

1 Anéis e corpos

Esta semana discutiremos o conceito de anéis. Eles são fundamentais em diversas áreas da matemática, e também são o primeiro passo para entendermos a tecnologia que permite classificar grupos (abelianos) de ordem infinita.

Definição 1. Um **anel** é um conjunto R munido de duas operações $+$ e $\cdot$, que satisfaz as seguintes propriedades:

- 1) $(R, +)$ é um grupo abeliano.
- 2) Vale a associatividade para a multiplicação:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

- 3) Vale a distributividade com respeito a soma:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Se, além disso, valerem as seguintes propriedades:

- 4) $a \cdot b = b \cdot a$, para todo $a, b \in R$, diremos que R é **comutativo**.
- 4) Se existir $1 \in R$, talque $1 \cdot a = a \cdot 1 = a$, para todo $a \in R$, diremos que R é **anel com identidade**.

Omitiremos frequentemente a notação " $\cdot$ " para denotar a multiplicação em um anel. Isto é, escreveremos ab para denotar $a \cdot b$. Quando quisermos enfatizar as operações do anel R , escreveremos o anel como $(R, +, \cdot)$.

Exemplo 1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ com a soma e produto usuais são exemplos de anéis comutativos com identidade.

Exemplo 2. O conjunto dos restos módulo n , $\mathbb{Z}_n$, com a soma e produto usuais é um anel comutativo com identidade.

Exemplo 3. O conjunto das matrizes de ordem n sobre com coeficientes em um anel comutativo R , denotado por $M(n, R)$ é um anel com identidade, quando consideramos a soma e produto usual de matrizes, mas não é comutativo.

Exemplo 4. Seja R um anel comutativo com identidade. O conjunto dos polinômios com coeficientes em R , dado por:

$$R[x] := \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n; a_i \in R\},$$

com a soma e produto usual de polinômios é um anel comutativo com identidade.

Exemplo 5. O conjunto dado por:

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

é um anel, conhecido como **anel dos inteiros de Gauss**.

Definição 2. Seja $(R, +, \cdot)$ um anel. $a \in R$ é dito **divisor de zero à esquerda**, se $a \neq 0$ e existe $b \in R \setminus \{0\}$ tal que $ab = 0$. Analogamente definimos divisores de zero a direita. $a \in R$ é dito **invertível à esquerda**, ou se $a \neq 0$ e existe $b \in R$ tal que $ba = 1$. Analogamente definimos invertíveis à direita. Um elemento que é invertível a esquerda e a direita é dito **unidade** do anel R . O conjunto de todas as unidades de R é denotado por R^* .

Exemplo 6. O elemento $A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$, é um divisor de zero à esquerda em $M(2, \mathbb{Z})$.

Definição 3. Um **domínio**, ou **domínio de integridade** ou ainda **anel de integridade** é um anel comutativo com identidade e sem divisores de zero. Um anel R é dito **anel de divisão**, se $(R \setminus \{0\}, \cdot)$ for um grupo. Um **corpo** é um anel de divisão comutativo.

Exemplo 7. $\mathbb{Z}$ é um domínio, mas não é corpo. $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos.

O próximo teorema é de fácil verificação.

Teorema 1. *Seja $(R, +, \cdot)$ um anel. Então valem as seguintes propriedades:*

1. *Se R é anel com identidade então 1 é único.*
2. *Se R tem mais de um elemento, e R possui identidade então $1 \neq 0$.*
3. *Se R é um anel que vale a lei do cancelamento a esquerda, então R não tem divisores de zero a esquerda. Analogamente para divisores de zero a direita.*

Podemos agora definir os homomorfismos de anéis, que são funções entre anéis que preservam sua estrutura.

Definição 4. Sejam $(R, +_R, \cdot_R), (S, +_S, \cdot_S)$ anéis e $f : R \rightarrow S$ uma função. Diremos que f é um **homomorfismo de anéis**, se f satisfizer:

- 1) $f(a +_R b) = f(a) +_S f(b), \forall a, b \in R.$
- 2) $f(a \cdot_R b) = f(a) \cdot_S f(b), \forall a, b \in R.$

Monomorfismos, epimorfismos e automorfismos são definidos de maneira análoga a de grupos. Alguns autores chamam um monomorfismo $R \rightarrow S$ de **mergulho**.

