Capítulo 8

O anel dos polinômios.

Neste capítulo vamos estudar um tipo de função que generaliza as funções "lineares afins", "quadráticas": polinômios.
Iremos um pouco mais a fundo porque estudaremos o comportamento destas funções em conjunto, o conjunto dos polinômios, formando uma estrutura algébrica.
O *conjunto dos polinômios* é fechado para algumas operações, por exemplo para a soma, e forma com ela um grupo.
Também vamos ver que a *multiplicação* é "defeituosa" neste conjunto, como acontece no conjunto dos números inteiros, assim, os polinômios com a adição e a multiplicação, tem uma estrutura mais fraca que a de corpo, é um anel. Quer dizer que o conjunto dos polinômios munidos da adição e da multiplicação se assemelha a $(\mathbf{Z}, +, \cdot)$.

O estudo do anel dos polinômios ainda é uma das área mais efervecentes dentro da construção Matemática. Entre 1998 e 2001 houve um acontecimento marcante neste sentido quando André Gilles anunciou a solução do último *problema* de Fermat, com alguns defeitos na solução anunciada e, finalmente, com a versão final corrigida.

Numa outra vertente, os polinômios servem para encriptar informações. Infelizmente o conteúdo deste livro não irá tão longe, em nenhuma das duas direções.

8.1 Os números são polinômios ?

*U*m professor levanta um saquinho de petecas na mão e, desafiante, pergunta aos alunos quantas petecas podem ter no saquinho, enquanto escreve na quadro os números:

$1000, 100, 10$

A resposta unânime, foi 10, pelo tamanho do saquinho.
Os alunos ficaram surpresos quando o professor disse que eram 1000 as bolinhas no saco. E explicou que na verdade havia oito, e que os valores, no quadro, "representavam" números na *base 2* e mostrou a relação entre as correspondentes "representações na *base 10*:

base 2	1	2	4	8
base 10	1	10	100	1000

Oito, escrito na base 2 se representa com 1000.
`''Representavam''` é a *palavra chave* nesta questão. Há muitas formas de representação, para os elementos de uma classe de objetos. Vamos precisar deste conceito, vamos usá-lo e explicá-lo a seguir. Mas, informalmente, "representar" é uma forma "atenuada" de falar "codificar"...

No exemplo do professor, ao fazer correspondências entre os valores que se podem obter numa base ou na outra, vemos as potências de 2 ou de 10.

Ao longo de sua História, a Hunidade construir um mode de representar as quantidades que chamamos de *decimal* e que certamente está intimamente ligado com a quantidade de dedos que temos nas mãos. Podemos facilmente inferir o método que nossos antepassdos usaram para registrar grandes quantidades:

- iam estabelecendo relação dos objetos com os dedos das mãos;
- quando dava *overflow* com os dedos, (quer dizer, não havia mais dedos para contar), faziam um tracinho na áreia da práia e voltam a contar com o primeiro dedo de novo;
- depois contavam os tracinhos, cada um representando uma dezena;

Claro, com o tempo, com a evolução, e com o aumento da riqueza, foram especializando o processo e possivelmente colocando zeros depois do traço... e aí apareceu o 10.

O sistema decimal se impôs naturalmente pela facilidade operatória. A soma de 1000 com 82 tem um aparência simples: o 82 ocupa os zeros do 1000 dando 1082. E sempre foi assim, a Humanidade aproveitou aquilo que melhor desempenho tinha, é uma lei da Biologia, "ao longo do desenvolvimento ficam as espécies mais fortes".

Depois que as regras se estabelecem nós seguimos atrás de justificá-las. Vejamos o que significa um número na base 10, por exemplo 438:

$$138 = 400 + 30 + 8 \tag{8.1}$$

$$138 = 4 * 10^2 + 3 * 10 + 8 \tag{8.2}$$

$$138 = 4 * 10^2 + 3 * 10 + 8 * 10^0 \tag{8.3}$$

uma soma de potências de 10 com coeficientes que são os algarismo.

Se considerarmos a soma

$$32 * 10^2 + 3 * 10 + 8 * 10^0$$

ela pode ser re-escrita como

$$3 * 10^3 + 2 * 10^2 + 3 * 10 + 8 * 10^0 \tag{8.4}$$
$$a_3 * 10^3 + a_2 * 10^2 + a_1 * 10^1 + a_0 * 10^0 \tag{8.5}$$

porque deu *overflow* na casa das dezenas... os algarismo na base 10 somente podem ser

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9$$

quer dizer que um número, escrito na *base 10* ou em qualquer outra *base*, é uma expressão do tipo

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

que chamamos polinômio. Os coeficientes são os algarismos, números menores que a base. Na base 10 *não existe o algarismo 10*.

As operações se explicam, agora algebricamente. Para somar dois números consideramos as potências de mesma base para ordená-los.

Na prática dizemos, colocamos casa decimal em baixo de casa decimal.

e observamos a regra do *overflow*, do *estouro*, da casa decimal.

Vamos multiplicar dois números usando as regras algébricas para ver como elas se aplicam. Multiplicar 328 e 243 .

$328 =$			$3 * 10^2$	$+2 * 10$	$+8$
$243 =$			$2 * 10^2$	$+4 * 10$	$+3$
	$6 * 10^4$	$+4 * 10^3$	$+16 * 10^2$		
		$+12 * 10^3$	$+8 * 10^2$	$+32 * 10^1$	
			$9 * 10^2$	$+6 * 10^1$	$+24$
	$6 * 10^4$	$+16 * 10^2$	$+33 * 10^2$	$+38 * 10^1$	$+24$

e vemos que há vários estouros de casas decimais para corrigir. Podemos começ ar a correção por qualquer lado. Vamos começar, como de hábito pela casa das unidades. Este método se verificou o mais fácil porque vai acumulando aos poucos nas casa mais altas.

Corrigindo o *estouro* nas casas decimais, temos:

$$
\begin{array}{ccccc}
6*10^4 & +16*10^2 & +33*10^2 & +38*10^1 & +24 \\
6*10^4 & +16*10^2 & +33*10^2 & +38*10^1 & +(20+4) \\
6*10^4 & +16*10^2 & +33*10^2 & +40*10^1 & +4 \\
6*10^4 & +16*10^2 & +33*10^2 & +(40+0)*10^1 & +4 \\
6*10^4 & +16*10^2 & +37*10^2 & 0*10^1 & +4 \\
6*10^4 & +16*10^2 & +(30+7)*10^2 & 0*10^1 & +4 \\
6*10^4 & +19*10^2 & +7*10^2 & 0*10^1 & +4 \\
6*10^4 & +(10+9)*10^2 & +7*10^2 & 0*10^1 & +4 \\
7*10^4 & +9*10^2 & +7*10^2 & 0*10^1 & +4 \\
7 & 9 & 7 & 0 & 4
\end{array}
$$

observe que na última linha, simplesmente, apagamos o operador + e as potências de 10 e apareceu o resultado que qualquer máquina de calcular vai mostrar no *display*.

8.2 O que é um polinômio?

Uma função linear afim, ou uma função quadrática, ambas se definem atravez de polinômios. Uma função quadrática, não é um polinômio, nem uma função linear o é.

