Estruturas Algébricas

Aula 1

Anéis

Abramo Hefez

2025

O que é a Álgebra?

Originalmente a Álgebra era definida como a arte de resolver problemas envolvendo operações nos conjuntos numéricos, confundindo-se com a Aritmética.

Por exemplo, resolver problemas que envolviam as operações de adição, subtração e multiplicação nos inteiros, acrescidos da operação de divisão no caso dos racionais ou dos reais.

No século **III**, Diofanto de Alexandria, considerado por muitos historiadores como o "paï" da Álgebra, escreveu uma obra com 13 livros que denominou de **Aritmética**, onde propunha problemas envolvendo inteiros que recaíam na resolução de equações algébricas para as quais oferecia soluções particulares.

Um exemplo típico é a resolução nos inteiros da Equação Pitagórica $X^2 + Y^2 = Z^2$.

Os trabalhos de Diofanto foram precedidos por Euclides, que em 300 aC escreveu **os Elementos**, um tratado em 13 volumes que marcou a matemática por mais de dois milênios.

Os *Elementos* revolucionaram o estudo da Geometria e continham três volumes dedicados aos números naturais e às sua propriedades relacionadas com as operações de adição e de multiplicação, pura Álgebra!

Em seguida, no Século 17, Pierre de Fermat faz reviver a Aritmética de Diofanto, provando inúmeros resultados e que ao estudar a Equação Pitagórica enunciou o famoso O **Último Teorema de Fermat**, sem porém dar-lhe uma prova e que só foi realizada no Século 20 pelo matemático Andrew Wiles.

No Século 18, temos os trabalhos de Leonhard Euler que aprofundam os estudos de Fermat.

Mais adiante, no final do Século 18 e adentrando o Século 19, temos os trabalhos de Carl Friedrich Gauss que se iniciam com a obra prima os **Disquisitiones Arithmeticae**, fonte de inspiração para vários desdobramentos da Álgebra.

Ainda no Século 18, com os seus trabalhos sobre a resolução das equações algébricas, mudando os paradigmas da Álgebra, Joseph Louis Lagrange considerou o conjunto das permutações munido de uma operação de "multiplicação" (a composição), permitindo a Evariste Galois introduzir a noção de grupo ao considerar subconjuntos especiais do conjunto das permutações e relacioná-los com certos corpos, resolvendo assim o problema da resolubilidade das equações algébricas de graus arbitrários.

A partir dessas contribuições e de muitas outras, para dar maior abrangência e aplicabilidade à Álgebra, foi se impondo no início do Século 20 a necessidade de introduzir a noção abstrata de **Estruturas Algébricas**, que consiste no estudo de conjuntos munidos de certas operações, focando nas propriedades das operações, sem levar em consideração a natureza dos objetos que compõem os conjuntos.

Neste curso, daremos início ao estudo das estruturas de **Anel** e de **Grupo**, dois vastos campos da Matemática.

Anéis

Dentre as estruturas algébricas, a estrutura de anel desponta naturalmente por ser a estrutura subjacente aos conjuntos numéricos:
dos números inteiros $\mathbb{Z}$,

dos números racionais $\mathbb{Q}$,

dos números reais $\mathbb{R}$,

dos números complexos $\mathbb{C}$,

bem como dos polinômios, das funções reais, etc.

A noção de Anel já aparece nos trabalhos de Richard Dedekind no século 19, mas foi apenas na década de 1920 que se definiu formalmente a essa noção.

Vamos inicialmente focar em dois conjuntos básicos que à primeira vista parecem muito distintos, mas do ponto de vista de suas estruturas algébricas são muito semelhantes, conforme ficará claro mais adiante.

O conjunto dos números inteiros que é representado como se segue:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

E o conjunto dos polinômios em uma indeterminada com coeficientes em A, onde A é, por exemplo, um dos conjuntos numéricos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. Trata-se do conjunto das expressões formais

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

onde n é um inteiro não negativo que pode variar e $a_0, \ldots, a_n$ são elementos arbitrários de A.

