupos, ao discursar sobre anéis é comum omitir as operações, referindo-se apenas ao conjunto A.
- Ao discursar sobre anéis, e a exemplo do que foi feito ao enunciar as propriedades distributivas, são utilizadas as convenções usuais sobre precedência de operações envolvidas por parênteses. Assim, $a + b \cdot c$ é interpretado como $a + (b \cdot c)$.
- Há textos que definem anéis sem incluir o elemento identidade 1. Nestes textos, a definição acima dá nome ao que chamam de *anéis com identidade*, ou *anéis com 1*. Nesse curso, não usaremos essa convenção, de modo que **todos nossos anéis possuem identidade**. De modo similar, alguns textos definem anéis como sendo comutativos. Também não adotaremos essa convenção. **Os nossos anéis podem ser não comutativos**.

- A definição de anel não exige que $0 = 1$.
- 0 é chamado de elemento nulo, e 1 de elemento identidade.

Proposição 3.2 (Propriedade multiplicativa do 0)**.** Seja A um anel. Então $\forall a \in A\ 0 \cdot a = a \cdot 0 = 0$.

Demonstração. Provaremos a primeira afirmação. A segunda é análoga e fica como exercício.
Temos que $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$. Cancelando, segue que $0 = 0 \cdot a$. □

Proposição 3.3 (Anel trivial)**.** Seja $A = x$ um conjunto qualquer. Defina $x \cdot x = x = x + x = 0 = 1$. Então $(A, +, \cdot, 0, 1)$ é um anel. Um anel dessa forma é chamado de *anel trivial*.
Além disso, se A é um anel tal que $0 = 1$, então A é um anel trivial.

Demonstração. A primeira afirmação (de que A como acima é um anel) fica como exercício.
Para a segunda afirmação, assuma que A é um anel tal que $0 = 1$. Fixe $a \in A$ qualquer. Então $a = a \cdot 1 = a \cdot 0 = 0$, ou seja, $a = 0$. Assim, A é o conjunto unitário $\{0\}$, que é um anel trivial. □

Proposição 3.4 (Regras de sinal II)**.** Seja A um anel e $a, b \in A$. Então:

a) $(-a)b = a(-b) = -(ab)$

b) $(-a)(-b) = ab$.

c) $(-1)a = -a$.

Demonstração. a): Temos que $ab + (-a)b = (-a)b + ab = [-a + a]b = 0b = 0$. Assim, $(-a)b = -(ab)$. Analogamente, $a(-b) = -(ab)$.
b): Temos que $(-a)(-b) = -[a(-b)] = -[-(ab)] = ab$ pela regra anterior.
c): Temos que $(-1)a = -(1a) = -a$. □

3.1 Elementos invertíveis

Definição 3.5 (Elemento invertível)**.** Seja A um anel. Um elemento $a \in A$ é dito *invertível*, ou uma *unidade* se $\exists b \in A$ tal que $a \cdot b = b \cdot a = 1$.
O conjunto de todas das unidades de A é denotado por A^*. □

Definição 3.6. Seja A um anel. Então, se $a \in A^*$, existe um **único** $b \in A$ tal que $a \cdot b = b \cdot a = 1$. Este elemento é denotado por a^{-1}, e é chamado de *inverso* de a. □

Observação: para que a definição acima faça sentido, é necessário mostrar que se a é unidade, existe um **único** $b \in A$ tal que $a \cdot b = b \cdot a = 1$. A existência é garantida pela definição de unidade, e a demonstração da unicidade é análoga à da unicidade do inverso em grupos (Proposição 2.3), ficando como exercício.

Proposição 3.7. Seja A um anel. Para todos $a, b \in A^*$, temos:

a) $ab \in A^U$ e $(ab)^{-1} = b^{-1}a^{-1}$.

b) $a^{-1} \in A^U$ e $(a^{-1})^{-1} = a$.

c) $1^{-1} = 1$.

Além disso, A^* é, com a restrição da operação de multiplicação do anel, um grupo com identidade 1. Caso A seja abeliano, A^* é um grupo abeliano.

Demonstração. a): Sejam $a, b \in A^*$. Pela associatividade, $(ab)(b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1})(ab)$, logo, pela unicidade do inverso, $(ab)^{-1} = b^{-1}a^{-1}$.

b): Seja $a \in A^*$. Temos que $a^{-1}a = 1 = a(a^{-1})$, logo, pela unicidade do inverso, $(a^{-1})^{-1} = a$.

c): Note que $1 \cdot 1 = 1 = 1 \cdot 1$, logo, pela unicidade do inverso, $1^{-1} = 1$.

A última afirmação é imediata e fica como exercício. □

Abaixo, segue a definição de anel de divisão e corpo. A noção de corpo será uma das noções mais importantes deste texto.

Definição 3.8 (Anel de divisão)**.** Um *anel de divisão* é um anel não trivial para o qual todo elemento não nulo é invertível. Um *corpo* é um anel de divisão comutativo. □

Exercício 3.9. Mostre que um anel A é um anel de divisão se, e somente se $A^* = A \setminus \{0\}$.

Definição 3.10. Um domínio de integridade é um anel comutativo não trivial A tal que $\forall a, b \in A$, se $ab = 0$, então $a = 0$ ou $b = 0$. □

Proposição 3.11. Seja K um corpo. Então K é um domínio de integridade.

Demonstração. Sabemos que K é um anel comutativo não trivial. Sejam $a, b \in K$ tais que $ab = 0$. Se $a = 0$, então segue a tese. Caso contrário, como K é um corpo, a^{-1} existe. Assim, temos que $b = (a^{-1}a)b = a^{-1}(ab) = 0$, logo, $b = 0$. □

3.2 Subanéis

Em Matemática, é comum que as estruturas estudadas possuam uma noção de subestrutura. Em geral, uma subestrutura de uma estrutura data é um subconjunto desta que seja, de forma natural, uma estrutura da mesma natureza daquela.

Veremos que, quando tratamos de anéis, nem todo subconjunto pode ser visto como uma subestrutura.

Definição 3.12 (Subanel)**.** Seja A um anel e $B \subseteq A$. Dizemos que B é subanel de A se, e somente se $(B, +|_{B^2}, \cdot|_{B^2}, 0_A, 1_A)$ é um anel, onde $+|_{B^2} : B^2 \to B$ e $\cdot|_{B^2} : B^2 \to B$ são as restrições das operações de A à B^2. □

Na definição acima, estamos pedindo que B seja um subconjunto de A que possua as mesmas operações que A, e que essas operações sejam restritas a B e satisfaçam todas as cláusulas da definição de anel. Aparentemente, na prática, provar que um dado subconjunto de A é um subanel pode parecer uma tarefa longa. Porém, a seguinte proposição encurta esta tarefa significativamente:

Definição 3.13 (Subanel)**.** Seja A um anel e $B \subseteq A$. Então B é um subanel de A se, e somente se:

- $1_A \in B$
- Para todos $a, b \in B$, $a - b \in B$.
- Para todos $a, b \in B$, $ab \in B$

Além disso, caso B seja um subanel de A, os opostos aditivos de B são os mesmos que os de A, ou seja, que $-b \in B$ para todo $B \in B$. □

Demonstração. Primeiro, notemos suponhamos que B seja um subanel de A. Então B é fechado por $+, \cdot$ e $1_A \in B$. Resta apenas ver que para todos $a, b \in B$, $a - b \in B$. Como B é fechado por soma, basta provar a última afirmação: que para todo $b \in B$, $-b \in B$. Fixe $b \in B$. Como $(B, +|_B^2, 0_A)$ é um grupo abeliano, existe $x \in B$ tal que $b + x = 0_B$. Então, em a, segue que $b + x = x + b = 0_A$. Pela unicidade dos opostos em A, segue que $-b = x \in B$.

