CONTEÚDO DOS POLINÔMIOS

HÉLIA MATIKO YANO KODAMA

ORIENTADOR

PROF. Dr. HU SHENG

Dissertação apresentada ao Instituto de Matemática , Estatística e Ciência da Computação da Universidade Estadual de Campinas como requisito - parcial para obtenção do título de - Mestre em Matemática .

Este trabalho foi realizado com o auxílio financeiro do Conselho Nacional de Pesquisas (CNPq)

Maio de 1982

Agradeço :

Ao Prof. Dr. Hu Sheng pela proposta do presente trabalho , por sua atenção e disponibilidade , e segura orientação na elaboração do mesmo .

Aos meus amigos e professores por seus estímulos e ensinamentos .

À minha família por seu apoio e compreensão.

Ao CNPq , que , com seu apoio financeiro , possibilitou a realização deste trabalho .

Ao Daniel

CONTEUDO DOS POLINÔMIOS

I N T R O D U Ç Ã O

Seja R um anel comutativo com unidade e um polinomio $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$. c(f) é dito conteúdo de f , se $c(f) = (a_0, a_1, \ldots, a_n)$ o ideal de R que é gerado pelos coefi - cientes de f .

Temos o seguinte Lema de Gauss : Se o polinomio primitivo f(x) pode ser fatorado como produto de dois polinomios com coeficientes racionais , então ele pode ser fatorado como produto de dois polinomios com coeficientes inteiros ; ou usando uma linguagem mais moderna , c(fg) = c(f)c(g) para $f,g \in Z[x]$. Como Domínio de Fatorização Única (U.F.D.) é uma generalização do domínio dos inteiros , naturalmente queremos a generalização do Lema de Gauss sobre U.F.D. , infelizmente o exemplo da página 29 mostra que isso não acontece em geral. Então , neste trabalho , temos por objetivo , estudar vários aspectos sobre a seguinte questão : Para um domínio R , c(fg) = c(f)c(g) onde f : fixo e g : arbritário acontece se , e somente se , c(f) é inversível . Também , obtemos algumas caracterizações dos Domínios com Máximo Divisor Comum (G.C.D.) , como consequências.

Sintetizando , no primeiro capítulo , colocamos defini - ções e alguns resultados básicos sobre anéis e ideais , ideais

inversíveis , domínios de fatorização única (U.F.D.) , polino - mios primitivos , domínios com máximo divisor comum (G.C.D.) e dependência integral.

A maioria dos resultados são apresentados sem demonstração, mas estas , podem ser encontradas na biliografia citada.

No segundo capítulo , damos alguns resultados parciais para a questão acima . É provado que tal é caso para R arbritário e c(f) inversível ; alguns casos especiais para a recíproca são examinados , como por exemplo $f = ax^n + b$ onde $ab \neq 0$, $n \geq 1$.

No terceiro capítulo , definimos polinomios super-primitivos e estudamos algumas condições equivalentes a super-primitivo, isto é , condições equivalentes a $c(f)^{-1} = R$; temos ainda um resultado mais geral , em que encontramos uma condição equivalente à $I^{-1} = R$, onde I é um ideal finitamente gerado qualquer ; também neste capítulo damos um critério para a determinação de ideais primos principais de $R[x]$, assim : Se R é um domínio , então (f) é um ideal primo de $R[x]$ se , e somente se f é super-primitivo e irredutível sobre K .

No quarto e último capítulo , damos quatro caracterizações dos domínios G.C.D., como consequências dos estudos feitos nos capítulos anteriores e finalmente mostramos que $R[x]$ é G.C.D. se R é G.C.D. ,que é um resultado importante obtido neste trabalho.

C A P I T U L O I

Todos os anéis considerados são anéis comutativos com identidade , e qualquer terminologia que não for explícita no texto, poderá ser encontrada na bibliografia [A-M] ou [K] ou [H] .

Neste capítulo , serão colocadas definições e algumas propriedades que serão utilizadas nos capítulos seguintes , cujas demonstrações são encontradas segundo as referências indicadas.

§ 1-1 ANÉIS E IDEAIS

Definição :

Sob a designação anel entenderemos um anel comutativo com elemento unidade , isto é , (R,+,.) é um anel se :

i) (R,+) é um grupo abeliano

ii) (R,.) é um semi-grupo comutativo com elemento unidade ; e

iii) $a.(b + c) = a.b + a.c$ para todo $a,b,c \in R$.

Definição :

O anel R é um domínio (ou anel de integridade) se, e somente se , vale a seguinte regra :

$\forall a,b \in R$, $a.b = 0$ então $a = 0$ ou $b = 0$.

Definição :

Um subconjunto não vazio I do anel R é um ideal do anel R se , e somente se :

i) Para todos $a,b \in I$, $a - b \in I$

ii) Para cada $a \in I$, para todo $b \in R$, $a.b \in I$.

Definição :

Um ideal própio P do anel R é primo se , e somente se :

$a.b \in P$ implica $a \in P$ ou $b \in P$

Definição :

Um ideal própio M do anel R é maximal se , e somente se, para qualquer ideal I de R , se $M \subset I \subset R$, então $M = I$ ou $I = R$, isto é , não existe nenhum ideal próprio entre M e R .

Proposição 1.1.1

(i) Todo anel não nulo possui ao menos um ideal maximal.

(ii) Se I é um ideal própio do anel R , então existe um ideal maximal M que contém I .

Demonstração : [[A-M] , pag. 3 e pag. 4]

Definição :

Seja R um anel . O radical de Jacobson de R : J(R) é a intersecção de todos os ideais maximais de R .

Proposição 1.1.2

$x \in J(R)$ se , e somente se , $1 - xy$ é unidade de R , para todo $y \in R$.

Demonstração : [[A-M], pag. 6]

O próximo resultado é conhecido como um corolário do Lema de Nakayama .

Proposição 1.1.3

Seja M um R-módulo finitamente gerado , N um submódulo de M e $I \subset J(R)$ um ideal . Então $M = IM + N$ implica $M = N$.

Demonstração : [[A-M], pag. 22]

Se I é um ideal tal que $I \subset P$ um ideal primo , então P pode ser reduzido a um ideal primo minimal sobre I .

Teorema 1.1.4

Seja I um ideal qualquer de R tal que $I \subset P$, onde P é um ideal primo de R . Então existe um ideal primo Q de R tal que $I \subset Q \subset P$ e Q é minimal sobre I (isto é , não existe nenhum ideal primo entre I e Q) .

Demonstração : [[K] , pag. 6]

Definição :

Sejam $a,b \in R$, o ideal quociente de a e b é um ideal

$(a):b = \{ r \in R : rb \in (a) \}$

Observações :

(1) Para $a,b \in R$, $a \neq 0$, então $\frac{b}{a} \in R$ se , e somente se, $(a):b = R$. Pois , $1 \in (a):b$ é o mesmo que $b \in (a)$.

(2) Se $a \neq 0$, então $a \in (a):b$, portanto $(a):b \neq (0)$.

(3) Se a não é uma unidade de R e $b \notin (a)$, então $(a):b \neq R$, e por (1.1.1) , existe um ideal maximal (primo) M que contém $(a):b$, logo , pelo teorema 1.1.4 , existe um ideal primo P que é minimal sobre $(a):b$, isto implica que o conjunto W definido por $W = \{ P : \text{ideal primo de } R : P \text{ é minimal sobre os ideais de forma } (a):b \text{ , para } a,b \in R \}$ não é vazio .

Definição :

Se $f: R \longrightarrow S$ é um homomorfismo de anéis e I é um ideal de R , definimos extensão de I , como sendo o ideal $S.f(I)$ gerado por $f(I)$ em S. Explicitamente :

$$S.f(I) = I^e = \left\{ \sum_{i=1}^{n} y_i f(x_i) : x_i \in I \text{ e } y_i \in S \right\} .$$

Se q é um ideal de S , então o ideal $q^c = f^{-1}(q)$ definido por :

$$q^c = \{ a \in R : \text{existe } b \in S \text{ tal que } f(a) = b \}$$

é chamado contração de q.

Lema 1.1.5

Se $f: R \longrightarrow S$ é um homomorfismo de anéis e se q é um ideal primo de S , então q^c é um ideal primo de R.

Demonstração : Sejam a_1, $a_2 \in R$ e $a_1.a_2 \in q^c$, então $f(a_1.a_2) = f(a_1).f(a_2) \in q$. Como q é um ideal primo, logo $f(a_1) \in q$ ou $f(a_2) \in q$, ou seja $a_1 \in q^c$ ou $a_2 \in q^c$.

Lema 1.1.6

A extensão I^e de um ideal finitamente gerado I é finitamente gerado.

Demonstração : Seja $I = (a_1, a_2, \ldots, a_n)$, então é fácil verificar que $I^e = (f(a_1), f(a_2), \ldots, f(a_n))$.

Definição :

Um subconjunto S do anel R é um sistema multiplicativo fechado se, para todo $s,t \in S$, então $st \in S$. ($0 \notin S$, $1 \in S$)

Exemplos :

(1) Se P é um ideal primo de R, então $S = R - P$ é um sistema multilpicativo fechado.

(2) Se $x \in R$ não é nilpotente, então $\{x^n : n \geq 0\}$ é um sistema multiplicativo fechado.

Apresentamos o teorema de Krull, que dá uma maneira de construir ideal primo.

Teorema 1.1.7

Seja R um anel e $S \subset R$ um sistema multiplicativo fechado.

Se P é um ideal de R , maximal com respeito à exclusão de S,(isto é , $P \cap S = \emptyset$ e se $Q \supset P$, então $Q \cap S \neq \emptyset$) , então P é um ideal primo .

Demonstração : [[K] , pag. 1]

Definição :

Sejam R um anel e $S \subset R$ um sistema multiplicativo fechado . O anel de frações de R por S é o conjunto :

$$S^{-1}R = \left\{ \frac{a}{s} : a \in R \text{ e } s \in S \right\}$$

munido das operações :

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \qquad \text{e} \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

, e onde vale a seguinte relação :

$\frac{a}{s} = \frac{b}{t}$ se , e somente se , existe $s' \in S$ tal que $s'(at - bs) = 0$.

Com as definições acima pode-se provar que ($S^{-1}R$, + , .) é um anel comutativo com elemento unidade .Ver [[A-M],pag. 36] .

Observações :

(1) Se P é um ideal primo de R e se $S = R - P$, então escrevemos R_P ao invés de $S^{-1}R$.

(2) Se R é um domínio e $S = R - \{0\}$, então $S^{-1}R$ é o corpo de frações de R .

(3) Se R é um anel comutativo e $S = \{ s \in R ; s$ não é divisor de zero$\}$, então $S^{-1}R$ é o anel total de frações .

Definição :

O anel R é um anel quasi-local se R tem um único ideal maximal .

Vejamos um anel quasi-local típico :

Lema 1.1.8

Se P é um ideal primo de R , então o anel R_p é quasi-local e P_p é o ideal maximal de R_p .

Demontração : [[A-M] , pag. 38]

Uma propriedade crítica de anel quasi-local é :

Lema 1.1.9

Seja R um anel quasi-local com ideal maximal M . Então $a \in R$ é uma unidade de R se , e somente se , $a \notin M$.

Demonstração : Claramente , $a \notin M$ se a é uma unidade de R . Se $a \notin M$, então $aR \not\subset M$, como M é o ideal maximal , então $aR = R$, logo a é uma unidade de R .

Proposição 1.1.10

Seja R um anel e S um sistema multiplicativo fechado de R . Então $S^{-1}(IJ) = S^{-1}(I).S^{-1}(J)$ para ideais I,J de R.

Demonstração : [[A-M] , pag. 42]

Uma propriedade P do anel R (ou de um R-módulo M) é chamada <u>propriedade local</u> se :

R tem P (M tem P) se , e somente se , R_P (M_P) tem P para todo ideal primo P de R .