Nesses conjuntos estão definidas essencialmente duas operações binárias: a adição e a multiplicação. Algumas das propriedades básicas comuns dessas operações nesses conjuntos servem de inspiração para definir a estrutura de anel, que detalhamos a seguir.

Um *anel* é um conjunto A munido de duas operações chamadas de *adição* e de *multiplicação* que simbolizamos por $+$ e $\times$, respectivamente, e que possuem as seguintes propriedades:

Propriedades da adição

Associatividade:
$a + (b + c) = (a + b) + c$, quaisquer que sejam $a, b, c \in A$;

Comutatividade:
$a + b = b + a$ quaisquer que sejam $a, b \in A$;

Existência de elemento neutro:
Existe um elemento $\zeta \in A$ tal que $a + \zeta = a, \quad$ para todo $a \in A$;

Existência de elemento simétrico:
Para todo $a \in A$, existe um elemento $b \in A$ tal que $a + b = \zeta$;

Propriedades da multiplicação

Associatividade:
$a \times (b \times c) = (a \times b) \times c$, quaisquer que sejam $a, b, c \in A$;

Existência de elemento neutro:
Existe um elemento $u \in A$, $u \neq \zeta$, tal que $a \times u = u \times a = a$, para todo $a \in A$;

Propriedade de ligação da multiplicação com a adição

Distributividade:
$a \times (b + c) = a \times b + a \times c \quad \text{e} \quad (b + c) \times a = b \times a + c \times a$.

No que se segue, daremos preferência à notação $a \cdot b$, ou ab, no lugar de $a \times b$. Quando quisermos dar destaque às operações de um anel A iremos representá-lo por $(A, +, \cdot)$.

Para ser mais abrangente, não se exige na definição geral de anel que a multiplicação seja comutativa.

Exemplo O conjunto da matrizes quadradas $M_{n \times n}(\mathbb{R})$ com $n \geq 2$, onde n é o número de linhas ou de colunas, com coeficientes números reais, juntamente com as operações de adição e de multiplicação de matrizes é um anel em que a multiplicação não é comutativa.

Por exemplo, para $n = 2$:

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

Anéis para os quais a multiplicação é comutativa serão chamados de **anéis comutativos**, caso contrário, diremos que o anel é *não-comutativo*, obviamente nos referindo à operação de multiplicação, já que a adição é sempre considerada comutativa.

Neste curso **estudaremos essencialmente os anéis comutativos.**

As propriedades que definem um anel acarretam várias outras propriedades conhecidas ou implicitamente assumidas no caso dos inteiros e dos polinômios, conforme veremos a seguir.

Você pode se perguntar se em algum anel podem existir vários elementos que desempenham os papéis de elementos neutros para a adição ou para a multiplicação.

Vamos mostrar que, de fato, os elementos neutros para a adição e para a multiplicação de um anel são únicos.

Se ζ e ζ' são dois elementos neutros de A para a adição, tem-se que

$$\zeta = \zeta + \zeta' = \zeta',$$

onde a primeira igualdade decorre do fato de ζ' ser elemento neutro para a adição e a segunda igualdade provém do fato de ζ também ser elemento neutro para a adição.

A prova da unicidade do elemento neutro da multiplicação é semelhante.

Como os elementos neutros para a adição e para a multiplicação são únicos, eles são usualmente denotados pelos símbolos 0 e 1, e chamados de zero e um (ou unidade), respectivamente.

Em situações particulares, essa pode não ser a notação usual.

Por exemplo, no caso de $M_{n\times n}(\mathbb{R})$, o elemento neutro para a multiplicação, a matriz identidade, é denotado por $\mathrm{I_n}$.

Outra unicidade que pode ser provada é a do elemento simétrico de um elemento de um anel.

De fato, suponha que existam dois elementos simétricos de a, digamos, b e b'. Logo $a + b = 0$ e $a + b' = 0$.
Portanto,

$$b = 0 + b = (a + b') + b = (b' + a) + b = b' + (a + b) = b' + 0 = b'.$$

A unicidade do elemento simétrico de um dado elemento a nos autoriza a usar uma notação $-a$ que realça esse fato.

