

1 Domínios, anéis Noetherianos e Teorema da Base de Hilbert

Nessas notas discutiremos como o conceito de anéis generaliza as noções que tínhamos para os números inteiros. Nessa seção todos os anéis serão comutativos com identidade.

Definição 1. Sejam D um domínio e $a, b \in D$. diremos que a **divide** b , se existe $x \in D$, tal que $b = a.x$. Caso contrário, diremos que a **não divide** b . Diremos que a e b são **associados**, se existe uma unidade $u \in D^*$ tal que $a = u.b$. Neste caso, denotaremos $a \sim b$.

Não é difícil ver que $\sim$ define em D uma relação de equivalência, ou seja é simétrica, reflexiva e transitiva. Além disso é fácil provar que :

Teorema 1. *Seja D um domínio, então para todos $a, b, c \in D$ temos:*

1. a divide a .
2. a divide b e b divide c , então a divide c .
3. a divide b e b divide a , então $a \sim b$.

A essa altura, é claro que $\mathbb{Z}$ é um domínio, e que o conceito de divisibilidade que acabamos de introduzir tem por objetivo mimicar a divisão em $\mathbb{Z}$.

Definição 2. Sejam D um domínio, e $a, b \in D$. Dizemos que a é um **divisor próprio** se $a \in D \setminus D^*$ e existe $x \in D \setminus D^*$ tal que $b = ax$. Um elemento $q \in D$ é dito **irredutível** se q não é nulo, e nem uma unidade de D , e além disso q não possui divisores próprios. $p \in D$ é dito **primo** se p não é nulo, e nem uma unidade de D , e além disso, para quaisquer $a, b \in D$ tais que p divide ab temos que p divide a , ou p divide b .

Teorema 2. *No anel $\mathbb{Z}$, os conceitos de elemento irredutível e elemento primo coincidem.*

Demonstração. Temos que provar que se $p \in \mathbb{Z}$ é um elemento primo, se, e somente se p é irredutível. Assuma que p é irredutível, e considere $a, b \in \mathbb{Z}$ tal que p divide $a.b$, e ademais que p não divide a . Como p é irredutível, temos que a não divide p , e assim o máximo divisor comum entre a e p é 1, e pelo Teorema de Bezout para os inteiros temos que existem x e y tal que $1 = ax + py$, assim $b = axb + pyb$, como p divide pyb e p divide axb por hipótese, segue que p divide b e assim p é primo.

Suponha agora que p é primo, e que exista $a \in \mathbb{Z}$ tal que a divide p . Assim existe $b \in \mathbb{Z}$ tal que $p = ab$. Assim, p divide ab , e como p é primo, segue que p divide a ou p divide b . Se p divide a temos que $p \sim a$, e temos o resultado. Se p divide b significa que existe $x \in D$ tal que $b = px$, daí teríamos que $p = ab = apx$, e portanto $ax = 1$ e assim $a \in D^*$. De onde também segue o resultado. $\square$

Note que, de fato a segunda parte da demonstração acima produz o seguinte resultado.

Corolário 1. *Seja D um domínio. Se $p \in D$ é primo, então p é irredutível.*

A recíproca desse corolário nem sempre é verdadeira, na demonstração do Teorema 2, usamos fortemente o teorema de Bezout, assim, fica claro que precisamos generalizar para o ambiente de anéis o conceito de divisão euclidiana.

Definição 3. Seja D um domínio. Uma função $N : D \setminus \{0\} \rightarrow \mathbb{N}$ é dita **norma euclidiana** se para todo $a, b \in D$, com $b \neq 0$, temos:

1. Se b divide a e $a \neq 0$ então $N(a) \leq N(b)$.
2. Existem $q, r \in D$, tais que $a = qb + r$, com $N(r) < N(b)$ ou $r = 0$.

Um domínio munido de uma norma euclidiana é dito **domínio euclidiano**, e frequentemente denotado por (D, N) , onde N é sua norma.

