Capítulo 1

Polinômios

1.1 Introdução

Neste capítulo estudaremos de maneira mais abstrata as expressões que definem nossas equações algébricas. Mais precisamente analisaremos o vínculo existente entre a natureza dos coeficientes encontrados numa tal expressão e a natureza da expressão em si; afim de esclarecer, vejamos um exemplo.

Exemplo 1.1.1. Consideremos a equação $x^2 - 3 = 0$; como sabemos é possível escrever $x^2 - 3 = (x - \sqrt{3})(x - \sqrt{3})$, onde $\pm\sqrt{3}$ são as soluções da equacão. Observemos, por um lado, que os coeficientes envolvidos na equação de grau dois sao números racionais enquanto as soluções desta são irracionais; por outro lado, a existência das soluções nos permitiu *fatorar* a expressão quadrática como produto de duas expressões lineares cujos coeficientes deixam de ser racionais. Não é dificil de se convencer que a equação quadrática original, não pode ser fatorada como produto de duas expressões lineares com coeficientes racionais (tente demonstrar isto).

1.2 O Anel de polinômios

Seja $\mathbb{D}$ um domínio de integridade (para efeitos práticos, basta supor que $\mathbb{D} = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$).

Definição 1.2.1. *Um polinômio com coeficientes em $\mathbb{D}$ é uma expressão da forma*

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n,$$

onde n é um inteiro não negativo e $a_0, a_1, \cdots, a_{n-1}, a_n \in \mathbb{D}$; a_i chama-se o coeficiente i-ésimo de $f(x)$, $i = 0, \ldots, n$. Se $a_n \neq 0$ dizemos que a_n é o coeficiente líder e que o inteiro n é o grau de $f(x)$.

Dois polinômios

$$f(x) = \sum_{k=0}^{n} a_kx^k, g(x) = \sum_{j=0}^{m} b_jx^j$$

são *iguais* se para todo inteiro não negativo i tal que $a_i \neq 0$ ou $b_i \neq 0$, temos

$$a_i = b_i;$$

desta forma o polinômio $f(x)$ é igual, por exemplo, ao polinômio

$$\sum_{k=0}^{n} a_k x^k + 0x^{n+1}.$$

Definimos o *Polinômio Nulo* que denotaremos $0(x)$ ou, quando não houver motivo para ambigüidade, simplesmente 0 como sendo qualquer um dos polinômios iguais cujos coeficientes são todos nulos; de maneira equivalente, o polinômio nulo é qualquer polinômio que não possui coeficiente líder. De maneira análoga, o *Polinômio Unidade* ou *Polinômio Um* é o polinômio de grau 0 cujo coeficiente líder é

$$a_0 = 1.$$

Denotaremos $\mathbb{D}[x]$ o conjunto de todos os polinômios com coeficientes em $\mathbb{D}$, isto é

$$\mathbb{D}[x] := \{\sum_{k=0}^{n} a_k x^k : n \geq 0, a_0, \ldots, a_n \in \mathbb{D}\}.$$

Por outro lado, os polinômios de grau 0 são aqueles cujo coeficiente líder acompanha à potência x^0 de x, isto é, aqueles polinômios que não possuem indeterminada. Segundo nossa noção de igualdade acima, podemos considerar estes polinômios como sendo iguais a um único elemento do domínio $\mathbb{D}$; desta maneira, podemos considerar o domínio $\mathbb{D}$ como estando contido no conjunto dos polinômios com coeficientes em $\mathbb{D}$; simbolicamente, podemos então escrever

$$\mathbb{D} \subset \mathbb{D}[x];$$

em particular estamos identificando o zero e a unidade de $\mathbb{D}$ com o polinômio nulo e o polinômio unidade respectivamente.

Aos efeitos do objetivo destas notas, podemos supor que o domínio $\mathbb{D}$ é um dos seguintes:

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C};$$

não obstante, e a título informativo (e porque não, formativo), vamos ver alguns exemplos de polinômios com coeficientes em outros domínios e também com coeficientes em um anel comutativo com unidade (veja definição **??**) que não é um domínio.

Comecemos lembrando os conjuntos de inteiros módulo um inteiro positivo. Formalmente, é o conjunto de classes de equivalência em $\mathbb{Z}$ associado à relação de equivalência *ser congruente a*. Mais precisamente, seja $r \in \mathbb{N}$ um inteiro positivo; dados $m, n \in \mathbb{Z}$, dizemos que m é congruente a n (ou que m e n são congruentes) módulo r, o que denotamos

$$m \equiv n \pmod{r},$$

se $m - n$ é múltiplo de r. Pela teoria da divisibilidade de números inteiros, é claro que dado um inteiro m arbitrário ele pode ser congruente a apenas um dos r inteiros

$$0, 1, \ldots, r - 1.$$

Denotamos por $\bar{i}$ o conjunto de todos os inteiros congruentes a $i \in \{0, 1, \ldots, r - 1\}$; podemos imaginar que aqueles inteiros que são congruentes a um mesmo inteiro i possuem

uma mesma cor, tendo cores diferentes aqueles não congruentes a ele; desta forma existirão r cores diferentes de inteiros, onde cada cor corresponde a uma única *classe*.

Denotamos

$$\mathbb{Z}_r := \{\overline{0}, \overline{1}, \ldots, \overline{r-1}\},$$

o conjunto de classes de congruência módulo r (ou cores diferentes). Usando as propriedades da divisibilidade (como apreendidas nos cursos elementares de aritmética) vê-se sem dificuldade que $\mathbb{Z}_r$ é um anel comutativo com unidade. Além disso, $\mathbb{Z}_r$ é um domínio se e somente se n é um número primo, pois $\bar{a}\bar{b} = \bar{0}$ se e somente se r divide ab: se r for primo, então n divide a ou b; reciprocamente, se r não for primo então ele é produto de dois inteiros positivos $a, b \leq n-1$.

Observação 1.2.2. De fato $\mathbb{Z}_r$ é um corpo se e somente se r é um número primo. Com efeito, é suficiente mostrar que todo elemento diferente de $\bar{0}$ possui inverso se e só se p é um número primo; se $a \in \mathbb{Z}$ não é divisível por p então $\text{MDC}(p, a) = 1$. Portanto existem $m, n \in \mathbb{Z}$ tais que

$$am + pn = 1.$$

Então $am \equiv 1 \ (\mod p)$ o que significa que $\bar{m}$ é inverso de $\bar{a}$ em $\mathbb{Z}_r$. Deixamos como exercício para o leitor a verificar que a recíproca desta afirmação também é verdadeira.

Exemplo 1.2.3. Consideremos $\mathbb{Z}_6$. Temos que $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$ em $\mathbb{Z}_6$. Como $\bar{2} \neq \bar{0}$ e $\bar{3} \neq \bar{0}$ concluímos que $\mathbb{Z}_6$ não é um domínio de integridade.

Vamos agora observar como as operações elementares em $\mathbb{D}$ "induzem" operações elementares em $\mathbb{D}[x]$ compatíveis com a inclusão $\mathbb{D} \subset \mathbb{D}[x]$.

Sejam $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{j=0}^{m} b_j x^j$ polinômios em $\mathbb{D}[x]$. Sem perda da generalidade suporemos $n \geq m$. Podemos então escrever

$$g(x) = \sum_{j=0}^{n} b_j x^j$$

onde $b_{m+1} = b_{m+2} = \cdots = b_n = 0$.

Soma: A soma $f(x) + g(x)$ de $f(x)$ e $g(x)$ é a expressão

$$f(x) + g(x) := \sum_{k=0}^{n} (a_k + b_k) x^k.$$

Como $a_k + b_k = b_k + a_k \in \mathbb{D}$ concluímos por ou lado que $f(x) + g(x) \in \mathbb{D}[x]$ e por outro lado que $f(x) + g(x) = g(x) + f(x)$, isto é, que a soma é comutativa; o leitor podera verificar sem dificuldade que também é associativa.

É fácil verificar que o polinômio nulo $0(x)$ é o neutro da soma (faça-o !).

Denotamos $-f(x) := \sum_{i=0}^{n} (-a_i) x^i$ onde $-a_i$ é o simétrico do elemento a_i. Temos então $f(x) + (-f(x) = 0(x)$ donde concluímos que $-f(x)$ é o simétrico de $f(x)$.

Multiplicação O produto $f(x) \cdot g(x)$ de $f(x)$ e $g(x)$ é a expressão

$$f(x) \cdot g(x) := \sum_{k=0}^{n+m} c_k x^k,$$

onde

$$c_k := \sum_{i+j=k} a_i b_j = (a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0), \ k = 0, \ldots, n+m.$$

Evidentemente $f(x) \cdot g(x) = g(x) \cdot f(x) \in \mathbb{D}[x]$. O leitor pode verificar que este produto ou multiplicação de polinômios é uma operação associativa. Quando não houver lugar para confusão denotaremos $f(x) \cdot g(x) = f(x)g(x)$.

Da definição de produto concluímos que se $f(x)$ e $g(x)$ não são nulos, ou seja $a_n \neq 0$ e $b_m \neq 0$. Como $\mathbb{D}$ é um domínio de integridade $a_n b_m = c_{n+m} \neq 0$ o que implica que $f(x)g(x) \neq 0$ (propriedade (D) de domínio de integridade (**??**)). Então

$$\text{grau}(f(x)g(x)) = \text{grau}\, f(x) + \text{grau}\, g(x) = n + m.$$

Como já vimos no caso de domínios de integridade, a propriedade (D) equivale a dizer que $f(x)g(x) = 0$ implica $f(x) = 0$ ou $g(x) = 0$.

O polinômio unidade $1(x)$ é o neutro da multiplicação (demonstre isto !). Analisemos agora a existência de inverso para a multiplicação. Suponhamos que $f(x)$ não é o polinômio nulo, isto é, $a_n \neq 0$. Suponhamos também que $f(x)g(x) = 1(x)$. Então $f(x)g(x)$ tem grau 0, donde colcluímos que $f(x)$ e $g(x)$ tem graus 0. Portanto $a_0 \neq 0$, $b_0 \neq 0$ e $a_0 = b_0 = 1$ e então os únicos polinômios que possuem inverso são os polinômios constantes, onde as constantes correspondentes são invertíveis em $\mathbb{D}$; dito de outra forma, o conjunto de poinômios invertíveis em $\mathbb{D}[x]$ é o conjunto de elementos invertíveis de $\mathbb{D}$.