Essa propriedade é uma das ferramentas fundamentais na álgebra comutativa . Por exemplo :

<u>Proposição 1.1.11</u>

Sejam M e N dois R-módulos . Então as seguintes afirmações são equivalentes :

i) $M = N$

ii) $M_P = N_P$ para todo ideal primo P de R.

iii) $M_m = N_m$ para todo ideal maximal m de R.

Demonstração : [[A-M] , pag. 40]

Finalmente , um fato de grande importância que será utilizado mais tarde .

<u>Lema 1.1.12</u>

Seja R um anel quasi-local e M seu ideal maximal . Se $I = (a_1, a_2, \ldots, a_n)$ é um ideal principal não nulo , então $I = (a_i)$ para algum i .

Demonstração : Seja $I = (a_1, a_2, \ldots, a_n) = (d)$, $d \in R$, então $a_i = r_i d$, $r_i \in R$, $\forall i$.

Se existe i tal que $r_i \notin M$, então r_i é uma unidade , por (1.1.9), daí $I = (d) = (a_i)$.

Se $r_i \in M$, para todo i , como temos :
$d = s_1 a_1 + \ldots + s_n a_n$, onde $s_i \in R$, $\forall$ i , então
$d = (r_1 s_1 + \ldots + r_n s_n)d$, daí , $(1 - \sum_{i=1}^{n} r_i s_i)d = 0$.

Claramente , $\sum_{i=1}^{n} r_i s_i \in M$, então $(1 - \sum_{i=1}^{n} r_i s_i)$ é uma unidade , por (1.1.2), daí $d = 0$, o que é uma contradição .

Portanto , $I = (a_i)$ para algum i .

§ 1-2 DIVISORES DE ZERO EM $R[x]$

Definição :

Seja R um anel e $R[x]$ o anel dos polinomios na indeterminada x . Um divisor de zero no anel $R[x]$, é um elemento $f \in R[x]$ que divide zero , isto é , para o qual existe um elemento $0 \neq g$ pertencente a $R[x]$ tal que $fg = 0$.

Lema 1.2.1

Se $c \in R$ é um divisor de zero em $R[x]$, então c é um divisor de zero de R .

Demonstração :

Se $c(a_0 + a_1x + \ldots + a_nx^n) = 0$, com $a_n \neq 0$, então $ca_n = 0$. Logo , c é um divisor de zero de R .

O resultado que vamos demonstrar a seguir é o Teorema de McCoy [Mc] , que simplifica a definição de divisores de zero em $R[x]$.

Teorema 1.2.2

Seja $f \in R[x]$, onde R é um anel comutativo , f é um divisor de zero em $R[x]$ se, e somente se , existe $0 \neq c \in R$ tal que $cf = 0$.

Demonstração : Se $0 \neq c \in R \subset R[x]$ tal que $cf = 0$, então f

é um divisor de zero em $R[x]$.

Por outro lado , se f é um divisor de zero em $R[x]$, então existe $0 \neq g \in R[x]$ tal que $g.f = 0$.

Seja $\mathcal{S} = \{0 \neq g \in R[x] ; g.f = 0\}$.

$\mathcal{S} \neq \emptyset$, pois f é um divisor de zero em $R[x]$, então existe $g \in \mathcal{S}$ tal que grau(g) $\leq$ grau(h) , para todo $h \in \mathcal{S}$.

Sejam $g = b_o + b_1x + \ldots + b_mx^m$, onde $b_m \neq 0$ e

$$f = a_o + a_1x + \ldots + a_nx^n \text{ , onde } a_n \neq 0 .$$

Temos que $n \geq 1$, pois no caso de $f = 0$ ou grau(f) = 0 o resultado é imediato , por (1.2.1) .

Como $g.f = 0$, temos $b_m a_n = 0$.

Como $a_n(gf) = (a_n g)f = 0$, se $a_n g \neq 0$, então $a_n g \in \mathcal{S}$ mas

$$a_n g = a_n b_o + \ldots + a_n b_{m-1}x^{m-1} + a_n b_m x^m = a_n b_o + \ldots + a_n b_{m-1}x^{m-1}$$

pois $a_n b_m = 0$,então temos que $a_n g = 0$ pois grau$(a_n g) <$ grau(g) e $a_n g \in \mathcal{S}$.

Daí temos , $a_n b_k = 0$ para $k = 0,1,\ldots,m-1,m$.

Então ,$f.g = (b_o + \ldots + b_mx^m)(a_o + \ldots + a_nx^n) =$

$$= (b_o + \ldots + b_mx^m)(a_o + \ldots + a_{n-1}x^{n-1}) = 0$$

Como $a_{n-1}b_m = 0$, da mesma maneira acima temos $a_{n-1}b_k = 0$

para $k = o,1,\ldots,m$.

Pelo mesmo processo , para cada t , $t = o,1,\ldots,n$ temos

$a_t b_k = 0$, para $k = 0,1,\ldots,m$.

Então temos $a_t b_m = 0$, $\forall\ t = 0,1,\ldots,n$, e então ,

$b_m f = 0$ e $b_m \neq 0$.

§ 1-3 IDEAIS INVERSIVEIS

Seja R um anel comutativo e K o seu anel total de frações.

Definição :

Um R-submódulo J de K é dito ideal fracional de R se existe $0 \neq a \in R$ tal que $aJ \subset R$. Se J é um ideal fracional de R , o inverso de J , $J^{-1} = \{ x \in K : xJ \subset R \}$ é um ideal fracional de R .

Definição :

Um ideal fracional J de R é dito inversível se $JJ^{-1} = R$. (Notamos que $JJ^{-1} \subset R$ é automática) .

Colocaremos algumas propriedades sobre ideais inversíveis que serão utilizadas mais tarde . O resultado a seguir foi demonstrado sobre domínio em [(K), pag. 37] , temos agora o mesmo resultado sobre anel .

Proposição 1.3.1

Um ideal inversível em um anel quasi-local é principal.

Demonstração : Seja I um ideal inversível em R ,então $II^{-1} = R$.

Daí , $\sum a_i b_i = 1$, onde $a_i \in I$ e $b_i \in I^{-1}$, $\forall$ i . Logo um dos $a_i b_i$ é uma unidade , pois caso contrário teríamos

$a_i b_i \in M$ para todo i , por (1.1.9) , logo $\sum a_i b_i \in M$, on-

de M é ideal maximal de R e isso é uma contradição .

Consideremos a_1b_1 como sendo uma unidade , então existe $y \in R$ tal que $(a_1b_1)y = 1$.

Assim , se $x \in I$, então $x = 1x = (a_1b_1y)x = (xb_1y)a_1 \in (a_1)$ pois $xb_1y \in R$.

Portanto , $I \subset (a_1)$ e daí $I = (a_1)$.

Inversibilidade é uma propriedade local :

Proposição 1.3.2

Seja J um ideal fracional de R . As seguintes afirmações são equivalentes :

i) J é inversível

ii) J é finitamente gerado e J_P é inversível para todo ideal primo P de R .

iii) J é finitamente gerado e J_M é inversível para todo ideal maximal M de R .

Demonstração : [(A-M) , pag. 97]

Lema 1.3.3

Sejam I , J ideais de R .

i) Se $IJ \subset R$, então $I \subset J^{-1}$ ou $J \subset I^{-1}$

ii) Se $I \subset J$, então $J^{-1} \subset I^{-1}$.

iii) $(IJ)^{-1} \supset I^{-1}.J^{-1}$

iv) Se $I^{-1} = R$ ou $J^{-1} = R$, então $(IJ)^{-1} = I^{-1}.J^{-1}$.

Demonstração :

i) É imediata pela definição .

ii) Como $J^{-1}.J \subset R$ e $I \subset J$, então $J^{-1}.I \subset J^{-1}.J \subset R$, daí $J^{-1} \subset I^{-1}$.

iii) Como $I^{-1}.J^{-1}.(JI) = I^{-1}.(J^{-1}.J)\ I \subset I^{-1}RI = I^{-1}.I \subset R$ então $I^{-1}.J^{-1} \subset (JI)^{-1} = (IJ)^{-1}$.

iv) Se $J^{-1} = R$, como $(IJ)^{-1}.IJ \subset R$, então $(IJ)^{-1}.I \subset J^{-1} = R$ daí , $(IJ)^{-1} \subset I^{-1} = I^{-1}.R = I^{-1}.J^{-1}$.

Portanto , $(IJ)^{-1} = I^{-1}.J^{-1}$.

Analogamente , se $I^{-1} = R$, então $(IJ)^{-1} = I^{-1}.J^{-1}$.

Lema 1.3.4

Produto de dois ideais inversíveis é inversível.

Demonstração :

Sejam $II^{-1} = R$ e $JJ^{-1} = R$ para ideais inversíveis I e J , então $1 = \sum_i a_i x_i$ e $1 = \sum_j b_j y_j$, onde $a_i \in I$, $x_i \in I^{-1}$, $b_j \in J$ e $y_j \in J^{-1}$.

Logo , $1 = \sum_{i,j} a_i b_j x_i y_j$. Como $a_i b_j \in IJ$ e $x_i y_j \in I^{-1}.J^{-1}$ e por (1.3.3 - iii) temos que $I^{-1}.J^{-1} \subset (IJ)^{-1}$, então concluímos que $1 \in (IJ)(IJ)^{-1}$, e portanto $(IJ)(IJ)^{-1} = R$.

§ 1-4 DOMÍNIOS DE FATORIZAÇÃO ÚNICA (U.F.D.)

Definição :

Seja R um domínio . Um elemento $a \in R$, não unidade , será denominado irredutível (ou elemento primo) se , sempre que $a = bc$, $b,c \in R$, então b ou c é uma unidade em R .

Uma generalização do domínio dos inteiros Z será :

Definição :

Um domínio R , é um domínio de fatorização única , denotamos por U.F.D. , se :

(1) Todo elemento não nulo em R é uma unidade ou pode ser escrito como produto de um número finito de elementos irredutíveis de R .

(2) A decomposição na parte (1) é única a menos da ordem dos elementos e de associados dos elementos irredutíveis .

Vejamos agora , algumas propriedades dos domínios U.F.D., primeiro , colocamos mais algumas definições .

Definição :

Para $a,b \in R$, diz-se que a divide b , denotamos por $a|b$, se existe $c \in R$ tal que $ac = b$.

Dizemos que $d \in R$ é o máximo divisor comum de a e b se :

(1) $d|a$ e $d|b$

(2) Se $c \in R$ é tal que $c \mid a$ e $c \mid b$, então $c \mid d$.

Notação : $d = [a,b]$

Analogamente , podemos definir $[a_1,a_2,\ldots,a_n]$, o máximo divisor comum de $a_i \in R$, $i = 1, \ldots, n$.

Lema 1.4.1

Para quaiquer dois elementos a,b em U.F.D. , sempre existe $d = [a,b]$ o máximo divisor comum de a e b , e $(a,b) = (d)$ como ideais .

Demonstração : [(H) , pag. 150]

Seja R um anel comutativo e $R[x]$ o anel dos polinomios na indeterminada x .

Definição :

Um polinomio $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$ é dito primitivo se para $d \in R$ tal que $d \mid a_i$ para $i = 0,1,\ldots,n$, então d é uma unidade de R .

Lema 1.4.2

Se R é U.F.D. , então qualquer $f \in R[x]$, $f = d.f'$ onde $d \in R$ e f' é primitivo .

Demonstração :

Seja $f = a_0 + a_1x + \ldots + a_nx^n$, por (1.4.1) , existe $d \in R$ tal que $d = [a_0,a_1,\ldots,a_n]$. Sejam $a_i = d.a_i'$, onde $a_i' \in R$ para

todo i , então $f = d(a_o' + a_1'x + \ldots + a_n'x^n) = d.f'$ e claramente f' é primitivo .

O fato em que o produto de dois polinomios primitivos é primitivo em $Z[x]$ é conhecido como Lema de Gauss . Temos uma generalização deste fato em U.F.D. .