Exemplo 1. O anel $\mathbb{Z}$ munido da função $N : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ dada por $N(x) = |x|$ é um domínio euclidiano.

A seguinte proposição nos dá uma útil caracterização das unidades de um domínio euclidiano.

Proposição 1. *Seja (D, N) um domínio euclidiano. Então:*

$$D^* := \{d \in D; N(d) = N(1)\}.$$

Demonstração. Vamos primeiro provar que toda unidade tem norma 1. Se $d \in D$ é uma unidade, então existe $x \in D$ tal que $dx = 1$ assim temos que d divide 1 e portanto $N(d) \leq N(1)$. Como 1 divide d , pois $d = d.1$ temos que $N(1) \leq N(d)$, de onde segue que $N(d) = N(1)$. Por outro lado, seja $d \in D$ tal que $N(d) = N(1)$. Pela segunda propriedade da norma temos que $1 = qx + r$, com $r = 0$ ou $N(r) < N(1)$. Mas se $r \neq 0$, como $r = 1.r$, teríamos pela primeira propriedade da norma que $N(1) \leq N(r) < N(1)$, o que é absurdo. Logo $r = 0$, ou seja $1 = qd$ e portanto $d \in D^*$. $\square$

Podemos agora construir um exemplo de um anel que possui elementos irredutíveis que não são primos.

Exemplo 2. Seja $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5}, a, b \in \mathbb{Z}\}$. É fácil ver que $\mathbb{Z}[\sqrt{-5}]$ é um anel com as operações de soma e produto usuais. Defina em $\mathbb{Z}[\sqrt{5}]$ a seguinte **função**: $N : \mathbb{Z}[\sqrt{-5}] \setminus \{0\} \rightarrow \mathbb{N}$, $N(a + b\sqrt{-5}) = a^2 + 5b^2$, que nada mais é do que a norma usual de um número complexo, restrita a $\mathbb{Z}[\sqrt{-5}]$. N **NÃO** é uma norma, como veremos mais adiante, mas ainda assim ela servirá aos nossos propósitos. Além disso é fácil verificar que $N(xy) = N(x).N(y)$ para quaisquer $x, y \in \mathbb{Z}[\sqrt{-5}]$, e que N satisfaz as propriedades da Proposição 1.

Afirmção 1: $3 \in \mathbb{Z}[\sqrt{-5}]$ é irredutível. Como $N(3) = 9 \neq 1 = N(1)$, temos pela Proposição 1 que 3 não é uma unidade de $\mathbb{Z}[\sqrt{-5}]$. Sejam $x, y \in \mathbb{Z}[\sqrt{-5}]$ tal que $3 = xy$. Suponha ainda que x seja divisor próprio de 3. Assim x não é unidade e portanto $N(x) > 1$. Como $3 = xy$, temos que $N(3) = N(x).N(y)$ o que implica que $N(x) = 3$ ou $N(x) = 9$. Se $N(x) = 3$ teríamos que existem $a, b \in \mathbb{Z}$, tal que $x = a + b\sqrt{-5}$ tal que $3 = N(x) = a^2 + 5b^2$. Mas essa equação não admite solução inteira, logo $N(x) \neq 3$. Se $N(x) = 9$, temos que $N(y) = 1$, e assim $x \sim 3$, o que é uma contradição pois assumimos que x era

um divisor próprio de 3. Logo 3 é irredutível.

Afirmção 2: $3 \in \mathbb{Z}[\sqrt{5}]$ não é primo. Note que:

$$9 = 3 \cdot 3 = (2 + \sqrt{5})(2 - \sqrt{5}).$$

Assim temos que 3 divide $(2 + \sqrt{5})(2 - \sqrt{5})$ mas 3 não divide $(2 + \sqrt{5})$, nem $(2 - \sqrt{5})$. Logo 3 não é primo em $\mathbb{Z}[\sqrt{5}]$.