Isso nos permite definir a **operação de subtração**:

$$a - b = a + (-b),$$

Outra propriedade que os anéis possuem é a seguinte:
Proposição Seja A um anel seja $a \in A$. Tem-se que

$$a \cdot 0 = 0.$$

Demonstração: De fato, temos que $0 + 0 = 0$
pela distributividade:

$$a0 = a(0 + 0) = a0 + a0.$$

Somando a ambos os membros $-(a0)$, obtemos

$$0 = -(a0) + a0 = -(a0) + [a0 + a0] = [-(a0) + a0] + a0 = 0 + a0 = a0.$$

Um subconjunto A' não-vazio de um anel A será chamado de **subanel** de A, se A', juntamente com as restrições a ele das operações de adição e de multiplicação de A, é um anel cujo elemento unidade é o elemento unidade de A.

Por exemplo, $\mathbb{Z}$ é subanel de $\mathbb{Q}$, que é um subanel de $\mathbb{R}$, que, por sua vez, é um subanel de $\mathbb{C}$. A é um subanel de $A[x]$. A propriedade de ser subanel é claramente transitiva.

Para provar que um subconjunto A' de A é um subanel de A é preciso verificar que:

- 0 e 1 são elementos de A',
- a soma e o produto de dois elementos quaisquer de A' estão em A'
- o simétrico de todo elemento de A' está em A'.

As demais propriedades de um anel são automaticamente satisfeitas para os elementos de A', pois o são para os elementos de A.

Integridade

Alguns anéis, como $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, por exemplo, possuem a seguinte importante propriedade adicional:

Integridade: $\forall a, b \in A, \;\; ab = 0 \Rightarrow a = 0$ ou $b = 0$.

Equivalentemente, a integridade se expressa do seguinte modo:

Se $a, b \in A$ são tais que $a \neq 0$ e $b \neq 0$, então $ab \neq 0$.

Os anéis que possuem essa propriedade são chamados de *domínios de integridade*, ou apenas *domínios*. Por exemplo, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e $A[x]$, onde A é um dos anéis supracitados, são domínios. Nem todo anel é um domínio.

Exemplo O anel $M_{n\times n}(\mathbb{R})$ não é um domínio. Segue um exemplo para $n = 2$ de duas matrizes não nulas cujo produto é nulo

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

Um exemplo de um anel comutativo que não é um domínio é o conjunto $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ munido das seguintes operações:

$$\begin{array}{c|cccc} + & [0] & [1] & [2] & [3] \\ \hline [0] & [0] & [1] & [2] & [3] \\ [1] & [1] & [2] & [3] & [0] \\ [2] & [2] & [3] & [0] & [1] \\ [3] & [3] & [0] & [1] & [2] \end{array} \qquad \begin{array}{c|cccc} \cdot & [0] & [1] & [2] & [3] \\ \hline [0] & [0] & [0] & [0] & [0] \\ [1] & [0] & [1] & [2] & [3] \\ [2] & [0] & [2] & [0] & [2] \\ [3] & [0] & [3] & [2] & [1] \end{array}$$

A verificação de que $\mathbb{Z}_4$ é efetivamente um anel é tediosa, mas veremos mais adiante como isso se insere em um quadro geral de exemplos cuja verificação de que são anéis é feita em bloco.

Esse anel não é um domínio, pois

$$[2] \cdot [2] = [0].$$

Proposição (Lei do Cancelamento) Seja A um domínio de integridade. Suponhamos que os elementos $a, b, c \in A$ sejam tais que $c \neq 0$ e $a \cdot c = b \cdot c$, então $a = b$.

Demonstração   Se $a \cdot c = b \cdot c$, segue que $(a - b) \cdot c = 0$.

Como A é um domínio de integridade e $c \neq 0$,

segue que $a - b = 0$, logo $a = b$.