O seguinte teorema resume as propriedades estruturais de $\mathbb{D}[x]$ relativas às operações de soma e multiplicação, cuja demonstração deixamos para o leitor.

Teorema 1.2.4. *A tripla $(\mathbb{D}[x], +, \cdot)$ é um domínio de integridade cujos invertíveis são os invertíveis de $\mathbb{D}$.*

1.3 Teoria da Divisibilidade em $\mathbb{D}[x]$

Dado que $\mathbb{D}[x]$ não é um corpo, sabemos que não teremos uma divisão exata em $\mathbb{D}[x]$, da mesma forma que ocorre com $\mathbb{Z}$. Gostariamos então de ter um argorítmo da divisão "não exata" análogo ao que temos no domínio $\mathbb{Z}$ de forma a poder dividir um polinômio por outro obtendo um quociente e um resto. Mais precisamente, consideremos polinômios $f(x), g(x) \in \mathbb{D}[x]$; nos perguntamos se existem polinômios $q(x)$ e $r(x)$, também em $\mathbb{D}[x]$, tais que

(i) $f(x) = g(x)q(x) + r(x)$

onde $r(x)$ é "menor" que $g(x)$ em algum sentido que não é muito claro pois até o momento não temos definido uma relação de ordem no conjunto $\mathbb{D}[x]$ dos polinômios.

De acordo com as propriedades das potências, quando pegarmos $f(x) = x^n$ e $g(x) = x^m$, nosso método devería fornecer um quociente $q(x) = x^{n-m}$ e um resto $r(x) = 0$ (o polinômio nulo); como x^{n-m} é um polinômio só no caso onde $n \geq m$, deveriamos pedir $\text{grau}(f) \geq \text{grau}(g)$.

Como inspiração, lembremos a divisão não exata de números inteiros escritos na base dez. Sejam

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0,$$

com $0 \leq a_n, a_{n-1}, \ldots, a_1, a_0 \leq 9$ inteiros, e $b > 0$ um inteiro $\leq a$. O algorítmo da divisão que apreendemos na escola é mais ou menos assim: calculamos o número de vezes que b "cabe" dentro de $a_n 10^n$ (a_n é o número de unidades quando $n = 0$, de dezenas quando $n = 1$, de centenas quando $n = 2$, etc) digamos q_1, que seria um quociente parcial, e subtraímos bq_1 de a obtendo um resto parcial r_1; se r_1 é zero, a divisão acabou e dizemos

que b divide a. Se $r_1 \neq 0$, nos perguntamos se r_1 é $\geq b$; caso negativo, a divisão acabou e escrevemos $q = q_1$ e $r = r_1$. Caso afirmativo, o procedimento se repete subtraíndo de r_1 o número máximo q_2 de vezes que b cabe em r_1; obtemos

$$a - bq_1 - bq_2 = r_2,$$

com $r_2 < r_1$ e $q_2 < q_1$. E recomeçamos até obter um resto parcial que seja 0 ou menor que b. Como os restos parciais diminuem a cada passo, estamos certos que o procedimento deve para. O último resto parcial e a soma dos quocientes parciais são, respectivamente, o resto e o quociente da divisão.

Exercício 1.3.1. Faça a divisão de $1235 = 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 5$ por 4 do jeito descrito acima.

Voltando aos polinômios, para generalizar o procedimento descrito acima ao caso destes, podemos tratar as potências de x como as potências de 10 para os números; em particular isto nos sugere que o "tamanho", que seria a magnitude a fazer decrescer no processo de divisão do polinômio, será entendido como sendo o grau deste. Além disto, o número de vezes que b cabe em $a_n 10^n$ deve ser substituído pelo número de vezes que o termo de maior grau de $g(x)$ cabe dentro do termo de maior grau de $f(x)$ e assim por diante; em particular, no caso dos polinômios, um quociente parcial, deverá forçosamente ter grau menor ou igual que o grau de $f(x)$ e cada quociente parcial terá grau menor que o anterior.

Guiados pela disgressão precedente, estamos prontos agora para construir um algorítmo da divisão de polinômios de forma coerente com o que já sabemos. Escrevamos

$$f(x) = a_n x^n + \hat{f}(x), g(x) = b_m x^m + \hat{g}(x),$$

onde $n \geq m$ e $\hat{f}(x)$, $\hat{g}(x)$ são polinômios de graus menores que n e m respectivamente. Como $x^{n-m} \in \mathbb{D}[x]$, podemos escrever

$$q_1(x) = \frac{a_n}{b_m} x^{n-m}, \quad r_1(x) = f(x) - g(x)q_1(x) = \hat{f}(x) - \hat{g}(x)q_1(x);$$

se $r_1(x) = 0$ a divisão acabou e temos $q(x) = q_1(x)$. Se $r_1(x) \neq 0$, nos perguntamos se $\operatorname{grau} r_1(x) \geq \operatorname{grau} g(x)$. Se a resposta é negativa, a divisão também acabou e temos $r(x) = r_1(x)$ e $q(x) = q_1(x)$. Caso afirmativo, recomeçamos o procedimento, até obter um resto parcial que, ou é zero, ou possui grau menor que $\operatorname{grau} g(x)$. Como o grau dos restos parciais diminui a cada iteração do procedimento, desde que não tenha se tornado nulo, concluímos que este deve parar após um número finito de iterações; de fato, precisamos não mais do que $\operatorname{grau} f(x)$ aplicações do procedimento.

Por outro lado, observemos que no procedimento empregado, precisamos dividir por b_m a cada passo. Se pretendermos que os resultados obtidos da divisão sejam polinômios com coeficientes no domínio $\mathbb{D}$ onde $f(x)$ e $g(x)$ tem os seus, devemos pedir que b_m seja um invertível em $\mathbb{D}$. Por exemplo, no caso onde $\mathbb{D} = \mathbb{Z}$, as únicas possibilidades são $b_m = 1$ ou $b_m = -1$. No caso onde $\mathbb{D}$ for um corpo, a divisão será possível para todo $b_m \neq 0$.

De fato temos o seguinte teorema:

Teorema 1.3.1. *Sejam* $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ *e* $g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$ *polinômios não nulos em* $\mathbb{D}[x]$. *Então, existem e são únicos polinômios* $q(x)$ *e*

$r(x)$ em $\mathbb{D}[x]$ tais que

$$f(x) = q(x)g(x) + r(x), \qquad com \qquad r(x) = 0 \quad ou \quad \text{grau}(r(x)) < \text{grau}(g(x)).$$

No caso $\mathbb{D} = \mathbb{Z}$ fazemos ainda a hipótese de que o coeficiente líder b_m de $g(x)$ seja invertível, isto é, igual a 1 ou -1.

Demonstração. Existência: A demonstração da existência será feita por indução em n, utilizando a segunda forma do Princípio da Indução. Para $n \in \mathbb{N}$, consideremos a proposição

$P(n)$: Se $f(x)$ e $g(x)$ são polinômios não nulos em $\mathbb{D}[x]$, com $\text{grau}(f(x)) = n$, então existem $q(x), r(x) \in \mathbb{D}[x]$ tais que $f(x) = q(x)g(x) + r(x)$, com $r(x) = 0$ ou $\text{grau}(r(x)) < \text{grau}(g(x))$.

Base de Indução: $P(0)$ é verdadeira.
Se $f(x) = a_0$ tem grau 0, podem ocorrer dois casos. Se $g(x)$ tem grau maior do que 0, tomamos $q(x) = 0$ e $r(x) = f(x)$. Se $g(x) = b_0$ também tiver grau 0, tomamos $q(x) = \dfrac{a_0}{b_0}$ e $r(x) = 0$.

Passagem de Indução: Suponhamos que, para um certo n, $P(k)$ seja verdadeira para todo $k < n$. Precisamos mostrar que isso implica que $P(n)$ é verdadeira.
Para isso, suponhamos que $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ tenha grau n. Como no enunciado, $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$. Precisamos mostrar a existência dos polinômios $q(x)$ e $r(x)$ com as propriedades desejadas. Dividimos em dois casos.

Se $n < m$, tomamos $q(x) = 0$ e $r(x) = f(x)$.

Se $n \geq m$, seja

$$f_1(x) = f(x) - \frac{a_n}{b_m}\, x^{n-m}.$$

Então, $f_1(x)$ é um polinômio de um certo grau $k < n$. Pela hipótese de indução, $P(k)$ é verdadeira e, portanto, existem polinômios $q_1(x)$ e $r_1(x)$ em $\mathbb{D}[x]$ tais que

$$f_1(x) = q_1(x)g(x) + r_1(x), \qquad \text{com} \qquad r_1(x) = 0 \quad \text{ou} \quad \text{grau}(r_1(x)) < \text{grau}(g(x)).$$

Segue que

$$f(x) = \left(\frac{a_n}{b_m}\, x^{n-m} + q_1(x)\right) g(x) + r_1(x).$$

Pondo $q(x) = \dfrac{a_n}{b_m}\, x^{n-m} + q_1(x)$ e $r(x) = r_1(x)$, temos que

$$f(x) = q(x)g(x) + r(x), \qquad \text{com} \qquad r(x) = 0 \quad \text{ou} \quad \text{grau}(r(x)) < \text{grau}(g(x)),$$

provando que $P(n)$ também é verdadeira.

Logo, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$, concluindo a indução.

Unicidade: Suponhamos que $f(x) = q(x)g(x) + r(x) = q'(x)g(x) + r'(x)$, com $r(x) = 0$ ou $\text{grau}(r(x)) < \text{grau}(g(x))$ e também $r'(x) = 0$ ou $\text{grau}(r'(x)) < \text{grau}(g(x))$. Segue daí que

$$(q(x) - q'(x))g(x) = r'(x) - r(x).$$

Se $q(x) \neq q'(x)$, então $q(x) - q'(x) \neq 0$. Logo,

$$\begin{aligned} \text{grau}(r'(x) - r(x)) &= \text{grau}((q(x) - q'(x))g(x)) \\ &= \text{grau}(q(x) - q'(x)) + \text{grau}(g(x)) \\ &\geq \text{grau}(g(x)), \end{aligned}$$

o que é um absurdo pois $r(x)$ e $r'(x)$ são nulos ou têm grau menor do que o grau de $g(x)$. Logo, $q(x) = q'(x)$. Daí segue que $r(x) = r'(x)$, provando a unicidade.