"Polinômio" é uma expressão que serve para definir *funções polinômiais* como é o caso das funções lineares ou das quadráticas.

Para definirmos uma função linear[1]precisamos de `dois coeficientes`, *um polinômio do primeiro grau*,

$$f(x) = a + bx$$

para definirmos uma função quadrática, precisamos de `tres coeficientes`, *um polinômio do segundo grau*:

$$g(x) = a + bx + cx^2.$$

Tanto f como g dizem-se funções *polinômiais* porque estão definidas a partir de polinômios.

Mas *polinômio* mesmo são os coeficientes! Acabamos de fazer uma *representação*[2].

Se "multiplicarmos" $h(x) = f(x)g(x)$ iremos obter uma outra função também descrita por coeficientes que será uma função polinomial do *grau 3*. Faça isto agora! Calcule h.

Observação 37 *Polinômios, operações e estrutura*

Com esta última frase acrescentamos duas idéias:

- *Operação com polinômios podemos* multiplicar *os polinômios, e*
- *classificação dos polinômios eles se classificam com auxílio de um conceito chamado* grau.

A maneira correta de fazer referência às funções lineares, é dizer que elas são funções polinômiais do primeiro grau. As funções quadráticas, são funções polinômiais do segundo grau, e h é uma função polinômial do terceiro grau. Ainda não definimos polinômios! até aqui estamos nos mantendo nos exemplos. Vamos insistir um pouco mais nesta técnica antes de partir para a definição. Os exercícios seguintes farão isto.

[1]Função linear é um tipo particular de função linear afim, mas de agora em diante vamos cometer o erro de chamá-las todas de funções lineares.

[2]Existe uma teoria em Matemática chamada, teoria das representações... que é grande como a teoria dos conjuntos. Não precisaremos estudá-la toda para fazer algum uso dela, entretanto.

Exercícios 36 *Coeficientes e grau.*

1. *Multiplicação de polinômios*

   Tente descobrir um esquema *para multiplicar dois polinômios usando apenas os coeficientes, (faça a multiplicação usual e depois apague a variável...). Verifique que é um esquema semelhante ao da multiplicação dos números.*

2. *representação polinomial dos números*

   (a) *Um número escrito na base 10 pode ser* representado *como se fosse um polinômio, faça isto e depois compare a multiplicação de dois número com a multiplicação de polinômios. Observe que agora os "coeficientes" tem uma regra especial, identifique esta regra.*

   (b) *Justifique com a comparação feita no item anterior a questão de* passar alguma coisa para a casa seguinte *nas multiplicações. Aliás, tente definir o que é* casa.

   (c) *Calcule a soma de dois números escritos polinomialmente e justifique a passagem para casa seguinte quando houver algarismos desobedecendo a regra que você construiu.*

3. *Um sistema de numeração complicado*

   Um sistema de numeração complicado, mas que você domina completamente.

   (a) *Observe uma data é um sistema de numeração*

   $$03/08/1998; 03 : 10 : 20$$

   dia, mes, ano, hora, minuto, segundo . . . Quais os "algarismos" que podem ser usados em cada uma das "casas" ?

   (b) *Dá para concluir que as datas são um sistema com bases de numeração diferentes ?*

   (c) *Quais são as operações admissíneste sistema de números ? Existe elemento neutro? elemento inverso ?*

   (d) *Você poderia resolver a equação*

   $$03/08/1970; 22 : 30 : 59 + dd/mm/aaaa = 10/02/1999; 03 : 10 : 20$$

4. *Verifique que não precisamos também da variável para somar polinômios, descreva isto.*

5. *Construa um* esquema *que permita a divisão de dois polinômios usando apenas os coeficientes.*

6. *Faça várias multiplicações, adições e divisões de polinômios usando os esquemas por você construidos para usar apenas os coeficientes.*

7. *Verifique qual das seguintes opções serve para* representar *o conjunto de todos os polinômios* com coeficientes reais*:*

   - *um polinômio é um elemento de* $\mathbf{R}^{n+1}$,

     $$(a_0, a_1, \cdots, a_n)$$

   - *um polinômio é uma sucessão de números reais.*
   - *um polinômio é uma sucessão finita de números reais.*

   Qual é a diferença entre a primeira e a última opção ?

8. *Tente uma definição de grau, claro você precisa primeiro resolver a questão anterior para saber onde* grau *está definido.*

8.3 A estrutura algébrica dos polinômios

Vamos começar respondendo as duas últimas questões.

O conjunto de todos os polinômios com coeficientes reais é designado com símbolo $\mathbf{R}[x]$ é formado de todas as sucessões finitas de números reais. Quer dizer que

$$(a_0, a_1, \cdots, a_n) \in \mathbf{R}^n \subset \mathbf{R}[x] \tag{8.6}$$

$$(a_0, a_1, \cdots, a_{n+1}) \in \mathbf{R}^{n+1} \subset \mathbf{R}[x] \tag{8.7}$$

$$(a_0, a_1, \cdots, a_{n+100}) \in \mathbf{R}^{n+100} \subset \mathbf{R}[x] \tag{8.8}$$

$$a_0 \in \mathbf{R} \subset \mathbf{R}[x] \tag{8.9}$$

Nós precisamos que os números também sejam polinômios, veja a última linha acima, poderiamos ter escrito (a_0), mas isto seria uma notação nada comum. Assim os números, simplesmente, são polinômios. Vem então a pergunta: qual seria o *grau* dos números ? A resposta é que você já espera, os números são polinômios de grau zero. O grau é um conceito hierárquico dentro do conjunto dos polinômios[3]. Nós vamos dizer que os números são polinômios de grau zero, eles tem exatamente um coeficiente. O polinômio

$$(a_0, a_1, \cdots, a_n) \equiv a_0 + a_1 x + \cdots + a_n x^n$$

é um polinômio de grau n, ele tem $n+1$ coeficientes. Observe que polinômio

$$1 + x^3 + x^5 \equiv (1, 0, 0, 1, 0, 1)$$

tem seis coeficientes. Quando escrevemos usando "expressão" algébrica podemos omitir os coeficientes nulos porque a "expressão algébrica" garante a informação correta. Mas $1 + x^3 + x^5$ tem seis coeficientes e não três. Enfim o grau corresponde åmaior potência do polinômio escrito como expressão algébrica ou *número de coeficientes menos 1*, considerando os coeficientes nulos.

Quer dizer que o $\mathbf{R}[x]$ deve ser entendido como um conjunto infinito de folhas, ou hiperplanos, de graus sucessivamente maiores:

$$\mathbf{R}[x] = \mathbf{R} \cup \mathbf{R}^2 \cup \mathbf{R}^3 \cdots \cup \mathbf{R}^n \cdots$$

Se ficassemos apenas com os polinômios de um certo grau teriamos uma estrutura algébrica deficiente. Por exemplo se nos fixassemos no conjunto dos polinômios do segundo grau. Nenhum deles poderia ter inverso aditivo porque

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

não seria um polinômio do segundo grau. Precisamos de ter polinômios de grau zero para que a operação acima possa ser efetuada. Se em vez de somar, multiplicarmos:

$$(1 + x - x^2)(1 - x + x^2) = 1 + x^2 + 2x^3 - x^4 \equiv (1, 0, 1, 2, -1)$$

vemos que o grau aumenta. Quer dizer que podemos discutir a estrutura de

$$(\mathbf{R}[x], +, \cdot)$$

a chamada "álgebra dos polinômios". Esta estrutura é muito semelhante a estrutura $(\mathbf{Z}, +, \cdot)$. A primeira semelhança consiste na *deficiência* da multiplicação. Como em $\mathbf{Z}$, em $\mathbf{R}[x]$ não tem inversos multiplicativos, de modo que $(\mathbf{R}[x], +, \cdot)$ é um anel.