Exemplo 8. Seja $f : \mathbb{Z} \rightarrow M(2, \mathbb{Z})$ dada por $f(a) = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$, é um mergulho.

Exemplo 9. Seja $f : \mathbb{Z} \rightarrow \mathbb{Z}_m$ dada por $f(a) = \bar{a}$, é um epimorfismo.

As seguintes propriedades são fácil verificação.

Teorema 2. *Seja $f : R \rightarrow S$ um homomorfismo de anéis. Então temos:*

- a) $f(0_R) = 0_S$
- b) $f(-a) = -f(a)$

c) Se R tem identidade, então $f(1_R) = 1_{f(R)}$.

d) Se a é uma unidade de R então $f(a^{-1}) = f(a)^{-1}$.

Analogamente ao caso do kernel de homomorfismos de grupos, se $f : R \rightarrow S$ é um homomorfismo de anéis, dizemos que o conjunto $\ker f := \{a \in R; f(a) = 0_S\}$ é dito kernel (ou núcleo) de f .

Análogo ao estudo de subgrupos e subgrupos normais, veremos a seguir o conceito de subanel e de ideal de um dado anel.

Definição 5. Sejam R um anel, $S \subset R$ um subconjunto de R . Diremos que S é **subanel** de R se S for um anel com as operações induzidas de R e também for fechado para as operações de soma e produto de R .

Definição 6. Sejam R um anel, $S \subset R$ um subconjunto de R . Diremos que S é **ideal à esquerda** de R , denotado por $S \triangleleft_e R$ se S for um subanel, e além disso, para todo $r \in R$ e todo $s \in S$ temos $rs \in S$. Analogamente, S será ideal à direita se S for subanel e $sr \in S$ para todo $r \in R$ e todo $s \in S$. I é dito **ideal bilateral**, ou simplesmente ideal de R se I for um ideal a esquerda e a direita.

Exemplo 10. É fácil ver 0 e R são ideais de R . 0 é dito **ideal trivial** de R .

Exemplo 11. É fácil ver que para todo $n \in \mathbb{Z}$, o grupo cíclico $\langle n \rangle$ é um ideal de $\mathbb{Z}$.

Exemplo 12. Não é difícil ver que para todo se $f : R \rightarrow S$ é um homomorfismo de anéis, então $\ker f$ é um ideal de R . Podemos ver que $\text{Im} f$ é um subanel de S .

Exemplo 13. Note que $\mathbb{Z} \subset \mathbb{Q}$ é um subanel, mas não um ideal.

Exemplo 14. Sejam R um anel, e considere o conjunto $Z(R) := \{a \in R; ax = xa \forall x \in R\}$, dito centro de R . É fácil ver que o centro sempre é um subanel de R , mas podemos construir exemplos onde $Z(R)$ não é ideal.

A seguinte caracterização de ideal será muito importante no que se segue. Sua verificação é imediata.

Teorema 3. *Seja R um anel, e $I \subset R$ um subconjunto. Então I é um ideal à esquerda de R se, e somente se, satisfaz as seguintes propriedades:*

1. *Para todos $a, b \in I$, tem-se que $a - b \in I$.*
2. *Para todo $a \in I$ e $r \in R$, tem-se que $ra \in I$.*

Ideais desempenham um papel semelhante ao de subgrupos normais em grupos. Com eles podemos definir a noção de anel quociente. De fato sejam R um anel, e I um ideal. Como $(R, +)$ é um grupo abeliano, e I é um subgrupo e portanto normal, segue que R/I é um grupo abeliano. O que podemos provar é que de fato R/I é um anel, dito **anel quociente** de R por I .

Teorema 4. *Sejam R um anel e M um ideal. São equivalentes:*

- 1) *M é maximal.*
- 2) *R/M não possui ideais bilaterais não triviais.*
- 3) *Para todo $x \in R \setminus M$, temos que $(x) + M = R$.*

Demonstração. 1) $\implies$ 2). Seja I/M um ideal de R/M . Pelo Teorema da correspondência temos que $M \subset I$. Por definição de ideal maximal temos $R = I$ ou $M = I$. Assim I/M é trivial.

2) $\implies$ 3). Para todo $x \in R \setminus M$, temos que $I = (x) + M$ é ideal de R que contém M e é diferente de M . Assim, I/M ideal não nulo de R/M , pois $x \notin M$ e $x \in I$. Assim por 2) segue que $R/M = (x) + M/M$, e portanto $R = (x) + M$.