Reciprocamente, provaremos que se B possui 1_B como elemento e é fechado por diferença e por produto, então B é um subanel de A. Iniciaremos verificando que B é fechado por soma, por opostos e que tem 0_A como elemento.

Como 1_A é elemento de B, temos que $0_A = 1_A - 1_A \in B$. Assim, B possui 0_A como elemento. Agora, dado $b \in B$, $0_A - b = -b \in B$, o que mostra que B é fechado por opostos. Finalmente, dados $a, b \in B$, $a - (-b) = a + b \in B$, o que mostra que B é fechado para soma.

As propriedades associativas, comutativas, distributivas e de identidade valem em B, pois valem em A e as operações de B são as mesmas de A, restritas. Para finalizar, basta observar que dado $a \in B$, $(-a) \in B$, como já mostrado, e que $a + (-a) = (-a) + a = 0_A$, o que mostra que B possui opostos aditivos. □

Exemplo 3.14. $\mathbb{N}$ não é um subanel de $\mathbb{Z}$, pois $-1 \notin \mathbb{Z}$. Porém, note que $\mathbb{N}$ tem 1 e é fechado por soma e produto, o que mostra que na proposição anterior, a expressão $a - b$ não pode ser substituída por $a + b$.

Exemplo 3.15 (Subanel trivial)**.** Para todo A, temos que A é subanel de si mesmo.

Exemplo 3.16. O único subanel de $\mathbb{Z}$ é $\mathbb{Z}$: se B é um subanel de $\mathbb{Z}$, então $0, 1 \in B$. Por indução, para todo $n \geq 1$ temos que $n \in \mathbb{B}$: com efeito, $1 \in B$, e, se $n \in B$, $n + 1 \in B$, logo vale o passo indutivo. Finalmente, $-n \in B$ para todo $n \geq 1$. Como $\mathbb{Z} = \{0\} \cup \{n \in \mathbb{Z} : n \geq 1\} \cup \{-n \in \mathbb{Z} : n \geq 1\}$, temos que $B = \mathbb{Z}$.

Como as operações de um subanel são as mesmas de um anel, um subanel de um anel comutativo é comutativo.

Proposição 3.17. Subanéis de aneis comutativos são comutativos.

Demonstração. Seja A um anel comutativo e B um subanel de A. Para todos $a, b \in B$, temos que o produto $a \cdot b$ em B é dado pelo produto (comutativo) $a \cdot b$ em A, logo $a \cdot b = b \cdot a$. □

Capítulo 4

Homomorfismos de anéis

Em matemática, boa parte das coleções de estruturas estudadas possui uma classe de funções que preservam, em algum sentido, suas propriedades. O estudo generalizado destas estruturas é o que chamamos de *teoria de categorias*, tema que não será tratado neste texto. Na classe dos anéis, estas funções são o que chamamos de *homomorfismos*.

4.1 Homomorfismos

Definição 4.1. Sejam A, R aneis. Uma função $f : A \to R$ é um *homomorfismo* se:

- $f(a+b) = f(a) + f(b)$ para todo $a, b \in A$.
- $f(-a) = -f(a)$ para todo $a \in A$.
- $f(0_A) = 0_R$
- $f(ab) = f(a)f(b)$ para todo $a, b \in A$.
- $f(1_A) = 1_R$.

Caso f seja injetora, dizemos que f é um *monomorfismo*. Caso f seja sobrejetora, dizemos que f é um *epimorfismo*. Caso f seja bijetora, dizemos que f é um *isomorfismo*. □

Proposição 4.2 (Propriedades de homomorfismos)**.** Seja $f : A \to R$ um homomorfismo de anéis. Então:

a) Para todo $a \in A^*$, temos $f(a) \in R^*$ e $f(a^{-1}) = f(a)^{-1}$.

b) O núcleo de f, definido como $\ker f = f^{-1}(\{0_R\}) = \{a \in A : f(a) = 0_R\}$, é um ideal de A.

c) A imagem de f, $\operatorname{ran} f = \{f(a) : a \in A\}$, é um subanel de R. Se A é comutativo, $\operatorname{ran} f$ também é.

d) Se f é injetora se, e somente se $\ker f = \{0_A\}$.

Demonstração. a) Se $a \in A^*$, então $f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_R$ e $f(a^{-1})f(a) = f(aa^{-1}) = f(1_A) = 1_R$. Assim, $f(a^{-1}) = f(a)^{-1}$ e $f(a) \in R^*$.

b) Temos que $0_A \in \ker f$, pois $f(0_A) = 0_R$. Sejam $a, b \in \ker f$. Então $f(a) = f(b) = 0_R$, logo, $f(a+b) = f(a) + f(b) = 0_R + 0_R = 0_R$. Assim, $a + b \in \ker f$.

Se $a \in \ker f$ e $x \in A$, vejamos que $ax, xa \in \ker f$: $f(ax) = f(a)f(x) = 0_R f(x) = 0_R$ e $f(xa) = f(x)f(a) = f(x)0_R = 0_R$. Assim, $ax, xa \in \ker f$.

Portanto, $\ker f$ é um ideal de A.

c) Seja $a, b \in \operatorname{ran} f$. Então existem $x, y \in A$ tais que $a = f(x)$ e $b = f(y)$. Assim, $a - b = f(x) - f(y) = f(x - y)$. Logo, $a - b \in \operatorname{ran} f$. Similarmente, $ab = f(x)f(y) = f(xy) \in \operatorname{ran} f$, e $1_R = f(1_A) \in \operatorname{ran} f$.

Portanto, $\operatorname{ran} f$ é um subanel de R. Se A é comutativo, $\operatorname{ran}(f)$ também é comutativo, pois dados $a, b \in \operatorname{ran} f$, existem $x, y \in A$ tais que $a = f(x)$ e $b = f(y)$. Assim, $ab = f(x)f(y) = f(xy) = f(yx) = f(y)f(x) = ba$.

d) Se f é injetora, então $f(a) = 0_R = f(0_A)$ implica que $a = 0_A$, logo, $\ker f = \{0_A\}$. Reciprocamente, se $\ker f = \{0_A\}$, então $f(a) = f(b)$ implica que $f(a-b) = 0_R$, logo, $a - b = 0_A$, ou seja, $a = b$. Assim, f é injetora. □

Proposição 4.3 (Critério de homomorfismo)**.** Seja $f : A \to R$ um homomorfismo de anéis. Então, f é um homomorfismo se, e somente se:

- $f(a + b) = f(a) + f(b)$ para todo $a, b \in A$.
- $f(ab) = f(a)f(b)$ para todo $a, b \in A$.
- $f(1_A) = 1_R$.