[3] O grau tem o que ver com *dimensão* ... mas não é exatamente a mesma coisa.

Exercícios 37 *Propriedades do anel dos polinômios Dado um polinô mio*

$$P(x) = \sum_{k=0}^{n} a_k x^k$$

podemos associar-lhe dois objetos diferentes:

- *a função* $[a, b] \ni x \ \mapsto P(x)$
- *a sucessão* $(a_0, \cdots, a_n)$ *dos coeficientes.*

Esta lista de exercícios é um laboratório em que estes dois tipos de objetos serão testados em diversas circunstâncias gerando novas estruturas.

1. *Defina a soma de dois polinômios, isto é erspecifique o algoritmo para somar* $P(x), Q(x)$, *como se você fosse executar a soma automaticamente com um programa.*
2. *Mostre que a soma de polinômios é comutativa e associativa.*
3. *Mostre que no conjunto* $\mathbf{R}[x]$ *existe um elemento neutro para adição e um elemento neutro para a multiplicação.*
4. *Mostre que* $(\mathbf{R}[x], +)$ *é um grupo comutativo.*
5. *Mostre que todo polinômio tem um inverso aditivo.*
6. *Escreva a fórmula que associa o grau do multiplicando, do multiplicador e do produto em* $\mathbf{R}[x]$.
7. *Mostre com um exemplo que em* $\mathbf{R}[x]$ *não há inversos multiplicativos.*
8. *Considere os polinômios* P, Q, R *e identifique* $P(x), Q(x), R(x)$ *com os valores assumidos pelas funções definidas por cada um destes polinômios quando* $x \in [a, b] \subset \mathbf{R}$. *Use esta representação para demonstrar que o produto de polinômios é comutativo, associativo e distributivo relativamente åadição.*
9. *Mostre que a multiplicação em* $\mathbf{R}[x]$ *é comutativa e associativa. Mostre que a multiplicação é distributiva relativamente åadição. Sugestão: use a representaçãp funcional.*
10. *Faça uma listagem ordenada e estruturada das propriedades de* $(\mathbf{R}[x], +, \cdot)$, *agrupando-as por operação.*
11. *Resolva as equações abaixo indicando a propriedade utilizada em cada passagem:*
    a)$P + 1 + x^2 = x^3$ *b)* $4P + x^3 = x - 1$ *c)* $\frac{P+2}{4} = x + 1$
12. *Tente uma solução para as equações abaixo indicando a propriedade utilizada em cada passagem:*
    (a) $(x^2 + 1)(P + 1 + x^2) = 1 + x + 2x^2 + x^3 + x^4$
    (b) $xP = x^2 - x^3 - x^5$
13. *A convolução de sucessões*
    (a) Calcule o produto dos polinômios definidos abaixo com seus coeficientes na ordem crescente (das potências):
        i. $(1, 2, 3, 4, 5)$, $(1, 0, 1, 0, 1, 0)$
        ii. $(1, 1, 1, 1, 1, 1)$, $(1, 1, 1, 1, 1, 1)$
        iii. $(a_0, a_1, a_2, a_3, a_4)$, $(a_0, a_1, a_2, a_3, a_4)$

iv. $(a_0, a_1, a_2, a_3, a_4)$, $(b_0, b_1, b_2, b_3, b_4)$

(b) Deduza da da última multiplicação feita acima, uma fórmula para o termo geral c_k do produto PQ de dois polinômios como uma soma envolvendo os termos de P e de Q.

(c) Chame a sucessão finita $(a_0, a_1, a_2, a_3, a_4)$ dos coeficientes do polinô-mio P de $\underline{a}$ e chame de $\underline{b}$ a sucessão finita dos coeficientes de Q :

$$a = (a_0, a_1, a_2, a_3, a_4), b = (b_0, b_1, b_2, b_3, b_4),$$

Expresse a fórmula do produto dos dois polinômios P, Q como uma função $c = a * b$ de modo que $a * b(k) = c_k$ é o coeficiente de ordem k do polinômio PQ, (use um somatório para isto).

(d) Mostre que a sucessão finita $a = (1, 0, \cdots, 0)$ que tem todas as coordenadas nulas, exceto a primeira, é a unidade relativamente åconvolução.

8.3.1 Comentários sobre alguns dos exercícios

Funções polinomiais

Nos primeiros exercícios estabelecemos uma *representação* entre o conjunto dos polinômios e um subconjunto do conjunto das funções definidas no intervalo $[a, b]$.

Vamos ver aqui o poder da generalização e até mesmo a razão pela qual fazemos generalizações ou representações.

Queremos demonstrar que o produto de dois polinômios é comutativo. Sejam P, Q os dois polinômios.

Vamos criar algumas notações, palavras novas desta linguagem chamada Matemática que falamos.

Vamos dar um nome a este conjunto de funções: $\mathcal{F}([a, b])$.

Observe que $\mathbf{R}[x]_{x\in[a,b]} \subset \mathcal{F}([a, b])$. Como se costuma dizer ainda, $\mathbf{R}[x]_{x\in[a,b]}$ é um subconjunto pró prio de $\mathcal{F}([a, b])$.

$$\mathbf{R}[x]_{x\in[a,b]} \ni P \mapsto p \in \mathcal{F}([a, b]) \tag{8.10}$$

quer dizer: P é o polinômio, p é a função polinomial definida por P. (8.11)

$$\mathbf{R}[x]_{x\in[a,b]} \ni P, Q \mapsto p, q \in \mathcal{F}([a, b]) \tag{8.12}$$

$$\mathbf{R}[x]_{x\in[a,b]} \ni PQ \mapsto pq \in \mathcal{F}([a, b]) \tag{8.13}$$

$$pq(x) \mapsto p(x)q(x) \text{ o produto de dois números reais} \tag{8.14}$$

$$pq(x) = p(x)q(x) = q(x)p(x) = qp(x) \tag{8.15}$$

$$pq \mapsto PQ \ ; \ qp \mapsto QP \tag{8.16}$$

$$\text{se a função, representação, } \mathbf{R}[x]_{x\in[a,b]} \to \mathcal{F}([a, b]) \tag{8.17}$$

$$\text{for bijetiva, então podemos concluir que} \tag{8.18}$$

$$pq = qp \quad \Rightarrow \quad PQ = QP \tag{8.19}$$

Fizemos uma demonstração incompleta, porque usamos uma hipótese que não foi ainda testada ou comprovada: *a representação do conjunto dos polinômios no conjunto das funções é "bijetiva".* Teremos que demonstrar esta afirmação para legalizar a demonstração que fizemos acima. Antes de prosseguir discutindo o próximo teorema,

vamos discutir a notação que estamos usando. $\mathbf{R}[x]$ representa o conjunto de todos os polinô mios, e nós podemos escrever um polinômio usando uma expressão algébrica:

$$P(x) = a_0 + a_2x^2 + a_5x^5 \equiv (a_0, a_1, a_2, a_3, a_4, a_5)$$

ou mais concretamente

$$P(x) = 3 + 4x^2 + 7x^5 \equiv (3, 0, 4, 0, 0, 7).$$

Se escrevermos $P(x)_{x=2} = 3+16+224 = 243$ que dizer que substituimos na expressão algébrica $P(x)$ a letra x pelo número 2. Uma outra forma de escrer isto é simplesmente

$$P(2) = 3 + 16 + 224 = 243.$$

Mas se quisermos indicar que x pode assumir qualquer valor no intervalo $[a, b]$, a única maneira de indicá-lo é esta que usamos acima: $\mathbf{R}[x]_{x\in[a,b]}$. Neste momento, $P \in \mathbf{R}[x]$; $P(x)_{x\in[a,b]}$ não é mais um polinômio, é uma função polinomial porque x agora representa um número.