3) $\implies$ 1). Seja I um ideal tal que $M \subset I$. Suponha $x \in I \setminus M$. Temos como $(x) \subset I$ e também $M \subset I$ temos $(x) + M \subset I$, mas por 3) temos que $(x) + M = R$, e portanto $R = I$, e então M é maximal. $\square$

De posse desse Teorema, podemos provar seguinte resultado que usaremos extensivamente no futuro.

Corolário 1. *Seja R um anel comutativo com identidade. Então um ideal M é maximal se, e somente se R/M é corpo.*

Demonstração. Se R/M é corpo seus únicos ideais são 0 e R/M , segue que M é maximal da equivalência com o item 2) do teorema anterior.

Suponha que M seja maximal. E considere $a + M \in R/M$. Queremos provar que $a + M$ admite inverso. Como $a \notin M$ temos pelo item 3) do teorema anterior que $(a) + M = R$. Assim, existem $b \in R$ e $m \in M$ tal que $1 = ba + m$, o que implica que $1 - ba \in M$, e logo $1 + M = ba + M$ e portanto $1 = (b + M)(a + M)$. Como queríamos.

2 Anéis de polinômios e critérios de irreduzibilidade

Nessa seção discutiremos os anéis de polinômios, pois eles fornecem exemplos concretos da teoria que desenvolvemos até aqui, além de serem ubíquos em toda matemática.

Vimos nas notas sobre anéis que o anel de polinômios na variável x sobre um anel R , denotado por $R[x]$, pode ser definido como o conjunto de símbolos $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$; $a_i \in R$. Vamos recapitular aqui as operações que tornam $R[x]$ um anel.

Definição 7. Sejam $p, q \in R[x]$, tais que $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ e $q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$. Diremos:

1. Que $p = q$ se $m = n$ e $a_i = b_i$ para todo i .
2. Que $(p + q)(x) = c_0 + c_1x + c_2x^2 + \cdots + c_ex^e$, onde $e = \max\{n, m\}$ e $c_i = a_i + b_i$, com $a_i = 0$ se $i \geq n + 1$ e $b_i = 0$ se $i \geq m + 1$.
3. Que $(p \cdot q)(x) = d_0 + d_1x + d_2x^2 + \cdots + d_fx^f$ com $f = m + n$ e $d_t = a_0b_t + a_1b_{t-1} + \cdots + a_tb_0$ onde $a_i = 0$ se $i \geq n + 1$ e $b_i = 0$ se $i \geq m + 1$.

Com as operações acima definidas, temos que $R[x]$ é anel.

A seguinte definição será útil.

Definição 8. Seja $p(x) = a_0 + a_1x + \cdots + a_nx^n$, com $a_n \neq 0$, então diremos que o **grau** de f é n , e denotaremos por $\deg f$ e a_n é dito o **coeficiente líder** de p .

Exemplo 15. Sejam $f(x) = 2x^2 + \pi x^3 \in \mathbb{C}[x]$, então o coeficiente líder de f é π e $\deg f = 3$.

Temos a seguinte importante propriedade sobre o grau de um polinômio.

Teorema 5. Se $f, g \in R[x]$, temos que $\deg(f + g) \leq \max\{\deg f, \deg g\}$ e $\deg(fg) \leq \deg f + \deg g$, se R for domínio, então $\deg(fg) = \deg f + \deg g$

Demonstração. Sejam $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$, com $a_n \neq 0 \neq b_m$. Note que pela Definição 7. Seja $e = \max\{n, m\}$ temos que o e -ésimo coeficiente de $f + g$ é $a_e + b_e$, assim, se $a_e + b_e \neq 0$ temos que $a_e + b_e$ é o coeficiente líder de $f + g$, e portanto $\deg(f + g) = \max\{n, m\}$, se $a_e + b_e = 0$ temos que o coeficiente líder de $f + g$ é $a_t + b_t$ com $t < \max\{n, m\}$, e assim $\deg(f + g) < \max\{n, m\}$ de onde vem o resultado.

Analogamente, note que podemos escrever $(f.g)(x) = d_0 + d_1x + d_2x^2 + \cdots + d_{m+n}x^{m+n}$ com $d_t = a_0b_t + a_1b_{t-1} + \cdots + a_tb_0$ e $d_{m+n} = a_nb_m$. Assim $\deg(f.g) \leq \deg f + \deg g$. Se R é domínio temos que $a_nb_m \neq 0$ e assim $\deg(f.g) = \deg f + \deg g$. $\square$

Em particular, é claro da demonstração acima que

Corolário 2. Se R é domínio então $R[x]$ é domínio.