Demonstração. Se f é um homomorfismo, então as duas propriedades acima são satisfeitas. Reciprocamente, se as duas propriedades acima são satisfeitas, então:

- $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A)$. Cancelando, temos $0_R = f(0_A)$.
- $f(-a) + f(a) = f(0_A) = 0_R$, logo, $f(-a) = -f(a)$.

$f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A) = 0_R$, e $f(-a) = f(0_A - a) = f(0_A) + f(-a) = 0_R - f(a) = -f(a)$ para todo $a \in A$. Assim, f é um homomorfismo. □

Capítulo 5

Ideais e Quocientes

5.1 Ideais

Definição 5.1 (Ideal à esquerda)**.** Seja A um anel. Um subconjunto $I \subseteq A$ é dito *ideal à esquerda* se:

- $0 \in I$.
- Para todos $a, b \in I$, temos $a + b \in I$.
- $\forall a \in A$ e $\forall b \in I$, temos $ab \in I$.

□

Definição 5.2 (Ideal à direita)**.** Seja A um anel. Um subconjunto $I \subseteq A$ é dito *ideal à direita* se:

- $0 \in I$.
- Para todos $a, b \in I$, temos $a + b \in I$.
- $\forall a \in I$ e $\forall b \in A$, temos $ab \in I$.

□

Definição 5.3 (Ideal)**.** Seja A um anel. Um subconjunto $I \subseteq A$ é dito *ideal* se for um ideal à esquerda e um ideal à direita. Ou seja, I é um ideal se:

- $0 \in I$.
- Para todos $a, b \in I$, temos $a + b \in I$.
- $\forall a \in A$ e $\forall b \in I$, temos $ab \in I$.
- $\forall a \in I$ e $\forall b \in A$, temos $ab \in I$.

□

Proposição 5.4 (Ideal trivial)**.** Seja A um anel. Então $\{0\}$ e A são ideais de A. Estes ideais são chamados de *ideais principais*

Demonstração. Exercício. □

Note que se A é um anel comutativo, então I é um ideal à esquerda se, e somente se, I é um ideal à direita. Assim, em anéis comutativos, a noção de ideal é equivalente à de ideal à esquerda ou à de ideal à direita.

Proposição 5.5 (Interseção de ideais)**.** Seja A um anel e $\mathcal{F}$ uma coleção não vazia de ideais à esquerda de A. Então $\bigcap_{I\in\mathcal{F}} I = \bigcap \mathcal{F}$ é um ideal de A. O mesmo vale para ideais à direita e ideais.

Demonstração. Provaremos para ideais à esquerda. A prova para ideais à direita é análoga e fica como exercício.

Seja $I = \bigcap \mathcal{F}$. Então $0 \in I$, pois $0 \in I$ para todo $I \in \mathcal{F}$.

Sejam $a, b \in I$. Então, para todo $I \in \mathcal{F}$, temos que $a, b \in I$, logo, $a + b \in I$. Assim, $a + b \in \bigcap \mathcal{F}$.

Finalmente, seja $a \in A$ e $b \in I$. Então, para todo $I \in \mathcal{F}$, temos que $b \in I$, logo, $ab \in I$. Assim, $ab \in \bigcap \mathcal{F}$. □

Proposição 5.6 (Ideal gerado)**.** Seja A um anel comutativo e $B \subseteq A$ um conjunto não vazio. Então, o conjunto $I = \{a_1b_1 + \cdots + a_nb_n : n \geq 1, a_i \in A, b_i \in B\}$ é o menor ideal à esquerda A que contém B (ou seja, além de ser um ideal contendo B, se J é qualquer ideal contendo B, então $I \subseteq J$). O ideal I é chamado de *ideal gerado por* B, e denotado por $\langle B\rangle$.

Se $B = \{x_0, \ldots, x_n\}$, então abreviamos $\langle B\rangle$ como $\langle x_0, \ldots, x_n\rangle$.

Demonstração. Primeiro, verificaremos que I é um ideal.

$0 \in I$, pois $0 = 0b$ para todo $b \in B$.

Sejam $x, y \in I$. Então existem $n, m \geq 1$, $a_1, \ldots, a_n \in A$, $b_1, \ldots, b_n \in B$, $c_1, \ldots, c_m \in A$ e $d_1, \ldots, d_m \in B$ tais que $x = a_1b_1 + \cdots + a_nb_n$ e $y = c_1d_1 + \cdots + c_md_m$. Assim, $x + y = (a_1b_1 + \cdots + a_nb_n) + (c_1d_1 + \cdots + c_md_m) = (a_1b_1 + \cdots + a_nb_n) + (c_1d_1 + \cdots + c_md_m) \in I$.

Finalmente, seja $a \in A$ e $b \in I$. Então existem $n \geq 1$, $a_1, \ldots, a_n \in A$ e $b_1, \ldots, b_n \in B$ tais que $b = a_1b_1 + \cdots + a_nb_n$. Assim, $ab = (a_1b_1 + \cdots + a_nb_n)a = a_1(b_1a) + \cdots + a_n(b_na) \in I$.

Agora, seja J um ideal de A que contém B. Então, como J é um ideal de A, temos que $\forall a_i \in A$, $\forall b_i \in B$, temos que $(a_ib_i) \in J$. Logo, $I \subseteq J$. Portanto, I é o menor ideal de A que contém B. □

Observação: note que o menor ideal contendo $B = \emptyset$ é o ideal nulo, $\{0\}$.

Definição 5.7 (Ideal principal)**.** Seja A um anel. Para todo $x \in A$, o conjunto $xA = \{xa : a \in A\}$ é um ideal à direita de A. O ideal xA é chamado de *ideal principal à direita gerado por* x. Analogamente, o conjunto $Ax = \{ax : a \in A\}$ é um ideal à esquerda de A, e é chamado de *ideal principal à esquerda gerado por* x. □

Demonstração. Mostraremos que xA é um ideal à direita. As demais afirmações ficam como exercício.

Note que $0 \in xA$, pois $x0 = 0$.

Sejam $a, b \in xA$. Então, existem $a_1, a_2 \in A$ tais que $a = xa_1$ e $b = xa_2$. Assim, $a + b = xa_1 + xa_2 = x(a_1 + a_2) \in xA$.

Finalmente, seja $a \in A$ e $b \in xA$. Então, existe $b_1 \in A$ tal que $b = xb_1$. Assim, $ab = (xa)b_1 = x(ab_1) \in xA$. □

Definição 5.8 (Ideal principal)**.** Seja A um anel. Para todo $x \in A$, o conjunto $xA = \{xa : a \in A\}$ é um ideal à esquerda de A. O ideal xA é chamado de *ideal principal à esquerda gerado por* x. Analogamente, o conjunto $Ax = \{ax : a \in A\}$ é um ideal à direita de A, e é chamado de *ideal principal à direita gerado por* x. Se A é comutativo, o ideal $xA = Ax$ é chamado de *ideal principal gerado por* x. □

Observação: note que, comparando as definições, se A é um anel comutativo com unidade, $xA = \langle x \rangle$.