Note que no exemplo anterior, o que nos ajudou a mostrar que 3 não era um número primo foi o fato de que 9 possuía duas fatorações por elementos irredutíveis distintas. Lembre-se que graças ao Teorema Fundamental da Aritmética, e ao Teorema 2, em $\mathbb{Z}$ isso não ocorre, isto é, em $\mathbb{Z}$ cada elemento admite uma fatoração única por elementos irredutíveis. Veremos a seguir como generalizar esse conceito para outros anéis.

Definição 4. Sejam D um domínio e $a \in D$ tal que $a \neq 0$. Diremos que $a = p_1 \cdot p_2 \cdots p_n$ é uma **fatoração** de a quando cada um dos p_i 's forem elementos irredutíveis de D e $p_i \neq p_j$ se $i \neq j$. Diremos que duas fatorações de $a = p_1 \cdots p_n = q_1 \cdots q_m$ são **equivalentes** quando $m = n$ e se existe $\sigma \in S_n$ tal que $p_i = q_{\sigma(i)}$ para todo i .

Definição 5. Diremos que um domínio D é um **domínio de fatoração única** quando todo $a \in D$ com $a \neq 0$ e $a \notin D^*$ admite uma fatoração, e sempre que tivermos duas fatorações para um mesmo elemento, elas serão equivalentes.

Exemplo 3. $\mathbb{Z}$ é um domínio de fatoração única.

Agora temos o seguinte resultado.

Proposição 2. *Seja D um domínio de fatoração única. Então todo elemento irredutível de D é primo.*

Demonstração. Seja $p \in D$ um elemento irredutível, e $a, b \in D$ tal que p divide ab . Tomando fatorações $a = p_1 \cdots p_m$ e $b = q_1 \cdots q_n$ temos que $ab = p_1 \cdots p_m \cdot q_1 \cdots q_n$. Como p divide ab , segue que existe $c \in D$ tal que $pc = ab = p_1 \cdots p_m \cdot q_1 \cdots q_n$. Assim, pela unicidade da fatoração, segue que p

divide algum p_i e nesse caso p divide a , ou p divide algum q_j e logo p divide b . Portanto p é primo. $\square$

Veremos mais adiante que todo domínio euclidiano é um domínio de fatoração única.

Agora que entendemos que é possível dividir em anéis mais gerais que os anéis dos inteiros, nos concentraremos no estudo dos ideais desses anéis. Primeiro note a seguinte propriedade interessante,

Exemplo 4. Seja I um ideal de $\mathbb{Z}$. É possível mostrar que $I = (m)$ para algum $m \in \mathbb{Z}$. De fato, se $I = (0)$, então I é um ideal principal e não há o que provar. Se I é não nulo, então I admite números positivos e negativos. Seja m o menor inteiro positivo tal que $m \in I$. Afirmamos que $I = (m)$. De fato, como $m \in I$, temos que $(m) \subset I$. Agora seja $a \in I$, tal que $a \neq m$. Pelo algoritmo da divisão de euclides, existem q, r tal que $a = qm + r$, com $0 \leq r < m$. Como $r = a - qm$, e como $a \in I$ e $qm \in I$ segue que $r \in I$, mas pela minimalidade da escolha de m temos então que $r = 0$, e concluímos que para todo $a \in I$, tem-se que $a = qm$ para algum q , isto é, $I \subset (m)$ de onde vem a igualdade.

Definição 6. Seja D um domínio. Diremos que D é **domínio de ideais principais**, se todo ideal de D for principal, ou seja, gerado por um único elemento.

Segue do Exemplo 4 que os inteiros são um domínio de ideais principais. Em domínios de ideais principais temos uma boa caracterização de ideais maximais.

Teorema 3. *Sejam D um domínio de ideais principais e I um ideal. Então I é maximal, se e somente se, existe $q \in D$ tal que q é irredutível e $I = (q)$.*

Demonstração. Seja I um ideal maximal. Como D é domínio de ideais principais segue que $I = (a)$ para algum $a \in D$. Se $b \in D$ tal que b divide a , pelo exercício 1, temos que $(a) \subseteq (b) \subseteq R$. Como (a) é maximal, temos que $(b) = R$, e novamente pelo Exercício 1, temos que b é uma unidade. Assim a é irredutível.