Segue que se f divide g em $R[x]$ teremos que $\deg f \leq \deg g$. Então para que $\deg$ nos dê uma norma euclidiana em $R[x]$ teremos que encontrar um algoritmo de divisão com respeito a $\deg$. Para isso precisaremos de hipóteses adicionais em R e do seguinte teorema.

Teorema 6. Sejam R um domínio, e $f, g \in R[x]$, com $\deg f = m$ e $\deg g = n$, e $k = \max\{m - n + 1, 0\}$ e $b = b_n \neq 0$ o coeficiente líder de g . Então existem únicos $q, r \in R[x]$ tais que $b^k.f(x) = q(x)g(x) + r(x)$. Com $r(x) = 0$ ou $\deg r < \deg g$

Demonstração. Existência: Se $m < n$ basta tomar $q = 0$ e $r = f$. Assim podemos assumir que $m \geq n$. Procederemos por indução em m . Se $m = 0$ não há nada a fazer. Suponha que o enunciado seja verdadeiro para todo polinômio de grau menor que m e vamos provar que vale para todo polinômio de grau m .

Seja $a \neq 0$ o coeficiente líder de f . O polinômio $ax^{m-n}g(x)$ tem grau m com coeficiente líder igual a $a \cdot b$, note que $b \cdot f(x)$ também é um polinômio de grau m com coeficiente líder $a \cdot b$. Assim $ax^{m-n}g(x) - b \cdot f(x)$ é um polinômio de grau m' estritamente menor que m . Logo, pela hipótese de indução, existem $q_1, r_1 \in R[x]$ e $k' = \max\{(m-1) - n + 1, 0\} = \max\{m-n, 0\}$ tais que $b^{k'} \cdot (ax^{m-n}g(x) - bf(x)) = q_1(x) \cdot g(x) + r_1(x)$ com $\deg r_1 < \deg g$, ou $r_1 = 0$. De onde segue que $b^k f(x) = (ax^{m-n} + q_1(x))g(x) + r_1(x)$. Assim basta tomar $q(x) = (ax^{m-n} + q_1(x))$ e $r(x) = r_1(x)$.

Unicidade: Suponha que existam q_1, q_2, r_1, r_2 satisfazendo as condições do teorema, tais que $b^k \cdot f = q_1 g + r_1 = q_2 g + r_2$, isto é, $(q_1 - q_2) \cdot g = r_1 - r_2$. Se $q_1 \neq q_2$, teríamos por um lado $\deg(q_1 - q_2) \cdot g \leq \deg(q_1 - q_2) + \deg g \geq n$ e $\deg(r_1 - r_2) \leq \max\{\deg r_1, \deg r_2\} < n$ o que é absurdo.

Pela existência e unidade, temos nosso resultado. $\square$

Uma observação que será útil no que segue é que as unidades de $R[x]$ coincidem com as unidades de R .

Definição 9. Sejam R um anel comutativo com identidade, e $f \in R[x]$. Diremos que f é **irredutível sobre** R , se f for um elemento irredutível do anel $R[x]$. Isto é, f é irredutível se, $f = r \cdot s$ implicar que $r \in R[x]^*$ ou $s \in R[x]^*$. Se $f = r \cdot s$ com r e s não unidades, diremos que f é **redutível** e que r, s são **fatores** de f .

Veremos que o conceito de irredutibilidade de um polinômio sobre um anel está intimamente ligado ao fato de ele possuir raízes.

Definição 10. Sejam $f \in R[x]$, com $f = a_0 + a_1x + \cdots + a_nx^n$, e $b \in R$. Diremos que $f(b) = a_0 + a_1b + \cdots + a_nb^n$ é o **valor** de f em b . Diremos que $a \in R$ é **raíz** de f se $f(a) = 0$.