Notemos que ideais triviais são principais à esquerda e à direita, pois $0A = \{0\} = A0$ e $A1 = A = 1A$.

Definição 5.9 (Domínio de ideais principais)**.** Um domínio de ideais principais (DIP), ou anel principal, é um domínio de integridade A tal que todo ideal de A é principal. □

Proposição 5.10 (Ideais de um corpo são triviais)**.** Todo ideal de um corpo é trivial. Em particular, todo corpo é um DIP. Reciprocamente, se A é um anel comutativo não trivial cujo todo ideal é trivial, então A é um corpo.

Demonstração. Seja K um corpo e I um ideal de K. Se $I = \{0\}$, então I é trivial. Se $I \neq \{0\}$, então existe $a \in I$ tal que $a \neq 0$. Daí $1 = a^{-1}a = \in I$. Logo, para todo $k \in K$, $k = 1k \in I$.

Para a recíproca, seja A um anel comutativo não trivial tal que todo ideal de A é trivial, e fixe $x \in A \setminus \{0\}$. Como Ax é um ideal trivial e $0 \neq x \in Ax$, temos que $Ax = A$. Logo, existe $a \in A$ tal que $ax = 1$. Assim, x é invertível. Portanto, A é um corpo. □

Proposição 5.11 (Um DIP que não é um corpo)**.** O anel dos inteiros $\mathbb{Z}$ é um domínio de ideais principais que não é um corpo.

Demonstração. Seja I um ideal de $\mathbb{Z}$. Veremos que I é um ideal principal. Se $I = \{0\}$, então I é principal. Caso contrário, I contém ao menos um elemento positivo, já que, sendo $x \in I \setminus \{0\}$, temos que $-x \in I$ e um dos $x, -x$ é positivo.

Seja n o menor inteiro positivo de I. Afirmamos que $I = n\mathbb{Z}$. De fato, se $x \in I$, então escreva $x = qn + r$, onde $q, r \in \mathbb{Z}$ e $0 \leq r < n$. Como $x \in I$, temos que $r = x - qn \in I$. Assim, $r = 0$, ou violaríamos a minimalidade de n. Logo, $x = qn \in n\mathbb{Z}$. Portanto, $I \subseteq n\mathbb{Z}$. Como $n\mathbb{Z} = \langle n \rangle$ e $n \in I$, temos que $n\mathbb{Z} \subseteq I$, o que completa a prova. □

5.2 Quocientes

Definição 5.12. Seja A um anel. Uma relação de congruência em A é uma relação de equivalência $\sim$ em A que "preserva operações". Explcitamente, tal que para todos $a, b, c, d \in A$, se Se $a \sim b$ e $c \sim d$, então $a + c \sim b + d$ e $ac \sim bd$. □

Quais são todas as relações de congruência em A? A proposição abaixo classifica-as a partir dos ideais de A.

Proposição 5.13 (Relações de congruência vs ideais)**.** Seja A um anel, $\mathcal{R}(A)$ o conjunto de todas as relações de congruência em A e $\mathcal{I}(A)$ o conjunto de todos os ideais de A. Então, existe uma bijeção entre $\mathcal{R}(A)$ e $\mathcal{I}(A)$ dada por $\sim \mapsto I_\sim = \{a \in A : a \sim 0\}$, cuja inversa se dá por $I \mapsto \sim_I = \{(a, b) \in A^2 : a - b \in I\}$.

Demonstração. Primeiro, vejamos que se $\sim$ é uma relação de congruência, então $I_\sim$ é um ideal de A.

- $0 \in I_\sim$, pois $0 \sim 0$.
- Se $a, b \in I_\sim$, então $a \sim 0$ e $b \sim 0$, logo $a + b \sim 0 + 0 = 0$, portanto, $a + b \in I_\sim$.
- Se $x \in A$ e $a \in I_\sim$, então $a \sim 0$ e $x \sim 0$, logo $ax \sim a0 = 0$ e $xa = 0a = 0$, portanto, $ax, xa \in I_\sim$.

Agora, vejamos que se I é um ideal, então $\sim_I$ é uma relação de congruência. De fato, temos que, para todos $a, b, c, d \in A$:

- $a \sim_I a$ pois $a - a = 0 \in I$.
- Se $a \sim_I b$, então $a - b \in I$, logo $(-1)(a - b) = b - a \in I$, e, portanto, $b \sim_I a$.
- Se $a \sim_I b$ e $b \sim_I c$, então $a - b \in I$ e $b - c \in I$, logo, $(a - b) + (b - c) = a - c \in I$, portanto, $a \sim_I c$.
- Se $a \sim_I b$ e $c \sim_I d$, então $a - b \in I$ e $c - d \in I$, logo, $(a - b) + (c - d) = (a + c) - (b + d) \in I$, portanto, $a + c \sim_I b + d$.
- Se $a \sim_I b$ e $c \sim_I d$, então $a - b \in I$ e $c - d \in I$, logo, $(a - b)c = ac - bc \in I$ e $b(c - d) = bc - bd \in I$, logo $(ac - bc) + (bc - bd) = ac - bd \in I$, portanto, $ac \sim_I bd$.

Se I é ideal, $I_{\sim_I} = I$, pois, para todo $a \in A$:

$$a \in I_{\sim_I} \Leftrightarrow a \sim_I 0 \Leftrightarrow a - 0 \in I \Leftrightarrow a \in I.$$

Finalmente, se $\sim$ é relação de congruência, $\sim_{I_\sim} = \sim$, pois, para todos $a, b \in A$:

$$a \sim_{I_\sim} b \Leftrightarrow a - b \in I_\sim \Leftrightarrow a - b \sim 0 \Leftrightarrow a \sim b.$$

Justificando a última equivalência: se $a - b \sim 0$, como $b \sim b$, temos que $a - b + b \sim b$, ou seja, que $a \sim b$. Reciprocamente, se $a \sim b$, como $(-b) \sim (-b)$, segue que $a + (-b) \sim b + (-b)$, ou seja, que $a - b \sim 0$. □

Como feito nos inteiros, podemos, ao invés de trabalhar com relações de congruência, encontrar anéis em que a congruência corresponda exatamente à igualdade.

Definição 5.14. Seja A um anel e $\sim$ uma relação de congruência. Define-se que $A/\sim$ é $A/\sim = \{[a]_\sim : a \in A\}$, onde $[a]_\sim = \{b \in A : b \sim a\}$ é a classe de equivalência de a com relação a $\sim$.

Define-se que $[a]_\sim + [b]_\sim = [a + b]_\sim$ e que $[a]_\sim[b]_\sim = [ab]\sim$.