□

Observação 1.3.2. No caso onde $f(x) = 0$, a divisão por qualquer $g(x) \neq 0$ é evidentemente possível obtendo $q(x) = r(x) = 0$. No caso onde $f(x)$ e $g(x)$ forem polinômios em $\mathbb{Z}[x]$, o coeficiente líder de $g(x)$ deve ser 1 ou -1, pois são estes os únicos inverítiveis em $\mathbb{Z}$; em particular, quando $f(x)$ e $g(x)$ forem polinômios constantes em $\mathbb{Z}[x]$, isto é, números inteiros, a divisão entre eles pensados como números inteiros não esta contemplada no teorema precedente, salvo quando $g(x) = \pm 1$.

Definição 1.3.3. *Sejam $f(x), g(x) \in \mathbb{D}[x]$, onde $g(x) \neq 0$. Dizemos que $f(x)$ é divisível por $g(x)$ em $\mathbb{D}[x]$, o que denotamos $g(x)|f(x)$, quando podemos dividir $f(x)$ por $g(x)$ obtendo resto 0.*

Exemplos 1.3.4. (a) Se $\mathbb{D}$ é um domínio e $g(x) = b_0$ é um polinômio constante com b_0 invertível em $\mathbb{D}$ (isto é, existe $a \in \mathbb{D}$ tal que $ab_0 = 1$), então

$$f(x) = b_0 \cdot (\frac{1}{b_0} f(x)).$$

Pela unicidade do teorema, temos

$$q(x) = \frac{1}{b_0} f(x),\ r(x) = 0.$$

(b) Se $g(x)$ é um polinômio mônico, então a divisão como no teorema é sempre possível. É facil ver que neste caso o coeficiente líder do quociente é o mesmo que o coeficiente líder de $f(x)$.

(c) Seja $g(x) = x - a, a \in \mathbb{D}$. Pelo teorema,

$$f(x) = (x - a)q(x) + r(x) \tag{1.1}$$

onde $r(x) = 0$ ou grau$(r) <$ grau$(g) = 1$. Concluímos que $r(x)$ é constante, isto é, zero ou uma constante não nula $r = r(x)$. Substituindo x por a na equação (1.1), obtemos o resto

$$r = f(a).$$

(d) Consideremos $f(x) = 3x^4 - 5x^3 + 2x^2 - x + 6,\ g(x) = x^2 - 3x + 1$; pelo teorema obteremos quociente e resto $q(x), r(x)$ em $\mathbb{Z}[x]$. Usando as notações introduzidas anteriormente, obtemos

$$q_1(x) = 3x^2,\ r_1(x) = 4x^3 - x^2 - x + 6.$$

Como grau$r_1(x) \geq$ grau$g(x)$ repetimos o procedimento, obtendo

$$q_2(x) = 4x,\ r_2(x) = 11x^2 - 5x + 6;$$

repetindo mais uma vez

$$q_3(x) = 11,\ r_3(x) = 28x - 5.$$

Concluímos

$$q(x) = q_1(x) + q_2(x) + q_3(x) = 3x^2 + 4x + 11,\ r(x) = r_3(x) = 28x - 5.$$

O exemplo (c) acima é conhecido como *Teorema do Resto*:

Teorema 1.3.5 (do Resto)**.** *O resto da divisão de $f(x) \in \mathbb{D}[x]$ por $x - a$ é $f(a)$.*

Este teorema, que parece apenas uma simples observação é muito importante. De fato, é a chave para compreender o vínculo entre a teoria algébrica que começamos a desenvolver neste capítulo e o nosso objetivo principal, a saber, o de resolver equaçãoes polinomiais. Para precisar isto, começamos com uma definição, onde estamos considerando a situação em que $\mathbb{D}$ é um domínio qualquer contido dentro do corpo dos números complexos, como por exemplo $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou mesmo o próprio $\mathbb{C}$.

Definição 1.3.6. *Sejam $f(x) \in \mathbb{D}[x]$ e $\alpha \in \mathbb{C}$. Dizemos que α é raiz de $f(x)$ se $f(\alpha) = 0$.*

O teorema do resto nos dá imediatamente o seguite vínculo espetacular que traduz esta noção em termos de divisibilidade, conhecido como Teorema de Ruffini, e cuja demonstração é deixada para o leitor:

Corolário 1.3.7 (Teorema de Ruffini)**.** *Um número complexo $\alpha \in \mathbb{C}$ é raiz de um polinômio $f(x) \in \mathbb{D}[x]$ se e somente se $f(x)$ é divisível por $x - \alpha$.*

A sguir descrevemos o chamado *esquema de Ruffini* (veja figura abaixo) para dividir um polinômio da forma

$$f(x) = \sum_{i=0}^{n} a_i x^i,$$

por $x-a$. Como no algoritmo da divisão começamos dividindo por x, o primeiro quociente parcial é $q_1(x) = a_n x^{n-1}$; multiplicando por $x - a$ e subtraíndo de $f(x)$ obtemos

$$r_1(x) = (a_n a + a_{n-1})x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0.$$

Repetindo o procedimento obteremos então

$$q_2(x) = (a_{n-1} + a a_n)x^{n-2},\ r_2(x) = (a_n a^2 + a_{n-1}a + a_{n-2})x^{n-2} + a_{n-3}x^{n-3} + \cdots + a_0.$$

Não é difícil de se convencer que os coeficientes do quociente e o resto $r(x)$ podem ser obtidos da seguinte forma: escrevemos numa linha horizontal todos os coeficientes de $f(x)$, da direita para a esquerda, começando pelo líder e não esquecendo aqueles que são nulos. Os coeficientes do quociente são, escritos na mesma ordem: o líder é o próprio a_n; para o seguinte multiplicamos o anterior (isto é, o líder neste caso) por a e somamos o resultado com o próximo coeficiente da linha horizontal, ou seja, com a_{n-1}; para obter o terceiro coeficiente de $q(x)$ repetimos o procedimento arterior, ou seja, multiplicamos o coeficiente obtido precedentemente por a e somamos o resultado com o terceito da linha horizontal, isto é, com a_{n-2}; etc...O resto $r(x)$ será o último resultado obtido pelo procedimento anterior, que é precisamente

$$f(a) = a_n a^n + a_{n-1}a^{n-1} + \cdots + a_1 a + a_0;$$

em particular redemonstramos o teorema do Resto 1.3.5.

Figura com esquema de Ruffini

Exemplo 1.3.8. Consideremos o polinômio

$$f(x) = x^4 + bx^2 - cx + 4$$

com $b, c \in \mathbb{R}$. Encontremos b, c para que o polinômio tenha raízes 1 e -1. Aplicando o corolário 1.3.7 temos um sistema de equações

$$b - c = -5; b + c = -5.$$

Concluímos $b = -5$ e $c = 0$.

Exemplo 1.3.9. Consideremos o polinômio

$$f(x) = x^2 + bx + c$$

com $b, c \in \mathbb{R}$. Se quisermos encontrar b, c para que o polinômio tenha raiz dupla igual a 1, o método utilizado no exemplo anterior não funciona pois obteremos a mesma equação duas vezes (verifique isto !). Por outro lado, se o fato de um polinômio possuir raiz 1 equivale a este polinômio ser divisível por $(x-1)$, é razoável pensar que ter raiz dupla 1 equivalha ao fato do polinômio poder ser dividido duas vezes por $(x-1)$ (observe que talvez ainda não tenhamos muito claro o quê significa um polinômio ter raiz dupla); como veremos, a é esta a definição correta da noção de *raiz dupla*. Levando isto em consideração, podemos dividir $f(x)$ por $(x-1)$ e logo dividir o quociente obtido também por $(x-1)$: ambos restos deverão ser nulos. Aplicando o esquema de Ruffini o primeiro resto é $1 + b + c$, o primeiro quociente tem coeficientes 1 e $b + 2$ e e o segundo resto é $b + 2$. Concluímos que $b = -2$ e $c = 1$.

Exercício 1.3.2. Trabalhando como no exemplo precedente obtenha condições para que o polinômio geral de grau 2 possua uma raiz dupla α; compare o resultado obtido com o que já sabe da discussão da equação quadrática.

O teorema de Ruffini (corolário 1.3.7) pode ser generalizado; no momento estamos em condições de generalizar apenas uma das implicações (para a implicação recíproca veja proposição **??**):

Proposição 1.3.10. *Sejam $f(x), g(x) \in \mathbb{D}[x]$. Se $g(x)|f(x)$, então toda raiz de $g(x)$ é raiz de $f(x)$.*

Demonstração. Temos $f(x) = g(x)q(x)$ para certo $q(x) \in \mathbb{D}[x]$. Se $\alpha \in \mathbb{C}$ é uma raiz de $g(x)$, então

$$f(\alpha) = g(\alpha)q(\alpha) = 0,$$

donde segue o resuntado. □

Quando estudamos aritmética em $\mathbb{Z}$ partimos do algorítmo da divisão para logo definirmos o conceito de divisor de um número. Entre os divisores, encontramos alguns muito especiais: por um lado, aqueles "triviais" que são o próprio número ou seu oposto, e ± 1. Por outro lado, encontramos certos números que admitem apenas divisores triviais como estes; quando positivos, chamamos esses números de *números primos*. Depois demonstramos o teorema fundamental da Aritmética que diz que todo número positivo fatora-se como produto de números primos; se o número é negativo, multiplicamos por -1 a fatoração do seu valor absoluto.

Agora que temos em $\mathbb{D}[x]$ um algorítmo de divisão, podemos nos perguntar sobre a fatoração de um polinômio como produto de fatores "primordiais", que não acietam mais fatoração que aquelas trivias; observe que fatores do tipo $x-\alpha$ correspondem a raízes do polinômio em questão. Vamos então definir os conceitos equivalentes, para polinômios, daqueles de número primo e divisor trivial de um número inteiro.

A seguinte definição é bastante intuitiva e omitimos comentários (reflita sobre ela; veja o exemplo (a) acima)

Definição 1.3.11. *Seja $f(x) \in \mathbb{D}[x]$. Os divisores triviais de $f(x)$ são os polinômios constantes $d(x) = d \in \mathbb{D}$ e os polinômios da forma $df(x)$, onde d é invertível em $\mathbb{D}$.*

Depois de termos a noção de divisor trivial, o equivalente ao conceito de número primo decorre imediatamente:

Definição 1.3.12. *Seja $f(x) \in \mathbb{D}[x]$ um polinômio de grau ≥ 1. Dizemos que $f(x)$ é irredutível, se seus únicos divisores em $\mathbb{D}[x]$ são os trivias. Caso contrário dizemos que $f(x)$ é redutível.*

Vejamos alguns exemplos para exclarecer esta noção.