É claro que essa propriedade não vale no caso em que $c = 0$, pois, por exemplo, $2 \cdot 0 = 3 \cdot 0$, sem que 2 seja igual 3.

Note que todo subanel de um domínio é um domínio.

Elementos invertíveis

Um elemento a de um anel A é dito *invertível* se existir um elemento $b \in A$ tal que $ab = ba = 1$. Tal elemento b será chamado de *inverso* de a

Aqui, novamente, com um argumento semelhante ao caso do elemento simétrico, temos que para o inverso b de um elemento invertível a vale a unicidade.

Devido a esse fato, denotaremos o inverso de a pelo símbolo

$$a^{-1} \text{ ou } \frac{1}{a}.$$

Os elementos invertíveis de um anel são chamados também de *unidades*, a não serem confundidos com o elemento 1 do anel, que é uma unidade.

Alguns anéis como $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, por exemplo, possuem a seguinte propriedade adicional:

Existência de inverso Dado $a \in A \setminus \{0\}$, existe $b \in A$ tal que

$$ab = ba = 1.$$

.

Os anéis comutativos que possuem a propriedade da existência de inversos de todos os elementos não-nulos são chamados *corpos*.

Portanto, são corpos: $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, enquanto que $\mathbb{Z}$ não é um corpo.

Todo corpo é um domínio de integridade.

De fato, se $ab = 0$ e $a \neq 0$, então existe a^{-1}, de modo que

$$b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0.$$

O conjunto dos elementos invertíveis de um anel A desempenha papel importante e será denotado por A^*.

Por exemplo:

$\mathbb{Z}^* = \{-1, 1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$,

$M_{n\times n}(\mathbb{R})^* = \{A;\ \det A \neq 0\}$.

Em um anel A, se $a, b \in A$ são invertíveis, então ab é invertível e

$$(ab)^{-1} = b^{-1}a^{-1},$$

mesmo que A não seja comutativo.

Exemplos de anéis

Produto cartesiano de anéis Dados dois anéis $(A, +, \cdot)$ e $(B, +, \cdot)$, podemos construir um novo anel $A \times B$, produto direto de A e B, em que as operações de adição e de multiplicação são definidas por

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \quad \text{e}$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2).$$

Se A e B são comutativos, então $A \times B$ é comutativo.

Os elementos neutros para a adição e para a multiplicação são, respectivamente, $(0, 0)$ e $(1, 1)$.

O simétrico de (a, b) é $(-a, -b)$.

Se $a \in A$ e $b \in B$ são invertíveis, então (a, b) é invertível e $(a, b)^{-1} = (a^{-1}, b^{-1})$.

Note que $A \times B$ nunca é um domínio, pois

$$(1, 0) \cdot (0, 1) = (0, 0).$$

Essa construção pode ser iterada, construindo anéis $A \times B \times C$. Se aplicamos essa construção a um mesmo anel A, podemos construir A^2, A^3, etc.

Funções a valores em um anel

Sejam dados um conjunto arbitrário não vazio X e um anel A.

Podemos fabricar um novo anel $\mathcal{F}(X, A)$ considerando o conjunto das funções cujo domínio é o conjunto X e contradomínio o anel A.

As operações de $\mathcal{F}(X, A)$ são definidas como se segue:

Dados $f : X \to A$ e $g : X \to A$, consideram-se $f + g : X \to A$ e $f \cdot g : X \to A$, onde

$$(f+g)(x) = f(x) + g(x) \quad \text{e} \quad (f \cdot g)(x) = f(x) \cdot g(x).$$

Este anel é comutativo se A é comutativo. Os elementos neutros para a adição e a multiplicação são, respectivamente, as funções constantes $f(X) = \{0\}$ e $f(X) = \{1\}$. O simétrico de f é a função $-f$, definida por $(-f)(x) = -f(x)$ para todos $x \in X$.

Se X tem mais de um elemento, esse anel não é um domínio, mesmo que A o seja (construa um exemplo para se convencer disto).