Vamos ao teorema agora.

Teorema **77** *Representação dos polinômios*

Seja $\mathbf{R}[x]_{x\in[a,b]} \xrightarrow{\phi} \mathcal{F}([a, b])$ *que associa um polinômio* $P \in \mathbf{R}[x]$ *a função polinomial* p ; $p(x) := P(x)_{x\in[a,b]}$; $p \in \mathcal{F}([a, b])$.

ϕ *é uma função injetiva.*

Dem:

Considere dois polinômios diferentes, $P \neq Q$ e as correspondentes funções polinomiais que eles induzem em $\mathcal{F}([a, b])$; p, q.

Mas dizer que dois polinômios são diferentes, quer dizer que existe pelo menos um dos coeficientes de um que não é igual ao correspondente coeficiente do outro, $a_k \neq b_k$, supondo que os coeficientes de P são $a_0 \ldots$ e os de Q são $b_0 \ldots$ Temos que mostrar que as duas funções induzidas por P, Q são diferentes.

Se fizermos a diferença, $p(x) - q(x)$, como estas funções estão definidas por polinômios, e estes são diferentes, então o polinômio que define esta diferenção é $P-Q$ que não é o polinômio zero, porque o coeficiente correspondente a diferença $a_k - b_k \neq 0$, logo a função $p(x) - q(x)$ é diferente de zero para algum x. Logo $p \neq q$. **q.e.d .**

Mas, infelizmente, não poderemos demonstrar, como nos propunhamos, que ϕ é bijetiva, pois em $\mathcal{F}([a, b])$ existem funções que não são polinomiais. Isto é $\phi(\mathbf{R}[x])$ é um subconjunto próprio de $\mathcal{F}([a, b])$. Observe a (fig. **??**), na página **??**. A representação ϕ cria uma imagem em $\mathcal{F}([a, b])$ que é idêntica a $\mathbf{R}[x]$ mas esta imagem não cobre todo o contra-domínio, então ϕ não é uma função sobrejetiva. Mas se reduzirmos a imagem ao que nos interessa, ao conjunto

$$\widetilde{\mathbf{R}[x]} = \mathcal{P}([a, b]) \text{ o conjunto das funções polinomiais}$$

então temos uma função bijetiva.

Isto chega para estabelecer uma idenficação no sentido de que podemos considerar o subconjunto $\mathcal{P}([a, b])$ de $\mathcal{F}([a, b])$ formado por todas as funções polinomiais, que é a imagem de ϕ. Quer dizer, podemos ir e voltar entre $\mathcal{P}([a, b])$ e $\mathbf{R}[x]$ logo, fica validada a demonstração do teorema. Podemos usar o mesmo método para provar que o produto de polinômios é associativo, e que o produto é distributivo relativamente a adição.

Nós usamos o conceito de *igualdade entre polinômios* sem definí-lo mas agora vamos fechar este buraco lógico:

Definição 59 *Igualdade entre polinômios*

Dois polinômios são iguais se todos os seus coeficientes coïncidem.

Compare agora a demonstração da comutatividade do produto se esta for feito com o produto de coeficientes:

Dem: Demonstração da comutatividade do produto de polinômios

Vamos começar comentando outro exercício. Precisamos saber como se escreve o termo geral do produto PQ.

Sejam $P = (a_0, a_1, a_2, \cdots, a_n)$ e $Q = (b_0, b_1, b_2, \cdots, b_m)$ dois polinômios.

Observe o quadro abaixo da multiplicação:

b_0	b_1	b_2	b_3	b_4		
a_0	a_1	a_2				
b_0a_0	b_1a_0	b_2a_0	b_3a_0	b_4a_0		
	b_0a_1	b_1a_1	b_2a_1	b_3a_1	b_4a_1	
		b_0a_2	b_1a_2	b_2a_2	b_3a_2	b_4a_2

Neste esquema, em cada linha, você pode ver cada um dos coeficientes a_j sendo multiplicado por todos os coeficientes b_i. No paralelogramo se encontram todos os pares (b_i, a_j) que é possível fazer com os coeficientes de cada um dos polinômios. Em baixo de cada coluna se faz a soma dos elementos da mesma, nelas a soma dos índices é constante. Por exemplo, em baixo da quarta coluna ficará:

$$b_3a_0 + b_2a_1 + b_1a_2$$

esta soma é coeficiente de x^3.

$$PQ = (a_0b_0, \cdots, \sum_{i+j=k} a_ib_j, \cdots a_nb_m)$$

$$QP = (b_0a_0, \cdots, \sum_{i+j=k} b_ja_i, \cdots b_na_m)$$

e nos temos que mostrar que $PQ = QP$. Basta mostra que o termo geral $\sum_{i+j=k} a_jb_k$ é igual a $\sum_{i+j=k} b_ja_k$. Um truque, na verdade uma nova representação, nos conduzem facilmente a esta verificação.

Para multiplicar polinômios, somos conduzidos *a fazer todas as multiplicações* a_kb_j e depois agrupar estes produtos de acordo com a regra dos expoentes que é que se encontra em baixo do somário:

$i + j = k$ a soma dos expoentes valendo k.

Retomando a frase, "*a fazer todas as multiplicações ...*" agora escrita assim: "*a fazer todos os pares* (a_k, b_j)" quer dizer, *construir o produto cartesiano dos conjuntos*

$$A = \{a_0, a_j, \cdots a_n\}, B = \{b_0, b_k, \cdots b_m\}$$

Observe abaixo o caso com $n = 2, m = 4$. Chame de A, B aos conjuntos dos coeficientes dos polinômios. Na tabela abaixo você tem A x B. Marcamos o conjunto dos coeficientes a_jb_k ; $j + k = 4$. O coeficiente de x^4 no produto será a soma destes coeficientes, faça as contas e verifique.

b_4	(a_0, b_4)	(a_1, b_4)	(a_2, b_4)
b_3	(a_0, b_3)	(a_1, b_3)	(a_2, b_3)
b_2	(a_0, b_2)	(a_1, b_2)	(a_2, b_2)
b_1	(a_0, b_1)	(a_1, b_1)	(a_2, b_1)
b_0	(a_0, b_0)	(a_1, b_0)	(a_2, b_0)
	a_0	a_1	a_2

Experimente agora você mesmo, considere as "linhas" desta tabela em que a soma dos índices é constante e verifique que são os coeficientes da mesma potência de "x" no produto. Por exemplo, quando a soma for 3 você terá

$$(a_0, b_3), (a_1, b_2), (a_2, b_1)$$

que somados:

$$(a_0 b_3 + a_1 b_2 + a_2 b_1) x^3$$

são os coeficientes de x^3 no produto dos dois polinômios. Podemos assim identificar todos as somas que correspondem a uma determinada potência no produto cartesiano dos conjuntos dos coeficientes.