Exemplos 1.3.13. (a) Seja $f(x) = ax + b \in \mathbb{D}[x]$. Suponhamos primeiramente que $\mathbb{D} = \mathbb{Z}$. Seja $d = \text{MDC}(a, b) \in \mathbb{Z}$. Temos

$$f(x) = d(a'x + b'),$$

onde $\text{MDC}(a', b') = 1$. Se $d > 1$, então d é um divisor não trivial em $\mathbb{D}[x]$ pois não é invertível em $\mathbb{D}$. Concluímos que, neste caso, $f(x)$ é redutível.

Se $d = 1$, suponhamos que $f(x)$ possui um divisor $g(x) \in \mathbb{Z}$; então

$$ax + b = g(x)q(x).$$

Por causa do grau de $f(x)$ ser um, concluímos que $g(x)$ ou $q(x)$ devem ser constantes; digamos $g(x) = a_1x + b_1$ e $q(x) = c \in \mathbb{Z}$. Então

$$a = a_1c,\ b = b_1c,$$

donde $c|\text{MDC}(a, b)$. Como $\text{MDC}(a, b) = d = 1$, que é invertível, concluímos que $f(x)$ é irredutível.

Finalmente, no caso onde $\mathbb{D}$ é um corpo, é evidente que $f(x) = ax + b$ será sempre irredutível.

(b) Consideremos o polinômio

$$f(x) = x^2 - 2 \in \mathbb{Z}[x].$$

É claro que temos a fatoração

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}),$$

o que mostra que $f(x)$ é redutível em $\mathbb{R}[x]$ e também em $\mathbb{C}[x]$. Porém ele é irredutível em $\mathbb{Q}[x]$: com efeito, soponhamos que $f(x)$ possui um divisor não trivial em $\mathbb{Q}[x]$. Por causa do grau de $f(x)$ ser 2, a única possibilidade é termos

$$x^2 - 2 = (ax + b)(a_1x + b_1),$$

com $a, b, a_1, b_1 \in \mathbb{Q}$. Um cálculo fácil mostra que

$$aa_1 = 1,\ ab_1 + ba_1 = 0,\ bb_1 = -2.$$

Multiplicando por ab_1 a igualdade do meio, obtemos

$$a^2b_1^2 - 2 = 0,$$

que não possui solução em $\mathbb{Q}$ (observe que $ab_1 \neq 0$). Então a fatoração acima não é possível em $\mathbb{Q}[x]$.

Um cálculo ainda mais simples mostra que o polinômio x^2-2 é irredutível em $\mathbb{Z}[x]$: com efeito, de $aa_1 = 1$ obtemos $a = \pm 1$ e $a_1 = \pm 1$; de $bb_1 = -2$ obtemos $b = \pm 1, b_1 = \pm(-2)$. Estes valores para a, a_1, b, b_1 são incompatíveis com a equação do meio $ab_1 + ba_1 = 0$.

(c) Seja $f(x) = 3x^2 - 6$. É redutível em $\mathbb{Z}[x]$ pois fatora-se como

$$3(x^2 - 2)$$

sendo $3 \in \mathbb{Z}$ um divisor não trivial em $\mathbb{Z}[x]$; trabalhando como no exemplo (b) mostra-se que o polinômio é irredutível em $\mathbb{Q}[x]$ e redutível quando $\mathbb{D} = \mathbb{R}$ ou $\mathbb{D} = \mathbb{C}$.

Quando estudamos aritmética em $\mathbb{Z}$, um inteiro n e seu oposto $-n$ possuem os mesmos divisores; isto deve-se ao fato de podermos passar de um para o outro multiplicando por -1 que é um invertível de $\mathbb{Z}$. Temos um fenômeno análogo em $\mathbb{D}[x]$, é o conteúdo da seguinte definição.

Definição 1.3.14. *Dizemos que dois polinômios $f(x), g(x) \in \mathbb{D}[x]$ são associados em $\mathbb{D}[x]$ (ou sobre $\mathbb{D}$), denotando $f(x) \sim g(x)$, se possuem os mesmos divisores.*

Se $f(x) \sim g(x)$ em $\mathbb{D}[x]$, como $f(x)|g(x)$ e $g(x)|f(x)$, temos

$$f(x) = g(x)q(x),\ g(x) = f(x)q'(x).$$

Então $f(x) = q(x)q'(x)f(x)$, donde segue que, ou $f(x) = g(x) = 0$, ou, caso contrário $q(x)$ e $q(x)$ são invertíveis em $\mathbb{D}[x]$, isto é, são constantes invertíveis em $\mathbb{D}$. Isto demonstra o seguinte resultado:

Proposição 1.3.15. *Dois polinômios $f(x), g(x) \in \mathbb{D}[x]$ são associados em $\mathbb{D}[x]$ se e somente se $f(x) = ag(x)$ com $a \in \mathbb{D}$ invertível; neste caso $g(x) = bf(x)$ com $b \in \mathbb{D}$ tal que $ab = 1$.*

Exemplo 1.3.16. Os polinômios $3x^2-6$ e x^2-2 não são associados em $\mathbb{Z}[x]$, pois o primeiro é múltiplo do segundo via uma constante que não é invertível em $\mathbb{Z}$.

A demonstração do seguinte corolário (da proposição precedente) é deixada como exercício para o leitor.

Corolário 1.3.17. *Se $f(x), g(x) \in \mathbb{D}[x]$ são polinômios associados, então $f(x)$ é irredutível em $\mathbb{D}[x]$ se e somente se $g(x)$ é irredutível em $\mathbb{D}[x]$.*

□

Definição 1.3.18. *Seja $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. O conteúdo de $f(x)$ é o máximo divisor comum dos coeficientes*

$$c(f) := \mathrm{MDC}(a_0, \ldots, a_n).$$

Exemplo 1.3.19. Se $f(x) = 3x^2 - 6$, temos $c(f) = 3$.

A seguinte proposição, cuja demonstração daremos mais adiante (veja a demonstração antes do lema **??**) explica o fenômeno aparentemente não intuitivo que acontece com o polinômio $3x^2 - 6$ que é irrédutível sobre $\mathbb{Q}$ mas não sobre $\mathbb{Z}$ que é um domínio muito menor (e então com menos possibilidade de escolha para os coeficientes).

Proposição 1.3.20. *Seja $g(x) \in \mathbb{Z}[x]$. Suponhamos que $g(x)$ é irredutível em $\mathbb{Q}[x]$. Se $c(g) = 1$, então $g(x)$ é irredutível em $\mathbb{Z}[x]$.*

□

Vamos agora introduzir os conceitos de *máximo divisor comum* e *mínimo múltiplo comum* de dois ou mais polinômios. Comecemos pelo primeiro: é importante observar as diferenças entre os casos onde $\mathbb{D}$ é $\mathbb{Z}$ e $\mathbb{D}$ é um corpo (de fato arbitrário contendo $\mathbb{Z}$, mas nos sempre pensaremos nos casos onde o corpo é um dos dos três corpos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$).

Definição 1.3.21. *Sejam $f(x), g(x) \in \mathbb{D}[x]$ polinômios não ambos nulos. Seja $d(x) \in \mathbb{D}[x]$ um polinômio que, quando $\mathbb{D}$ for um corpo suporemos mônico e quando $\mathbb{D} = \mathbb{Z}$ suporemos de coeficiente líder positivo. Dizemos que $d(x)$ é o máximo divisor comum de $f(x)$ e $g(x)$ se satisfaz as seguintes condições:*
(i) $d(x)|f(x)$ e $d(x)|g(x)$.
(ii) se $c(x)|f(x)$ e $c(x)|g(x)$, então $c(x)|d(x)$. Neste caso denotamos

$$\mathrm{MDC}(f, g) := d(x)$$

Exemplo 1.3.22. Se $f(x) = -3x^2 + 6$ e $g(x) = 12x^2 - 24$ é mais ou menos evidente que $\mathrm{MDC}(f, g) = 3x^2 - 6$ em $\mathbb{Z}[x]$ mas $x^2 - 2$ em $\mathbb{D}[x]$ para $\mathbb{D}$ sendo um corpo pois o máximo divisor comum é mônico por definição neste caso.

Vamos agora introduzir o *Algoritmo de Euclides* para calcular o MDC de dois polinômios. Por simplicidade concentraremos nossa atenção no caso onde $\mathbb{D}$ é um corpo; o leitor interessado, poderá tentar obter o MDC para polinômios em $\mathbb{Z}[x]$ usando o algorítmo no caso de $\mathbb{Q}[x]$ com ligeiras modificações.

Precisamos do seguinte lemma cuja demonstração é deixada para o leitor.

Lema 1.3.23. *Sejam $f(x), g(x) \in \mathbb{D}[x]$. Se $d(x) \in \mathbb{D}[x]$ é um divisor commun de $f(x)$ e $g(x)$, então $d(x)$ divide o polinômio*

$$f(x)h(x) + g(x)k(x)$$

para todos $h(x) \in \mathbb{D}[x]$ e $k(x) \in \mathbb{D}[x]$.

□

Seja $\mathbb{D}$ um corpo que contém os números inteiros (o leitor pode pensar no caso onde $\mathbb{D}$ é um dos três corpos numéricos). Sejam $f(x), g(x) \in \mathbb{D}[x]$ polinômios não nulos com $\mathrm{grau}(f) \geq \mathrm{grau}(g)$. Pelo algorítmo da divisão, existem únicos $q(x)$ e $r(x)$, polinômios em $\mathbb{D}[x]$, tais que

(i) $f(x) = g(x)q(x) + r(x)$ e (ii) $r(x) = 0$ ou $\mathrm{grau}(r) < \mathrm{grau}(g)$.

Por outro lado, do lema precedente segue facilmente que todo divisore comum de $f(x)$ e $g(x)$ é divisor comum de $g(x)$ e $r(x)$: com efeito, se $d(x)|f(x)$ e $d(x)|g(x)$, então o lema aplicado com $h(x) = 1$ e $k(x) = -q(x)$ mostra que $d(x)|r(x)$, pois

$$r(x) = f(x) + g(x)\left(-q(x)\right).$$

Reciprocamente, se $d(x)|g(x)$ e $d(x)|r(x)$, aplicamos o lema aos polinômios $g(x)$ e $r(x)$ multiplicando o primeiro por $h(x) = q(x)$ e o segundo por $k(x) = 1$ para concluir que $d(x)|f(x)$.

Do raciocínio acima concluímos mais ou menos diretamente o seguinte resultado, que é a clave para construir o algorítmo de Euclides.