Teorema 1.4.3

Se R é U.F.D. , então o produto de dois polinomios primitivos é primitivo .

Demonstração :

Sejam $f,g \in R[x]$ dois polinomios primitivos . Suponhamos que f.g não seja primitivo , como R é U.F.D. , existe $p \in R$, $p \neq 0$, p : primo , tal que p divide todos os coeficientes de f.g , por (1.4.2)

Como p é primo , temos que o ideal (p) é um ideal primo e então $R_{/(p)}$ é um domínio .

Logo , $R_{/(p)}[x] = \{ \bar{a}_o + \bar{a}_1 x + \ldots + \bar{a}_n x^n : \bar{a}_i = a_i + (p), \forall i \}$ também é um domínio .

Consideremos a seguinte aplicação :

$\emptyset : R[x] \longrightarrow R_{/(p)}[x]$, definida da seguinte maneira :

$\emptyset(a_o + a_1x + \ldots + a_nx^n) = \bar{a}_o + \bar{a}_1x + \ldots + \bar{a}_nx^n$, para todo $a_o + a_1x + \ldots + a_nx^n \in R[x]$.

Claramente , $\emptyset$ é um homomorfismo , então $\emptyset(f.g) = \emptyset(f)\emptyset(g)$.

Consideremos $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{j=0}^{m} b_j x^j$ e mais $(f.g)(x) = \sum_{k=0}^{n+m} c_k x^k$, onde $c_k = \sum_{i+j=k} a_i b_j$.

Como p divide todos os coeficientes de f.g , temos que $c_i \in (p)$, $\forall$ i .

Logo , $\emptyset(f.g) = \emptyset(f)\emptyset(g) = \bar{0}$. Mas $R_{/(p)}[x]$ é um domínio , então $\emptyset(f) = \bar{C}$ ou $\emptyset(g) = \bar{0}$ e isso implica em $a_i \in (p)$, $\forall$ i , ou $b_j \in (p)$, $\forall$ j , isto é , $p \mid a_i$, $\forall$ i , ou $p \mid b_j$, $\forall$ j , o que é um absurdo pois f e g são polinomios primitivos.

Portanto , f.g é um polinomio primitivo .

Corolário 1.4.4

Se R é U.F.D. , então o produto de um número finito de polinomios primitivos é primitivo .

Proposição 1.4.5

Se K é um corpo , então K[x] é U.F.D. .

Demonstração : [[H] ,pag. 152]

Definição :

Seja R um domínio , K o corpo de frações de R . Um polinomio $f \in K[x]$ é dito irredutível sobre K se sempre que f = g.h com $g,h \in K[x]$, então g ou h é uma constante .

Lema 1.4.6

O ideal (f) em K [x] é um ideal maximal se , e somente se f é irredutível sobre K .

Demonstração : [[H] , pag. 142]

§ 1-5 DOMINIOS COM MÁXIMO DIVISOR COMUM (G.C.D.)

Definição :

Seja R um domínio . Dizemos que R é um domínio com máximo divisor comum , denotamos por G.C.D. , se para dois elementos quaisquer a e b de R , existe $d \in R$ tal que $d = [a,b]$, o máximo divisor comum de a e b .

Por (1.4.1) , temos que U.F.D. é G.C.D. , então o nosso assunto é , a generalização do Lema de Gauss em G.C.D. . Fazemos isto e caracterizamos G.C.D. no capítulo 4 . Vejamos agora , algumas propriedades básicas dos domínios G.C.D. .

Lema 1.5.1

Seja R um domínio G.C.D. , $a,b,c \in R$, então :

i) $[ab,ac] = a[b,c]$

ii) Se $d = [a,b]$, então $\left[\frac{a}{d} , \frac{b}{d}\right] = 1$

iii) Se $[a,b] = [a,c] = 1$, então $[a,bc] = 1$

Demonstração :

i) Consideremos $m = [ab,ac]$. Então , desde que a divide ab e ac , temos que a divide m , assim $m = ax$, $x \in R$.

Como $m = ax$ divide ab e ac , então x divide b e c . Então temos que $x = [b,c]$ pois , se $n \mid b$ e $n \mid c$, então $an \mid ab$ e $an \mid ac$, e então $an \mid m = ax$. Logo , n divide x .

ii) Se $d = [a,b]$, então $a = d.\frac{a}{d}$ e $b = d.\frac{b}{d}$. Logo ,

$$d = [a,b] = \left[d.\frac{a}{d} , d.\frac{b}{d} \right] = d . \left[\frac{a}{d} , \frac{b}{d} \right]$$

iii) Suponhamos que t divide a e bc . Então , t divide ab e bc e assim t divide $[ab,bc] = b[a,c] = b.1 = b$

Logo , t divide a e b , daí temos $t = 1$ pois $[a,b] = 1$.

Portanto , $[a,bc] = 1$.

Daí , podemos dar o seguinte resultado :

Corolário 1.5.2

Seja R um G.C.D. , $a,b_1,\ldots,b_n$ e $a_1,\ldots,a_n \in R$. Então :

i) $[ab_1,ab_2,\ldots,ab_n] = a[b_1,b_2,\ldots,b_n]$

ii) se $[a_1,a_2,\ldots,a_n] = d$, então $\left[\frac{a}{d}1,\ldots\ldots, \frac{a}{d}n \right] = 1$

Demonstração : A demonstração é feita por indução sobre n , utilizando a proposição 1.5.1

Lema 1.5.3

Seja R um G.C.D. . Se $[u,a] = 1$ e u divide ab , então

u divide b .

Demonstração :

Como $[u,a] = 1$, por (1.5.1 - i) , $b = [ub,ab]$. Mas , u divide ab e ub , então u divide $[ub,ab] = b$

Lema 1.5.4

Sejam R um G.C.D. e $a_o,a_1,b_o,b_1,d_o,d_1 \in R$ tais que $[a_o,a_1] = [b_o,b_1] = [d_o,d_1] = 1$ e $d_1a_1 \mid d_oa_o$ e $d_1b_1 \mid d_ob_o$, então $d_1a_1b_1 \mid d_o[a_ob_1,a_1b_o]$

Demonstração :

Como $d_1a_1 \mid d_oa_o$ e $d_1b_1 \mid d_ob_o$, então $d_1a_1b_1 \mid d_oa_ob_1$ e $d_1a_1b_1 \mid d_oa_1b_o$, daí $d_1a_1b_1 \mid [d_oa_ob_1,d_oa_1b_o]$. Mas , por (1.5.1-i), $[d_oa_ob_1,d_oa_1b_o] = d_o[a_ob_1,a_1b_o]$.

Portanto , $d_1a_1b_1 \mid d_o[a_ob_1,a_1b_o]$.

Lema 1.5.5

$K[x]$ é G.C.D. para qualquer corpo K .

Demonstração :

Temos que $K[x]$ é U.F.D. , por (1.4.5) , e U.F.D. é G.C.D. , por (1.4.1)

Finalmente , daremos uma condiçaõ suficiente para a existência de alguns máximos divisores comuns num domínio qualquer.

Proposição 1.5.6

Seja $A = (a_1, a_2, \ldots, a_n)$ ideal não nulo num domínio R, e seja $0 \neq d \in R$. Então, as seguintes afirmações são equivalentes:

i) $A^{-1} = \frac{1}{d} \cdot R$

ii) Para todo $b \in R$, $(ba_1, ba_2, \ldots, ba_n) = b.d$

iii) Para todo $k \in A^{-1}$, $(ka_1, ka_2, \ldots, ka_n) = k.d$

Demonstração:

i) $\rightarrow$ iii) Como $A^{-1} = \frac{1}{d} .R$, então $\frac{1}{d} \in A^{-1}$, logo, $\frac{1}{d} \cdot A \subset R$ e assim temos $\frac{a}{d} i \in R$, para todo i, para $k \in A^{-1}$ $ka_i \in R$ e $kd \in R$. Como $ka_i = kd.\frac{a}{d} i$, então $kd \mid ka_i$, para todo i.

Seja agora, $g \mid ka_i$, para todo i, logo, $\frac{ka}{g} i \in R$, daí $\frac{k}{g} \in A^{-1} = \frac{1}{d} .R$, e então $\frac{k}{g} = \frac{r}{d}$ para algum $r \in R$ e portanto, $g \mid kd$.

Concluimos então que $(ka_1, ka_2, \ldots, ka_n) = kd$ para todo $k \in A^{-1}$.

iii) $\rightarrow$ ii) Imediato

ii) $\rightarrow$ i) Para todo $b \in R$, temos $(ba_1, \ldots, ba_n) = bd$, logo, $bd \mid ba_i$ para todo i, daí $\frac{a}{d} i \in R$, donde para $r \in R$, $r.\frac{a}{d} i \in rR \subset R$, portanto $\frac{1}{d} .R \subset A^{-1}$. Para o outro lado

se $k = \frac{r}{s} \in A^{-1}$, $s \neq 0$, $r,s \in R$, então $\frac{r}{s} . a_i \in R$ para todo i , logo $s \mid ra_i$ para todo i .

Como $\left(ra_1,\ldots,ra_n \right) = rd$, temos $s \mid rd$, daí $\frac{rd}{s} \in R$, isto é , $kd \in R$, ou seja $k \in \frac{1}{d} .R$. Portanto , $A^{-1} = \frac{1}{d} .R$.

§ 1-6 DEPENDÊNCIA INTEGRAL

Definição :

Seja R um anel e $A \subset R$ um subanel com $1_R \in A$. Um elemento $r \in R$ é dito integral sobre A se r satisfaz uma equação da forma $r^n + a_1 r^{n-1} + \ldots + a_n = 0$, onde $a_i \in A$, para todo i .

Definição :

Um domínio R é chamado fechado integralmente se para qualquer $x \in K$, o corpo de frações de R , se x é integral sobre R então $x \in R$.

Proposição 1.6.1

Se R é um domínio G.C.D. então R é fechado integralmente.

Demonstração : [[K] , pag. 33]

Definição :

Um anel comutativo R é dito um anel de valorização se para quaisquer $a,b \in R$, então a divide b ou b divide a .

Observação :

Se R é um domínio de valorização , então para cada $x \in K$, o corpo de frações de R , temos $x \in R$ ou $x^{-1} \in R$.

Proposição 1.6.2

Todo ideal finitamente gerado é principal em um anel de valorização .

Demonstração : [[K] , pag. 38]

Temos agora , uma ligação entre fechado integralmente e anel de valorização :

Teorema 1.6.3

Seja R um domínio fechado integralmente com corpo de frações K . Então , $R = \bigcap V_\alpha$, onde V_α's são domínios de valorização entre R e K .

Demonstração : [[K] , pag. 36]

C A P I T U L O II

A definição clássica do conteúdo do polinomio $f \in Z[x]$ é o máximo divisor comum dos coeficientes de f . Evidentemente , dado qualquer polinomio $f \in Z[x]$, ele pode ser escrito como $f = d.g$, onde d é o conteúdo de f e $g \in Z[x]$ um polinomio primitivo .

Neste capítulo , definimos conteúdo de um polinomio em uma situação mais geral , e damos algumas propriedades multiplicativas dos conteúdos .

§ 2-1 CONTEÚDO DE UM POLINOMIO

<u>Definição</u> :

Seja R um anel comutativo e um polinomio $f = a_0 + \ldots + a_n x^n \in R[x]$. $c(f)$ é dito o <u>conteúdo</u> de f , se $c(f) = (a_0, \ldots, a_n)$, o ideal que é gerado pelos coeficientes de f .

<u>Lema 2.1.1</u>

$c(af) = (a).c(f)$ para $a \in R$ e $f \in R[x]$.

Demonstração :

Seja $f = a_0 + a_1 x + \ldots + a_n x^n$. Então $c(af) = (aa_0, \ldots, aa_n) = (a).(a_0, \ldots, a_n) = (a).c(f)$.

