Prova: $\begin{cases} \text{abre} & 15:00 \\ \text{Fecha} & 23:59 \end{cases}$

http://www.mat.ufmg.br/museu.

Def: Um polinomio $P(x) \in A[x]$ A (DFU) é **primitivo** se

$P(x) = a_n x^n + \dots + a_1 x + a_0$ com

$mdc(a_n, a_{n-1}, \dots a_1, a_0) = 1$.

, isto é, não existe $a \in A \setminus U(A)$ tal que a divide todos os coeficientes de $P(x)$

Em particular todo polinomio mônico é primitivo

$$x^2 - 3x + 2 = (x-2)(x-1)$$

---

(4) Pag 364 Se $g(x)$ primitivo em $R[x]$ mostrar que todo polinomio não constante que divide $g(x)$ tambem é primitivo

Suponhamos falso, logo existe

$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$ ✓

NÃO primitivo, logo existe $d \mid a_j \ \forall j = 0 \ldots m$, $d \in R \setminus U(R)$

e $f(x)$ divide

$g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$

$g(x) = f(x) \cdot h(x)$ $\quad h(x) \in R[x]$

$h(x) = c_\ell x^\ell + \cdots + c_1 x + c_0$

$$f(x)\, h(x) = \underbrace{(a_m x^m + \cdots + a_1 x + a_0)(c_\ell x^\ell + c_{\ell-1} x^{\ell-1} + \cdots + c_1 x + c_0)}_{\displaystyle \sum_{k=0}^{m+\ell} \Big(\underbrace{a_k c_0 + a_{k-1} c_1 + \cdots + a_0 c_k}\Big) x^k}$$

$d \quad d \quad d \quad d$

o coeficiente de $g(x)$ é divisível por d, assim $g(x)$ não seria primitivo, o que é contraditório.

2. Dar um exemplo de polinomios $f(x)\, g(x) \in R[x]$ tal que $f(x)$ e $g(x)$ são associados no anel do corpo de frações $F[x]$ mas não são associados em $R[x]$

$f(x), g(x)$ são associados em $R[x]$ se existe uma unidade $c \in U(R)$ tal que $f(x) = c\, g(x)$

$$R = \mathbb{Z} \rightsquigarrow F = \mathbb{Q}$$

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

$$f(x) = 2x^2 + 2 \longleftrightarrow g(x) = 3x^2 + 3$$

$$f(x) = \frac{2}{3}\, g(x) \qquad \frac{2}{3} \in \mathbb{Q} \qquad \frac{3}{2} \in \mathbb{Q}$$

não são associados em $\mathbb{Z}$ pois

$$\frac{2}{3} \notin U(\mathbb{Z}) = \{1, -1\}$$

Corolario 10.3.6: R DFU F corpo de frações. Sejam $f(x)\, g(x)$ polinomios primitivos em $R[x]$. Se $f(x)$ e $g(x)$ são associados em $F[x]$ então eles são associados em R.

(5) Provar que um polinomio é primitivo $\Leftrightarrow$ 1_R é o mdc do coeficientes

($\Rightarrow$) Suponhamos $f(x)$ primitivo: Se existe c tal que c divide todos os coeficientes de f(x) então $c \notin R \setminus U(R)$ i.e $c \in U(R)$ logo o mdc dos coeficiente é 1_R

associados

$$\boxed{mdc(4,9) = 1 \quad (-1) \qquad mdc(6,15) = 3 \quad (\pm 3)}$$

$\mathbb{Z}[i]$

$$mdc(4, 3+i) = 1 \quad (-1, i, -i)$$

$$4 = 2^2 = (1+i)^4$$

$$mdc(6, 1+3i)$$

$$6 = 2 \cdot 3 = (1+i)^2 \cdot 3$$

3 é primo em $\mathbb{Z}[i]$

$$N(1+3i) = 1+9 = \underline{10}$$

$$2 \cdot 5$$

$1 \pm i \qquad 1 \pm 2i$

$$N(P_1 P_2 \ldots P_k) = N(P_1) \ldots N(P_k)$$

$$(a+ib)\cdot(c+id) = 1+3i \qquad \begin{cases} ac-bd = 1 \\ bc+ad = 3 \end{cases}$$