Inteiros Gaussianos

Esse é um anel estudado por Gauss e utilizado por ele para provar resultados de aritmética. Como conjunto trata-se de

$$\mathbb{Z}[i] = \{a + bi;\ a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

As operações de adição e de multiplicação são as de $\mathbb{C}$.

Os elementos neutros para a adição e a multiplicação são, respectivamente, $0 = 0 + 0i$ e $1 = 1 + 0i$.

Este anel é um subanel de $\mathbb{C}$, logo é um domínio e é comutativo.

Define-se a *norma* de um elemento $z = a + bi \in \mathbb{Z}[i]$ como

$$N(a + bi) = z\bar{z} = a^2 + b^2 \in \mathbb{N} \cup \{0\}.$$

É um exercício de rotina verificar que, dados $z, z' \in \mathbb{Z}[i]$, tem-se que

i) $N(z) = 0$ se, e somente se, $z = 0$;

ii) $N(z) = 1$ se, e somente se, $z \in \mathbb{Z}[i]^*$;

iii) $N(zz') = N(z)N(z')$;

iv) Se $z' \neq 0$, então $N(zz') \geq N(z)$.

Utilizando as propriedades acima é fácil mostrar que os elementos invertíveis de $\mathbb{Z}[i]$ são os elementos $\pm 1, \pm i$, ou seja,

$$\mathbb{Z}[i]^* = \{-1, 1, -i, i\}.$$

Desafio: Um número natural a é dito soma de dois quadrados se existirem dois números naturais b e c tais que $a = b^2 + c^2$.

Mostre que o produto de dois números que são somas de dois quadrados é soma de dois quadrados.

Inteiros de Kummer

Seja d um número inteiro que não é um quadrado. Define-se

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d};\ a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

Esses são subanéis de $\mathbb{C}$ e englobam $\mathbb{Z}[i]$, quando $d = -1$ e é um exemplo importante na teoria quando $d = 5$.

Quatérnios

Sejam $\mathbf{i}, \mathbf{j}, \mathbf{k}$ símbolos. O anel dos quatérnios sobre $\mathbb{R}$ consiste nos elementos do conjunto

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k};\ \ a, b, c, d \in \mathbb{R}\},$$

munido das operações de adição e de multiplicação que descrevemos a seguir:

$$(a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}) + (a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) =$$
$$(a_1 + a_2) + (b_1 + b_2)\mathbf{i} + (c_1 + c_2)\mathbf{j} + (d_1 + d_2)\mathbf{k};$$

$$(a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}) \cdot (a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) =$$
$$(a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)\mathbf{i}+$$
$$(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)\mathbf{j} + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)\mathbf{k}.$$

Trata-se de um anel que não é comutativo, pois, por exemplo, $\mathbf{ij} \neq \mathbf{ji}$.

Não se assuste com a definição da multiplicação, pois usando essa fórmula deduz-se que os símbolos **i**, **j** e **k** satisfazem as relações:

$$\begin{aligned} &\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \\ &\mathbf{ij} = \mathbf{k}, \ \mathbf{jk} = \mathbf{i}, \ \mathbf{ki} = \mathbf{j}, \\ &\mathbf{ji} = -\mathbf{k}, \ \mathbf{kj} = -\mathbf{i}, \ \mathbf{ik} = -\mathbf{j}, \end{aligned}$$

e que o produto pode ser obtido usando essas relações e as operações usuais de distributividade e associatividade.

Esse anel tem uma peculiaridade, dado um elemento $q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \neq 0$, o elemento

$$q' = \frac{a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2}$$

é tal que $qq' = q'q = 1$.

Portanto, o anel $\mathbb{H}$ apesar de não ser comutativo, tem a propriedade de que todo elemento não-nulo possui um inverso multiplicativo. Esse tipo de anel é chamado de *anel de divisão*.

Corpo de Galois

O conjunto $A = \{[0], [1]\}$ munido das seguintes operações:

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

e

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

é um anel.

Como $[1]$ é o único elemento não nulo de A e é invertível, segue-se que A é um corpo. Esse é o corpo com menor número possível de elementos, denotado por $\mathbb{Z}_2$ e é chamado *Corpo de Galois*, em homenagem a Evariste Galois.