Para $f \in R[x]$, se $c(f) = R$, então f é primitivo , mas a recíproca não vale , por exemplo :

Exemplo :

Seja $R = Z[\sqrt{5}\ i]$. Sabemos que as unidades de R são 1 e -1 e que $1 + \sqrt{5}\ i$ e 2 são primos de R . Seja $f = 1 + \sqrt{5}\ i + 2x$, logo , f é primitivo , mas $c(f) = (1 + \sqrt{5}\ i\ ,\ 2) \neq R$ pois , se $1 = (a + b\sqrt{5}\ i)(1 + \sqrt{5}\ i) + (c + d\sqrt{5}\ i)2 \in c(f)$, onde $a,b,c,d \in Z$, então $a - 5b + 2c = 1$ e $a + b + 2d = 0$, que implica em $2(-3b + c - d) = 1$ que é um absurdo . Logo , $1 \notin c(f)$, ou seja , $c(f) \neq R$.

Lema 2.1.2

Para qualquer $0 \neq f \in R[x]$. Se $c(f) = R$, então f é primitivo.

Demonstração :

Seja $f = a_0 + a_1x + \ldots + a_nx^n$ e $d \mid a_i$ para todo $i = 0,1,..,n$, logo , $a_i = da_i'$ para algum $a_i' \in R$. Daí $R = c(f) \subset dR$, que implica em $R = dR$,portanto d é uma unidade.

Em U.F.D. , $c(f) = R$ e f é primitivo são equivalentes .

Lema 2.1.3

Seja R U.F.D. , $0 \neq f \in R[x]$. Então $c(f) = R$ se, e somente se , f é primitivo .

Demonstração :

É suficiente mostrar que se f é primitivo , então c(f) = = R .

Seja $f = a_o + a_1x + \ldots + a_nx^n$, como R é U.F.D. e f é primitivo , então o máximo divisor comum dos coeficientes de f , $d = (a_o, a_1, \ldots, a_n)$, é uma unidade e $d = \sum_{i=0}^{n} b_i a_i \in c(f)$, por (1.4.1) , donde temos $R = dR \subset c(f)$, daí $R = c(f)$.

Sejam $R \subset S$ dois anéis comutativos e $f = a_o + a_1x + \ldots + a_nx^n \in R[x]$.

Claramente , $f \in S[x]$. Seja $c_S(f)$ o ideal de S , que é gerado pelos coeficientes de f , temos a seguinte relação entre c(f) e $c_S(f)$.

Lema 2.1.4

$c_S(f) = c(f).S$

Demonstração :

Como $c(f) = a_oR + \ldots + a_nR$; $c_S(f) = a_oS + \ldots + a_nS$ e $c(f).S = (a_oR + \ldots + a_nR).S$, é claro que $c_S(f) = c(f).S$.

Definição :

Seja K o anel total de frações de R . Se $\overline{f} = \sum_{i=0}^{n} \frac{a_i}{s_i} x^i$, $\overline{f} \in K[x]$ onde $\frac{a_i}{s_i} \in K$, então definimos o conteúdo de $\overline{f}$ em K igual a $c(\overline{f}) = \frac{a_o}{s_o} R + \ldots + \frac{a_n}{s_n} R$, que é um R-submódulo de K,

e para $s = s_0 s_1 \ldots s_n \in R$ temos $s.c(\bar{f}) \subset R$ (aqui ,identificamos $R = i(R)$, onde $i : R \longrightarrow K$ definida por $i(r) = \frac{r}{1}$, para todo $r \in R$) , logo $c(\bar{f})$ é um ideal fracional de R .

Observação :

Sejam $f = a_0 + a_1 x + \ldots + a_n x^n$ e $\bar{f} = \frac{a_0}{1} + \ldots + \frac{a_n}{1} x^n$, então pelo lema anterior $c(\bar{f}) \subset c_K(f) = c(f).K = S^{-1}c(f)$.

§ 2-2 PROPRIEDADES MULTIPLICATIVAS DOS CONTEÚDOS

Um assunto principal aqui , é estudar quando a propriedade multiplicativa dos conteúdos : $c(fg) = c(f)c(g)$ para f e g em $R[x]$, vai acontecer [H] . Podemos facilmente ver que $c(fg) \subset c(f)c(g)$ para quaisquer $f, g \in R[x]$, mas a igualdade não acontece em geral . Por exemplo :

Exemplo :

Seja $R = Z\left[\sqrt{5}\, i\right]$ e $f = 2x + 1 + \sqrt{5}\, i$, $g = 2x + 1 - \sqrt{5}\, i$ em $R[x]$, então $fg = 4x^2 + 4x + 6$, Como 2 , $1 + \sqrt{5}\, i$, $1 - \sqrt{5}\, i$ são primos em R , então $c(f) = R$ e $c(g) = R$ mas $c(fg) = (2)$.

Vamos agora , dar alguns casos elementares da propriedade multiplicativa dos conteúdos

Proposição 2.2.1

Se R é U.F.D., então para $f,g \in R[x]$ temos que $c(fg) = c(f)c(g)$.

Demonstração :

Dados $f,g \in R[x]$, por (1.4.2) temos que $f = af'$ e $g = bg'$ onde $a,b \in R$, e f' e g' são primitivos em $R[x]$.

Logo , $c(f) = (a)c(f') = (a)$ e $c(g) = (b)c(g') = (b)$, por (2.1.1) e (2.1.3).

No entanto , $fg = abf'g'$ e $c(fg) = (ab)c(f'g') = (ab) = (a)(b) = c(f)c(g)$, pois $c(f'g') = R$, por (1.4.3) e (2.1.3) .

Lema 2.2.2

Seja R um anel quasi-local com ideal maximal M tal que $M^2 = (0)$. Então , $c(fg) = c(f)c(g)$ para todos $f,g \in R[x]$.

Demonstração :

Sejam $f = a_n x^n + \ldots + a_o$ e $g = b_m x^m + \ldots + b_o$ pertencentes a $R[x]$ e $fg = c_{n+m}x^{n+m} + \ldots + c_o$, onde $c_k = \sum_{i+j=k} a_i b_j$.

Se $a_i, b_j \in M$ para todo $i = o,1,\ldots,n$ e $j = o,1,\ldots,m$, então $c(f)c(g) = c(fg) = (0)$ pois $M^2 = (0)$.

Se existe $a_i \notin M$ tal que $a_o, a_1, \ldots, a_{i-1} \in M$, então a_i é uma unidade de R , por (1.1.9) , e $c_o = c_1 = \ldots = c_{i-1} = 0$ pois $M^2 = (0)$, temos também que $c_i = a_i b_o$, $c_{i+1} = a_{i+1} b_o + a_i b_1 \ldots$, $c_{i+m} = a_n b_{m+i-n} + \ldots + a_i b_m$.

Por indução sobre m , vemos que $a_i b_j \in c(fg)$ para todo $j = 0,1,\ldots,m$.

Como a_i é um unidade e $c(f) = R$, então $c(f)c(g) \subset c(fg)$, daí $c(fg) = c(f)c(g)$.

Analogamente , se existe $b_j \notin M$, então $c(fg) = c(f)c(g)$.

Agora , queremos mostrar que se $c(f)$ é inversível , então $c(fg) = c(f)c(g)$ para todo $g \in R[x]$, onde R é um anel comutativo qualquer . O caminho para isso será , primeiro demonstrar para o caso local e depois passamos para o caso global , utilizando a inversibilidade que é uma propriedade local .

Começamos então , com o caso local :

Teorema 2.2.3

Seja R um anel quasi-local e $f \in R[x]$ tal que $c(f)$ é inversível . Então, $c(fg) = c(f)c(g)$ para todo $g \in R[x]$.

Demonstração :

Seja $f = a_n x^n + \ldots + a_o$, como $c(f)$ é principal , por(1.3.1), temos por(1.1.12) que um dos a_i's gera $c(f)$.

Seja a_k o primeiro coeficiente que pode ser tomado como gerador . Afirmamos que $a_i \in Ma_k$ para todo $i < k$, onde M é ideal maximal de R . De fato , pois se $a_i = da_k$, onde $i < k$ e $d \notin M$, segue-se que d é uma unidade , por(1.1.9), e assim a_i

é o gerador de c(f) o que contradiz com a escolha de a_k .

Seja $g = b_m x^m + \ldots + b_o$, $I = c(fg)$ e $J = c(f)c(g)$. Temos que $J = (a_k b_o, a_k b_1, \ldots, a_k b_m)$. É suficiente mostrar que $J = I + MJ$, então por (1.1.3), $J = I$ ocorrerá .

Como $I \subset J$, claramente $I + MJ \subset J$.

Para completar a prova temos que verificar que $a_k b_i \in I + MJ$ para $i = 0,1,\ldots,m$, e essa prova é feita por indução sobre i :

O fato de $a_k b_o + a_{k-1} b_1 + \ldots + a_o b_k \in I$ e $a_i \in Ma_k$ para todo $i < k$, temos que $a_{k-1} b_1 + \ldots + a_o b_k \in MJ$, isso reduz que $a_k b_o \in I + MJ$.

Suponhamos que $a_k b_i \in I + MJ$ para todo $i = 0,1,\ldots,j$. Como o coeficiente de x^{k+j+1} de fg é :

$$c_{k+j+1} = (a_o b_{k+j+1} + \ldots + a_{k-1} b_{j+2}) + a_k b_{j+1} + (a_{k+1} b_j + \ldots + a_{k+j+1} b_o)$$

$\in I$; $a_o b_{k+j+1} + \ldots + a_{k-1} b_{j+2} \in M(a_k b_{k+j+1} + \ldots + a_k b_{j+2}) \subset MJ$

$\subset I + MJ$ e

$a_{k+1} b_j + \ldots + a_{k+j+1} b_o \in R(a_k b_j + \ldots + a_k b_o) \subset I + MJ$, então temos que $a_k b_{j+1} \in I + MJ$. Portanto , $J = I + MJ$.

Teorema 2.2.4

Seja R um anel comutativo com identidade . Se f é um polinomio com c(f) um ideal inversível , então c(fg) = c(f)c(g) pa-

ra $g \in R[x]$ arbritário .

Demonstração :

Como c(f) é inversível , então $c(f)_P$ é inversível para - todo ideal primo P de R , por (1.3.2).

Então , em R_P temos $c(fg)_P = c(f)_P.c(g)_P$ para todo ideal primo P , por (2.2.3) . Mas , $c(f)_P.c(g)_P = (c(f)c(g))_P$, por (1.1.10) .

Portanto , por (1.1.11) temos , c(fg) = c(f).c(g) , para $g \in R[x]$ arbritário .

Recordamos que um domínio de Dedekind é um domínio em que todo ideal fracional não nulo é inversível , então temos :

Corolário 2.2.5

Se R é um domínio de Dedekind , então c(fg) = c(f)c(g) para polinomios f e g em R[x] .

Agora , queremos estudar quando a recíproca do teorema 2.2.4 acontece , especificando , para qual $f \in R[x]$, se c(fg)= = c(f)c(g) para todo $g \in R[x]$, implica que c(f) é inversível.

Para evitar a situação no Lema 2.2.2 , assumimos que R é um domínio .

O próximo lema é necessário para o caso $f = ax^n + b$, onde $ab \neq 0$ e $n \geq 1$.

Lema 2.2.6

Seja R um domínio quasi-local , M o ideal maximal de R , $a,b \in R$ e $ab \neq 0$. Se $(a^2,b^2) = (ab,a^2+b^2)$, então (a,b) é inversível .

Demonstração :

Como $(a^2,b^2) = (ab,a^2+b^2)$, então existem $r,s \in R$ tal que $a^2 = rab + s(a^2+b^2)$, logo $(1-s)a^2 = rab + sb^2$ (1) . Para $s \in R$, temos $s \notin M$ ou $s \in M$.

Se $s \notin M$, então s é uma unidade , por (1.1.9) , daí $b^2 \in (ab,a^2)$.