Quando comutarmos os polinômios, na multplicação, isto significa que vamos passar a olhar o produto cartesiano $B \text{ x } A$ que são diferentes, é verdade, mas que tem alguma identidade:

$$(x, y) \in A \text{ x } B \Rightarrow (y, x) \in B \text{ x } A$$

e como a multiplicação de números é comutativa, então as duas linhas cuja soma de índices vale k produzem o mesmo coeficiente no produto, para o coeficiente de grau k.

Quer dizer, o produto de polinômios é comutativo. **q.e.d .**

Observação 38 *Representação.*

Obviamente "arroz com feijão" e "baião de dois" são duas coisas diferentes, como

$$1 + x^2 + x^3 \neq (1, 0, 1, 1).$$

São diferentes, mas para muitos efeitos representam a mesma coisa, é esta idéia sob o conceito de representação. Temos conjuntos diferentes mas identificados através de uma bijeção.

Em ambos os casos usamos representações. Num caso representamos o conjunto dos polinômios no conjunto das funções definidas no intervalo $[a, b]$, *identificando*

$$\mathbf{R}[x]_{x \in [a,b]} \text{ com } \mathcal{P}([a, b]) \subset \mathcal{F}([a, b]).$$

É rigorosamente a mesma que fazemos quando identicamos os inteiros com as frações de denominador 1. São dois objetos diferentes. Também estamos fazendo representação quando identificamos *os números racionais com pontos da reta.*

Talvez para alguns dos leitores, uma das demonstrações que fizemos da comutatividade do produto é a mais fácil. É esta a razão porque fazemos representações, para buscar uma maneira mais fácil de entender o que está acontencendo num conjunto complicado. Esta é uma das principais atividades da Matemática, fazer representações para explicar os fatos dentro de outra estrutura.

Exercícios 38 *Associatividade do produto*

1. *Prove que o produto de tres polinômios,* P, Q, R *é associativo, use a representação*
$$\mathbf{R}[x]_{x \in [a,b]} \to \mathcal{F}([a, b])$$
2. *Prove que o produto de tres polinômios,* P, Q, R *é associativo, use a representação dos polinômios no conjunto das sucessões finitas e veja como fica o produto cartesiano onde você vai representar os coeficientes do produto.*

Convolução de sucessões

Na seção anterior discutimos o produto de polinômios e fomos levados a fazer uma representação de $\mathbf{R}[x]$ num conjunto de funções para ver melhor o que significava a comutatividade.

Representamos também os polinômios no conjunto das sucessões finitas. Podemos então observar que

$$\mathbf{R}[x] \ni P, Q \ ; \ PQ \equiv p * q \ ; \ p, q \text{ sucessões finitas.}$$

A operação $p * q$ com as sucessões finitas, se chama *convolução.*

Vamos dar um nome ao conjunto das sucessões finitas: $\mathbf{R}^{\infty}$. Observe que tem sentido o "expoente" ∞, não num sentido operatório. $\mathbf{R}^3$ é o conjunto de todas as sucessões que tem "exatamente" tres elementos. $\mathbf{R}^n$ é o conjunto de todas as sucessões que têm "exatamente" n elementos. $\mathbf{R}^{\infty}$ é a reunião de todos os $\mathbf{R}^n$ para qualquer que seja n. Depois você vai encontrar este conjunto em Matemática mais avançada com outro nome. No momento usaremos este. Temos então dois conjuntos diferentes, $\mathbf{R}[x], \mathbf{R}^{\infty}$. Mas podemos mostrar que

- A todo polinômio $P \in \mathbf{R}[x]$ corresponde exatamente uma sucessão finita $p \in \mathbf{R}^{\infty}$.
- Reciprocamente, a toda sucessão finita $p \in \mathbf{R}^{\infty}$ corresponde exatamente um polinômio $P \in \mathbf{R}[x]$.
- Se chamarmos ϕ a representação que acabamos de mencionar,

  $$\mathbf{R}[x] \ni P \overset{\phi}{\mapsto} p \in \mathbf{R}^{\infty}$$

  podemos afirmar que

  $$\phi(PQ) = \phi(P) * \phi(Q)$$

  em outras palavras, dá no mesmo fazer o produto de polinômios e depois passar ϕ ou primeiro, passar ϕ e fazer a convolução.

  Também podemos afirmar que

  $$\phi(P + Q) = \phi(P) + \phi(Q)$$

  em outras palavras, dá no mesmo fazer a soma de polinômios e depois passar ϕ ou primeiro, passar ϕ e fazer a soma de sucessões.

Isto significa que as duas estruturas $(\mathbf{R}[x], +, \cdot)$ e $(\mathbf{R}^{\infty}, +, *)$ são "idênticas". Como de fato elas não "idênticas", temos uma palavra em Matemática para dizer isto: dizemos que

$$(\mathbf{R}[x], +, \cdot) \text{ e } (\mathbf{R}^{\infty}, +, *) \text{ são isomorfas.}$$

Dizemos ainda que $\mathbf{R}[x] \overset{\phi}{\to} \mathbf{R}^{\infty}$ é um `isomorfismo`.

Definição 60 *Isomorfismo*

Uma representação entre duas estruturas que seja bijetiva e preserve as duas estruturas se chama um isomorfismo.

Nos discutiremos com mais detalhes a *estrutura* de $\mathbf{R}[x]$ na próxima seção.

Exercícios 39 *1. Calcule separadamente os coeficientes de todos os graus de x no produto de polinômios*

$$(\frac{3}{4} + \frac{4x}{3} + x^4)(\frac{-x}{3} + \frac{x^2}{3} + x^5)$$

2. *Considere os polinômios*

$$P(x) = a_0 + a_1x + \cdots + a_nx^n, Q(x) = b_0 + b_1x + \cdots + b_mx^m.$$

Escreva os quatro primeiros coeficientes do produto PQ.

3. *Calcule a convolução*

$$(1,1,1,1,1,1,1) * (1,1,1,1,1,1,1,1,1).$$

4. *Calcule a convolução*

$$(1) * (1,2,3,4,5,6,7,8,9).$$

5. *Calcule a convolução*

$$(1,0,0,0,0,0,0,0) * (1,2,3,4,5,6,7,8,9)$$

6. *Considere os polinômios*

$$P(x) = a_0 + a_1x + \cdots + a_nx^n, \tag{8.20}$$
$$Q(x) = b_0 + b_1x + \cdots + b_mx^m, \tag{8.21}$$
$$R(x) = c_0 + c_1x + \cdots + c_lx^l. \tag{8.22}$$

Calcule os quatro primeiros coeficientes do produto $P(QR)$. Calcule também os quatro primeiros coeficientes do produto $(PQ)R$. Que conclusão o resultado sugere? Prove esta sugestão.