Suponha agora que $I = (p)$ com p irredutível. Suponha que exista $b \in D$ tal que $(p) \subsetneq (b) \subsetneq R$. Assim b é divisor próprio de p o que é absurdo. Logo I é maximal. $\square$

Nosso objetivo será estudar agora as relações entre domínios de ideais principais, de fatoração única e euclidianos.

Teorema 4. *Todo domínio euclidiano é um domínio de ideais principais.*

Demonstração. A demonstração segue, mutatis mutandis, a demonstração do Exemplo 4. $\square$

Para relacionar domínios de ideais principais e de fatoração única precisaremos do seguinte Lema.

Lema 1. *Se D é um domínio de ideais principais e $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ é uma cadeia de ideais em D , então existe $m \in \mathbb{N}$ tal que $I_m = I_{m+i}$ para todo $i \in \mathbb{N}$.*

Demonstração. Considere $I = \bigcup_{j=1}^{\infty} I_j$. Não é difícil ver que I é ideal de D .

Como D é domínio de ideais principais, segue que existe $a \in I$ tal que $I = (a)$.

Como $a \in I = \bigcup_{j=1}^{\infty} I_j$, segue que existe $m \in \mathbb{N}$ tal que $a \in I_m$, assim, $(a) \subseteq I_m$.

Mas como $I_n \subseteq \bigcup_{j=1}^{\infty} I_j = (a)$, temos que $(a) = I_n$. Agora, para todo $i > 0$,

segue que $I_n \subseteq I_{n+i} \subseteq \bigcup_{j=1}^{\infty} I_j = I_n$. Portanto $I_n = I_{n+i}$ para todo $i > 0$. $\square$

Segue diretamente que

Corolário 2. *Se D é um domínio de ideais principais, e $(a_i)_{i>0}$ é uma sequência de elementos de D tais que a_{i+1} divide a_i , para todo $i > 0$, então existe $n \in \mathbb{Z}$ tal que $a_i \sim a_n$ para todo $i \geq n$.*

Deixaremos o seguinte lema ao leitor.

Lema 2. *Seja D um domínio de ideais principais. Então todo elemento irredutível é primo.*

Podemos agora provar o seguinte.

Teorema 5. *Se D é um domínio de ideais principais então também é um domínio fatoração única.*

Demonstração. Sejam D um domínio de ideais principais e $a \in D$ um elemento não nulo que não é uma unidade. Vamos mostrar que a admite uma única fatoração. Dividiremos a prova em duas partes:

Parte 1: Existência Se a é irredutível não há o que provar. Suponha que a não é irredutível. Assim existem a_1 e b_1 divisores próprios de a . Ou seja $a = a_1 b_1$, com $a \not\sim a_1$ e $a \not\sim b_1$. Se a_1 e b_1 são irredutíveis encontramos uma decomposição para a , caso contrário, existem a_2^a, b_2^a , divisores próprios para a_1 , $a_1 = a_2^a b_2^a$, e o mesmo para b_1 , $b_1 = a_2^b b_2^b$. Se um dos elementos $a_2^a, b_2^a, a_2^b, b_2^b$ não for irredutível, podemos supor sem perda de generalidade que será o a_2^a . Repetindo o procedimento de obter os divisores próprios de a_i^a como $a_i^a = a_{i+1}^a b_{i+1}^a$, obtemos uma sequência de (a_i^a) de modo que cada a_{i+1}^a divide a_i^a , e que $a_{i+1} \not\sim a_i$, o que contradiz o Corolário 2 Assim, conseguimos escrever $a = p_1 \cdots p_s$ onde cada p_i é irredutível.

Parte 2: Unicidade Sejam $a = p_1 \cdots p_r = q_1 \cdots q_s$ duas decomposições de a , com $r \leq s$. Procederemos por indução em r . Se $r = 1$ temos que $a = p_1 = q_1 \cdots q_r$, logo a é irredutível, e temos o resultado. Suponha que o resultado seja válido para todo elemento que pode ser fatorado por até $r - 1$ irredutíveis.