$$ac-bd+i(bc+ad) = 1+3i$$

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

$$\begin{pmatrix} c \\ d \end{pmatrix} = \frac{1}{a^2+b^2}\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} 1 \\ 3 \end{pmatrix} = \frac{1}{a^2+b^2}\begin{pmatrix} a+3b \\ -b+3a \end{pmatrix}$$

$$\underbrace{c = \frac{a+3b}{a^2+b^2} \in \mathbb{Z}} \qquad \underbrace{d = \frac{-b+3a}{a^2+b^2} \in \mathbb{Z}}$$

$$a = \pm 1 \qquad b = \pm 1$$

$$a = b = 1 \Rightarrow c = \frac{4}{2} = 2 \qquad d = \frac{2}{2} = 1$$

$$\underbrace{(1+i)}_{i}\underbrace{(2+i)}_{-i} = 1+3i$$

$$((\ \underline{(-1+i)}\ \underline{(1-2i)}$$

$$\text{mdc}(6, 1+3i) = 1+i \quad (-1+i,\ -1-i,\ 1-i)$$

($\Leftarrow$) Se o mdc dos coeficientes é 1_R

Logo todo divisor comum dos coeficientes tem que ser uma unidade $U(R)$.

③ Se $c_1 \dots c_n f(x) = g(x)$ $c_i \in R$
e $g(x)$ é primitivo então $c_j \in U(R)$

Se para algum j c_j não é unidade
então c_j divide todos os coeficientes
do produto $\underbrace{c_1 c_2 \dots c_n f(x)} = g(x)$

Logo $g(x)$ não seria primitivo.

Critério de Eisenstein: Seja $f(x) \in \mathbb{Z}[x]$
tal que $f(x) = a_n x^n + \dots + a_1 x + a_0$ de
tal forma que existe um primo $p \in \mathbb{Z}$

com $p \nmid a_n$ $p \mid a_j$ $\forall j = 0, 1 \dots, n-1$
e $p^2 \nmid a_0$

Então $f(x)$ é irredutível em $\mathbb{Z}[x]$

O critério vale trocando $\mathbb{Z}$ por
R DFU

Prova: Suponhamos que $f(x) \in R[x]$ é redutível em $R[x]$

$$f(x) = g(x)\, h(x) \qquad \begin{array}{l} g(x) = b_m x^m + \dots + b_1 x + b_0 \\ h(x) = c_\ell x^\ell + \dots + c_1 x + c_0 \end{array}$$

com $m, \ell \geq 1$ $\quad m + \ell = n \quad \Big\Vert \begin{array}{l} m < n \\ \ell < n \end{array}$

$$g(x)h(x) = \underbrace{c_\ell b_m}_{=\, a_n} x^{m+\ell} + (c_\ell b_{m-1} + c_{\ell-1} b_m) x^{m+\ell-1} + \dots + \underbrace{b_0 c_0}_{=\, a_0}$$

Como $p \mid a_0 = b_0 c_0$ mas $p^2 \nmid b_0 c_0$

Logo p divide somente um dos dois b_0 e c_0

Podemos supor s.p.g que $p \mid b_0$ e $p \nmid c_0$

$$b_0 c_1 + b_1 c_0 = a_1 \qquad p \mid a_1 \qquad p \mid b_1 \underbrace{c_0}_{} $$

divide $\quad$ Não divide $\quad$ divide

$$b_1 c_0 = \underline{a_1} - \underline{b_0} c_1$$

Logo $p \mid b_1$

Indutivamente suponhamos que $p \mid b_j$ para $j = 1, 2, \dots, s$

Consideremos o coeficiente de x^{s+1} em $f(x)$

$$b_0 c_{s+1} + b_1 c_s + b_2 c_{s-1} + \dots b_s c_1 + b_{s+1} c_0 = a_{s+1}$$

a_{s+1} é divisível por p se $s+1 < \underline{n}$

logo $b_{s+1} c_0$ é divisível por p

$\Rightarrow \quad p \mid b_{s+1}$

Concluimos que Todos os coeficientes de $g(x)$ são divisíveis por $\underline{p}$