Se $s \in M$, então 1-s é uma unidade , por (1.1.2) , daí $a^2 \in (ab,b^2)$.

Digamos que 1-s é uma unidade , podemos tornar a escrever (1) da seguinte maneira :

$a^2 - tab - ub^2 = 0$ para algum $t,u \in R$.

Desde que $b \neq 0$, temos $\left(\frac{a}{b}\right)^2 - t\left(\frac{a}{b}\right) - u = 0$, então $\frac{a}{b} \in K$, o corpo de frações de R , e $\frac{a}{b}$ é integral sobre R .

Logo , sobre K , temos a fatorização $z^2 - tz - u =$

$\left(z - \frac{a}{b}\right)(z - c)$ para algum $c \in K$.

Tomando o conteúdo em K de ambos os lados , por (2.2.2) , temos :

$R = \left(1 , \frac{a}{b}\right)(1,c)$, que implica em $\frac{a}{b} \in R$, daí (a,b)

é principal e assim é inversível .

Se s é uma unidade , utilizamos o mesmo raciocínio com $\frac{b}{a}$.

Teorema 2.2.7

Se $f = ax^n + b$, onde $ab \neq 0$ e $n \geq 1$, e $c(fg) = c(f).c(g)$ para todo $g \in R[x]$, então $c(f)$ é inversível .

Demonstração :

É suficiente mostrar que $c(f)_P$ é inversível para todo ideal primo P de R , por (1.3.2).

Assumimos que R é quasi-local , para $g = ax^n - b$, então $fg = a^2x^{2n} - b^2$, logo temos $c(fg) = (a^2, b^2)$ e $c(f)c(g) = (a,b)^2$ e por hipótese temos $(a^2, b^2) = (a,b)^2$.

Fazendo , $g = bx^n + a$, então $fg = abx^{2n} + (b^2 + a^2)x^n + ab$, novamente por hipótese obtemos $(ab, a^2 + b^2) = (a,b)^2$.

Daí , $(a^2, b^2) = (a,b)^2 = (ab, a^2 + b^2)$, por (2.2.6) temos que (a,b) é inversível e portanto c(f) é inversível .

Corolário 2.2.8

Seja R um domínio quasi-local e $c(fg) = c(f).c(g)$ para todos $f,g \in R[x]$. Então , todo ideal finitamente gerado é inversível .

Demonstração :

Seja $I = (a_1, a_2, \ldots, a_n)$ um ideal finitamente gerado com

$a_i \neq 0$ para todo i .

Seja $f = a_1x + a_2$, por (2.2.7) $c(f) = (a_1,a_2)$ é inversível , então é principal , por (1.3.1) , e por (1.1.12) temos que $(a_1,a_2) = (a_1)$ ou $(a_1,a_2) = (a_2)$. Digamos que $(a_1,a_2) = (a_1)$, agora tomamos $f = a_1x + a_3$,novamente temos $(a_1,a_3) = (a_1)$ ou $(a_1,a_3) = (a_3)$.

Repetimos este processo um número finito de vezes , finalmente , chegamos que $(a_1,a_2,\ldots,a_n)$ é principal , logo I é inversível .

Uma consequência dos teoremas (2.2.4) e (2.2.8) é o seguinte resultado caracterizando domínios Prüfer , que todo ideal finitamente gerado não nulo é inversível , independentemente obtidos por $[T]$ e $[G]$.

Se $c(fg) = c(f).c(g)$ para $f,g \in K[x]$, então R é um domínio Prüfer .

Corolário 2.2.9

Um domínio R é Pruferiano se , e somente se , $c(fg) = c(f)c(g)$, para todos polinomios $f,g \in R[x]$.

Corolário 2.2.10

Seja R um domínio de valorização ,então $c(fg) = c(f)c(g)$ para todos $f,g \in R[x]$.

Demonstração :

Como todo ideal finitamente gerado de R é principal por (1.6.2) , então é inversível . Logo, R é um domínio Prüfer, daí, por (2.2.9), $c(fg) = c(f)\ c(g)$ para todo $f,g \in R[x]$.

O seguinte caso que veremos é : $f = f_1 f_2$ é tal que $c(f_1)$ é inversível e $f_2 = ax^n + b$, onde $ab \neq 0$ e $n \geq 1$.

Teorema 2.2.11

Seja $f = f_1 f_2$ tais que $c(f_1)$ é inversível e $f_2 = ax^n + b$ onde $ab \neq 0$ e $n \geq 1$. Se $c(fg) = c(f).c(g)$ para todo $g \in R[x]$, então c(f) é inversível.

Demonstração :

Como $c(f_1)$ é inversível , pelo teorema 2.2.4 , temos que $c(fg) = c(f_1 f_2 g) = c(f_1).c(f_2 g)$ e $c(fg) = c(f).c(g) = c(f_1 f_2).c(g) = c(f_1).c(f_2).c(g)$.

Como $c(f_1).c(f_1)^{-1} = R$, então $c(f_2 g) = c(f_2).c(g)$ para todo $g \in R[x]$, daí o teorema 2.2.7 produz que $c(f_2)$ é inversível , assim $c(f) = c(f_1).c(f_2)$ é inversível , por (1.3.4)

O seguinte exemplo mostra que $c(fg) = c(f).c(g)$ para todo g , é uma condição suficiente no teorema 2.2.11 .

Exemplo :

Seja R um anel guarda -chuva [V] , então R é um domínio

quasi-local e seu ideal maximal $M = (a,b)$ não é principal .

Tomamos $f = (cx + c)(ax + b)$, $c \neq 0$, $ab \neq 0$, então $c(f) = (ca, cb)$ não é principal , pois se $(ca, cb) = (d)$ para algum $d \in R$, então $ca = sd$ e $cb = td$ para $s,t \in R$.

Como $cta = std = csb$, então $ta = sb$, isto implica que $s,t \in M$, do contrário M é principal .

Se $d = mca + ncb = (ms + nt)d$ para algum $m,n \in R$, então $1 = ms + nt \in M$, o que é uma contradição.

C A P I T U L O III

Veremos no capítulo precedente uma condição mais fraca do que primitivo , chama-se super-primitivo , e provaremos algumas condições equivalentes para super-primitivo .

Veremos também que super-primitivo nos dá um critério para a determinação de ideais primos principais de $R[x]$.

§ 3-1 POLINOMIOS SUPER-PRIMITIVOS

Sejam R um domínio , K o corpo de frações de R e o seguinte subconjunto de K , $S = \left\{ \frac{1}{r} \in K : r \neq 0 , r \in R \right\}$. Colocamos uma condição equivalente para polinomio primitivo .

Lema 3.1.1

$f \in R[x]$ é primitivo se , e somente se , $c(f)^{-1} \cap S = R \cap S$.

Demonstração :

Seja $f = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$ um polinomio primitivo . Como $R \subset c(f)^{-1}$, logo $R \cap S \subset c(f)^{-1} \cap S$; agora , se $\frac{1}{r} \in c(f)^{-1} \cap S$, então $\frac{1}{r} . c(f) \subset R$, isto é , $r \mid a_i$ para $i = 0,1,\ldots,n$, daí r é uma unidade pois f é primitivo .

Portanto, $\frac{1}{r} \in R \cap S$ e $c(f)^{-1} \cap S = R \cap S$.

Por outro lado , dado $0 \neq r \in R$ tal que $r \mid a_i$ para $i = 0, 1, \ldots, n$, então $\frac{1}{r} \cdot c(f) \subset R$, ou seja , $\frac{1}{r} \in c(f)^{-1}$, logo $\frac{1}{r} \in c(f)^{-1} \cap S = R \cap S$.

Assim , $\frac{1}{r} \in R$, daí r é uma unidade . Portanto , f é primitivo .

Claramente , para um polinomio $f \in R[x]$,se $c(f)^{-1} = R$, então f e´ primitivo , mas o exemplo a seguir mostra que o contrário não vale .

Exemplo :

Seja $R = Z[\sqrt{5}\, i]$. Temos que $f = (1+ \sqrt{5}\, i\,) + 2x$ é um polinomio primitivo e $c(f) = (\, 1 + \sqrt{5}\, i\, , 2\,)$. É claro que $\frac{3}{1 + \sqrt{5}\, i} = \frac{3(1 - \sqrt{5}\, i\,)}{6} = \frac{1 - \sqrt{5}\, i}{2} \in K - R$, onde K é o corpo de frações de R , mas

$$\frac{3}{1 + \sqrt{5}\, i}\left[(a + b\sqrt{5}\, i)(1 + \sqrt{5}\, i) + (c + d\sqrt{5}\, i).2\right] =$$

$(3a + 3b\sqrt{5}\, i) + (1 - \sqrt{5}\, i)(c + d\sqrt{5}\, i) \in R$, onde $a, b, c, d \in Z$.

Logo , $\frac{3}{1 + \sqrt{5}\, i} \in c(f)^{-1}$, portanto $R \subsetneq c(f)^{-1}$.

Sabemos que $c(f)^{-1} = R$ é uma condição mais fraca do que primitivo , e essa é a condição para que um polinomio seja super-primitivo , e queremos estudá-la detalhadamente .

Definição :

Dizemos que $f \in R[x]$ é um polinomio super-primitivo se, $c(f)^{-1} = R$.

Lema 3.1.2

Em domínio G.C.D. , polinomio primitivo é equivalente a polinomio super-primitivo .

Demonstração :

Basta mostrar que $c(f)^{-1} = R$ se f é primitivo . Sejam $f = a_0 + a_1x + \ldots + a_nx^n$ e $0 \neq k \in c(f)^{-1}$. Como R é G.C.D. , escrevemos $k = \frac{a}{b}$ onde $a,b \in R$, $a \neq 0$, $b \neq 0$ e $[a,b] = 1$.

Como $k.c(f) \subset R$, temos que $\frac{a}{b} . a_i \in R$ para todo i , isto é , $b \mid aa_i$ para todo i .

Por (1.5.3) e do fato de $[a,b] = 1$, temos que $b \mid a_i$ para todo i , então b é uma unidade pois f é primitivo . Assim , $k \in R$, ou seja $c(f)^{-1} = R$.

Para estudar algumas condições equivalentes de super-primitivo , consideremos um homomorfismo natural $\emptyset : R[x] \longrightarrow K[x]$ e notamos que $(f)^e = (f)K[x] = \left\{ \frac{h.f}{t} \;/\; h \in R[x],\ 0 \neq t \in R \right\}$ a extensão do ideal (f) pela $\emptyset$ é um ideal de $K[x]$ e $(f)^{ec} = (f)^e \cap R[x]$ a contração de $(f)^e$ em $R[x]$ é um ideal de $R[x]$.

Temos sempre que $(f) \subset (f)^{ec}$, quando $(f) = (f)^{ec}$ veremos que f é super-primitivo e vice-versa . Para verificar , precisamos de um corolário do teorema de McCoy (1.2.2) .

Lema 3.1.3

Seja R um domínio e $f \in R[x]$ com $\text{grau}(f) > 0$. Então

$c(f)^{-1} = R$ se, e somente se , $c(fg) \subset Rt$, $0 \neq t \in R$ implica em $c(g) \subset Rt$ para todo $g \in R[x]$.

Demonstração :

Dado qualquer $0 \neq k \in c(f)^{-1}$, então $k = \frac{a}{t} \in K$ com $t \neq 0$ $a,t \in R$ e $\frac{a}{t}.f \in R[x]$, daí $c(af) \subset Rt$, logo , $c(a) = Ra \subset Rt$ por hipótese , portanto $k = \frac{a}{t} \in R$, ou seja , $c(f)^{-1} = R$.

Por outro lado , definimos $\emptyset : R[x] \longrightarrow R/_{Rt}[x]$ da seguinte maneira : $\emptyset(f) = \bar{a}_0 + \bar{a}_1 x + \ldots + \bar{a}_n x^n$, para todo $f = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$, onde $\bar{a}_i = a_i + Rt$ e $a_i \in R, \forall i$.

