1. Aneis comutativos unitários

Definição 1 (**Anel unitário**). *Um anel unitário é um conjunto A que tem duas operações binarias $+$ e $\cdot$ (soma e produto) tais que*

(1) *A com a operação $+$ é um grupo comutativo com elemento neutro 0 e o inverso (aditivo) de a é $-a$.*
(2) *A com a operação $\cdot$ é um monoide, isto é, $\cdot$ é associativa e existe um elemento neutro 1.*
(3) *Propriedade distributiva (compatibilidade entre soma e produto): $a(b+c) = ab + ac$ e $(a+b)c = ac + bc$ para todo $a, b, c \in A$.*

A palavra "unitário" refere-se à existência do elemento 1 (elemento neutro do produto). Observe que em geral um anel não é um grupo com a multiplicação. Quando falamos "anel" queremos sempre dizer anel unitário. Um anel A é dito **comutativo** se a sua operação de multiplicação é comutativa, isto é, se $ab = ba$ para todo $a, b \in A$.

Multiplicação por zero. Se A é um anel e $a \in A$ então $a \cdot 0 = 0$. De fato $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$ logo adicionando $-(a \cdot 0)$ aos dois lados $0 = a \cdot 0$. Observe que a igualdade $a \cdot 0 = 0$ é uma consequência da propriedade distributiva. Isso implica em particular que 0 admite inverso multiplicativo se e somente se $0 = 1$, e neste caso o inverso de 0 é 0 e $A = \{0\}$ (porque se $a \in A$ então $a = a \cdot 1 = a \cdot 0 = 0$).

Por exemplo $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ são aneis comutativos com as operações usuais.

Um exemplo importante de anel é $\mathbb{Z}/n\mathbb{Z}$ com soma e produto modulares. A propriedade distributiva neste caso é uma consequência imediata da propriedade distributiva em $\mathbb{Z}$: se $a, b, c \in \mathbb{Z}$ então

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

Todos os aneis considerados serão unitários.

Definição 2 (Corpo). *Um anel comutativo A é dito* ***corpo*** *se todo elemento $a \in A$ diferente de zero admite inverso multiplicativo a^{-1}.*

Por exemplo $\mathbb{Z}$ não é um corpo (pois por exemplo $2 \in \mathbb{Z}$ mas $2a \neq 1$ para todo $a \in \mathbb{Z}$) mas $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos.

Proposição 1. *O anel comutativo $A = \mathbb{Z}/n\mathbb{Z}$ é um corpo se e somente se n é um número primo.*

Demonstração. A é um corpo se e somente se todo elemento $\overline{a} \neq 0$ admite inverso multiplicativo, ou seja todo $a \in \{1, 2, \ldots, n-1\}$ é coprimo com n, ou seja n é um número primo. $\square$

Se A é um anel comutativo considere $U(A)$, o conjunto dos elementos de A que admitem inverso multiplicativo. $U(A)$ é um grupo multiplicativo (um grupo com a operação de multiplicação) chamado de "**grupo das unidades**" de A (grupo dos elementos inversíveis de A). Por exemplo já estudamos o grupo $U(\mathbb{Z}/n\mathbb{Z})$. Observe que $U(\mathbb{Z}) = \{1, -1\}$ (pois os únicos inteiros que admitem inverso multiplicativo inteiro são 1 e -1), logo $U(\mathbb{Z})$ é um grupo cíclico de ordem 2 (gerado por -1). Vimos que $U(\mathbb{Z}/n\mathbb{Z})$ é um grupo de ordem $\varphi(n)$ e que é cíclico de ordem $n-1$ se n for primo.

Observe que é imediato da definição de corpo que o anel comutativo A é um corpo se e somente se $U(A) = A - \{0\}$. Por exemplo $\mathbb{Z}/6\mathbb{Z}$ não é um corpo pois $U(\mathbb{Z}/6\mathbb{Z}) = \{1, 5\} \neq \{1, 2, 3, 4, 5\} = \mathbb{Z}/6\mathbb{Z} - \{0\}$, e $\mathbb{Z}/5\mathbb{Z}$ é um corpo pois $U(\mathbb{Z}/5\mathbb{Z}) = \{1, 2, 3, 4\} = \mathbb{Z}/5\mathbb{Z} - \{0\}$. Observe que no anel $\mathbb{Z}/6\mathbb{Z}$ temos $2 \neq 0$, $3 \neq 0$ mas $2 \cdot 3 = 6 = 0$. Isso mostra que em um anel pode acontecer que o produto de dois elementos não nulos é igual a zero. Isso não acontece em um corpo:

Proposição 2 (Lei de cancelamento). *Seja K um corpo, e sejam $a, b \in K$. Então $ab = 0$ se e somente se $a = 0$ ou $b = 0$. Em outras palavras se $a \neq 0$ e $b \neq 0$ então $ab \neq 0$.*

Demonstração. Sendo a segunda implicação imediata, mostraremos somente a primeira implicação. Suponha $ab = 0$. Se $a \neq 0$ existe $a^{-1} \in K$ (sendo K um corpo) logo multiplicando os dois lados da igualdade $ab = 0$ por a^{-1} obtemos $b = 0$. Se $b \neq 0$ existe $b^{-1} \in K$ (sendo K um corpo) logo multiplicando os dois lados da igualdade $ab = 0$ por b^{-1} obtemos $a = 0$. □

2. Aneis de polinômios

Seja K um anel comutativo. Um "polinômio com coeficientes em K" é uma função $f : \mathbb{N} \to K$ tal que $C = \{i \in \mathbb{N} \ : \ f(i) \neq 0\}$ é finito. A representação canônica de polinômio é

$$P(X) = \sum_{i=0}^{n} a_i X^i = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n$$

onde $a_i = f(i) \in K$ e $f(i) = 0$ para $i > n$. Os elementos $a_0, a_1, \ldots, a_n$ são chamados de "**coeficientes**" do polinômio $P(X)$. Observe que C pode ser vazio, neste caso o polinômio $P(X)$ é chamado de **polinômio nulo**: $P(X) = 0$. Se C não for vazio na escrita $P(X) = \sum_{i=0}^{n} a_i X^i$ supomos por coerência de notação que o coeficiente de X^n seja não nulo: $a_n \neq 0$. Em outras palavras $n = \max(C)$. Se C não for vazio (ou seja se $P(X)$ não for o polinômio nulo), o máximo elemento de C (que existe pois C é finito) é chamado de **grau** do polinômio. Por exemplo o polinômio $6X^3 + 2X^2 + 1$ tem grau 3, e C neste caso é $\{0, 2, 3\}$ (que está contido propriamente em $\{0, 1, 2, 3\}$). Observe que $a_0 = 1$, $a_1 = 0$, $a_2 = 2$, $a_3 = 6$, e $a_i = 0$ para todo $i \geq 4$. Ou seja os a_i que não aparecem são iguais a zero. Se C for vazio então $P(X) = 0$ é o polinômio nulo e normalmente digamos que o grau do polinômio nulo é $-\infty$, um número menor de todos os números. Os polinômios de grau zero são da forma a com $0 \neq a \in K$ (polinômios "constantes"), os polinômios de grau 1 são da forma $aX + b$ com $a, b \in K$ e $a \neq 0$, os polinômios de grau 2 são da forma $aX^2 + bX + c$ com $a, b, c \in K$ e $a \neq 0$, etc.

Dois polinômios $P_1(X) = \sum_{i=0}^{n} a_i X^i$, $P_2(X) = \sum_{i=0}^{n} b_i X^i$ são iguais exatamente quando são iguais as funções correspondentes $f(i) = a_i$, $g(i) = b_i$, ou seja exatamente quando $a_i = b_i$ para todo $i \in \mathbb{N}$. Esse fato é as vezes chamado de "principio de identidade dos polinômios", se trata de uma consequência imediata da definição de polinômio.

Podemos introduzir duas operações entre polinômios.

- **Soma**.
$$\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} b_i X^i = \sum_{i=0}^{n} (a_i + b_i) X^i.$$
- **Produto**. Se trata da regra $X^i X^j = X^{i+j}$ extendida por distributividade, ou seja
$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot \left(\sum_{i=0}^{m} b_i X^i\right) := \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j\right) X^k.$$

PROPOSIÇÃO 3. *Seja K um corpo. Se $P(X), Q(X) \in K[X]$ são dois polinômios não nulos de graus n e m, o grau de $P(X)Q(X)$ é $n + m$.*

DEMONSTRAÇÃO. Escrevendo $P(X) = \sum_{i=0}^{n} a_i X^i$ e $Q(X) = \sum_{i=0}^{m} b_i X^i$ com $a_n \neq 0$, $b_m \neq 0$ é imediato ver, usando a distributividade, que $P(X)Q(X) = a_n b_m X^{n+m} + J(X)$ com $J(X)$ de grau menor que $n+m$, logo o grau de $P(X)Q(X)$ é $n + m$: de fato $a_n b_m \neq 0$ sendo K um corpo, $a_n, b_n \in K$, $a_n \neq 0$ e $b_m \neq 0$. $\square$