Lema 1.3.24. *Temos*

$$\text{MDC}(f, g) = \text{MDC}(g, r)$$

Algorítmo Dados de entrada: $f(x)$ e $g(x)$ com $g(x) \neq 0$ e grau$(f) \geq$ grau(g).
1. Primeiro passo: Dividimos $f(x)$ por $g(x)$, obtendo

$$f(x) = g(x)q(x) + r(x)$$

Usando o corolário, temos duas situações:
(1) $r(x) = 0$; neste caso, o MDC procurado é o $g(x)$ multiplicado pelo inverso de seu coeficiente líder (para "tornar" mônico o polinômio, de acordo com a definição de MDC).
(2) $r(x) \neq 0$; neste caso grau$(r) <$ grau(g). Então repetimos o feito no primeiro passo:
2. Segundo passo: Dividimos $g(x)$ por $r(x)$, obtendo

$$g(x) = r(x)q_1(x) + r_1(x).$$

Novamente temos duas situações:
(1) $r_1(x) = 0$; neste caso o MDC procurado é $r(x)$ multiplicado pelo inverso de seu coeficiente líder.
(2) $r_1(x) \neq 0$; neste caso grau$(r_1) <$ grau(r). Pelo corolário teremos

$$\text{MDC}(f, g) = \text{MDC}(g, r) = \text{MDC}(r, r_1)$$

Então recomeçamos, dividindo agora $r(x)$ por $r_1(x)$, e assim em diante.

Os restos $r(x), r_1(x), r_2(x)$, etc, serão chamados de *restos parciais*.

É claro que o procedimento acima pára em algum momento: isto é, não pode acontecer que toda vez que dividimos, a primeira situação não aconteça (ou seja, o resto da divisão correspondente não seja zero), pois a cada repetição do procedimento o resto obtido, quando não nulo, tem grau menor que o anterior. De fato, teremos no máximo, grau(g) passos a realizar. Concluímos desta forma, que o MDC(f, g) é o último resto parcial diferente de zero, multiplicado pelo inverso de seu coeficiente líder.

Teorema 1.3.25. *Sejam $f(x), g(x) \in \mathbb{D}[x]$ com $\mathbb{D}$ um corpo. Então existe um único máximo comum divisor de $f(x)$ e $g(x)$.*

Demonstração. A existência foi provada usando o algorítmo de Euclides. A demonstração da unicidade é deixada para o leitor. □

Numa primeira instância o MDC de dois polinômios depende do domínio $\mathbb{D}[x]$ onde estamos trabalhando; não obstante, no caso onde $\mathbb{D}$ for um corpo, segue do algorítmo de Euclides que MDC(f, g) independe de $\mathbb{D}$, isto é, o polinômio achado pelo algorítmo é o mesmo independentemente do fato de trabalharmos com $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, quando isto fizer sentido (ou seja, quando os polinômios $f(x)$ e $g(x)$ puderem ser considerados com coeficientes em um ou outro corpo): é o conteúdo do seguinte corolário.

Corolário 1.3.26. *Suponhamos que $\mathbb{D}$ é um corpo. Então* $\mathrm{MDC}(f,g)$ *independe de* $\mathbb{D}$.

Demonstração. Basta observa que os dois lemas utilizados para demonstrar o algorítmo de Euclides independem de $\mathbb{D}$. □

Exemplo 1.3.27. Sejam

$$f(x) = x^8+5x^7-3x^6-42x^5-25x^4+92x^3-+78x^2-35x-15, g(x) = x^5+5x^4-27x^2-25x+10.$$

Dividindo $f(x)$ por $g(x)$ obtemos

$$q(x) = x^3 - 3x,\ r(x) = x^3 + 3x^2 - 5x - 15;$$

dividindo $g(x)$ por $r(x)$ obtemos

$$q_1(x) = x^2 + 2x - 1,\ r_1(x) = x^2 - 5.$$

Finalmente, ao dividir $r(x)$ por $r_1(x)$ obtemos

$$q_2(x) = x + 3,\ r_2(x) = 0.$$

Concluímos

$$\mathrm{MDC}(f,g) = x^2 - 5.$$

Em particular temos que $\mathrm{MDC}(f,g) = g(x) + r(x)(-q_1)$; utilizando que $f(x) = g(x)q(x) + r(x)$ podemos eliminar $r(x)$ para obter

$$\mathrm{MDC}(f,g) = g(x) + (f(x) + g(x)(-q(x))(-q_1(x)),$$

donde

$$\mathrm{MDC}(f,g) = (-q_1(x))f(x) + (1 + q(x)q_1(x))$$

o que mostra que $\mathrm{MDC}(f,g)$ é uma *combinação linear* de $f(x)$ e $g(x)$ com coeficientes em $\mathbb{D}[x]$; neste caso podemos supor $\mathbb{D} = \mathbb{Q}$.

O raciocínio feito no exemplo precedente pode ser generalizado, obtendo o seguinte resultado (a demonstração pode ser omitida numa primeira leitura):

Teorema 1.3.28. *Sejam $f(x), g(x) \in \mathbb{D}[x]$. Existem polinômios $h(x), k(x) \in \mathbb{D}[x]$ tais que*

$$\mathrm{MDC}(f,g) = f(x)h(x) + g(x)k(x).$$

Demonstração. ..... □

Corolário 1.3.29. *Sejam $f(x), g(x) \in \mathbb{D}[x]$ e $\alpha \in \mathbb{C}$. Então α é uma raiz comum de $f(x)$ e $g(x)$ se e só se α é uma raiz de* $\mathrm{MDC}(f,g)$.

Demonstração. Se α é raiz de $f(x)$ e de $g(x)$, pelo teorema α também é raiz de $\mathrm{MDC}(f,g)$. Reciprocamente, seja α uma raiz de $d(x) = \mathrm{MDC}(f,g)$; como $d(x)$ é um divisor comum de $f(x)$ e $g(x)$ temos

$$f(x) = d(x)q_1(x),\ g(x) = d(x)q_2(x)$$

para certos $q_1(x), q_2(x) \in \mathbb{D}[x]$. Então

$$f(\alpha) = d(\alpha)q_1(\alpha) = 0,\ g(\alpha) = d(\alpha)q_2(\alpha) = 0,$$

donde segue a afirmação. □

O corolário precedente mostra o vínculo existente entre o MDC é a resolução de sistemas de equações, como mostra o exemplo seguinte.

Exemplo 1.3.30. Vamos resolver o sistema de equaçãoes:

$$\begin{cases} x^4 + x^3 + 3x - 2 = 0 \\ x^3 - 3x + 2 = 0. \end{cases}$$

Se $f(x) = x^4 + x^3 + 3x - 2$ e $g(x) = x^3 - 3x + 2$, queremos encontrar as raízes comuns de $f(x)$ e $g(X)$; denotemos $d(x) = \text{MDC}(f, g)$. Pelo corolário, isto corresponde a encontrar as raízes de $d(x)$.

Utilizando o algorítmo de Euclides, obtemos

$$d(x) = x + 2,$$

donde concluímos que $x = -2$ é a única solução do sistema de equações.

Definição 1.3.31. *Dois polinômios $f(x), g(x) \in \mathbb{D}[x]$ são primos entre si se* $\text{MDC}(f, g) = 1$.

Proposição 1.3.32. *Suponhamos que existem $k(x), h(x) \in \mathbb{D}[x]$ tais que*

$$1 = k(x)f(x) + h(x)g(x).$$

Então $\text{MDC}(f, g) = 1$.

Demonstração. Se $d(x)$ é um divisor comum de $f(x)$ e de $g(x)$, então $d(x)$ divide 1 pelo lema 1.3.23. Então $\text{MDC}(f, g) = 1$ □

Corolário 1.3.33. *Sejam $f(x), g(x) \in \mathbb{D}[x]$. Se $d(x) = \text{MDC}(f, g)$, então*

$$f(x) = d(x)f_1(x),\ g(x) = d(x)g_1(x),$$

onde $f_1(x)$ e $g_1(x)$ polinômios em $\mathbb{D}[x]$ primos entre si.

Demonstração. Pelo teorema 1.3.28

$$d(x) = k(x)f(x) + h(x)g(x),$$

donde segue facilmente

$$1 = k(x)f_1(x) + h(x)g_1(x).$$

O corolário é então consequência da proposição precedente. □

Teorema 1.3.34 (Teorema de Euclides)**.** *Sejam $f(x), g(x), g_1(x) \in \mathbb{D}[x]$. Se $f(x)|g(x)g_1(x)$ e $\text{MDC}(f, g) = 1$, então $f(x)|g_1(x)$.*

Demonstração. Pelo teorema 1.3.28 existem $h(x), k(x) \in \mathbb{D}[x]$ tais que

$$1 = f(x)h(x) + g(x)k(x). \tag{1.2}$$

Por outro lado $g(x)g_1(x) = f(x)q(x)$ para certo $q(x) \in \mathbb{D}[x]$.

Multiplicando a igualdade da equação (1.2) por $g_1(x)$ obtemos então

$$\begin{aligned} g_1(x) &= f(x)g_1(x)h(x) + g(x)g_1(x)k(x) \\ &= f(x)g_1(x)h(x) + f(x)q(x)k(x) \\ &= f(x)\left(g_1(x)h(x) + q(x)k(x)\right) \end{aligned}$$

demonstrando que $f(x)$ divide $g_1(x)$. □

O seguinte corolário do teorema de Euclides é deixado como exercício para o leitor.

Corolário 1.3.35. *Sejam $f(x), g(x), h(x) \in \mathbb{D}[x]$. Se $f(x)$ é irredutível e $f(x)|g(x)h(x)$, então $f(x)|g(x)$ ou $f(x)|h(x)$.*

Exercício 1.3.3. Sejam $f(x), f_1(x), \ldots, f_\ell(x) \in \mathbb{D}[x]$. Suponha que $f(x)|f_1(x)\cdots f_\ell(x)$. Demonstra por indução matemática no número ℓ de fatores que se $f(x)$ é irredutível, então existe $j,\ 1 \leq j \leq \ell$ tal que $f(x)|f_j(x)$.

A continuação introduzimos o conceito de *Mínimo Múltiplo Comum.*

Definição 1.3.36. *Seja $f(x) \in \mathbb{D}[x]$. Um múltiplo de $f(x)$ em $\mathbb{D}[x]$ é um polinômio da forma $f(x)q(x)$, onde $q(x) \in \mathbb{D}[x]$.*

Um polinômio $m(x)$ é múltiplo de $f(x)$ em $\mathbb{D}[x]$ se e somente se $f(x)|m(x)$ (demonstre isto !).