Como $a = p_1 \cdots p_r = q_1 \cdots q_s$, temos pelo Lema 2 que p_r divide algum dos q_j , sem perda de generalidade, assumamos que p_r divide algum dos q_s . Como q_s é irredutível, segue que existe uma unidade u tal que $p_r = u q_s$. Assim, temos que $a = p_1 \cdots p_{r-1} u q_s = q_1 \cdots q_{s-1} q_s$, e como D é domínio, segue que $a = u p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1}$, e pela hipótese de indução temos que $r - 1 = s - 1$, que implica $r = s$, e que existe $\sigma \in S_{r-1}$ tal que $p_i \sim q_{\sigma(i)}$, como $p_r \sim q_r$, temos o nosso resultado. $\square$

Segue deste teorema que $\mathbb{Z}[\sqrt{-5}]$ não é um domínio de ideais principais, portanto nem um domínio euclideo, pois 9 admite duas fatorações por irredutíveis distintas.

Segue também do Teorema anterior e da Proposição 2 o seguinte resultado:

Corolário 3. *Seja D um domínio de ideais principais, então um elemento é irredutível se, e somente se for primo.*

Uma generalização natural da ideia de domínio de ideais principais, é quando todos os ideais de um dado anel são finitamente gerados. Veremos a seguir que anéis com essa propriedade são bastante ricos do ponto de vista teórico. Lembre-se que um conjunto parcialmente ordenado (*conjunto*) é um conjunto munido de uma operação binária ($\leq$) que é simétrica ($a \leq a$), antireflexiva ($a \leq b$ e $b \leq a$ implica $b = a$), e transitiva (($a \leq b$ e $b \leq c$ implica $b \leq a$)).

Considere Σ um conjunto por uma relação $\leq$.

Proposição 3. *As seguintes afirmações são equivalentes em Σ :*

- i) (Condição de cadeia crescente) Toda cadeia ascendente $x_1 \leq x_2 \leq \dots$ em Σ é estacionária (isto é, existe N tal que para todo $n \geq N$ tem-se $x_n = x_{n+1}$.);*
- ii) (Condição de elemento maximal) Todo subconjunto não-vazio S de Σ possui (pelo menos) um elemento maximal m , isto é, não existe $a \in S$ tal que $m \leq a$.*

Demonstração. *ii) implica i)* é óbvio. Vamos provar *i) $\Rightarrow$ ii)*. Seja $S \subset \Sigma$ tal que $S \neq \emptyset$. Se S é finito, claramente possui elemento maximal. Se S é infinito, suponha que S não admite elemento maximal. Dado $s_0 \in S$, como S não admite elemento maximal, existe $s_1 \in S$ tal que $s_0 \leq s_1$ e $s_1 \neq s_0$. Analogamente, existe $s_2 \in S$ tal que $s_1 \leq s_2$ e $s_2 \neq s_1$. Procedendo desta forma, construímos uma cadeia ascendente de elementos $s_0 \leq s_1 \leq \dots \leq s_n \leq \dots$ que não estabiliza, contradizendo *i)*, o que é um absurdo. $\square$

Definição 7. Sejam A um anel comutativo com identidade e Σ o subconjunto de todos os ideais de A ordenados com a relação $\subseteq$. Se A satisfaz uma (e portanto a duas) condições da proposição anterior dizemos que A é **Noetheriano**.

Exemplo 5. Todo corpo $\mathbb{K}$ é Noetheriano. De fato, o único ideal próprio de $\mathbb{K}$ é (0) logo a única cadeia possível é (0) que claramente estabiliza.

Exemplo 6. Pelo Lema 1, segue que todo domínio de ideais principais é Noetheriano. Em particular, o anel dos inteiros é Noetheriano.