O conjunto de todos os polinômios com coeficientes no anel comutativo unitário K é indicado por $K[X]$. Se trata de um anel comutativo unitário com elemento neutro da soma 0 (o polinômio nulo) e elemento neutro do produto 1 (o polinômio constante 1). Em geral os elementos não admitem inverso multiplicativo, por exemplo consideramos o polinômio X. Não existe nenhum polinômio $P(X)$ tal que $XP(X) = 1$, sendo o grau de $XP(X)$ igual a $1 + n$ onde n é o grau de $P(X)$, e $1 + n \geq 1$.

TEOREMA 1 (Divisão com resto para polinômios.). *Sejam $A(X), B(X) \in K[X]$ dois polinômios não nulos. Existem $Q(X)$, $R(X)$ em $K[X]$ (quociente e resto) polinômios com $R(X)$ nulo ou de grau menor que o grau de $B(X)$, tais que*
$$A(X) = Q(X)B(X) + R(X).$$

DEMONSTRAÇÃO. Considere o conjunto
$$U = \{A(X) - S(X)B(X) \ : \ S(X) \in K[X]\}.$$
Se $0 \in U$ então existe $Q(X)$ com $A(X) = Q(X)B(X)$ e basta escolher $R(X) = 0$. Agora suponha $0 \notin U$. Então o conjunto dos graus dos elementos de U admite

mínimo. Seja $R(X) = A(X) - Q(X)B(X)$ um polinômio de U de grau mínimo. Precisamos mostrar que o grau n de $R(X)$ é menor que o grau m de $B(X)$. Seja a o coeficiente de X^n em $R(X)$ multiplicado pelo inverso do coeficiente de X^m em $B(X)$ (que existe pois K é corpo!). Se for $n \geq m$ (por contradição) então escrevendo $n = m + k$, $k \geq 0$ e por definição de a, $L(X) = R(X) - aX^kB(X)$ é nulo ou tem grau menor que n. Obtemos

$$A(X) - Q(X)B(X) = R(X) = L(X) + aX^kB(X)$$

logo $A(X) - (Q(X) + aX^k)B(X) = L(X)$ daí $L(X) \in U$. Mas isso implica que $L(X) \neq 0$ (pois $0 \notin U$) e $L(X)$ tem grau menor que o grau de $R(X)$. Isso contradiz a minimalidade do grau de $R(X)$. $\square$

Por exemplo se $A(X) = X^2 + X + 2$ e $B(X) = X$ o problema da divisão com resto é reduzida a "colocar X em evidência": $A(X) = X(X+1) + 2 = (X+1)B(X) + 2$ logo $Q(X) = X + 1$ e $R(X) = 2$. Observe que $R(X)$ tem grau zero, e $B(X)$ tem grau 1, o que faz sentido pois $0 < 1$.

Um outro exemplo fácil é $A(X) = X^2+1$, $B(X) = X+1$, neste caso $X^2+1 = (X-1)(X+1) + 2$ logo $Q(X) = X - 1$ e $R(X) = 2$.

Para resolver exemplos mais complicados precisamos de um algoritmo de divisão. O algoritmo para fazer a divisão com resto entre dois polinômios $A(X)$ e $B(X)$ é o seguinte. Sejam n o grau de $A(X)$, m o grau de $B(X)$, daí existem polinômios $H(X)$ (de grau menor que n) e $J(X)$ (de grau menor que m) tais que $A(X) = a_nX^n + H(X)$ e $B(X) = b_mX^m + J(X)$.

$$\begin{array}{c|c} A(X) = a_nX^n + H(X) & B(X) = b_mX^m + J(X) \\ & \\ Q_1(X)B(X) & Q_1(X) = \frac{a_n}{b_m}X^{n-m} \\ & \\ \hline & \\ A(X) - Q_1(X)B(X) & \end{array}$$

Feito isso, o algoritmo continua com $A(X) - Q_1(X)B(X)$ no lugar de $A(X)$. Isso nos dá um "segundo quociente" $Q_2(X)$, etc. No final teremos que o resto da divisão é o último polinômio da primeira coluna e o quociente é $Q_1(X)+Q_2(X)+\dots$

Observe que o polinômio $\frac{a_n}{b_m}X^{n-m}$ é um elemento de $K[X]$, e isso explica porque escolhemos K como sendo um corpo. Por exemplo o anel $\mathbb{Z}[X]$ não admite divisão com resto.