Definição 1.3.37. *Sejam $f(x), g(x) \in \mathbb{D}[x]$. Sejam a, b os coeficientes líder de $f(x)$ e $g(x)$ quando $\mathbb{D}$ for um corpo e seus conteúdos quando $\mathbb{D}$ for $\mathbb{Z}$, respectivamente. O Mínimo comum múltiplo de $f(x)$ e $g(x)$ é o polinômio em $\mathbb{D}[x]$, que denotaremos* $\mathrm{MMC}(f, g)$ *quociente de dividir $f(x)g(x)$ por $ab\mathrm{MDC}(f, g)$.*

Com esta definição fica claro que $\mathrm{MMC}(f, g)$ está univocamente definido, porém não é claro que seja um múltiplo comum de $f(x)$ e $g(x)$ nem que seja o menor possível.

Teorema 1.3.38. *Sejam $f(x), g(x), m(x) \in \mathbb{D}[x]$. Então $m(x)$ é o mínimo múltiplo comum de $f(x)$ e $g(x)$ se e somente se satisfaz as seguintes condições:*
(i) $f(x)|m(x)$, $g(x)|m(x)$.
(ii) Se $h(x)|f(x)$ e $h(x)|g(x)$, então $m(x)|h(x)$.
(iii) $m(x)$ é mônico quando $\mathbb{D}$ for um corpo e um inteiro positivo quando $\mathbb{D}$ for $\mathbb{Z}$.

Demonstração. Faremos a prova no caso onde $\mathbb{D}$ é um corpo; o caso onde $\mathbb{D} = \mathbb{Z}$ é deixado para o leitor interessado e pode ser demonstrado adaptando a demonstração que faremos.

Denotemos $d(x) = \mathrm{MDC}(f, g)$. Temos $f(x) = d(x)f_1(x)$ e $g(x) = d(x)g_1(x)$ com $\mathrm{MDC}(f_1, g_1) = 1$.

Suponhamos que $m(x) = \mathrm{MMC}(f, g)$ e demonstremos que $m(x)$ satisfaz as condições (i), (ii) e (iii). Observemos que a condição (i) segue diretamente da definição; a condição (ii) é conseqüência do fato que $d(x)$ é mônico.

Como $f(x)$ e $g(x)$ dividem $h(x)$, temos

$$h(x) = d(x)f_1(x)q(x) = d(x)g_1(x)q'(x)$$

para certos $q(x), q'(x) \in \mathbb{D}[x]$; em particular $g_1(x)|d(x)f_1(x)q(x)$. Pelo teorema de Euclides, $g_1(x)|d(x)q(x)$.

Finalmente, dado que $m(x) = abd(x)f_1(x)g_1(x)$ concluímos que $m(x)|h(x)$, o que demonstra (ii).

Reciprocamente, suponhamos que $m(x)$ satisfaz (i), (ii) e (iii). Temos

$$f(x)g(x) = abd^2(x)f_1(x)g_1(x).$$

A primeira parte da demonstração nos diz que o polinômio $abd(x)f_1(x)g_1(x)$ satisfaz (i), (ii) e (iii). Basta então mostrar que dois polinômios que satisfazem estas trêss condições são iguais.

Seja $m'(x)$ um polinômio satisfazendo (i), (ii), e (iii). Temos $m'(x)|m(x)$ e $m(x)|m'(x)$. Então

$$m(x) = cm'(x), \quad m'(x)c'm(x),$$

com $c, c' \in \mathbb{D}$. Como ambos polinômios são mônicos eles devem coincidir. □

Exemplo 1.3.39. Sejam $f(x) = x^8+5x^7-3x^6-42x^5-25x^4+92x^3-+78x^2-35x-15, g(x) = x^5 + 5x^4 - 27x^2 - 25x + 10$. Como vimos no exemplo 1.3.27 temos

$$\text{MDC}(f, g) = x^2 - 5.$$

Basta dividir $f(x)g(x)$ por $x^2 - 5$ para obter $\text{MMC}(f, g)$ (faça-o !).

Terminamos este parágrafo generalizando o conceito de máximo comum divisor e mínimo múltiplo comum para o caso de um número finito de polynômios (o que pode ser omitido numa primeira leitura). Porém, não demonstraremos só enunciaremos, sem demonstração, as principais propriedades destes.

Definição 1.3.40. *Sejam $f_1(x), \ldots, f_\ell(x) \in \mathbb{D}[x]$. O* Máximo divisor comum *dos polinômios $f_1(x), \ldots, f_\ell(x)$ é um polinômio $d(x) \in \mathbb{D}[x]$ tal que:*

(i) $d(x)|f_i(x)$ para $i = 1, \ldots, \ell$.

(ii) Se $c(x)|f_i(x)$ para $i = 1, \ldots, \ell$, então $c(x)|d(x)$.

(iii) $d(X)$ é mônico se $\mathbb{D}$ for um corpo e com coeficiente líder positivo se $\mathbb{D} = \mathbb{Z}$.

Denota-se $d(x) = \text{MDC}(f_1, \ldots, f_\ell)$.

De maneira análoga ao que acontece no caso $\ell = 2$ pode-se demonstrar que dois polinômios satisfazendo (i), (ii) e (iii) são necessariamente inguais, o que prova que a definição está bem posta, isto é, que não pode haver dois polinômios diferentes virificando a definição acima.

Por exemplo se $\ell = 3$, não é difícil demonstrar que $\text{MDC}(\text{MDC}(f_1, f_2), f_3)$ e $\text{MDC}(f_1, \text{MDC}(f_2, f_3))$ satisfazem as condições (i), (ii) e (iii), donde que eles concidem (ambos) com o MDC dos três polinômios. O leitor pode imaginar como é que devemos proceder para obter o MDC de mais do que três polinômios...

Analogamente, o MMC de ℓ polinômios $f_1(x), \ldots, f_\ell(x) \in \mathbb{D}[x]$, que denota-se $\text{MMC}(f_1, \ldots, f_\ell)$, pode ser definido como satisfazendo

$$f_1(x) \cdots f_\ell(x) = a_1 \cdots a_\ell \text{MDC}(f_1, \ldots, f_\ell),$$

onde $a_1, \ldots, a_\ell \in \mathbb{D}$ os coeficientes líder dos respectivos polinômios.

1.4 Irredutibilidade e Fatoração Canônica

Agora vamos estudar o problema da fatoração de polinômios, com coeficientes num corpo, como produto de polinômios irredutíveis.

Comecemos analizando alguns casos particulares. Seja $f(x) \in \mathbb{D}[x]$ de grau $n \geq 1$.

1 Se $n = 1$, como sabemos pelo exemplo 1.3.13a), o polinômio é irredutível e nada temos a fatorar.

2 Se $n = 2$, temos duas possibilidades mutuamente excluentes:

(i) $f(x)$ é irredutível em $\mathbb{D}[x]$, e nada temos para fatorar, como acontece por exemplo com o polinômio $x^2 - 2$ em $\mathbb{Q}[x]$ (ref. 1.3.13b)) ou $x^2 + 1$ em $\mathbb{R}[x]$.

(ii) $f(x)$ é redutível, como acontece com $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ em $\mathbb{R}[x]$ ou $x^2 + 1 = (x - \imath)(x + \imath)$ em $\mathbb{C}[x]$. Neste caso podemos escrever

$$f(x) = f_1(x)f_2(x),$$

onde $f_1(x)$ e $f_2(x)$ são divisores não triviais de $f(x)$; isto é, são polinômios de grau 1. Concluímos, pelo visto no item (i) que $f_1(x)$ e $f_2(x)$ são irredutíveis, e então a fatoração acima é a fatoração procurada.

3 Se $n = 3$ temos novamente duas possibilidades mutuamente excluentes:

(i) $f(x)$ é irredutível (conhece algum exemplo ?).

(ii) $f(x)$ é redutível, então

$$f(x) = f_1(x)g(x),$$

com $f_1(x)$ de grau 1 e $g(x)$ de grau 2. Se $g(x)$ for irredutível, esta é a fatoração procurada. Senão, aplicamos o feito no caso de polinômios de grau 2 acima e obtemos uma fatoração para $g(x)$ como $g(x) = f_2(x)f_3(x)$ com $f_2(x)$ e $f_3(x)$ de grau 1; neste caso

$$f(x) = f_1(x)f_2(x)f_3(x)$$

é uma fatoração de $f(x)$ como produto de polinômios irredutíveis.

Este raciocínio pode ser continuado agora para grau 4, utilizando o já feito para grau 3, e asim por diante. Este procedimento é um caso particular do que chama-se um procedimento "indutivo", onde a "indução" acontece no grau dos polinômios envolvidos. O caso geral, demonstra-se por indução matemática, no grau n do polinômio $f(x)$. Mais precisamente, temos:

Teorema 1.4.1 (Teorema de fatoração)**.** *Seja $f(x) \in \mathbb{D}[x]$ um polinômio de grau $n \geq 1$. Então*

i) Existem polinômios irredutíveis $f_1(x), \ldots, f_\ell(x) \in \mathbb{D}[x]$ tais que

$$f(x) = f_1(x) \cdots f_\ell(x).$$

ii) Se temos outra fatoração

$$f(x) = g_1(x) \cdots g_m(x)$$

onde $g_1(x), \ldots, g_m(x)$ são irredutíveis, então $m = \ell$ e cada $g_i(x)$ é associado a algum $f_j(x)$.

Demonstração. Existência. Vamos mostrar a parte (i) por indução matemática no grau n.

Se $n = 1$, o resultado é claro, pois todo polinômio de grau um com coeficientes num corpo é irredutível.

Suponhamos como hipótese de indução que o resultado é verdadeiro para todo polinômio de grau menor que k. Vamos então demonstrar que o resultado também é verdadeiro para todo polinômio de grau k.

Seja $f(x)$ um polinômio de grau k. Se $f(x)$ é irredutível, nada temos a demonstrar. Se $f(x)$ é redutível, então

$$f(x) = g(x)h(x)$$

com $g(x)$ e $h(x)$ divisores não triviais de $f(x)$; em particular o grau de $g(x)$ e de $h(x)$ não pode ser nem 0 nem k.

Por hipótese de indução existem fatorações para $g(x)$ e $h(x)$ como produto de polinômios irredutívis

$$g(x) = f_1(x) \cdots f_r(x), \quad h(x) = f_{r+1} \cdots f_\ell(x).$$

Concluímos

$$f(x) = f_1(x) \cdots f_\ell(x),$$

como queriamos demonstrar.