Anéis Booleanos

Um anel $(A, +, \cdot)$ é dito *um anel Booleano* se $a^2 = a$, para todo $a \in A$.
Um exemplo concreto de anel Booleano é dado a seguir:

Seja X um conjunto não vazio qualquer e denotemos $\mathcal{P}(X)$ o conjunto das partes de X.

Definimos $\mathfrak{B} = \mathcal{P}(X)$ como conjunto e consideremos as seguintes operações em $\mathfrak{B}$:

$$A + B = (A \cup B) \setminus (A \cap B) \quad \text{e} \quad A \cdot B = A \cap B.$$

A verificação de que $(\mathfrak{B}, +, \cdot)$ é um anel é deixada como exercício.

Anéis Booleanos são comutativos.

Corpo de frações de um domínio

Dado um domínio de integridade, é possível imergi-lo num corpo, de modo totalmente análogo ao que se faz com o anel dos inteiros e o corpo dos números racionais.
Seja A um domínio de integridade.

Define-se o *corpo de frações* de A como sendo o conjunto

$$Q(A) = \left\{ \frac{a}{b};\ a, b \in A \ \text{ e } \ b \neq 0 \right\},$$

onde $\frac{a}{b}$ é apenas um símbolo com a convenção de considerar iguais $\frac{a}{b}$ e $\frac{c}{d}$ sempre que $ad = bc$.

Vamos munir $Q(A)$ com as operações de adição e multiplicação:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

e

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

respectivamente.

Observe que estas operações em $Q(A)$ estão bem definidas, pois $bd \neq 0$ e o resultado independe da representação escolhida para os elementos de $Q(A)$.
De fato, se
$$\frac{a}{b} = \frac{a'}{b'} \text{ e } \frac{c}{d} = \frac{c'}{d'},$$
é fácil verificar que
$$(ad + bc)b'd' = (a'd' + b'c')bd,$$
e
$$(ac)b'd' = (a'c')bd.$$
Portanto,
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'} = \frac{a'}{b'} + \frac{c'}{d'}$$
e
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{a'c'}{b'd'} = \frac{a'}{b'} \cdot \frac{c'}{d'}.$$

Uma série de verificações diretas mostra que $Q(A)$ é um corpo, onde $\frac{0}{1}$ e $\frac{1}{1}$ são respectivamente os elementos neutros da adição e da multiplicação, e o inverso de $\frac{a}{b} \neq \frac{0}{1}$ é $\frac{b}{a}$.

Pelo fato de todo elemento $a \in A$ poder ser escrito de modo único na forma $\frac{a}{1}$, temos que
$$A \subset Q(A).$$

Com esta construção temos que o corpo de frações do anel dos inteiros $\mathbb{Z}$ é o corpo do números racionais $\mathbb{Q}$. Em símbolos:

$$Q(\mathbb{Z}) = \mathbb{Q}.$$

O corpo de frações de $\mathbb{R}[x]$ é o conjunto $\mathbb{R}(x)$ das frações de polinômios cujo denominador é não-nulo.

É fácil verificar que o corpo de frações do anel dos inteiros Gaussianos $\mathbb{Z}[i]$ é o corpo

$$\mathbb{Q}(i) = \{x + yi;\ x, y \in \mathbb{Q}\}.$$

Pequena Bibliografia Nacional

1) Curso de Álgebra, Vol.1 - A. Hefez. Coleção Matemática Universitária-IMPA, sexta edição 2024.
2) Elementos de Álgebra - A. Garcia, Y. Lequain. Coleção Projeto Euclides-IMPA, sétima edição 2022.
3) Introdução à Álgebra - A. Gonçalves. Coleção Projeto Euclides-IMPA, sexta edição 2017.
4) Álgebra exemplar - um estudo da Álgebra através de exemplos - S.T. Martins, E. Tengan. Coleção Projeto Euclides-IMPA, 2020.

FIM DA AULA 1