Se I é um ideal, $A/I = A/\sim_I$, e o mapa quociente de A em A/I se dá por $q : A \longrightarrow A/I$ dada por $q(a) = [a]_{\sim_I}$. □

Pelas propriedades das relações de congruência, a soma e produto de $A/\sim$ (ou A/I) estão bem definidas. Além disso:

Lema 5.15 (Propriedades do quociente)**.** Na notação acima:

a) q é epimorfismo de anéis.

b) $\ker q = I$.

c) $q(a) = a + I = \{a + x : x \in I\}$ para todo $a \in A$.

d) Se A é anel comutativo, A/I também é.

Demonstração. a) Seja $a, b, c, d \in A$. Temos que $q(a+b) = q(a) + q(b)$ e $q(ab) = q(a)q(b)$ por definição da soma em A/I, e q é sobrejetora pela definição de q. Finalmente, $q(1_A)$ é identidade pois para todo $a \in A$, $q(1_A)q(a) = q(1_A a) = q(a)$ e $q(a)q(1_A) = q(a1_A) = q(a)$, logo, $q(1_A) = 1_{A/I}$.

b) Temos que $\ker q = \{a \in A : q(a) = q(0)\} = \{a \in A : a \sim_I 0\} = \{a \in A : a \in I\} = I$.

c) Temos que $q(a) = [a]_{\sim_I} = \{b \in A : b \sim_I a\} = \{b \in A : b - a \in I\} = \{a + x : x \in I\}$ pois se $b - a \in I$ se, e somente se $a - b = x$ para algum $x \in I$.

d) Se A é comutativo, então $A/I = \operatorname{ran} q$ também é, pois q é homomorfismo de anéis. □

5.3 Teoremas do isomorfismo

Teorema 5.16 (Teorema do homomorfismo)**.** Seja $f : A \to R$ um homomorfismo de anéis e J um ideal tal que $J \subseteq \ker f$. Então, existe um único homomorfismo de anéis $g : A/J \to R$ tal que $g \circ q = f$, onde $q : A \to A/J$ é o mapa quociente canônico dado por $q(a) = a + J$.

Demonstração. Definimos $g : A/J \to R$ por $g(a + J) = f(a)$. Então, g é bem definido, pois se $a + J = b + J$, então $a - b \in J \subseteq \ker f$, logo, $f(a - b) = 0_R$, ou seja, $f(a) = f(b)$.

Agora, vejamos que g é um homomorfismo de anéis. De fato, para todo $a', b' \in A/J$, sendo $a' = a + J$ e $b' = b + J$, temos que:

- $g(a'+b') = g((a+J)+(b+J)) = g((a+b)+J) = f(a+b) = f(a)+f(b) = g(a+J)+g(b+J)$.
- $g(a'b') = g((a + J)(b + J)) = g(ab + J) = f(ab) = f(a)f(b) = g(a + J)g(b + J)$.
- $g(1_{A/J}) = g(1_A + J) = f(1_A) = 1_R$.

□

Teorema 5.17 (Primeiro Teorema do Isomorfismo)**.** Seja $f : A \to R$ um homomorfismo de anéis. Então, existe um único homomorfismo de anéis $g : A/\ker f \to R$ tal que $g \circ q = f$, onde $q : A \to A/J$ é o mapa quociente canônico dado por $q(a) = a + J$, e $g : A\ker f \to \operatorname{ran} f$ é isomorfismo.

Demonstração. Pelo Teorema do homomorfismo com $J = \ker f$, existe um único homomorfismo de anéis $g : A/\ker f \to \operatorname{ran} f$ tal que $g \circ q = f$. Como $g \circ q = f$ e q é sobrejetora, então $\operatorname{ran} g = \operatorname{ran}(g \circ q) = \operatorname{ran} f$, logo, q é sobre $\operatorname{ran} f$.

Resta ver que g é injetora. De fato, seja $q(a) \in A/\ker f$ tal que $g(q(a)) = 0_R$. Então, $f(a) = 0_R$, logo, $a \in \ker f = J$. ou seja, $a \sim_I 0$, logo $q(a) = q(0) = 0_{A/\ker f}$. Assim, g é injetora. □

Capítulo 6

Produtos de anéis

6.1 Produtos de anéis

Definição 6.1 (Produto Direto de dois anéis)**.** Sejam R, S anéis. O produto direto de R e S é o conjunto $R \times S$ munido das operações "ponto à ponto": dados $a = (a_1, a_2) \in R \times S$ e $b = (b_1, b_2) \in R \times S$, temos:

$$a + b = (a_1 + b_1, a_2 + b_2)$$
$$a \cdot b = (a_1 \cdot b_1, a_2 \cdot b_2)$$
$$0 = (0_R, 0_S)$$
$$1 = (1_R, 1_S)$$

□

Exemplo: Seja $R = \mathbb{Z}_3$ e $S = \mathbb{Z}_4$. Então $(2, 2) \in R \times S$ e $(1, 2) \in R \times S$. Temos:

$$(2, 2) + (1, 2) = (2 + 1, 2 + 2) = (0, 0)$$
$$(2, 2) \cdot (2, 2) = (2 \cdot 2, 2 \cdot 2) = (1, 0)$$

Definição 6.2 (Produtos de anéis)**.** Seja $(R_i)_{i \in I}$ uma família de anéis, onde cada R_i tem as operações $+_i, \cdot_i$ e constantes $0_i, 1_i$.

O produto (direto) de $(R_i)_{i \in I}$ é o conjunto $\prod_{i \in I} R_i$ munido das operações "ponto à ponto": dados $a = (a_i : i \in I), b = (b_i : i \in I)$ em $\prod_{i \in I} R_i$:

$$a + b = (a_i : i \in I) + (b_i : i \in I) = (a_i +_i b_i : i \in I) = (a_i +_i b_i)_{i \in I}$$
$$a \cdot b = (a_i : i \in I) \cdot (b_i : i \in I) = (a_i \cdot_i b_i : i \in I) = (a_i \cdot_i b_i)_{i \in I}$$

□

Lema 6.3 (O produto de anéis está bem definido)**.** Seja $(R_i)_{i \in I}$ uma família de anéis. Então seu produto direto $\prod_{i \in I} R_i$ é um anel com $0 = (0_i : i \in I)$ e $1 = (1_i : i \in I)$.

Demonstração. Sejam $a = (a_i : i \in I), b = (b_i : i \in I)$ e $c = (c_i : i \in I)$ em $\prod_{i \in I} R_i$.

- **Associatividade da soma:** $(a + b) + c = (a_i +_i b_i)_{i \in I} + c = ((a_i +_i b_i) +_i c_i)_{i \in I} = (a_i +_i (b_i +_i c_i))_{i \in I} = a + (b + c)$

- **Associatividade do produto:** Análogo.
- **Comutatividade da soma:** $a + b = (a_i +_i b_i)_{i\in I} = (b_i +_i a_i)_{i\in I} = b + a$
- **Neutro da soma:** $a + 0 = (a_i +_i 0_i)_{i\in I} = (a_i)_{i\in I} = a$
- **Inverso da soma:** Dado $a = (a_i)_{i\in I}$, considere $-a = (-a_i)_{i\in I}$. Então $a + (-a) = (a_i +_i (-a_i))_{i\in I} = (0_i)_{i\in I} = 0$.
- **Distributividade:** $a \cdot (b + c) = (a_i \cdot_i (b_i + c_i))_{i\in I} = (a_i \cdot_i b_i + a_i \cdot_i c_i)_{i\in I} = a \cdot b + a \cdot c$.
- **Distributividade II:** $(a + b) \cdot c = ((a_i + b_i) \cdot_i c_i)_{i\in I} = (a_i \cdot_i c_i + b_i \cdot_i c_i)_{i\in I} = a \cdot c + b \cdot c$.
- **Neutro do produto:** $a \cdot 1 = (a_i \cdot_i 1_i)_{i\in I} = (a_i)_{i\in I} = a$ e $1 \cdot a = (1_i \cdot_i a_i)_{i\in I} = (a_i)_{i\in I} = a$.