Condições de cadeia não são computacionalmente convenientes para se trabalhar. Por isso a seguinte caracterização será muito útil.

Proposição 4. *Sejam A um anel comutativo com identidade. Então A é Noetheriano se, e somente se, todo submódulo $I \triangleleft A$ é finitamente gerado.*

Demonstração. $(\Rightarrow)$ Suponha A Noetheriano. Sejam I um ideal de A e $\Sigma_I = \{I_i \text{ ideal de } I \mid I_i \text{ é finitamente gerado}\}$. Então $\Sigma_I \neq \emptyset$, pois $0 \in \Sigma_I$, logo possui um elemento maximal I_0 . Se $I_0 = I$ segue que I é finitamente gerado pela definição de Σ_I . Se $I_0 \neq I$, existe $x \in I$ tal que $x \notin I_0$. Considere o submódulo $I_1 = I_0 + x.A$ que é finitamente gerado e portanto $I_1 \in \Sigma_I$ e $I_0 \subsetneq I_1$. Logo I_0 não é maximal, uma contradição. Portanto, $I_0 = I$ e I é finitamente gerado.

$(\Leftarrow)$ Agora suponha que todo ideal de I é finitamente gerado e tome uma cadeia ascendente $I_1 \subset I_2 \subset \dots$ de ideais de A . Então $J = \bigcup_{i=1}^{\infty} I_i$ é um ideal em A e, portanto, finitamente gerado por hipótese, e considere $x_1, \dots, x_r$ os seus geradores. Para cada $i = 1, \dots, r$ existe n_i tal que $x_i \in I_{n_i}$. Seja $n = \max\{n_i\}$, então $x_i \in I_n$ para todo i . Logo $I_m = J$ para todo $m \geq n$ e a cadeia é estacionária. $\square$

A proposição anterior nos diz os anéis noetherianos são os anéis que de certa forma generalizam os domínios de ideais principais, uma vez que neles, todo ideal é finitamente gerado. (Cuidado: Sabemos que o número de geradores é finito, mas não sabemos quantos geradores o ideal tem, e note que um anel não precisa ser domínio para ser noetheriano).

O teorema a seguir nos dá uma forma de produzir anéis noetherianos novos, a partir de anéis conhecidos.

Teorema 6 (Teorema da Base de Hilbert). *Seja A um anel Noetheriano, então $A[x]$ o anel de polinômios com coeficiente em A é Noetheriano.*

Demonstração. Seja J um ideal de $A[x]$. O conjunto dos graus de todos os polinômios em J é limitado inferiormente.

Seja $f_1 \in J$ um polinômio com o menor grau (é possível escolher tal elemento pelo axioma da escolha). Se $J = \langle f_1 \rangle$ então J é finitamente gerado, como J foi escolhido de maneira arbitrária, segue que $A[x]$ é Noetheriano.

Se $J \neq \langle f_1 \rangle$ escolha $f_2 \in J \setminus \langle f_1 \rangle$ de menor grau. Se $J = \langle f_1, f_2 \rangle$ segue que J é finitamente gerado e $A[x]$ é Noetheriano. Indutivamente, seja f_i o elemento de menor grau em $J \setminus \{f_1, \dots, f_{i-1}\}$. Se $J = \langle f_1, \dots, f_i \rangle$ então $A[x]$ é Noetheriano. Caso contrário existe um conjunto $F = \{f_1, f_2, \dots, f_m, \dots\} \subset J$ tal que $f_m \in J \setminus \{f_1, \dots, f_{m-1}\}$, com f_m de menor grau. Seja a_j o coeficiente líder de f_j e considere o ideal $I = \langle a_1, \dots, a_m, \dots \rangle \subset A$. Como A é Noetheriano, segue que existe $N \in \mathbb{N}$ tal que $I = \langle a_1, \dots, a_N \rangle$.

Afirmção: $J = \langle f_1, \dots, f_N \rangle$.