7. *Representando $\mathbf{R}[x]$ em $\mathcal{F}([a,b])$, prove usando a associatividade do produto de números reais, que o produto de polinômios é associativo. Escreva cuidadosamente todas as passagens, (idas e voltas).*

8. *Prove que o produto de polinômios é distributivo relativamente åadição de polinômios.*

9. *Calcule $2P, P^2, P^2 - 1$ se*

$$P(x) = \frac{-3}{4} + \frac{4x}{3} + 2x^2 + x^3 + x^4.$$

10. *Calcule $(x + a_1)(x + a_2)$.Escreva separadamente todos os coeficientes deste produto. Identifique a estrutura destes coeficientes com uma relação entre os números a_1, a_2.*

11. *Calcule $(x + a_1)(x + a_2)(x + a_3)$. Escreva separadamente todos os coeficientes deste produto. Identifique a estrutura destes coeficientes com uma relação entre os números a_1, a_2, a_3.*

12. *Calcule $(x+a_1)(x+a_2)(x+a_3)(x+a_4)$. Escreva separadamente todos os coeficientes deste produto. Identifique a estrutura destes coeficientes com uma relação entre os números a_1, a_2, a_3, a_4.*

13. *Considere o produto*

$$(x + a_1)(x + a_2)\cdots(x + a_n)\ ;\ n > 2.$$

Escreva separadamente todos os coeficientes deste produto. Você poderia identificar no resultado algo ligado a Análise Combinatória? Identifique a estrutura destes coeficientes entre uma relação com os números $a_1, a_2, \cdots, a_n$.

14. *Considere o polinômio* $6 + 5x + x^2$. *Ele pode ser o produto* $(x + a_1)(x + a_2)$. *Verifique se isto é possível e então fatore* $6 + 5x + x^2$.

15. *Observe se é possível fatorar os polinômios abaixo:*

    $-6 + x + x^2$ $\quad -6 - x + x^2$ $\quad 12 + 7x + x^2$
    $-12 - 7x + x^2$ $\quad -12 - x + x^2$ $\quad 4 - 2x + x^2$ *Quando for possível, resolva*
    $8 + 6x + x^2$ $\quad -8 - 2x + x^2$ $\quad 12 - 7x + x^2$

    a equação $P(x) = 0$.

16. *Observe se é possível fatorar os polinômios abaixo:*

    $3 + 6x + 6x^2 + x^3$ $\quad -8 + 2x + 5x^2 + x^3$
    $-8 + -9x + x^2 + x^3$ $\quad 10 + 2x + 5x^2 + x^3$

    Quando for possível, resolva a equação $P(x) = 0$.

8.4 Estrutura do conjunto dos polinômios a coeficientes reais.

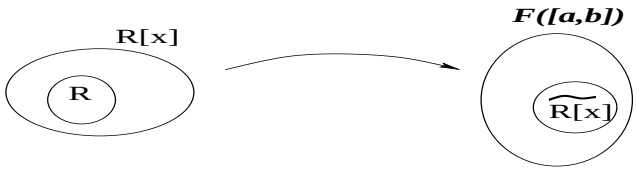

Figura 8.1: $\mathbf{R} \subset \mathbf{R}[x] \subset \mathcal{F}([a, b])$

Vamos descrever a estrutura do conjunto dos polinômios a coeficientes reais com base nas experiências que desenvolvemos na seção anterior.

Fizemos diversas experiências e exercícios nas seções anteriores que agora devem nos permitir a discussão da estrutura do conjunto dos polinômios $\mathbf{R}[x]$ na presença das operações de adição e multiplicação de polinômios.

Já verificamos que o produto de polinômios é comutativo. Num dos exercícios se pediu que você provasse que este produto é associativo, vamos resolver o tal exercício.

Considere tres polinômios:

$$P(x) = a_0 + a_1 x + \cdots + a_n x^n \overset{\phi}{\mapsto} p \in \mathcal{P}([a,b]) \tag{8.23}$$

$$Q(x) = b_0 + b_1 x + \cdots + b_m x^m \overset{\phi}{\mapsto} q \in \mathcal{P}([a,b]) \tag{8.24}$$

$$R(x) = c_0 + c_1 x + \cdots + c_l x^l \overset{\phi}{\mapsto} r \in \mathcal{P}([a,b]). \tag{8.25}$$

Primeiro vamos mostrar que esta representação ϕ é um isomorfismo: é bijetiva, preserva as operações. A bijetividade já foi discutida anteriormente.

- preserva a multiplicação Porque tanto PQ como pq são identificados pelo produto dos coeficientes, logo $\phi(PQ) = \phi(P)\phi(Q)$.
- preserva o elemento neutro da multiplicação Porque $\phi(1) = 1$ a função constante $x \mapsto 1$ se encontra ådireita enquanto que åesquerda, temos o polinômio de grau zero de coeficiente 1.
- preserva a adição Porque tanto $P + Q$ como $p + q$ são identificados pelo soma dos coeficientes, logo $\phi(P + Q) = \phi(P) + \phi(Q)$.
- preserva o elemento neutro da adição Porque $\phi(0) = 0$ a função constante $x \mapsto 0$ se encontra ådireita enquanto que åesquerda, temos o polinômio de grau zero de coeficiente 0. O polinômio nulo.

Sabemos que ϕ preserva as estruturas de $\mathbf{R}[x]$ e de $\mathcal{P}([a,b])$, mas ainda não discutimos que estrutura é esta. Quando soubermos qual é a estrutura de $\mathbf{R}[x]$, automaticamente teremos demonstrado, via isomorfismo, que a mesma estrutura vale em $\mathcal{P}([a,b])$. É esta outra vantagem dos isomorfismos.

- estrutura de $(\mathbf{R}[x], +)$. Como a soma é comutativa, associativa e tem um elemento neutro, e todo polinômio tem um inverso aditivo (que se obtem trocando os sinais de todos os coeficientes), então $(\mathbf{R}[x], +)$ é um grupo comutativo.
- estrutura de $(\mathbf{R}[x], \cdot)$. A única propriedade para que tenhamos um grupo, que não vale é a existência de um inverso multiplicativo. Chamamos esta estrutura de *monoide*. O produto é associativo, comutativo, e existe um elemento neutro para a multiplicação que é o polinômio de grau zero 1.
- O produto é distributivo relativamente åadição, que se prova facilmente usando a representação de $\mathbf{R}[x]$ em $\mathcal{F}([a,b])$.
- O produto do polinômio nulo por qualquer outro, produz o polinômio nulo.

Estas propriedades são idênticas àspropriedades de $(\mathbf{Z}, +, \cdot)$. Vemos assim que $(\mathbf{R}[x], +, \cdot)$ é um anel comutativo como os inteiros.

Consequentemente $(\mathcal{P}([a,b]), +, \cdot)$ é também um anel comutativo. Observe que aqui tivemos o cuidado de usar $\mathcal{P}$ porque o isomorfismo é

$$\mathbf{R}[x] \overset{\phi}{\to} \mathcal{P}([a,b]).$$

Os objetos isomorfos são $\mathbf{R}[x], \mathcal{P}([a,b])$. Como um é um anel, então o outro também o é.