Como $f(x) = \underline{g(x)}\, h(x)$ temos que todos os coeficientes de $f(x)$ são divisíveis por p, o que contradiz o fato que $p \nmid a_n$.

12. Mostrar que

$$f(x) = x^3 - \underline{6}x^2 + \underline{4}ix + \underline{(1+3i)} \in (\mathbb{Z}[i])[x]$$

DE $\Rightarrow$ $\underline{\underline{\text{DFU}}}$

$$1+3i = \overset{p}{\overset{\shortparallel}{(1+i)}}(2+i)$$

$1+i$ divide $1+3i$ mas

$p^2 = (1+i)^2 = 1+2i-1 = 2i$ não divide $1+3i$

6 e 4 são divisíveis por 2

e 2 é divisível por $1+i$

Pelo critério e Eisenstein

$f(x)$ é irredutível!

<u>Def</u>: Um domínio D cumpre a Condição da cadeia ascendente se sempre que temos uma cadeia de ideais

$$I_1 \subseteq I_2 \subseteq I_3 \ldots \subseteq I_n \subseteq \ldots \subseteq D$$

existe $N > 0$ tal que

$$I_N = I_{N+1} = I_{N+2} = \ldots$$

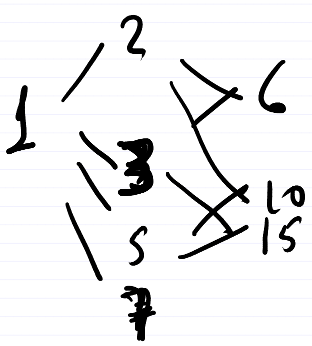
Dada uma coleção de ideais $\{I_j\}_{j\in J}$

existe $j_0 \in J$ tal que I_{j_0} é maximal. isto é não existe $j \in J$ tal que $I_{j_0} \subsetneq I_j$

CCA $\Rightarrow$ Existência de Maximais

$\Leftarrow$ trivial

$(\mathbb{N}_{>0}, \leq)$ $\qquad a \leq b \iff a | b$



Tirando 1 com esta ordem temos elementos minimais que são os primos

Lema de Zorn

$\Rightarrow$

Noetheriano $\iff$ CCA $\iff$ Têm Maximais

$(\Leftarrow)$

2.5. D Domínio. $U(D[x_1, \dots, x_n]) = U(D)$

$U(D) = U(D[x]) = U(D[x_1][x_2])$

Seja $f(x) \in U(D[x])$

logo existe $g(x) \in D[x]$ tal qe

$$f(x)g(x) = 1$$

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$
$$g(x) = b_m x^m + \cdots + b_0$$
$$\begin{cases} a_n \neq 0 \\ b_m \neq 0 \end{cases}$$

$$f(x)g(x) = \underline{\underline{a_n b_m}} x^{m+n} + \cdots = 1$$

como D é dominio $a_n b_m \neq 0$

$\Rightarrow \quad m+n = 0 \quad$ como $m, n \geq 0$

$\Rightarrow \quad m = n = 0 \quad \Rightarrow f(x)$ e $g(x)$

são constantes $\Rightarrow f(x) \in D$

e é uma unidade ie $\underline{f(x)} \in U(\underline{D})$

$$\Rightarrow U(D[x]) = U(D)$$

Indutivamente temos qe

$$U(D) = U(D[x_1, \ldots, x_n]).$$