Teorema 7. *Sejam D um domínio, $f \in D[x]$ e $a \in D$. Então o resto da divisão de f por $x - a$ é $f(a)$.*

Demonstração. Como $x - a$ é um polinômio não nulo de $D[x]$, segue que existem q, r tais que $f(x) = q(x)(x - a) + r(x)$ com $r(x) = 0$ ou $\deg r < \deg(x - a) = 1$. Assim, ou $r(x) = 0$, ou $\deg r = 0$ e portanto $r \in D$. Mas, $f(a) = (q(a)(a - a)) + r$ Assim $f(a) = r$. $\square$

Teorema 8. *Sejam D um domínio e $f \in D[x]$. Então $a \in D$ é raiz de f se, e somente se, $x - a$ é fator de f .*

Demonstração. Se $x - a$ é fator de f , é claro que $f(a) = 0$. Vamos provar a outra direção. Seja a uma raiz de f . Assim $f(a) = 0$. Pelo Teorema 7, segue que $f(x) = q(x)(x - a) + f(a)$. Como $f(a) = 0$, segue que $f(x) = q(x)(x - a)$, logo $(x - a)$ divide $f(x)$. $\square$

Corolário 3. *Sejam D um domínio e $f \in D[x]$, se f possui raiz em D , então f é redutível.*

Note que irredutibilidade depende do anel R . Por exemplo, $f(x) = x^2 + 1$ é irredutível em $\mathbb{R}[x]$ mas não é em $\mathbb{C}[x]$, uma vez que $f(x) = (x - i)(x + i)$.

O polinômio $(x - 1)^2$ tem como raiz apenas o número 1, mas como $(x - 1)^2 = (x - 1)(x - 1)$, é como se o 1 “aparecece duas vezes” no conjunto de todas as raízes de $(x - 1)^2$. Isso motiva a seguinte:

Definição 11. Sejam R um anel comutativo com identidade, e $f \in R[x]$. Diremos que $a \in R$ é **raiz múltipla**, ou **raiz com multiplicidade m** , se $m \geq 2$ e $(x - a)^m$ divide f .

O seguinte teorema é uma interessante versão mais fraca do Teorema Fundamental da Álgebra, e será deixado como exercício ao leitor.

Teorema 9. *Sejam D um domínio, e $f \in D[x]$. Então f possui no máximo $\deg f$ raízes distintas em D .*

Gostaríamos de focar nossa atenção a pergunta “Quando $D[x]$ é um domínio de fatoração única” no caso em que D não é um corpo. Para que

possamos fazer isso, precisamos primeiro definir o corpo de frações de um domínio.

Sejam D um domínio, e considere $S = D \times (D \setminus \{0\})$. Definimos em S a relação $\sim$ dada por: $(a, b) \sim (c, d)$ se, e somente se, $ad = cb$. É fácil ver que $\sim$ é uma relação de equivalência. Note que podemos escrever os elementos de S como $\frac{a}{b}$, com $a \in D$ e $b \in D \setminus \{0\}$. Essa notação será mais conveniente para nossos propósitos. Agora vamos colocar em S uma estrutura de anel. Para isso, vamos definir uma operação de soma e de produto. Dados $\frac{a}{b}$, com $a \in D$ e $b \in D \setminus \{0\}$ e $\frac{c}{d}$, com $c \in D$ e $d \in D \setminus \{0\}$, diremos que $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$ e $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

Nosso primeiro passo será mostrar que as operações estão bem definidas.

Lema 1. *As operações acima definidas em S estão bem definidas.*

Demonstração. Faremos apenas a soma, a multiplicação é inteiramente análoga e será deixada ao leitor.

Dados $\frac{a}{b}, \frac{c}{d}, \frac{e}{f}, \frac{g}{h} \in S$, tais que $\frac{a}{b} = \frac{c}{d}$ e $\frac{e}{f} = \frac{g}{h}$. Isso implica que $ad = cb$ e que $eh = fg$. Queremos provar que

$$\frac{a}{b} + \frac{e}{f} = \frac{c}{d} + \frac{g}{h},$$

Mas isso ocorre se, e somente se, $dh(af + be) = fb(ch + dg)$. Mas veja que $dh(af + be) = dha f + dhbe = cbhf + dbfg = fb(ch + dg)$ como queríamos.

A demonstração da boa definição do produto é análoga e por isso fica como exercício. $\square$

Podemos por fim, demonstrar o critério de Eisenstein, que é um dos critérios de irredutibilidade mais úteis para os nossos trabalhos. Para isso, focaremos nossa atenção. Antes, vamos definir a noção de polinômios mônicos.