Demonstramos assim:

Teorema **78** *Anel dos polinômios* $(\mathbf{R}[x], +, \cdot)$ *é um anel comutativo.*

e como corolário:

Teorema 79 *Anel das funções polinomiais*
$(\mathcal{P}([a,b]),+,\cdot)$ *é um anel comutativo.*

8.5 A divisão de polinômios

Como nos inteiros, a divisão no anel dos polinômios cria estruturas riquíssimas, exatamente porque não é "exata".

Vamos começar comparando com a divisão de números inteiros, porque foi assim que os nossos antepassados construiram a divisão de polinômios. No anel dos inteiros encontramos o "conjunto" dos restos na divisão por um determinado inteiro, por 5, digamos:

$$\mathbf{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

e a soma de restos se comporta algebricamente bem, veja a tabela operatória abaixo:

Tabuada com restos na divisão por 5.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Nós escrevemos $\overline{1}$ em vez de escrever 1 porque o resto 1 não é a mesma coisa que o número 1, inclusive a adição com restos não tem a mesma "tabuada" que a adição com números. Mas as propriedades são as mesmas:

1. A adição é comutativa.
2. A adição é associativa.
3. Existe um elemento neutro para a adição.
4. Todo resto tem um inverso aditivo.

Destas propriedades, a única que é trabalhosa é a associatividade uma vez que teriamos que analisar todos ternos $(a+b)+c = a+(b+c)$.

Mas se usarmos o *algoritmo da divisão euclidiana* esta demonstração fica simples, veja.

Vamos antes demonstrar um teorema que torna tudo simples, é a regra que permite passar do *resto da soma* para a *soma dos restos*.

Considere dois números inteiros x, y.

Chame $r_1 = resto_5[x]$; $r_2 = resto_5[y]$.

Podemos então escrever sucessivamente:

$$y = 5q + r_2 \tag{8.26}$$

$$x = 5q' + r_1 \tag{8.27}$$

$$x + y = 5q'' + r_2 + r_1 = 5q''' + r \ ; \ r = resto_5[r_1 + r_2] \tag{8.28}$$

$$resto_5[x+y] = resto_5[x] + resto_5[y] \tag{8.29}$$

A seqüência de equações acima mostra que *resto* preserva a adição dos inteiros, não é um *iso*morfismo porque não é identificação entre os dois conjuntos $\mathbf{Z}$ e o conjunto dos restos na divisão por 5 $\mathbf{Z}_5$. Temos então uma palavra menos forte para este caso, *morfismo*:

Definição 61 *Morfismo*

Um morfismo entre duas estruturas é uma representação que preserva a(as) operação(ões) entre as duas estruturas.

Como o *resto* preserva a adição na passagem de $\mathbf{Z}$ para $\mathbf{Z}_5$ então é um *morfismo*[4] *de grupos.*

Definição 62 *Morfismo de grupos*

Dados dois grupos $(G_1, o_1), (G_2, o_2)$ *uma função* $G_1 \xrightarrow{f} G_2$ *tal que*

- $f(ao_1b) = f(a)o_2f(b)$
- $f(e_1) = e_2$ *em que* e_1 *é o elemento neutro de* (G_1, o_1) *e* e_2 *é elemento neutro de* (G_2, o_2) *se chama um* morfismo de grupos.

E demonstramos assim o teorema:

Teorema **80** *Morfismo dos grupos* $(\mathbf{Z}, +), (\mathbf{Z}_5, +)$. *A função* $resto_5$ *é um morfismo de grupos.*

$$resto_5[x] + (resto_5[y] + resto_5[z]) = \tag{8.30}$$
$$\text{como } resto \text{ é morfismo de grupos:} \tag{8.31}$$
$$resto_5[x + (y + z)] = resto_5[(x + y) + z] \tag{8.32}$$
$$\text{porque a soma em } \mathbf{Z} \text{ é associativa} \tag{8.33}$$
$$\overline{x} + (\overline{y} + \overline{z}) = (\overline{x} + \overline{y}) + \overline{z} \tag{8.34}$$
$$\text{porque } resto_5 \text{ é um morfismo de grupos.} \tag{8.35}$$

Portanto $(\mathbf{Z}_5, +)$ é um grupo comutativo, como os inteiros, relativamente åsoma:

Teorema **81** $(\mathbf{Z}_5, +)$ *é um grupo comutativo*

Podemos ver que semelhanças deste tipo ocorrem na divisão com polinômios. Vamos estudar uma delas, construir um exemplo que mostrará como construir as congruências, inclusive no caso dos inteiros.

8.5.1 Os restos na divisão por $1 + x^2$.

Dados dois polinômios, definimos a divisão usando um algoritmo que é semelhante ao divisão de inteiros:

Definição 63 *Algoritmo da divisão euclidiana. Seja* P, D *dois polinô mios. Dizemos que o polinômio* Q *e o polinômio* R *são respectivamente o quocieente e o resto na divisão de* P *por* D *se e somente se*

$$P = DQ + R$$

[4] Há autores que insistem numa denominação antiga, *homomorfismo*

Esta expressão é uma cópia do algoritmo usado na divisão de inteiros. Para os inteiros a justificativa do algoritmo é a seguinte:

- Se P for divisível por D então o resto é zero e a expressão fica: $P = DQ$.
- Se P não for divisível por D então existe um múltiplo de D pelo inteiro m que é menor que P e outro que pelo inteiro $m+1$ que é maior do que P. Neste caso escolhemos o inteiro m como quociente e calculamos a diferença:

$$P - mD = R$$

- O número inteiro R é menor do que D, caso contrário poderiamos ter escolhido $m+1$ como quociente. Reescrevendo a última expressão vem a fórmula do algoritmo da divisão euclidiana:

$$P = mD + R \ ; \ 0 \leq R < D$$

quer dizer que os restos possíveis na divisão por D são

$$0, 1, \cdots, D-1.$$

Quando se foi fazer divisão com polinômios, se experimentou este algoritmo e deu certo. As regras são um pouco mais complicadas, porque temos que pensar no grau, em vez de "menor do que".

- Querendo dividir P por $1+x^2$ sabemos que o resto deve ter grau menor do que o do divisor, portanto R é um polinômio do primeiro grau:

$$R(x) = a + bx.$$

Se a divisão der exata, então:

$$P = (1+x^2)D \ ; \ \text{grau}(D) = \text{grau}(P) \text{ - } 2$$

- Se a divisão não der exata esta regra segue sendo obedecida. Então estamos procurando um polinômio cujo grau seja duas unidades menor do que o grau de P para ser o quociente, e um resto do primeiro grau.