Claramente , $\emptyset$ é um homomorfismo e seu núcleo é dado por:

$$\text{Ker } \emptyset = \{ h \in R[x] : c(h) \subset Rt \} .$$

Como $c(fg) \subset Rt$, então $\emptyset(fg) = \bar{0} = \emptyset(f)\emptyset(g)$.

Se $\emptyset(g) = \bar{0}$, então $c(g) \subset Rt$.

Se $\emptyset(g) \neq \bar{0}$, então $\emptyset(f)$ é um divisor de zero em $R/_{Rt}[x]$. Então por (1.2.2) , existe $\bar{k} = k + Rt \neq \bar{0}$ ($k \notin Rt$) tal que $k.\emptyset(f) = \emptyset(k.f) = \bar{0}$, então temos $c(k.f) \subset Rt$.

Assim , $\frac{k}{t}.c(f) \subset R$, donde $\frac{k}{t} \in c(f)^{-1} = R$ e então concluimos que $k \in Rt$, o que é uma contradição.

Portanto , $\emptyset(g) = \bar{0}$, isto é , $c(g) \subset Rt$.

Seja $J = c(f)^{-1}.(f) = \left\{ \sum_{i=1}^{n} a_i(g_i.f) : a_i \in c(f)^{-1} , g_i \in R[x] \text{ e } 0 < n \in Z \right\}$, um ideal de $R[x]$. Então temos :

Lema 3.1.4

Seja $f \in R[x]$ com grau(f) > 0 , então $(f) \subset J \subset (f)^{ec}$.

Demonstração :

Trivialmente , $(f) \subset J$ pois $R \subset c(f)^{-1}$. Para qualquer $h \in J$, temos $h = \sum_{i=1}^{n} a_i(g_i f) = \sum_{i=1}^{n} (a_i f)g_i$, onde $g_i \in R[x]$ e $a_i \in c(f)^{-1}$, então $a_i f \in R[x]$, daí $h \in R[x]$; entretanto $h = \sum_{i=1}^{n} (a_i g_i)f \in (f)K[x]$. Logo , $h \in (f)^{ec}$ e daí $J \subset (f)^{ec}$.

Introduziremos agora , em primeiro lugar , condições para que (f) coincida com $(f)^{ec}$, e depois , condições para que J coincida com $(f)^{ec}$.

Teorema 3.1.5

Seja $f \in R[x]$ com grau(f) > 0 e $S = \left\{ \frac{1}{r} \ / \ 0 \neq r \in R \right\}$ .Então as seguintes condições são equivalentes :

i) $(f) = (f)^{ec}$

ii) $(f) = J$

iii) $c(f)^{-1} = R$ (ou f é super-primitivo)

iv) $c(g)^{-1} \cap S = c(fg)^{-1} \cap S$ para todo $g \in R[x]$.

Demonstração :

Faremos i)$\longrightarrow$ii)$\longrightarrow$iii)$\longrightarrow$iv)$\longrightarrow$ i).

i)$\longrightarrow$ii)

Como $(f) \subset J \subset (f)^{ec}$ e $(f) = (f)^{ec}$, então $(f) = J = (f)^{ec}$

ii)$\longrightarrow$ iii)

Como $(f) = J = c(f)^{-1}.(f)$, então para qualquer $k \in c(f)^{-1}$,

temos $k.f \in (f)$, daí , existe $g \in R[x]$ tal que $k.f = g.f \in R[x]$.

Como $R[x]$ é um domínio , então $k = g \in R[x] \cap K = R$. Assim $c(f)^{-1} = R$.

iii) $\longrightarrow$ iv)

Como $c(fg) \subset c(f)c(g)$, então $c(fg)^{-1} \supset [c(f)c(g)]^{-1} = c(f)^{-1}c(g)^{-1} = c(g)^{-1}$ pois $c(f)^{-1} = R$ e por (1.3.3-iv)

Logo , $c(fg)^{-1} \cap S \supset c(g)^{-1} \cap S$.

Por outro lado , se $\frac{1}{t} \in c(fg)^{-1} \cap S$, então $c(fg) \subset Rt$ e por (3.1.3) e do fato de $c(f)^{-1} = R$ temos que $c(g) \subset Rt$.

Assim , $\frac{1}{t} \in c(g)^{-1} \cap S$ e portanto $c(fg)^{-1} \cap S = c(g)^{-1} \cap S$.

iv) $\rightarrow$ i)

Se $\frac{fg}{t} \in (f)^{ec} \subset R[x]$; então $\frac{1}{t} \in c(fg)^{-1} \cap S = c(g)^{-1} \cap S$.

Logo , $\frac{g}{t} \in R[x]$ e $\frac{fg}{t} \in (f)$. Assim $(f) = (f)^{ec}$.

Lema 3.1.6

Seja $f \in R[x]$ com grau$(f) > 0$ e $S = \left\{ \frac{1}{r} / 0 \neq r \in R \right\}$. Então , $J = (f)^{ec}$ se , e somente se , $[c(f)c(g)]^{-1} \cap S = c(fg)^{-1} \cap S$ para todo $g \in R[x]$.

Demonstração :

Para qualquer $\frac{g}{t}.f \in (f)^{ec}$, onde $g \in R[x]$ e $0 \neq t \in R$, devemos mostrar que $\frac{g}{t}.f \in J$.

Como $\frac{1}{t}.fg \in (f)^{ec} \subset R[x]$, então $\frac{1}{t} \in c(fg)^{-1}$, logo ,

$\frac{1}{t} \in c(fg)^{-1} \cap S = [c(f)c(g)]^{-1} \cap S$, isto é , $\frac{1}{t} .c(f)c(g) \subset R$. ou seja , $\frac{1}{t} .c(g) \subset c(f)^{-1}$, assim $\frac{g}{t} .f \in c(f)^{-1}.(f) = J$.

Portanto , $J = (f)^{ec}$.

Por outro lado , como $c(fg) \subset c(f)c(g)$, temos por (1.3.3) que $[c(f)c(g)]^{-1} \subset c(fg)^{-1}$, logo , $[c(f)c(g)]^{-1} \cap S \subset c(fg)^{-1} \cap S$.

No entanto , se $\frac{1}{t} \in c(fg)^{-1} \cap S$, ou seja , $\frac{1}{t} .c(fg) \subset R$, então $\frac{1}{t} . fg \in R[x]$, onde $\frac{fg}{t} \in (f)^{ec} = J = c(f)^{-1}.(f)$ por hipótese , daí temos $\frac{g}{t} = \sum a_i g_i$ onde $a_i \in c(f)^{-1}$ e $g_i \in R[x]$ e podemos escrever $\sum a_i g_i = \sum k_j x^j$, com $k_j \in c(f)^{-1}$, então , $\frac{1}{t} .c(g) \subset c(f)^{-1}$, donde $\frac{1}{t} .c(g)c(f) \subset R$, ou seja $\frac{1}{t} \in$ $\in [c(g)c(f)]^{-1} \cap S$ e portanto $c(fg)^{-1} \cap S \subset [c(f)c(g)]^{-1} \cap S$.

Concluimos então que $c(fg)^{-1} \cap S = [c(f)c(g)]^{-1} \cap S$.

Como $[c(f)c(g)]^{-1} \subset c(fg)^{-1}$ sempre , perguntamos agora quando $[c(f)c(g)]^{-1} = c(fg)^{-1}$ vai acontecer .

<u>Teorema 3.1.7</u>

Se R é um domínio fechado integralmente , então para todos $f,g \in R[x]$, $c(fg)^{-1} = [c(f)c(g)]^{-1}$.

Demonstração :

Basta mostrar que $c(fg)^{-1} \subset [c(f)c(g)]^{-1}$. Como R é fechado integralmente , por (1.6.3) , $R = \cap V_\alpha$, onde V_α é um domínio de valorização entre R e K , o corpo de fraçoes de R ,

Agora , seja V um domínio de valorizaçao tal que $R \subset V \subset K$, entao por (2.2.10) temos , $c_V(fg) = c_V(f)c_V(g)$, para todo $f,g \in R[x] \subset V[x]$, daí $c(f)c(g) \subset c_V(f)c_V(g) = c_V(fg) = c(fg).V$, por (2.1.4) .

Dado qualquer $k \in c(fg)^{-1}$, temos $k.c(fg) \subset R$, então $k.c(f)c(g) \subset k.c(fg).V \subset RV \subset V$.

Portanto , $k.c(f)c(g) \subset \cap V_\alpha = R$, ou seja , $k \in [c(f)c(g)]^{-1}$ e daí $c(fg)^{-1} \subset [c(f)c(g)]^{-1}$ e temos o resultado desejado .

Corolário 3.1.8

Se R é G.C.D. , então $c(fg)^{-1} = [c(f)c(g)]^{-1}$ para todos $f,g \in R[x]$.

Demonstração :

É imediata por(1.6.1).

Corolário 3.1.9

Se R é um dominio fechado integralmente , entao $v = (f)^{ec}$ para todo $f \in R[x]$ com grau(f) > 0 .

Demonstração :

É imediata através de (3.1.6) e (3.1.7)

Como c(f) é sempre um ideal finitamente gerado e vimos algumas condiçoes equivalentes à $c(f)^{-1} = R$, uma pergunta agora é, quais sao as condiçoes equivalentes à $I^{-1} = R$, onde I é um ideal finitamente gerado qualquer ? Temos a seguinte resposta :

Teorema 3.1.10

Seja R um domínio e I um ideal finitamente gerado , então $I^{-1} \neq R$ se , e somente se , $I \subset P$ para algum $P \in W$, onde $W = \{ P$: ideal primo de R : P é minimal sobre os ideais da forma (a):b para $a,b \in R \}$.

Demonstração :

Suponhamos que $I \subset P$, onde P é minimal sobre (a):b e $I^{-1} = R$, então $I \not\subset (a):b$, pois , se $I \subset (a):b$, temos $bI \subset (a)$, isto é , $\frac{b}{a} . I \subset R$, o que implica em $\frac{b}{a} \in I^{-1} = R$, ou seja , $(a):b = R \subset P$, o que é uma contradição .

Apanhamos $x \in I - (a):b$. Seja $A = \left(R/_{(a):b} \right)_P$ e tomemos $\alpha = \frac{\bar{x}}{\bar{I}} \in A$, onde $\bar{x} = x + (a):b$, notamos $\alpha \neq \bar{0}$.

Afirmamos que existe $n > 1$, tal que $^n = \bar{0}$.

Com efeito , se $\alpha^n \neq \bar{0}$ para todo $n > 0$, então $\{\alpha^n\}_{n \geq 0}$ é um sistema multiplicativamente fechado e pelo teorema de Krull (1.1.7), existe um ideal primo Q de A tal que $\{\alpha^n\}_{n \geq 0} \cap Q = \emptyset$.

Como P é minimal sobre (a):b , então o único ideal primo de A é P_P , portanto $Q = P_P$. Mas , $\alpha \in P_P$ e $\alpha \notin Q$, o que é um absurdo.

Seja $\bar{I}_P = \left\{ \frac{\bar{I}}{\bar{I}} \in A : \bar{I} = i + (a):b , i \in I \right\}$ a extensão do ideal I em A . Como I é finitamente gerado por $x_1, x_2, \ldots, x_n$ em R, então $\bar{I}_P$ é finitamente gerado pelos $\bar{a}_i = \frac{\bar{x}_i}{\bar{1}}$ para $i = 1, \ldots, n$ onde $\bar{x}_i = x_i + (a):b$, por (1.1.6) , e para cada gerador $\bar{a}_i \neq \bar{0}$,

existe um inteiro positivo n_i, tal que $\bar{a}_i^{n_i} = \bar{0}$. Pelo princípio do menor inteiro, existe um inteiro positive n, tal que $\bar{I}^n = (\bar{0})$ e $\bar{I}^{n-1} \neq (\bar{0})$, isto significa que existe $s \in R - P$ tal que $s \cdot I^n \subset (a):b$ e $s\, I^{n-1} \not\subset (a):b$. Logo, $sb \cdot I^n \subset (a)$ e daí $s \cdot \frac{b}{a} \cdot I^n \subset R$.