□

Definição 6.4 (Os mapas de projeção)**.** Seja $(R_i)_{i\in I}$ uma família de anéis e seja $R = \prod_{i\in I} R_i$. Para cada $i \in I$, o mapa de projeção $\pi_i : R \to R_i$ é dado por $\pi_i(a) = a_i$.

Escrevendo de outra forma, $\pi_i((a_j : j \in I)) = a_i$. □

Lema 6.5 (Os mapas de projeção são homomorfismos)**.** Seja $(R_i)_{i\in I}$ uma família de anéis e seja $R = \prod_{i\in I} R_i$. Para cada $i \in I$, o mapa de projeção $\pi_i : R \to R_i$ é um homomorfismo de anéis.

Demonstração. Sejam $a = (a_j : j \in I), b = (b_j : j \in I)$ em R. Então:

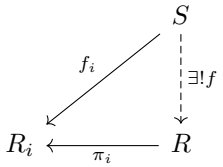
- $\pi_i(a + b) = \pi_i((a_j + b_j)_{j\in I}) = a_i + b_i = \pi_i(a) + \pi_i(b)$
- $\pi_i(a \cdot b) = \pi_i((a_j \cdot b_j)_{j\in I}) = a_i \cdot b_i = \pi_i(a) \cdot \pi_i(b)$
- $\pi_i(1_R) = \pi_i((1_j)_{j\in I}) = 1_i$

□

Notação: se R, S são anéis, o produto direto de (R, S) é denotado também como $R \times S$. Assim, se $(r, s), (r', s') \in R \times S$ e

6.2 A propriedade universal do produto direto de anéis

Teorema 6.6 (Propriedade universal do produto direto de anéis)**.** Seja $(R_i)_{i\in I}$ uma família de anéis e seja $R = \prod_{i\in I} R_i$ seu produto direto. Então, para cada anel S e cada família de homomorfismos de anéis $f_i : R_i \to S$, existe um único homomorfismo de anéis $f : R \to S$ tal que $\pi_i \circ f = f_i$ para todo $i \in I$.



Além disso, se R' e $(p_i : R' \to R)_{i\in I}$ é um anel e uma família de homomorfismos de anéis, respectivamente, tal que para cada anel S e cada família de homomorfismos de anéis $f_i : R_i \to S$, existe um único homomorfismo de anéis $f : R' \to S$ tal que $p_i \circ f = f_i$ para todo $i \in I$., então existe um único isomorfismo de anéis $\phi : R \to R'$ tal que $p_i \circ \phi = \pi_i$ para todo $i \in I$.

Demonstração. Seja $R = \prod_{i\in I} R_i$ e seja S um anel comutativo. Para cada $i \in I$, considere $f_i : S \to R_i$ um homomorfismo de anéis. Defina $f : S \to R$ tal que, dado $s \in S$:

$$f(s) = (f_i(s))_{i\in I}.$$

Então, para cada $i \in I$, $\pi_i \circ f(s) = \pi_i(f_j(s) : j \in I) = f_i(s)$, ou seja, $\pi_i \circ f = f_i$. Vejamos que f é homomorfismo de anéis. Dados $s, t \in S$, temos:

- $f(s + t) = (f_i(s + t))_{i\in I} = (f_i(s) + f_i(t))_{i\in I} = (f_i(s))_{i\in I} + (f_i(t))_{i\in I} = f(s) + f(t)$.
- $f(s \cdot t) = (f_i(s \cdot t))_{i\in I} = (f_i(s) \cdot f_i(t))_{i\in I} = (f_i(s))_{i\in I} \cdot (f_i(t))_{i\in I} = f(s) \cdot f(t)$.
- $f(1_S) = (f_i(1_S))_{i\in I} = (1_i)_{i\in I} = 1_R$.

Vejamos que f é único. Se $g : R \to S$ é um homomorfismo de anéis tal que $\pi_i \circ g = f_i$, então, para cada $s \in S$, temos, que, para cada $i \in I$:

$$\pi_i(g(s)) = f_i(s).$$

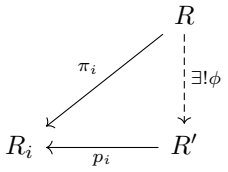
Assim:

$$g(s) = (\pi_i(g(s)) : i \in I) = (f_i(s) : i \in I) = f(s).$$

Portanto, $g = f$.

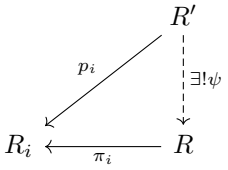
Agora suponha que R' e $(p_i : R' \to R)_{i\in I}$ são como no enunciado.

Aplicando a propriedade de R' para $(\pi_i : i \in I)$, existe um homomorfismo de anéis $\phi : R' \to R$ tal que $p_i \circ \phi = f_i$ para todo $i \in I$.

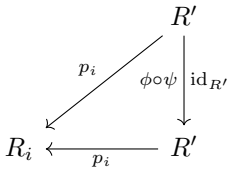


Nosso objetivo é mostrar que ϕ é isomorfismo. Construiremos uma inversa.

Aplicando a propriedade de R para $(\pi_i : i \in I)$, existe um homomorfismo de anéis $\psi : R' \to R$ tal que $\pi_i \circ \psi = p_i$ para todo $i \in I$.

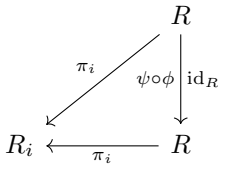


Tanto os mapas $\phi \circ \psi$ quanto a identidade $\mathrm{id}_{R'} : R' \to R'$ são homomorfismos de anéis que satisfazem o seguinte diagrama:



Pois $p_i \circ \mathrm{id}_{R'} = p_i$ e $p_i \circ \phi \circ \psi = \pi_i \circ \psi = p_i$. Assim, pela unicidade do homomorfismo de anéis, $\phi \circ \psi = \mathrm{id}_{R'}$.

Analogamente, tanto os mapas $\psi \circ \phi$ quanto a identidade $\mathrm{id}_R : R \to R$ são homomorfismos de anéis que satisfazem o seguinte diagrama:



Pois $\pi_i \circ \mathrm{id}_R = \pi_i$ e $\pi_i \circ \psi \circ \phi = p_i \circ \phi = \pi$. Assim, pela unicidade do homomorfismo de anéis, $\psi \circ \phi = \mathrm{id}_R$. Assim, ψ e ϕ são isomorfismos inversos.