Suponha que existe $f_{N+1} \in F \setminus \langle f_1, \dots, f_N \rangle$, mas como I é finitamente gerado, segue que seu coeficiente líder $a_{N+1} = \sum_{i=1}^N u_i a_i$, com $u_i \in A$. Como o grau de f_{N+1} é maior igual que os graus dos polinômios f_i para $i = 1, \dots, N$ segue que o polinômio

$$g(x) = \sum_{i=1}^N u_i f_i(x) x^{(\deg f_{N+1} - \deg f_i)},$$

tem o mesmo grau que f_{N+1} e $g(x) \in \langle f_1, \dots, f_N \rangle$. Como $f_{N+1} \notin \langle f_1, \dots, f_N \rangle$, segue que $f_{N+1} - g \notin \langle f_1, \dots, f_N \rangle$. Mas $f_{N+1} - g$ possui grau menor que f_{N+1} o que contradiz sua minimalidade. Portanto $J = \langle f_1, \dots, f_N \rangle$ e $A[x]$ é Noetheriano. $\square$

Corolário 4. Se A é Noetheriano, então $A[x_1, \dots, x_n]$ é Noetheriano.

Demonstração. Prova por indução em n . O caso $n = 1$ é o Teorema da base de Hilbert. Suponha que se A é Noetheriano então $A[x_1, \dots, x_{n-1}]$ é Noetheriano, como $A[x_1, \dots, x_n] = A[x_1, \dots, x_{n-1}][x_n]$ segue do teorema da base de Hilbert que $A[x_1, \dots, x_n]$ é Noetheriano. $\square$

Corolário 5. Se $\mathbb{K}$ é corpo, então $\mathbb{K}[x_1, \dots, x_n]$ é Noetheriano.

Exercícios

1. Sejam D um domínio, e $a, b \in D$. Prove que:
 - a) a divide b se, e somente se, $(b) \subseteq (a)$.
 - b) $a \sim b$ se, e somente se, $(a) = (b)$.
 - c) a é divisor próprio de b se, e somente se, $(a) \neq R$ e $(b) \subsetneq (a)$.
 - d) $(a) = D$ se, e somente se, $a \in D^*$
2. Prove o Lema 2.
3. Seja R um anel comutativo com identidade. Prove que $p \in R$ é um elemento primo se, e somente se (p) é um ideal primo.
4. Prove que $\mathbb{Z}[x]$, o anel de polinômios com coeficientes em inteiros, não é um domínio de ideais principais.
5. Dê exemplo de um domínio de fatoração única que não seja:
 - a) Domínio de ideais principais.
 - b) Domínio euclideo.
6. Dê exemplo de um domínio de ideais principais que não seja euclideo.
7. Prove que os inteiros de Gauss ($\mathbb{Z}[i] := \{a + bi; i^2 = -1\}$) são um domínio euclideo.
8. Sejam A e B anéis comutativos com identidade, com A noetheriano, e $f : A \rightarrow B$ um epimorfismo. Prove que B é noetheriano.
9. Sejam D um domínio e $a, b \in D$. Diremos que um elemento é **máximo divisor comum** entre a e b denotado por $\text{mdc}(a, b)$ se $\text{mdc}(a, b) \in D$ satisfaz:
 - a) $\text{mdc}(a, b)$ divide a e também divide b .
 - b) Se c divide a e b , então c divide $\text{mdc}(a, b)$.

Prove que se o $\text{mdc}(a, b)$ existe em D , então ele é único a menos de associados.

10. Considere o anel dos inteiros de Gauss, $\mathbb{Z}[i]$. Prove que

- $a + bi \in \mathbb{Z}[i]$ é irredutível, se $a^2 + b^2$ é primo.
- Mostre que 2 não é irredutível em $\mathbb{Z}[i]$.
- Encontre todos os associados de 3 e 5 em $\mathbb{Z}[i]$.
- Sejam D um domínio de ideais principais, e $a, b \in D \setminus \{0\}$. Então o $\text{mdc}(a, b)$ existe, e existem $x, y \in D$ tais que $\text{mdc}(a, b) = ax + by$.