Unicidade. Agora mostraremos a parte (ii). Suponhamos que

$$f(x) = g_1(x) \cdots g_m(x),$$

com $g_1(x), \ldots, g_m(x)$ irredutíveis em $\mathbb{D}[x]$. Fixemos $i \in \{1, \ldots, m\}$ e denotemos $g(x) = g_i(x)$. Temos

$$g(x) | f_1(x) \cdots f_\ell(x).$$

Como $g(x)$ é irredutível, pelo exercício 1.3.3 existe j tal que $g(x)$ divide $f_j(x)$; como $g_i(x) = g(x)$ e $f_j(x)$ são ambos irredutíveis, eles são associados. Em particular $m \leq \ell$.

Refazendo o argumento com $f_i(x)$ no lugar de $g_i(x)$ também obtemos que cada $f_i(x)$ divide algum $g_j(x)$ e então $\ell \leq m$, o que completa a demonstração. □

Observação 1.4.2. a) Os polinômios irredutíveis em (i) podem aparecer muitas vezes, como mostra o seguinte exemplo:

$$(3x^2 - 6)^2(x^2 + 1)^3(4x - 1)$$

que é uma fatoração em $\mathbb{Q}[x]$.

b) A parte (ii) do teorema significa que dadas duas fatorações, o número de fatores irredutíveis deve ser o mesmo em ambas, e, além disso, os polinômios que aparecem nestas ou são, a menos da ordem de aparição, os mesmos, ou diferem pela multiplicação de uma constante. Por exemplo, a fatoração dada acima, pode ser modificada como

$$\frac{1}{9}(4x^2 - 8)(3x^2 - 6)(3x^2 + 3)^3(x - \frac{1}{4}).$$

Observe que pondo em evidência os coeficientes líderes de cada fator irredutível da fatoração e multiplicando-os entre si, devemos obter o coeficiente líder de $f(x)$. Isto, junto com a observação acima mostra o seguinte corolário:

Corolário 1.4.3. *Seja $f(x) \in \mathbb{D}[x]$ um polinômio de grau $n \geq 1$ com coeficiente líder a_n. Então Existem polinômios irredutíveis e mônicos $f_1(x), \ldots, f_k(x) \in \mathbb{D}[x]$ tais que*

$$f(x) = a_n f_1^{n_1}(x) \cdots f_k^{n_k}(x).$$

Vamos chamar a fatoração de $f(x)$ enunciada no corolário 1.4.3 da *fatoração canônica* de $f(x)$ em $\mathbb{D}[x]$.

A continuação vamos analizar, separadamente, o que acontece quando $\mathbb{D}$ é $\mathbb{C}, \mathbb{R}$ ou $\mathbb{Q}$. Começamos enunciando o famoso e mais imporante teorema na teoria de polinômios com coeficientes complexos: o *Teorema Fundamental da Álgebra* cujo enunciado é adjudicado ao matemático francés A. Girard e cuja demonstração foi obtida por Gauss em 1799 na sua tese de doutorado. Existem hoje em dia muitas demonstrações deste teorema, algumas delas relativamente elementares, mas todas envolvendo conceitos qeu escapam do escopo deste livro, motivo pelo qual será omitida.

Teorema 1.4.4 (Teorema Fundamental da Álgebra)**.** *Seja $f(x) \in \mathbb{C}[x]$ de grau maior ou igual que 1. Existe $\alpha \in \mathbb{C}$ tal que $f(\alpha) = 0$.*

Como sabemos, todo polinômio de grau 1, em particular aqueles com coeficientes complexos, é irredutível. Se $f(x) \in \mathbb{C}[x]$ é de grau maior que um, pelo teorema fundamental, existe uma raíz $\alpha \in \mathbb{C}$; pelo corolário 1.3.7 temos então

$$f(x) = (x - \alpha)q(x)$$

para certo $q(x) \in \mathbb{C}[x]$, com grau$(q) > 0$. Concluímos que $f(x)$ é redutível. Ou seja:

Corolário 1.4.5. *Os unicos polinômios irredutíveis em $\mathbb{C}[x]$ são os polinômios de grau um.*

Como conseqüência se $f(x)$ é um polinômio de grau $n \geq 1$ com coeficiente líder a_n, o corolário 1.4.3, no caso onde $\mathbb{D} = \mathbb{C}$, fica na forma seguinte

$$f(x) = a_n(x - \alpha_1)^{n_1} \cdots (x - \alpha_k)^{n_k}, \tag{1.3}$$

onde $n = n_1 + \cdots + n_k$ e $\alpha_1, \ldots, \alpha_k$ são as raízes distintas de $f(x)$.

Diremos que esta é a *fatoração canônica complexa* de $f(x)$. O expoente n_i é a *multiplicidade* da raíz α_i, $i = 1, \ldots, k$. Dizemos também que α_i é uma *raiz simple* quando $n_i = 1$ e *múltipla* quando $n_i > 1$, sendo este n_i a *ordem* ou *multiplicidade*. Se $n_i = 2, 3$,etc. tabém diremos que a raiz é *dupla, tripla* etc. No fim do parágrafo analisaremos mais detalhadamente a relação entre a multiplicidade de uma raiz e a divisibilidade (ref. corolário do teorema do resto 1.3.7).

Um corolário importante da fatoração de $f(x)$ como produto de fatores irredutíveis mônicos de grau um é a relação entre coeficientes e raízes de um polinômio, problema este que já tratamos no (ver §2 do capítulo 1) de maneira menos sistemática do que o faremos agora; em particular o leitor poderá verificar as relações obtidas surgiam como consequência de considerar expressões que estavam fatoradas como produto de binômios de grau 1. Para isso comecemos observando que

$$\prod_{i=1}^{\ell}(x - \gamma_i) = x^n - \left(\sum_j \gamma_j\right) + \left(\sum_{i<j} \gamma_i\gamma_j\right) + \cdots + (-1)^n\gamma_1 \cdots \gamma_n.$$

Esta expressão é então um polinômio mônico de grau n com coeficientes, fora o líder que é um, certas funções cujas variáveis são precisamente as raízes $\gamma_1, \ldots, \gamma_n$.

Mais explicitamente, definimos as *funções simétricas* $s_1, \ldots, s_\ell$ de $\gamma_1, \ldots, \gamma_n$, como sendo

$$s_j(\gamma_1, \ldots, \gamma_n) = \sum_{i_1 < \ldots, i_j} \gamma_{i_1} \cdot \gamma_{i_2} \cdots \gamma_{i_j}, \quad j = 1, \ldots, n.$$

Por simplicidade, e quando não houver perigo de confusão, denotaremos

$$s_j = s_j(\gamma_1, \ldots, \gamma_n), j = 1, \ldots, n;$$

s_j é a *j-ésima função simétrica* de $\gamma_1, \ldots, \gamma_n$.

A demonstração do seguinte corolário deveria ser um exercício relativamente fácil para o leitor

Corolário 1.4.6. *Seja $g(x) \in \mathbb{C}[x]$ um polinômio mônico de grau n; denotemos $\gamma_1, \ldots, \gamma_n$ as raízes (eventualmente repetidas) de $g(x)$. Então*

$$g(x) = \sum_{j=1}^{n} (-1)^n s_j x^j,$$

onde $s_0 = 1$ e, para $j \geq 1$, s_j é a j-ésima função simétrica de $\gamma_1, \ldots, \gamma_n$.

Para analisar a fatoração de polinômios com coeficientes reais, precisamos de um resultado preliminar que é interessante em si mesmo.

Lema 1.4.7. *Sejam $f(x) \in \mathbb{R}[x]$ e $\alpha \in \mathbb{C}$ um número complexo imaginário. Então $f(\alpha) = 0$ se e só se $f(\overline{\alpha}) = 0$.*

Demonstração. Escrevemos

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad a_i \in \mathbb{R}, 0 \leq i \leq n.$$

Por hipótese

$$f(\alpha) = 0 = \sum_{i=0}^{n} a_i \alpha^i.$$

Comecemos observando que, por um lado $\overline{\alpha^i} = \overline{\alpha}^i$; por outro lado $\overline{a_i} = a_i$ para todo $i = 0, \ldots, n$, pois $a_i \in \mathbb{R}$.

Tendo em conta que o conjugado de uma soma de números é a soma dos conjugados destes números, concluímos

$$\begin{aligned} 0 &= \overline{f(\alpha)} \\ &= \overline{\sum_{i=0}^{n} a_i \alpha^i} \\ &= \sum_{i=0}^{n} a_i \overline{\alpha}^i \\ &= f(\overline{\alpha}) \end{aligned}$$

o que termina a demonstração. □

Exemplo 1.4.8. No lema precedente é essencial que os coeficientes do polinômio sejam reais. Por exemplo se

$$f(x) = x^2 - \imath,$$

as duas raízes de $f(x)$ são as raízes quadradas da unidade imaginária $\imath$, isto é

$$\frac{\sqrt{2}}{2} + \imath\frac{\sqrt{2}}{2} \quad \text{e} \quad -\frac{\sqrt{2}}{2} - \imath\frac{\sqrt{2}}{2}.$$

O seguinte é um exercício fácil que deixamos para o leitor.

Exercício 1.4.1. Seja $f(x) \in \mathbb{R}[x]$ um polinômio de grau 2. Mostre que $f(x)$ é irredutível sobre $\mathbb{R}$ se e somente se ele possui uma raiz imaginária.