Exemplo. Sejam $A(X) = X^4 + X^2 + 1$, $B(X) = X^2 + X$ em $\mathbb{Q}[X]$. Faremos a divisão com resto entre $A(X)$ e $B(X)$.

$$\begin{array}{c|c}
X^4 + X^2 + 1 & X^2 + X \\
X^4 + X^3 & X^2 - X + 2 \\
\hline
-X^3 + X^2 + 1 & \\
-X^3 - X^2 & \\
\hline
2X^2 + 1 & \\
2X^2 + 2X & \\
\hline
-2X + 1 &
\end{array}$$

Obtemos que $A(X) = B(X)Q(X) + R(X)$ onde $Q(X) = X^2 - X + 2$ (quociente) e $R(X) = -2X + 1$ (resto).

Exemplo. Sejam $A(X) = X^4 - 2X^3 + X^2 - X - 1$ e $B(X) = 3X^2 + X$. Faremos a divisão com resto entre $A(X)$ e $B(X)$.

$$\begin{array}{c|c}
X^4 - 2X^3 + X^2 - X - 1 & 3X^2 + X \\
X^4 + \frac{1}{3}X^3 & \frac{1}{3}X^2 - \frac{7}{9}X + \frac{16}{27} \\
\hline
-\frac{7}{3}X^3 + X^2 - X - 1 & \\
-\frac{7}{3}X^3 - \frac{7}{9}X^2 & \\
\hline
\frac{16}{9}X^2 - X - 1 & \\
\frac{16}{9}X^2 + \frac{16}{27}X & \\
\hline
-\frac{43}{27}X - 1 &
\end{array}$$

Obtemos que $A(X) = B(X)Q(X) + R(X)$ onde $Q(X) = \frac{1}{3}X^2 - \frac{7}{9}X + \frac{16}{27}$ (quociente) e $R(X) = -\frac{43}{27}X - 1$ (resto).

Lembrando que em $\mathbb{Z}/5\mathbb{Z}[X]$ temos $3^{-1} = 2$, podemos fazer a divisão entre $A(X) = X^4 - 2X^3 + X^2 - X - 1$ e $B(X) = 3X^2 + X$ em $\mathbb{Z}/5\mathbb{Z}[X]$. Temos

$$\begin{array}{c|c}
X^4 - 2X^3 + X^2 - X - 1 & 3X^2 + X \\
X^4 + 2X^3 & 2X^2 + 2X + 3 \\
\hline
X^3 + X^2 + 4X + 4 & \\
X^3 + 2X^2 & \\
\hline
4X^2 + 4X + 4 & \\
4X^2 + 3X & \\
\hline
X + 4 &
\end{array}$$

Tendo divisão com resto, podemos aplicar o algoritmo de Euclides exatamente como o aplicamos em $\mathbb{Z}$. Ou seja se K é corpo então no anel $K[X]$ pode se aplicar o algoritmo de Euclides.

Uma "raiz" de $P(X) \in K[X]$ é um elemento $a \in K$ tal que $P(a) = 0$.

Proposição 4. *Seja K um corpo e seja $P(X) \in K[X]$ de grau $n \geq 1$. Então $P(X)$ tem no máximo n raizes em K.*

Demonstração. Por indução sobre n. Se $n = 1$ então $P(X) = cX + d$ (com $c, d \in K$ e $c \neq 0$) tem exatamente uma raiz, $-d/c = -d \cdot c^{-1}$ (observe que c^{-1} existe porque K é um corpo e $c \neq 0$). Suponha o resultado verdadeiro para n e seja $P(X)$ um polinômio de grau $n + 1$. Se $P(X)$ não tiver raizes em K então $P(X)$ tem no máximo $n + 1$ raizes (pois $0 \leq n + 1$) e o resultado é demonstrado, então suponha que $P(X)$ tenha uma raiz $a \in K$. Fazendo a divisão com resto entre $P(X)$ e $X - a$ obtemos $P(X) = (X - a)Q(X) + R(X)$ com $R(X)$ nulo ou de grau menor que o grau de $X - a$, ou seja $R(X) = r \in K$ é uma constante (que pode ser nula). Sendo $P(a) = 0$ obtemos

$$0 = P(a) = (a - a)Q(a) + r = r$$

daí $r = 0$ logo $P(X) = (X - a)Q(X)$, logo $Q(X)$ tem grau n (pois $P(X)$ tem grau $n + 1$ e $X - a$ tem grau 1). Uma raiz de $P(X)$ diferente de a tem que ser uma raiz de $Q(X)$ (pois se $P(b) = 0$ então $(b - a)Q(b) = 0$ logo $Q(b) = 0$ se $b \neq a$, sendo K um corpo), por hipótese $Q(X)$ tem no máximo n raizes em K (pois o resultado é verdadeiro para n) logo $P(X)$ tem no máximo $n + 1$ raizes em K. □