A unicidade de ϕ como isomorfismo vem de sua unicidade como homomorfismo. □

Capítulo 7

Polinômios

7.1 Séries Formais

Se R é um anel comutativo, intuitivamente uma série formal é um objeto que se escreve na forma:

$$a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{i=0}^{\infty} a_i x^i$$

onde $a_i \in R$.

Que propriedades gostaríamos que esse objeto tivesse?

- **Igualdade:** igualdade de objetos desse tipo fosse determinada por uma condição de igualdade entre os coeficientes. Ou seja, que:

$$\sum_{i=0}^{\infty} a_i x^i = \sum_{i=0}^{\infty} b_i x^i \Leftrightarrow \forall i \in \mathbb{N}\, a_i = b_i.$$

- **Soma:** que a soma de dois objetos desse tipo fosse dada por:

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) + \left(\sum_{i=0}^{\infty} b_i x^i\right) = \left(\sum_{i=0}^{\infty} (a_i + bi) x^i\right)$$

- **Produto:** que o produto de dois objetos desse tipo fosse dada por:

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i$$

- **Preservação:** que as operações do anel sejam preservadas.

- Notação: $R[\![x]\!]$ é o conjunto de todas as séries formais em R.

Definição 7.1. Seja R um anel comutativo. Definiremos $R[\![x]\!] = R^{\mathbb{N}}$.

Um elemento de $R[\![x]\!]$ é da forma $p = (p_0, p_1, \dots) = (p_n)_{n\in\mathbb{N}} = (p(n))_{n\in\mathbb{N}} = (p(0), p(1), \dots)$ onde $p_i = p(i) \in R$ para todo $i \in \mathbb{N}$.

O suporte de $p \in R[\![x]\!]$ é o conjunto $\text{supp}(p) = \{i \in \mathbb{N} : p_i \neq 0\}$. O grau de $p \in R[x]$ é o maior elemento de $\text{supp}(p)$, denotado por $\deg(p)$. Se $p = 0$, então $\deg(p) = -\infty$

Intuição: $p = (a_0, a_1, \dots)$ corresponderá à $a_0 + a_1 x + \cdots + a_n x^n + \dots$.

Operações: Se $p, q \in R[x]$, define-se:

$$p + q = (p_0 + q_0, q_1 + p_1, \dots) = (p_i + q_i)_{i \in \mathbb{N}} \in R^{\mathbb{N}}$$

$$p \cdot q = (p_0 q_0, p_1 q_0 + p_0 q_1, p2q_0 + p_1 q_1 + p_0 q_2, \dots) = \left(\sum_{j=0}^{i} p_{i-j} q_j \right)_{i \in \mathbb{N}}$$

$$1_{R[\![x]\!]} = (1, 0, 0, \dots)$$

$$0_{R[\![x]\!]} = (0, 0, 0, \dots)$$

□

Lema 7.2 (Séries formais formam anéis)**.** Se R é um anel comutativo, então $R[\![x]\!]$ é um anel comutativo.

Demonstração. A operação de soma de $\mathbb{R}[\![x]\!]$ é a mesma de $\mathbb{R}^{\mathbb{N}}$, que já verificamos satisfazer as propriedades de grupo Abeliano. Assim, $R[\![x]\!]$ é um grupo abeliano sob a soma.

- **Distributividade:**

$$p \cdot (q + r) = p \cdot (q_i + r_i)_{i \in \mathbb{N}} = \left(\sum_{j=0}^{i} p_{i-j}(q_j + r_j) \right)_{i \in \mathbb{N}}$$

$$= \left(\sum_{j=0}^{i} p_{i-j} q_j \right)_{i \in \mathbb{N}} + \left(\sum_{j=0}^{i} p_{i-j} r_j \right)_{i \in \mathbb{N}} = p \cdot q + p \cdot r.$$

- **Elemento Neutro:**

$$p \cdot 1 = \left(\sum_{j=0}^{i} p_{i-j} \delta_{0j} \right)_{i \in \mathbb{N}} = (p_i)_{i \in \mathbb{N}}.$$

- **Comutatividade:** A i-ésima coordenada de $p \cdot q$ é $\sum_{j=0}^{i} p_{i-j} q_j = \sum (p_{i_j} q_j : j \in A_j)$, onde $A_j = \{0, \dots, i\}$. A função $\phi : A_j :\to A_j$ dada por $\phi(j) = i - j$ é bijetora, pois é injetora e A_j é finito. Assim:

$$\sum_{j=0}^{i} p_{i-j} q_j = \sum_{j=0}^{i} p_{i-\phi(j)} q_{\phi(j)} = \sum_{j=0}^{i} p_j q_{i-j} = \sum_{j=0}^{i} q_{i-j} p_j$$

  E esta é a i-ésima coordenada de $q \cdot p$.

- **Associatividade:** Temos que a i-ésima coordenada de $(p \cdot q) \cdot r$ é dada por:

$$\pi_i((p \cdot q) \cdot r) = \sum_{j=0}^{i} \pi_{i-j}(p \cdot q) \cdot q_j = \sum_{j=0}^{i} \left(\sum_{k=0}^{i-j} p_{i-j-k} q_k \right) \cdot q_j$$

$$= \sum_{j=0}^{i} \sum_{k=0}^{i-j} p_{i-j-k} q_k q_j = \sum \left(p_{i-j-k} q_k r_j : (j,k) \in A \right)$$

Onde $A = \{(j,k) : 0 \leq j \leq i, 0 \leq k \leq i-j\}$.

Temos que a i-ésima coordenada de $p \cdot (q \cdot r)$ é dada por:

$$\pi_i(p \cdot (q \cdot r)) = \sum_{s=0}^{i} p_{i-s} \pi_s(q \cdot r) = \sum_{s=0}^{i} p_{i-s} \left(\sum_{t=0}^{s} q_{s-t} r_t \right)$$

$$= \sum_{s=0}^{i} \sum_{t=0}^{s} p_{i-s} q_{s-t} r_t = \sum \left(q_{i-s} q_{s-t} r_t : (s,t) \in B \right)$$

onde $B = \{(s,t) : 0 \leq t \leq s \leq i\}$. A função $\phi : A \to B$ dada por $\phi(j,k) = (j+k, j)$ é bijetora: é em B, pois $0 \leq j \leq j+k \leq j+(i-j) = i$. É injetora, pois se $(j+k, j) = (j'+k', j')$ então $j = j'$ e, cancelando, $k = k'$. Finalmente, é sobrejetora, pois se $0 \leq t \leq s \leq i$, sendo $j = t$ e $k = s - t$, temos que $0 \leq j \leq i$, $0 \leq k = s - t \leq i - t = i - j$ e $j + k = s$. Assim, ϕ é bijetora. Portanto:

$$\sum \left(q_{i-s} q_{s-t} r_t : (s,t) \in B \right) = \sum \left(q_{i-(j+k)} q_{(j+k)-j} r_j : (j,k) \in A \right)$$

$$= \sum \left(q_{i-j-k} q_k r_j : (j,k) \in A \right).$$

□

Dado $p \in \mathbb{R}_x$, utilizamos a notação

$$p = p(x) = \sum_{i=0}^{\infty} p_i x^i.$$

É importante observar que não há, de fato, uma "soma infinita" acontecendo aqui. É possível dar sentido à essa soma infinita utilizando a teoria de limites diretos de anéis, mas não faremos isso aqui. Por ora, isso é apenas uma notação especial para tratar desses objetos. Note que, ao menos por enquanto, a letra x é apenas parte da notação, e que não faz sentido, por enquanto, "substituir x" por algo.