Seja $f(x) \in \mathbb{R}[x]$ um polinômio com coeficientes reais de grau $n \geq 1$. Suponhamos que suas raízes em $\mathbb{C}$ sejam

$$\alpha_1, \ldots, \alpha_r, \overline{\alpha_1}, \ldots, \overline{\alpha_r}, \beta_1, \ldots, \beta_s,$$

onde α_j é imaginária para todo j e β_k é real para todo k. A fatoração de $f(x)$ em $\mathbb{C}[x]$ pode ser escrita na forma

$$f(x) = a_n(x-\alpha_1)^{n_1}(x-\overline{\alpha_1})^{m_1}\cdots(x-\alpha_r)^{n_k}(x-\overline{\alpha_r})^{n_k}(x-\beta_1)^{m_1}\cdots(x-\beta_s)^{m_s}.$$

Por outro lado, um cálculo direto mostra que se α é imaginário, então o polinômio

$$(x-\alpha)(x-\overline{\alpha}) = x^2 - 2\Re(\alpha)x + |\alpha|^2,$$

que é evidentemente um polinômio com coeficientes reais, é irredutível (vide exercício 1.4.1); se $\alpha = a + \imath b$, o polinômio acima também escreve-se como

$$(x-a)^2 + b^2,$$

o que evidencia a existência de soluções imaginárias. Aplicando este cálculo à fatoração de $f(x)$ concluímos

$$f(x) = a_n\left((x-a_1)^2 + b_1^2\right)^{n_1}\cdots\left((x-a_r)^2 + b_r^2\right)^{n_r}(x-\beta_1)^{m_1}\cdots(x-\beta_s)^{m_s}. \tag{1.4}$$

Diremos que esta é a *fatoração canônica real* de $f(x)$

Como vimos no exemplo 1.3.4, todos os fatores de grau 2 e 1 nesta fatoração são irredutíveis em $\mathbb{R}[x]$. Em particular, podemos enunciar o seguinte corolário:

Corolário 1.4.9. *Um polinômio com coeficientes reais é irredutível se e somente se for de grau 1 ou de grau 2 com raízes imaginárias.*

Exemplo 1.4.10. O polinômio

$$(x^2+1)(x^2+2)$$

possui todas suas raízes imaginárias, mas é redutível.

Exemplo 1.4.11. Consideremos o polinômio

$$f(x) = x^4 + x^2 + 1.$$

Se ω é a raiz cúbica primitiva da unidade, é claro que ω e seu oposto $-\omega$ são raízes de $f(x)$; logo $\overline{\omega}$ e $-\overline{\omega}$ também o serão. Estas são quatro raízes de $f(x)$. Um cálculo direto mostra que a fatoração canônica real de $f(x)$ é então

$$f(x) = (x^2 + x + 1)(x^2 - x + 1).$$

Agora nos resta compreender a fatoração canônica no caso racional; em outras palavras, precisamos saber que polinômios com coeficientes racionais podem aparecer como fatores irredutíveis. Isto é um problema bem mais delicado como iremos vendo aos poucos. Uma forma de obter a fatoração canônica no caso racional de um polinômio $\mathbb{Q}[x]$, é de escrevermos primeiro a fatoração canônica real de $f(x)$; se os fatores que aparecem nesta forem polinômios com coeficientes racionais, pela unicidade da fatoração, esta será a *fatoração canônica racional* de $f(x)$: com efeito, todo polinômio irredutível em $\mathbb{R}[x]$ o será também em $\mathbb{Q}[x]$. A fatoração canônica real do polinômio do exemplo 1.4.11 é então a fatoração canônica racional.

Quais são os graus possíveis de um polinômio irredutível em $\mathbb{Q}[x]$? Analizaremos, para começar, alguns exemplos do que pode acontecer.

Exemplo 1.4.12. Seja $f(x) = x^3 - 5$. As raízes de $f(x)$ são precisamente as três raízes cúbicas de 5, isto é,

$$\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5}.$$

É então claro que

$$x^3 - 5 = g(x)(x - \sqrt[3]{5}),$$

onde $g(x)$ é o polinômio mônico de grau 2 em $\mathbb{R}[x]$ cujas raízes são $\omega\sqrt[3]{5}, \omega^2\sqrt[3]{5}$ (como exercício o leitor poderia escrever explicitamente $g(x)$). É conhecido que $\sqrt[3]{p}$ é um número irracional sempre que $p \in \mathbb{Z}$ for um número primo (por quê ?). Concluímos então que $f(x)$ é irredutível.

Outra forma de estudar o polinômio do exemplo 1.4.12 pode ser a partir da própria definição de irredutibilidade. Mais geralmente, seja $f(x) \in \mathbb{Q}[x]$ um polinômio de grau 3. Ele é redutível se e somente se

$$f(x) = f_1(x)f_2(x),$$

com $f_1(x)$ e $f_2(x)$ polinômios com coeficientes racionais de graus 1 e 2 respectivamente. Em particular $f_1(x) = ax + b$ para certos $a, b \in \mathbb{Q}$, com $a \neq 0$. Mas então $\alpha := -b/a$, que é um número racional, será raiz de $f(x)$, necessariamente. Então, um polinômio de grau 2 será irredutível quando não possuir raízes racionais. Em particular, isto mostra, de uma outra forma, que $x^3 - 5$ é irredutível; porém como sabemos, calcular as raízes de um polinômio de grau 3, salvo casos particulares, não é tarefa fácil. Mas no nosso raciocínio, precisamos apenas conhecer a natureza das raízes, isto é, não queremos calcular todas as raízes, mas apenas saber se há alguma racional: isto é muito mais fácil, como observaremos a continuação.

Seja $f(x) \in \mathbb{Z}[x]$ um polinômio de grau n com coeficientes inteiros, ou seja

$$f(x) = \sum_{i=0}^{n} a_i x^i,\ a_n, \ldots, a_0 \in \mathbb{Z}.$$

Suponhamos que $\alpha = p/q$ é uma raíz racional de $f(x)$ com $p, q \in \mathbb{Z}$ números primos entre si. Então $f(p/q) = 0$, ou, de maneira equivalente

$$q^n f(\frac{p}{q}) = 0,$$

isto é

$$a_n p^n + a_{n-1} p^{n-1} q + a_{n-2} p^{n-2} q^2 + \cdots + a_1 p q^{n-1} + a_0 q^n = 0.$$

Portanto p divide $a_0 q^n$ e q divide $a_n p^n$. Como p e q são primos entre si, tanto p e q^n como q e p^n serão primos entre si; pelo teorema de Euclides no caso dos números inteiros, concluímos que

$$p|a_0,\ q|a_n. \tag{1.5}$$

Estas relações de divisibilidade são conhecidas como *condições necessárias para existência de raiz racional*.

No caso do polinômio $x^3 - 5$, q só pode ser 1 ou -1 e $p \in \{1, -1, 5, -5\}$. As únicas raízes racionais deste polinômio podem ser então $1, -1, 5, -5$; é facil de verificar que nenhum destes números anula o polinômio.

Observação 1.4.13. (a) Se $a_0 = a_n = 1$ as únicas raízes racionais possíveis são 1 e -1. Isto mostra facilmente que o polinômio do exemplo 1.4.11 não possui raízes racionais; observe não obstante que ele é redutível em $\mathbb{Q}[x]$, o que mostra que nosso método acima funciona apenas para polinômios de grau 3 (evidentemente também para polinômios de graus 1 e 2).

(b) Se os coeficientes de $f(x)$ forem números racionais da forma

$$a_i = \frac{b_i}{c_i},\ i = 0, 1 \ldots, n,$$

com $b_i, c_i \in \mathbb{Z}$ para todo $i = 0, 1 \ldots, n$, escolhemos um múltiplo comum m dos denominadores (por exemplo o produto deles ou o MMC). É fácil constatar que $mf(x)$ é um polinômio com coeficientes inteiros. Como as raízes de $f(x)$ e de $mf(x)$ são as mesmas, podemos aplicar o método acima a este último para saber se $f(x)$ possui ou não raízes racionais.

Resumindo, se $f(x)$ for de grau 3, ou ainda menor, ele será irredutível em $\mathbb{Q}[x]$ só quando não tiver raízes racionais; na direção contrária, se um polinômio, agora de qualquer grau maior que um, tiver uma raiz racional, digamos $\alpha \in \mathbb{Q}$, então será divisível por $x - \alpha$ em $\mathbb{Q}[x]$. Logo, todo polinômio de grau maior que um em $\mathbb{Q}[x]$ que possui raiz racional é redutível.

Vejamos agora um exemplo um pouco mais complicado.

Exemplo 1.4.14. Seja

$$f(x) = 2x^4 - 20x + 2.$$

É $f(x)$ irredutível em $\mathbb{Q}[x]$? Encontrar todas as raízes de $f(x)$ é ainda mais difícil que nos casos anteriores; elém disto, corremos o risco de obtê-las de maneira aproximada, o

que impederia de encontrar a fatoração canônica real e em conseqüência a correspondente fatoração racional.

É fácil constatar que $f(x)$ não posui raízes racionais, mas isto não implica que o polinômio seja irredutível. Com efeito, não possuir raízes racionais nos diz apenas que $f(x)$ não aceita fatores de grau um, como já sabemos (e utilizamos, novamente, acima). Conseqüêntentente, $f(x)$ será redutível em $\mathbb{Q}[x]$ só se pudermos escrever

$$f(x) = 2g(x)h(x)$$

com $g(x)$ e $h(x)$ polinômios mônicos de grau 2; ou seja, se existirem $a, b, c, d \in \mathbb{Q}$ tais que

$$x^4 - 10x + 1 = (x^2 + ax + b)(x^2 + cx + d).$$

Neste caso, logo de desenvolver o produto de polinômios acima, deveremos ter

$$c + a = 0,\ ac + b + d = 0,\ ad + bc = -10, bd = 1.$$

Substituíndo $c = -a$ nas duas equações do meio, obtemos

$$b + d = a^2,\ a(d - b) = -10;$$

donde:

$$2b = a^2 + \frac{10}{a},\ 2d = a^2 - \frac{10}{a}.$$

Como $bd = 1$, multiplicando as duas equações temos

$$a^6 - 4a^2 - 100.$$

Ou seja que a^2 é uma solução racional da equação com coeficientes inteiros

$$y^3 - 4y - 100 = 0.$$

Finalmente, é fácil constatar que esta equação não possui raízes racionais (observe que toda raiz racional desta equação deve ser inteira, positiva e menor que 10). Isto mostra que a suposição de termos uma fatoração de $f(x)$ como produto de polinômios de grau dois, nos leva a uma contradição, demonstrando então que $f(x)$ é efetivamente irredutível.

Se considerarmos agora um polinômio de grau 5, as possíveis fatorações (não triviais) são como produto de dois poinômios de graus 1 e 4, ou 2 e 3; não é difícil de imaginar que os argumentos utilizados no exemplo 1.4.14 possam ser adaptados, mas a complexidade dos cálculos cresce rezoavelmente. De fato, na medida que o grau do polinômio é maior, tanto maior será a complexidade dos cálculos. Isto torna inviável o tratamento da irredutibilidade nesta perspectiva, desde que o grau do polinômio é "sufucientemente grande". Como veremos mais adiante, existe um critério muito eficaz que nos permite concluir que certo tipo de polinômios é irredutível; infelizmente não existe um critério geral. Mas postergaremos esta análise para o último parágrafo do presente capítulo.