Todo polinômio $P(X) \in K[X]$ induz uma função polinomial $f_P : K \to K$, $f_P(x) := P(x)$. Dois polinômios diferentes podem induzir a mesma função polinomial. Por exemplo $X^2 + X$ e 0 induzem a função nula $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

Exercícios.

(1) Faça a divisão com resto entre $X^6 - X$ e $2X^2 + X + 1$ em $\mathbb{Q}[X]$ e em $\mathbb{Z}/7\mathbb{Z}[X]$.

(2) Encontre dois polinômios $G(X), H(X) \in \mathbb{Q}[X]$ tais que
$$G(X)(X^3 + 2) + H(X)(X^2 + X + 1) = 1.$$

(3) Existe uma formula para o grau de $A(X) + B(X)$ que depende só dos graus de $A(X)$ e $B(X)$?

(4) Encontre todos os $x \in \mathbb{Z}/17\mathbb{Z}$ tais que $x^2 + 8x + 14 = 0$.

(5) Conte os polinômios de grau 4 em $\mathbb{Z}/3\mathbb{Z}[X]$.

(6) Calcule $X(X - 1)(X - 2)(X - 3)(X - 4)$ em $\mathbb{Z}/5\mathbb{Z}[X]$.

(7) Encontre todos os $x \in \mathbb{Z}/16\mathbb{Z}$ tais que $x^4 = 0$.

(8) Sejam A e B dois aneis (comutativos, unitários). Seja $R = A \times B$ o produto cartesiano entre A e B. Mostre que R é um anel (comutativo, unitário) com as operações
$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$

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

Mostre que $U(R) = U(A) \times U(B)$. R é um corpo?

(9) Seja A o conjunto das funções $f : \mathbb{R} \to \mathbb{R}$. Mostre que A é um anel comutativo unitário com as operações

$$(f + g)(x) := f(x) + g(x), \qquad (f \cdot g)(x) := f(x)g(x).$$

Calcule $U(A)$.

(10) Seja A um anel unitário. Mostre que $U(A)$ com a multiplicação é um grupo.

(11) Seja K um corpo. Mostre que $U(K[X]) = U(K) = K - \{0\}$.

(12) Seja G um grupo abeliano aditivo e seja $A = End(G)$ o conjunto dos endomorfismos de G, ou seja os homomorfismos $G \to G$. Mostre que A é um anel com as operações $(f + g)(x) = f(x) + g(x)$ (para todo $x \in G$) e $(fg)(x) = f(g(x))$ (para todo $x \in G$).

(13) Seja A um anel unitário. Mostre que se $b^2 = b$ para todo $b \in A$ então A é comutativo. Mostre que se $b^3 = b$ para todo $b \in A$ então A é comutativo.

(14) Seja p um número primo ímpar e seja K o corpo $\mathbb{Z}/p\mathbb{Z}$. Mostre que o polinômio $X^2 + 1 \in K[X]$ admite uma raiz em K se e somente se $p \equiv 1 \mod 4$. [Dica: lembre-se que $U(K) \cong C_{p-1}$.]

(15) Mostre que existem infinitos primos congruentes a 1 módulo 4.

[Dica: suponha isso falso por contradição e seja m o produto de todos os primos congruentes a 1 módulo 4. Seja $P(X) = X^2 + 1$ e seja p um divisor primo de $P(2m)$. Mostre que $P(X)$ admite uma raiz em $K = \mathbb{Z}/p\mathbb{Z}$ e deduza que $p \equiv 1 \mod 4$ usando o exercício anterior.]

(16) Seja K um corpo infinito e seja $P(X)$ um polinômio em $K[X]$. Então $P(X)$ é o polinômio nulo se e somente se $P(a) = 0$ para todo $a \in K$.

(17) Seja K um corpo, e seja F o conjunto das funções $K \to K$. Seja $g : K[X] \to F$ a função definida por $g(P(X))(a) := P(a)$. Mostre que g é injetiva se e somente se K é infinito.