Mas, $s.\frac{b}{a}.I^n = s.\frac{b}{a}.I^{n-1}.I \subset R$. Logo, $s.\frac{b}{a}.I^{n-1} \subset I^{-1} = R$, isto é, $sbI^{n-1} \subset (a)$, ou seja, $s\, I^{n-1} \subset (a):b$, o que é uma contradição. Portanto, $I^{-1} \neq R$.

Por outro lado, seja $I^{-1} \neq R$, então existe $x \in I^{-1} - R$. Escrevemos $x = \frac{b}{a}$, onde $a \neq 0$, $a,b \in R$ e temos $\frac{b}{a}.I \subset R$, ou seja $I \subset (a):b$. Como $x = \frac{b}{a} \notin R$, então $(a):b \subsetneq R$. Por (1.1.1) e (1.1.4), existe um ideal primo P de R que é minimal sobre $(a):b$ e $I \subset P$.

§ 3-2 PRIMOS PRINCIPAIS DE $R[x]$

Seja R um domínio e $f \in R[x]$, o objetivo principal deste parágrafo é estudar as condiçoes equivalentes a (f) ser um ideal primo de $R[x]$. É importante saber quando o ideal entre (f) e $(f)^{ec}$ vai ser um ideal primo .

Proposiçao 3.2.1

Seja $f \in R[x]$ com grau(f) > 0 . Se N é um ideal em $R[x]$ tal que $(f) \subset N \subset (f)^{ec}$, entao N é um ideal primo se, e somente se , f é irredutível sobre K , o corpo de fraçoes de R , e $N = (f)^{ec}$.

Demonstraçao :

Como f é irredutível sobre K , por (1.4.6) , $(f)^{ec} = (f)K[x]$ é um ideal primo (maximal) de $K[x]$, assim $(f)^{ec} = N$ é primo , por (1.1.5).

Por outro lado , se existe $g \in (f)^{ec} - N$, escrevemos $g = \frac{h}{t}.f$, onde $0 \neq t \in R$ e $h \in R[x]$, então $t.g = h.f \in (f)$ e $(f) \subset N$, como N é um ideal primo e $g \notin N$, então $t \in N \subset (f)^{ec}$, daí $t \in (f)^{ec} \cap R = (0)$ pois grau(f) > 0 , o que é um absurdo.

Portanto , $(f)^{ec} = N$.

Mostremos agora , que f é irredutível sobre K . Com efeito :

Suponhamos cue $f = g.h$, onde $g,h \in K[x]$, como

$f = g.h \in (f) \subset N$, temos que $g \in N$ ou $h \in N$.

Digamos que $h \in N$, então $h = h_1.f$, onde $h_1 \in K[x]$ e assim $f = g.h_1.f$, logo g é uma unidade de $K[x]$.

Portanto , f é irredutível sobre K .

Então temos uma consequencia imediata :

Teorema 3.2.2

Seja R um domínio . Então (f) é um ideal primo de $R[x]$ se, e somente se , f é irredutível sobre K e $c(f)^{-1} = R$.

Demonstração :

Se (f) é um ideal primo , tomamos $N = (f)$ na proposiçao a cima , temos então que f é irredutível sobre K e $(f) = (f)^{ec}$, e por (3.1.5) temos $c(f)^{-1} = R$.

Por outro lado , como $c(f)^{-1} = R$ então por (3.1.5) temos $(f) = (f)^{ec}$ e como f é irredutível sobre K , por (3.2.1) temos que (f) é um ideal primo .

C A P I T U L O IV

CARACTERIZAÇÕES DOS DOMÍNIOS G. C. D.

Neste capítulo , daremos quatro caracterizações dos domínios G.C.D. , especificamente :

Seja R um domínio , K o corpo de frações de R :

1) Para qualquer $f = ax + b \in R[x]$ com $ab \neq 0$, temos que $f = d.f'$ onde $d \in R$ e f' é um polinomio linear super-primitivo em $R[x]$.

2) Todo polinomio linear em $R[x]$ é o produto de um elemento em R com um polinomio primitivo e o produto de dois polinomios primitivos é primitivo .

3) Todo ideal primo não nulo P de $R[x]$ com $P \cap R = (0)$ é principal , gerado por um polinomio primitivo .

4) Se $a \neq 0$ e $b \neq 0$ são dois elementos de R , então $(ax + b)K[x] \cap R[x]$ é principal , gerado por um polinomio primitivo .

Utilizando essas caracterizações mostramos também que $R[x]$ é G.C.D. se R é G.C.D. .

Preparamos alguns fatos básicos :

Lema 4.1

Seja R um domínio G.C.D. . Se f é um polinomio não constante em R[x] , então f = d.f' , onde d ∈ R e f' é um polinomio primitivo em R[x] .

Demonstração :

Seja $f = a_o + a_1x + \ldots + a_nx^n$, $n \geq 1$; como $a_i \in R$ e R é um G.C.D. , então existe $d \in R$ tal que $d = [a_o, a_1, \ldots, a_n]$.

Sejam $b_i = \frac{a_i}{d}$, $i = 0,1,\ldots,n$ e $f' = b_o + b_1x + \ldots + b_nx^n$, logo , temos f = d.f' e f' é primitivo pois , por (1.5.2) temos

$$[b_o, b_1, \ldots, b_n] = \left[\frac{a_o}{d}, \frac{a_1}{d}, \ldots, \frac{a_n}{d}\right] = 1$$

Corolário 4.2

Dado qualquer polinomio não constante f em K[x] , K o corpo de frações do domínio G.C.D. R , então $f = \frac{c}{d} . f'$, onde $d \neq 0$, $c,d \in R$, $[c,d] = 1$ e f' um polinomio primitivo em R[x].

Demonstração :

Seja $f = \frac{a_o}{b_o} + \frac{a_1}{b_1}x + \ldots + \frac{a_n}{b_n}x^n$, $n \geq 1$ e $b_i \neq 0$, $a_i, b_i \in R$, para todo i .

Logo , $f = \frac{1}{b} . \left(c_o + c_1x + \ldots + c_nx^n\right)$ onde $b = b_ob_1\ldots b_n$ e $c_i = \frac{a_i.b}{b_i} \in R$.

Por (4.1) , $c_0 + c_1x + \ldots + c_nx^n = a.f'$, onde $a \in R$ e f' é um polinomio primitivo em $R[x]$, daí , $f = \frac{a}{b}.f'$. Como R é G.C.D. , então existe $t = [a,b]$. Sejam $a = tc$ e $b = td$, então $\frac{a}{b} = \frac{c}{d}$ e $[c,d] = 1$, portanto $f = \frac{c}{d}.f'$.

Lema 4.3

Seja R um G.C.D. , se f é um polinomio primitivo em $R[x]$, $a,b \in R$, $b \neq 0$ tal que $\frac{a}{b}.f \in R[x]$, então $b \mid a$.

Demonstração :

Seja $f = a_0 + a_1x + \ldots + a_nx^n$, como $\frac{a}{b}.f \in R[x]$, temos $\frac{aa_i}{b} \in R$, $i = 0,1,\ldots,n$.

Como R é G.C.D. , seja $t = [a,b]$, então $a = ta'$ e $b = tb'$ para algum $a',b' \in R$ e $[a',b'] = 1$.

Então , $\frac{aa_i}{b} = \frac{a'a_i}{b'}$, daí $b' \mid a_i$ para todo i , por (1.5.3) , donde temos que b' é uma unidade pois f é primitivo .

Como $b = tb'$, então $b \mid t \mid a$.

Em R (G.C.D.) , primitivo e super-primitivo são equivalentes , por (3.1.2) , , entao qualquer polinomio não constante em $R[x]$ é um múltiplo de um polinomio super-primitivo ; para examinar o contrário , sobre polinomios lineares , temos a primeira caracterização de G.C.D. .

Teorema 4.4

R é G.C.D. se , e somente se , para qualquer polinomio linear $f = ax + b \in R[x]$, onde $ab \neq 0$, $f = d.f'$ onde $d \in R$ e f' é um polinomio linear super-primitivo .

Demonstraçao :

Dados quaiquer $a,b \in R$, $a \neq 0$ e $b \neq 0$, queremos mostrar que existe máximo divisor comum de a e b . (Caso $a = 0$, então $[a,b] = b$, caso $b = 0$, então $[a,b] = a$)

Seja $f = ax + b \in R[x]$ e por hipótese temos $ax + b = d(a_o x + b_o)$, onde $d \in R$ e $(a_o,b_o)^{-1} = R$.

Como $a = da_o$ e $b = db_o$, então d é um divisor comum de a e b .

Afirmamos que $d = [a,b]$; para qualquer $c \in R$, se $c \mid a$ e $c \mid b$, então $c \mid da_o$ e $c \mid db_o$, daí $\frac{d}{c} . (a_o,b_o) \subset R$, isto é , $\frac{d}{c} \in (a_o,b_o)^{-1} = R$, portanto , $c \mid d$, e assim $d = [a,b]$.

O outro lado é imediato por (4.1) e (3.1.2) .

Caso substituimos super-primitivo por uma condiçao mais forte que é primitivo , e no teorema acima colocarmos mais uma outra condiçao que é : o produto de dois polinomios primitivos é primitivo , temos uma caracterizaçao interessante de G.C.D. , que é também uma generalização do Lema de Gauss sobre G.C.D..

Teorema 4.5

As seguintes condiçoes sao equivalentes :

I) R é G.C.D.

II) (i) Todo polinomio linear em $R[x]$ é o produto de um elemento em R com um polinomio primitivo .

(ii) O produto de dois polinomios primitivos é primitivo .

Demonstraçao :

I)$\longrightarrow$II)

A parte (i) de II) é imediata por (4.4) e (3.1.2) . Demonstremos entao a parte (ii) de II) . Sejam $f,g \in R[x]$ polinomios primitivos , então f,g são super-primitivos , por (3.1.2) , daí $c(f)^{-1} = c(g)^{-1} = R$.

Por (1.3.3 -iv) e (3.1.8) temos $c(fg)^{-1} = \left[c(f)c(g)\right]^{-1} = c(f)^{-1}.c(g)^{-1} = R$.

Assim fg é super-primitivo , entao é primitivo , por(3.1.2).

II)$\longrightarrow$I)

Dado qualquer polinomio linear ax + b , por (i) , temos que $ax + b = d(a'x + b')$, onde $d \in R$ e $a'x + b'$ é primitivo .

Se $(a',b')^{-1} = R$, então R é G.C.D. , (por (4.4)) .

Com efeito , seja $0 \neq \frac{c}{d} \in (a',b')^{-1}$, temos por (i) que , $cx + d = e(c'x + d')$, onde $e \in R$ e $c'x + d'$ é primitivo .

Como $c = ec'$ e $d = ed'$, então $\frac{c}{d} = \frac{c'}{d'} \in (a',b')^{-1}$,

daí $\frac{a'c'}{d'} \in R$ e $\frac{b'c'}{d'} \in R$.

Por (ii) $(a'x + b').(c'x + d') = a'c'x^2 + (a'd' + b'c')x + b'd'$ é primitivo ; como d' divide todos os coeficientes ,então d' é uma unidade de R , ou $\frac{c}{d} \in R$, isto é , $(a',b')^{-1} = R$.

Um fato bem conhecido é que em um anel fatorial (U.F.D.) R , todo ideal I em R [x] tal que $I \cap R = (0)$, é principal .Temos uma generalização deste fato sobre G.C.D. , para um ideal primo. Precisamos do seguinte lema :

Lema 4.6

Seja R G.C.D. , se a.g = h.f , onde $0 \neq a \in R$, g,h,f $\in$ R [x] e g e f são primitivos , então $\frac{1}{a} \in c(h)^{-1}$ ou $\frac{1}{a}.h \in R[x]$.