Exemplo 50 *Uma divisão*

$$\begin{aligned}
(x^4+3x^3+x^2+x+1) \div (x^2+1) \\
x^4+3x^3+x^2+x+1 = (x^2+1)Q + R \\
x^4+3x^3+x^2+x+1 = (x^2+1)Q + ax + b \\
x^4+3x^3+x^2+x+1 = (x^2+1)(d_2x^2+d_1x+d_0) + ax + b \\
x^4+3x^3+x^2+x+1 = d_2x^4+d_1x^3+(d_0+d_2)x^2+d_1x+d_0+ax+b \\
x^4+3x^3+x^2+x+1 = d_2x^4+d_1x^3+(d_0+d_2)x^2+(d_1+a)x+(d_0+b) \\
d_2 = 1 \ ; \ d_1 = 3 \ ; \ d_0+d_2 = 1 \ ; \ d_1+a = 1 \ ; \ d_0+b = 1 \\
d_2 = 1 \ ; \ d_1 = 3 \ ; \ d_0 = 0 \ ; \ a = -2 \ ; \ b = 1 \\
x^4+3x^3+x^2+x+1 = (x^2+1)(x^2+3x) + (-2x+1) \\
\textit{o resto da divisão é} -2x+1
\end{aligned}$$

Podemos fazer as mesmas contas sem usar a variável[5] *Quando usamos apenas os coeficientes se* costuma *escrever os polinômios em potências crescentes, assim*

$$P \equiv (1,1,1,3,1) \equiv 1 + x + x^2 + 3x^3 + x^4$$

$$\begin{aligned}
(1,1,1,3,1) &\div (1,0,1) \\
(1,1,1,3,1) &= (1,0,1)Q + R \\
(1,1,1,3,1) &= (1,0,1)Q + (b,a) \\
(1,1,1,3,1) &= (1,0,1)(d_0,d_1,d_2) + (b,a) \\
(1,1,1,3,1) &= (d_0,d_1,d_0+d_2,d_1,d_2) + (b,a) \\
(1,1,1,3,1) &= (d_0+b,d_1+a,d_0+d_2,d_1,d_2) \\
d_2 = 1 \ ; \ d_1 = 3 \ ; \ d_0 + d_2 = 1 \ ; \ d_1 + a = 1 \ ; \ d_0 + b &= 1 \\
d_2 = 1 \ ; \ d_1 = 3 \ ; \ d_0 = 0 \ ; \ a = -2 \ ; \ b &= 1 \\
(1,1,1,3,1) &= (1,0,1)(0,3,1) + (1,-2) \\
\textit{o resto da divisão é } &(1,-2)
\end{aligned}$$

Quer dizer que o resto na divisão por (x^2+1) *é o conjunto de* **todos** *os polinômios do primeiro,* $\mathbf{R}_1[x]$*, ou todos os pares de números* $(a,b) \in \mathbf{R}^2$*. Observe as comparações que estamos fazendo, (mais representações...*

Vamos explorar um pouco mais este exemplo, veremos alguns fatos excitantes. Vamos fazer algumas contas:

Exercícios 40 *Cálculo com restos*

1. *Use o algoritmo da divisão euclidiana para calcular o resto de*

$$(a + bx)(c + dx)$$

   na divisão por $1 + x^2$

2. *congruência Tente estabelecer uma regra para as operações de soma e multiplicar com os restos:*

$$\overline{a + bx} + \overline{c + dx} \ ; \ (\overline{a + bx})(\overline{c + dx})$$

A resposta do último exercício é:

- Como os restos são polinômios do primeiro, então a soma dos restos é a soma dos dois polinômios do primeiro grau: $\overline{a + bx} + \overline{c + dx} = (a + c) + (b + d)x$
- No caso do produto, multiplicando os dois restos temos:

$$bdx^2 + (ad + bc)x + ac$$

que dividido por $x^2 - 1$ é:

bd	$(ad+bc)$	ac	1	0	1
$-bd$	0	$-bd$	bd		
0	$ad+bc$	$ac-bd$			

A regra que procuravamos é: o resto será: $(ad+bc)x+(ac-bd)$. Compare com a multiplicação de números complexos...

[5] Usar ou não a variável é uma questão de gosto.

Este conjunto, o dos restos de um polinômio qualquer na divisão por $1+x^2$ vai ser denominado $\mathbf{R}[x]/(1+x^2)$. Como os restos são classes de equivalência, a notação acompanha a idéia, temos um *conjunto quociente*. Ele é formado de todos os polinômios do primeiro grau e nele valem as regras operatórias que terminamos de descobrir.

Exercícios 41 *Congruências*

1. *Calcule as duas taboadas, de adição e de multiplicação para os restos na divisão por 5.*
2. *Verifique que* $(\mathbf{Z}_5,+,\cdot)$ *tem as mesmas propriedades que* $(\mathbf{Q},+,\cdot)$ *e portanto é um corpo.*
3. *classes de equivalência Observe que os restos são etiquetas, eles representam todos os números inteiros que deixam aqule resto na divisão. Apresente as classes de cada resto na divisão por 5, (*estas classes se chamam "classes módulo 5"*).*
4. *classes de equivalência Apresente todas as classes módulo 4, mó dulo 3, módulo 2.*
5. *Resolva a equação* $3x+4=2$ *em* $(\mathbf{Z}_5,+,\cdot)$.
6. *Calcule as duas taboadas, de adição e de multiplicação para os restos na divisão por 4.*
7. *Verifique que* $(\mathbf{Z}_4,+,\cdot)$ *não tem as mesmas propriedades que* $(\mathbf{Z}_5,+,\cdot)$, *verifique qual a propriedade que falha. Verifique que em* $\mathbf{Z}_4$ *é possível encontrar* $x\neq 0, y\neq 0$ *tal que* $xy=0$. *Chamam-se divisores de zero.*
8. *Verifique que* $(\mathbf{Z}_6,+,\cdot)$ *não tem as mesmas propriedades que* $(\mathbf{Z}_5,+,\cdot)$, *verifique qual a propriedade que falha. Verifique que em* $\mathbf{Z}_6$ *é possível encontrar* $x\neq 0, y\neq 0$ *tal que* $xy=0$. *Chamam-se divisores de zero.*
9. *Verifique que* $(\mathbf{Z}_7,+,\cdot)$ *tem as mesmas propriedades que* $(\mathbf{Q},+,\cdot)$ *e portanto é um corpo.*
10. *Resolva a equação* $5x+4=3$ *em* $(\mathbf{Z}_7,+,\cdot)$.
11. *Defina um isomorfismo entre os restos na divisão por* x^2+1 *do conjunto de todos os polinômios e o conjunto* $\mathbf{R}^2$. *Naturalmente agora você sabe somar e multiplicar em* $\mathbf{R}^2$. *Calcule*

    $(1,2)+(3,4)\quad (1,2)(3,4)\quad (1,0)(1,0)\quad (0,1)(0,1)$

    Compare com as operações dos números complexos.
12. *Prove*[6] *que em* $\mathbf{R}[x]/(x^2+1)$ *existe um elemento neutro para multiplicação e que para todo resto* $a+bx$ *existe outro resto* $c+dx$ *tal que* $(a+bx)(c+dx)=1$.
13. *Prove que* $\mathbf{R}[x]/(x^2+1)$ *é um corpo, quer dizer, que* $(\mathbf{R}^2,+,\cdot)$ *em que a adição é aquela definida pelo isomorfismo, assim como o produto, é um corpo.*

    Este corpo, definido com o conjunto $\mathbf{R}^2$ *tem uma representação geométrica, é o plano, é o conjunto dos números complexos.*

[6] se voce usar apenas os coeficientes e a regra operatória já descoberta, fica tudo mais fácil.