7.2 Anéis de Polinômios

Na subseção anterior, introduzimos o anel das séries formais de um anel comutativo dado. Vimos que tal anel é um anel comutativo.

Deste anel, podemos extrair o anel de polinômios.

Definição 7.3. Seja R um anel comutativo. O anel de polinômios $R[x]$ é o subconjunto de $R[\![x]\!]$ dado por:

$$R[x] = \{p \in R[\![x]\!] : \deg(p) < \infty\}$$

□

Note que uma série formal tem grau $< \infty$ se, e somente se, todos os coeficientes, a partir de algum ponto, são nulos.

Lema 7.4. Seja R um anel comutativo. O anel de polinômios $R[x]$ é um subanel de $R[\![x]\!]$. Mais especificamente, dados $p(x), q(x) \in R[\![x]\!]$, temos que, se $\operatorname{gr}(p(x)) < \infty$ e $\operatorname{gr}(q(x)) < \infty$, então:

a) $\operatorname{gr} p(x)q(x) \leq \operatorname{gr} p(x) + \operatorname{gr} q(x)$ caso ambos sejam não nulos, e a igualdade vale se R for um domínio de integridade.

b) $\operatorname{gr} p(x) + q(x) \leq \max\{\operatorname{gr} p(x), \operatorname{gr}(q(x))\}$.

Demonstração. Para a primeira afirmação, sejam n, m os graus de $p(x)$ e $q(x)$, respectivamente. Calculemos o coeficiente $n+m$ de $p(x)q(x)$.

$$\pi_{n+m}(p(x)q(x)) = \sum_{j=0}^{n+m} p_{n+m-j}q_j.$$

Se $0 \leq j < m$ temos que $n+m-j > 0$, e $p_{n+m-j} = 0$. Se $j > m$, temos que $q_j = 0$. Assim, o único termo não nulo da soma é quando $j = m$, e temos que $p_{n+m-m}q_m = p_n q_m$, que é não nulo se R for um domínio. Por outro lado, se $l > n+m$ temos que:

$$\pi_l(p(x)q(x)) = \sum_{j=0}^{l} p_{l-j}q_j.$$

Se $0 \leq j \leq m$ temos que $l - j > m + n - m = n$, e $p_{l-j} = 0$. Se $j > m$, temos que $q_j = 0$. Assim, todos os coeficientes da soma são 0.

Para a segunda afirmação, se $l > \max\{\operatorname{gr} p(x), \operatorname{gr} q(x)\}$, temos que o l-ésimo coeficiente de $p(x) + q(x)$ é 0, pois este é $p_l + q_l = 0 + 0$.

Agora, para a afirmação principal, as duas afirmações itemizadas nos mostram que $R[x]$ é fechado pela soma e produto de $R[\![x]\!]$. Finalmente, note que o grau da série $1 = (1, 0, 0, \dots)$ é 0, logo, $1 \in R[x]$. □

Agora vamos trabalhar um pouco mais nossa notação.

Definição 7.5. Seja R um anel comutativo. Em $R[x]$, seja $x = (0, 1, 0, 0, \dots)$ e, para cada $r \in R$, seja $\hat{r} = (\hat{r}, 0, 0, \dots)$. □

Lema 7.6. Na notação anterior, para todo $r \in R$ e $n, i \geq 0$:

$$\pi_i(\hat{r}x^n)(i) = \begin{cases} 0 & \text{se } i \neq n \\ r & \text{se } i = n. \end{cases}$$

Ou seja, $\hat{r}x^n = (0, 0, \dots, r, 0, \dots)$ onde o r está na posição n.

Demonstração. Fixe r Seguimos por indução. Para $n = 0$, temos que $\hat{r}x^0 = \hat{r} = (r, 0, 0, \dots)$ e para $n = 1$ temos que $\hat{r}x^1 = x = (0, r, 0, \dots)$.

Para o passo $n+1$, onde $n \geq 1$, temos que, sendo $i \geq 1$:

$$\pi_i(\hat{r}x^{n+1}) = \pi_i((\hat{r}x^n) \cdot x) = \sum_{j=0}^{i} \pi_{i-j}(\hat{r}x^n) \cdot \pi_j(x) = \pi_{i-1}^{\hat{r}x^n}$$

Assim, se $i = n+1$, temos que a coordenada é r, e 0 caso contrário. Resta apenas verificar que a coordenada 0 é 0. Ora, a coordenada 0 se dá por $\pi_0(\hat{r}x^n)\pi_0(x) = 0$. □

Lema 7.7. Na notação anterior, seja $h : R \to R[x]$ dada por $h(r) = \hat{r}$. Então h é um homomorfismo injetor.

Demonstração. Sejam $r, s \in R$. Então:

- $h(r+s) = (r+s, 0, 0, \dots) = \hat{r} + \hat{s} = h(r) + h(s)$
- $h(rs) = (rs, 0, 0, \dots) = \hat{r} \cdot \hat{s} = h(r) \cdot h(s)$
- $h(1_R) = \hat{1} = (1_R, 0, 0, \dots) = 1_{R[x]} = 1_{R[x]}$.

A injetividade é óbvia. □

Proposição 7.8. Na notação anterior, para todo $p(x) \in R[x]$, existem $n \geq 0$ e $r_0, r_1, \dots, r_n \in R$ tais que $p(x) = \sum_{i=0}^{n} \hat{r}_i x^i$.

Demonstração. Se $p(x) = 0$, seja $n = 0$ e $r_0 = 0$. Caso contrário, seja $n = \operatorname{gr} p(x)$ e $r_i = p_i$ para todo $i \leq n$. Então:

$$p(x) = (p_0, \dots, p_n, 0, \dots, 0) = (r_0, \dots, r_n, 0, \dots, 0) = \sum_{i=0}^{n} \hat{r}_i x^i$$

□

Proposição 7.9. Na notação anterior, se $r_1, \dots, r_n$ e $s_1, \dots, s_n$ são elementos de R, então: $\sum_{i=0}^{n} \hat{r}_i x^i = \sum_{i=0}^{n} \hat{s}_i x^i$ se, e somente se, $r_i = s_i$ para todo $i \leq n$.

Demonstração. A recíproca é imediata. Para a implicação direta, note que a igualdade nos diz que $(r_0, \dots, r_n, 0, 0, \dots) = (s_0, \dots, s_n, 0, 0, \dots)$, ou seja, $r_i = s_i$ para todo $i \leq n$. □

Notação: abandona-se $\hat{r}$ em favor de r, mesmo havendo ambiguidade de notação.