Demonstração :

Por (3.1.2) , $c(g)^{-1} = R$, então temos $c(a.g)^{-1} = [(a).c(g)]^{-1} = (a)^{-1}.c(g)^{-1} = (a)^{-1}$, por (1.3.3-iv) e (3.1.8) .

Analogamente , $c(hf)^{-1} = [c(h)c(f)]^{-1} = c(h)^{-1}.c(f)^{-1} = c(h)^{-1}$ pois $c(f)^{-1} = R$.

Como a.g = h.f , temos $(a)^{-1} = c(ag)^{-1} = c(h.f)^{-1} = c(h)^{-1}$, daí , $\frac{1}{a} \in (a)^{-1} = c(h)^{-1}$ ou $\frac{1}{a}.c(h) \subset R$, portanto $\frac{1}{a}.h \in R[x]$.

Teorema 4.7

Seja $P \neq (0)$ um ideal primo de $R[x]$ tal que $P \cap R = (0)$. Então , P é principal , gerado por um polinomio primitivo .

Demonstraçao :

Pelo princípio do menor inteiro , existe um polinomio $f_o = d_o + d_1x + \ldots + d_nx^n \in P$ com $n \geq 1$ (pois $P \cap R = (0)$) , tal que $grau(f_o) = n \leq grau(g)$ para todo $g \in P$. Por (4.1) , $f_o = d.f$, onde $d \in R$ e $f \in R[x]$ é primitivo . Como $f_o = d.f \in P$ e $d \notin P$ (pois $P \cap R = (0)$) , entao $f \in P$, pois P é um ideal primo , daí $(f) \subset P$.

Para qualquer $g \in P$, devemos mostrar que $g \in (f)$.

Sejam $f = a_o + a_1x + \ldots + a_nx^n$ e $g = b_o + b_1x + \ldots + b_mx^m = d.g'$, onde $a_n \neq 0$, $b_m \neq 0$, $m \geq n$ (pois $f \in P$ com menor grau) $d \in R$ e $g' \in R[x]$ é primitivo .

Seja $h = b_mx^{m-n}.f - a_n.g \in P$. Agora , temos dois casos para analisar : $m = n$ ou $m > n$.

Caso (1) $m = n$

Como $h \in P$ e $grau(h) < n$, entao $h = 0$, daí $b_n.f = a_n.g = a_n.d.g'$ e por (4.6) temos que $\frac{b_n}{a_n.d} \in R[x]$.

Assim , $\frac{b_n}{a_n}.f = d.\frac{b_n}{a_n.d}.f \in (f)$.

caso (2) $m > n$

Seja $m = n + k$, $k > 0$. A demonstraçao deste caso é por induçao sobre k .

Se $k = 1$, então $h = b_{n+1}x.f - a_n.g$ com $grau(h) \leq n$.

Se $grau(h) < n$ e $h \in P$, entao $h = 0$, daí $b_{n+1}x.f = a_n.g = a_n d.g'$, então , por (4.6), $\frac{b_{n+1}}{a_n d}x \in K[x]$, logo , $g = \frac{b_{n+1}}{a_n} x.f \in (f)$.

Se $grau(h) = n$, pelo caso (1) , $h \in (f)$, ou seja , $h = c.f$ onde $c \in R$ (pois $grau(h) = grau(f)$), donde temos $c.f = b_{n+1}x.f - a_n.g$, escrevendo novamente temos :

$$(b_{n+1}x - c).f = a_n.g = a_n d.g' \quad , \text{ logo ,}$$

$\frac{1}{a_n d} (b_{n+1}x - c) \in R[x]$, por (4.6) , daí temos :

$$g = \frac{1}{a_n} (b_{n+1}x - c).f \in (f)$$

Agora , dado qualquer g com $grau(g) = n + k$, devemos mostrar que $g \in (f)$.

Seja , $h = b_{n+k}x^k.f - a_n.g$, claramente $h \in P$ e $grau(h) < n+k$, pela hipótese de indução , $h \in (f)$, ou , $h = c.f$, onde $c \in R[x]$, com $grau(c) < k$.

Logo , temos $(b_{n+k}x^k - c).f = a_n g = a_n d.g'$ e novamente , por (4.6), $\frac{1}{a_n d} (b_{n+k}x^k - c) \in R[x]$.

Portanto , $g = \frac{1}{a_n}(b_{n+k}x^k - c).f \in (f)$.

Uma pergunta natural surge : Todo ideal nao nulo em $R[x]$ com contração trivial é principal ? Essa vai ser mais uma caracterização de G.C.D. , temos a seguinte resposta :

Teorema 4.8

As seguintes afirmações são equivalentes :

i) R é um domínio G.C.D.

ii) Todo $(0) \neq P$ ideal primo de $R[x]$ tal que $P \cap R = (0)$ é principal gerado por um polinomio primitivo .

iii) $0 \neq a$ e $0 \neq b$ são elementos de R , então $(ax + b)K[x] \cap R[x]$ é principal , gerado por um polinomio primitivo.

Demonstração :

i)$\longrightarrow$ii)

É imediato por (4.7)

ii)$\longrightarrow$iii)

Seja $P = (ax + b)K[x] \cap R[x]$. É claro que P é um ideal de $R[x]$ e $P \cap R = (0)$. É suficiente mostrar que P é um ideal primo. Temos que $f = ax + b$ é irredutível sobre K e $(f)^{ec} = P$, por (3.2.1) , temos que P é um ideal primo .

iii) $\rightarrow$ i)

Dado $ax + b \in R[x]$, onde $ab \neq 0$. Basta provar que $ax + b = df$, onde $d \in R$ e $f \in R[x]$ é um polinomio super-primi-

tivo , pois por (4.4) teremos então que R é G.C.D. .

Por hipótese , $(ax + b)K[x] \cap R[x] = (f)R[x]$ onde f é um polinomio primitivo .

Logo , $ax + b = f.d$, onde $d \in R[x]$ e $f = (ax + b).k$ onde $k \in K[x]$.

Daí , $f = f.d.k$ e como $K[x]$ é um domínio , temos $d.k = 1$ assim $d \in R$ e $k \in K$.

Como , $(f)K[x] = (ax + b)K[x]$, logo , $(f)R[x] = (ax + b)K[x] \cap R[x] = (f)K[x] \cap R[x] = (f)^{ec}$.

Claramente , $f = (ax + b)k$ é irredutível sobre K , então por (3.2.1) temos que $(f)R[x]$ é um ideal primo , e portanto $c(f)^{-1} = R$, por (3.2.2) .

Afinal , apresentamos um resultado bem importante :

Lema 4.9

Se R é G.C.D. , então $R[x]$ é G.C.D. .

Demonstração :

Por (4.4) é suficiente mostrar que para qualquer $f = Ay + B \in R[x][y]$, onde $AB \neq 0$, $A,B \in R[x]$, temos $f = D.(A'y + B')$, onde $D,A',B' \in R[x]$ e $(A',B')^{-1} = R[x]$.

Como $f \in R[x][y] \subset K[x][y]$ onde K é o corpo de fraçoes de R e $K[x]$ é G.C.D. , por (1.5.5) , então $f = d(ay + b)$ onde $d,a,b \in K[x]$ e $(a,b)^{-1} = K[x]$, por (4.4) .

Então , por (4.2) , podemos escrever $d = \frac{d_o}{d_1} .d', a = \frac{a_o}{a_1} .a'$ e $b = \frac{b_o}{b_1} .b'$, onde $d_i, a_i, b_i \in R$, $i = 0,1$, $d_1 \neq 0$, $a_1 \neq 0$, $b_1 \neq 0$ e $[d_o, d_1] = [a_o, a_1] = [b_o, b_1] = 1$, pois R é G.C.D. e $d', a', b' \in R[x]$ são primitivos .

Como R é G.C.D. , tomamos $t = [a_o b_1, a_1 b_o]$, então existem $t_1, t_2 \in R$, tais que $a_o b_1 = t_1 t$ e $a_1 b_o = t_2 t$, logo $[t_1, t_2] = 1$, por (1.5.1- ii) .

Assim , $f = d(ay + b) = \frac{d_o}{d_1 a_1 b_1} .d'(a_o b_1 a'y + a_1 b_o b') =$

$= \frac{d_o t}{d_1 a_1 b_1} .d'(t_1 a'y + t_2 b')$, mas

$f = \frac{d_o}{d_1} .d'(\frac{a_o}{a_1} a'y + \frac{b_o}{b_1} b') \in R[x][y]$, logo , $\frac{d_o a_o}{d_1 a_1} d'a' \in R[x]$ e $\frac{d_o b_o}{d_1 b_1} d'b' \in R[x]$, e por (4.5) temos que d'a' e d'b' são primitivos ; então temos que $d_1 a_1 \mid d_o a_o$ e $d_1 b_1 \mid d_o b_o$ por (4.3) e por (1.5.4) temos que existe $k \in R$ tal que $d_o t = d_1 a_1 b_1 k$, portanto $f = kd'(t_1 a'y + t_2 b')$.

Para terminar a demonstração tomamos $D = kd'$, $A' = t_1 a'$ e $B' = t_2 b'$ e precisamos verificar que $(t_1 a', t_2 b')^{-1} = R[x]$, ou

seja , $\frac{u}{v} \in K(x)$ onde $u,v \in R[x]$ e $v \neq 0$ e assumimos $[u,v] = 1$ pois $K(x)$ é G.C.D. e $\frac{u}{v}(t_1a', t_2b') \subset R[x]$. Afirmamos que $\frac{u}{v} \in R[x]$.

Como $(a,b) = \left(\frac{a_o}{a_1}a', \frac{b_o}{b_1}b'\right) = \left(\frac{b_1a_oa'}{a_1b_1} \cdot \frac{a_1b_ob'}{a_1b_1}\right) =$ $\left(\frac{t_1ta'}{a_1b_1} \cdot \frac{t_2tb'}{a_1b_1}\right)$, entao $a_1b_1\frac{u}{v}(a,b) = \frac{u}{v}(tt_1a', tt_2b') =$ $= t\frac{u}{v}(t_1a', t_2b') \subset tR[x] \subset R[x] \subset K[x]$.

Daí, $\frac{a_1b_1u}{v} \in (a,b)^{-1} = K[x]$ o que implica que $v \in K \cap R[x] = R$.

Escrevemos $u = u_ou'$, onde $u_o \in R$ e u' é primitivo , então $[u_o,v] = 1$ pois $[u,v] = 1$ em $K(x)$.

Como $\frac{u}{v}t_1a' = t_1\frac{u_o}{v}u'a' \in R[x]$ e $\frac{u}{v}t_2b' = t_2\frac{u_o}{v}u'b'$ $\in R[x]$, então $v \mid [t_1,t_2] = 1$, por (4.3) , logo , v é uma unidade e portanto $\frac{u}{v} \in R[x]$.

B I B L I O G R A F I A

[A - M] - ATIYAH, M. F. and MACDONALD, H. G. : Introduction to Commutative Algebra - Addison Wesley, Reading , Mass. (1969)

[K] - KAPLANSKY, I. : Commutative Rings, Allyn and Ba - con, Mass. (1970)

[H] - HERSTEIN, I. N. : Tópicos de Álgebra

[Mc] - MACCOY, N. H. : Rings and ideals - Carus Math. Monografs, nº 8, Math. Assoc. of América, Buffalo (1948)

[G] - GILMER, R. : Some applications of the Hilfssatz von Dedekind - Mertens. Math. Scand. 20. (1967), (240-244)

[T] - TSANG, H. : Gauss' Lemma. University of Chicago thesis. (1965)

[S] - SHENG, H. : On the content of polinomials, Atas do 13º Colóquio Brasileiro de Matemática. (1981)

[V] - VASCONCELOS, W. V. : Rings of global dimension two. Proc. Comm. Algebra Conf., Lecture Notes in Math. . Vol. 311. Springer - Verlag - New York . Berlin . (1972)