Definição 12. Sejam R um anel com identidade e $f \in R[x]$. f é dito **mônico** se o coeficiente líder de f é a identidade de R .

Exemplo 16. $f(x) = x^{2023} + 3x^{1984}$ é mônico em $\mathbb{Z}[x]$.

Teorema 10 (Critério de Eisenstein). *Sejam D um domínio de fatoração única e $f \in D[x]$. Se p é um primo de D tal que p divide cada um dos coeficientes de f , mas p não divide a_n e p^2 não divide a_0 , então f é irredutível em $D[x]$, logo irredutível em $\text{cfr}(D)[x]$.*

Demonstração. Como f é mônico e portanto primitivo, temos que $c(f) = 1$. Então pelo lema de Gauss, vemos que se $f(x) = g(x)h(x)$ podemos supor que g e h são primitivos com coeficientes em D , e ademais, que g e h são mônicos. Agora, escrevamos $g(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$ e $h(x) = x^k + c_{k-1}x^{k-1} + \cdots + c_0$, note que $a_0 = b_0c_0$ e portanto b_0 e c_0 não podem ambos serem divisíveis por p , uma vez que p^2 não divide a_0 . Sem perda de generalidade, suponha que p divide b_0 (logo p não divide c_0), e seja r o menor inteiro tal que p não divide b_r . Note que temos:

$$a_r = b_rc_0 + b_{r-1}c_1 + \cdots + b_0c_r,$$

como p divide b_i para $0 \leq i \leq r-1$, temos que p divide $b_{r-1}c_1 + \cdots + b_0c_r$, mas como p não divide c_0 nem b_r , segue que p não divide c_0b_r e então p não divide a_r o que é absurdo. Logo f é irredutível em $D[x]$, e pelo Lema de Gauss, temos que f é irredutível em $\text{cfr}(D)[x]$. $\square$

O critério de Eisenstein nos dá um método eficiente para determinar quando um polinômio é irredutível.

Exemplo 17. É fácil ver que $x^2 + 7x + 21$ e $x^{87} - 2021x^{65} + 43$ são irredutíveis em $\mathbb{Q}$.

O critério de Eisenstein nos dá uma prova muito rápida de que $\sqrt[n]{p}$ com n natural e p primo não é racional. De fato, o polinômio $x^n - p$ é irredutível em $\mathbb{Q}[x]$, pelo critério de Eisenstein, e então $x^n - p$ não possui solução em $\mathbb{Q}$ e logo $\sqrt[n]{p}$ não é racional.

Exemplo 18. Vamos mostrar que $x^2 + y^2 - 1$ é irredutível em $\mathbb{Q}[x, y]$. De fato, note que $\mathbb{Q}[x, y] \simeq \mathbb{Q}[x][y]$ e assim podemos ver $f(x, y) = y^2 + (x^2 - 1)$ como um polinômio com variável y com coeficientes em $\mathbb{Q}[x]$. Neste caso, o “termo constante” de f é $x^2 - 1 = (x - 1)(x + 1)$. Como $(x - 1)$ é primo

(Prove!!) note temos que f é mônico, $(x - 1)$ divide $(x^2 - 1)$ e $(x - 1)^2$ não divide $x^2 - 1$, assim, pelo critério de Eisenstein, f é irredutível.

Exercícios

1. Seja F um corpo. É verdade que $F[x]$ é corpo?
2. * Mostre que se $R[x]$ é um domínio euclidiano então R é um corpo.
3. Dê exemplos de E e D domínios, tais que $E \subset D$, e $f \in E[x]$ é redutível mas $f \in D[x]$ não é. Dê também exemplo de $f \in D[x]$ irredutível, com $f \in E[x]$ redutível.
4. Prove o Teorema 9.
5. Mostre que a hipótese de o anel ser domínio em no Teorema 9 não pode ser melhorada.
6. Sejam D um domínio, e F um corpo tal que $D \subset F \subset cfr(D)$, prove que $F = cfr(D)$.
7. Prove que $x^3 + (1329!)x^2 + 3002x + 12001$ é irredutível $\mathbb{Q}[x]$.
8. Prove que se p é primo e $\Phi_p = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$ então Φ_p é irredutível em $\mathbb{Q}[x]$.
9. * Prove que $f(x, y, z) = x^2 + y^2 + z^2 \in \mathbb{Z}[x, y, z]$ é irredutível em $\mathbb{Q}[x, y, z]$