OS ANÉIS R(X) E R(X)

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida pelo Sr. Alberto Mariano Rivero Zapata e aprovada pela Comissão Julgadora.

Campinas, 12 de Setembro de 1990

Prof. Dr. Antonio Paques
Orientador

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para a obtenção do Título de Mestre em Matemática.

Esta tese é dedicada
a Liliana, minha futura esposa
no espírito das palavras
de vida eterna de Jesus Cristo

AGRADECIMENTO

Agradeço ao meu orientador de tese, o professor Dr. Antonio Paques, pelo seu constante estímulo e pelo seu apoio. Ele é um ótimo professor, admiro seu entusiasmo para trabalhar, sua segurança, sua claridade didática e sua ordem; estou satisfeito com seus ensinamentos.

Agradeço também ao professor Dr. Paulo Brumatti pelos seus ensinamentos e pela sua receptividade para frequentes discussões.

Expresso meu agradecimento à UNICAMP, CAPES e CNPQ, pelo apoio financeiro.

Finalmente desejo agradecer aos meus colegas o professor Félix Escalante, o professor Mauro Chumpitaz e o professor Armando Venero, da Universidad Nacional de Ingenieria (Lima-Perú), e a todas as pessoas que me apoiaram para eu poder vir ao Brasil fazer o Mestrado em Matemática.

ÍNDICE

CAPÍTULO I

INTRODUÇÃO

Esta tese trata sobre os anéis $R\langle X\rangle = R[X]_U$ e $R(X) = R[X]_S$, onde R é um anel comutativo com identidade, R[X] é o anel de polinômios numa indeterminada X com coeficientes em R, $U = \{f \in R[X];\ f \text{ é mônico}\}$ e $S = \{f \in R[X];\ C(f) = R\}$ (C(f) denota o ideal de R gerado pelos coeficientes de f). O objetivo é estabelecer as propriedades dos anéis $R\langle X\rangle$ e R(X) em termos das propriedades do anel base R, aplicando os métodos da Teoria Multiplicativa de Ideais.

Supõe-se que é conhecida a teoria dos anéis noetherianos, a teoria básica dos R-módulos e grande parte do material contido no livro "Multiplicative Ideal Theory" de R. Gilmer (Dekker, New York 1972).

Se A e B são conjuntos, então $A\backslash B$ denotará o conjunto dos elementos de A que não pertencem a B. O conjunto dos números inteiros será denotado por $\mathbb{Z}$ e $\mathbb{Z}^+$ denotará o conjunto $\{n \in \mathbb{Z};\ n > 0\}$.

Seja A um anel comutativo com identidade. Sejam $a, b \in A$. Dizemos que a divide b e escrevemos a/b se e só se existe $c \in A$ tal que ac = b. Denotamos por MDC(a,b) o máximo divisor comúm de a e b e MMC(a,b) denota o mínimo múltiplo comúm de a e b. Denotamos por Reg(A) o conjunto dos elementos regulares de A e por U(A) o conjunto das unidades de A. Seja A[X] o anel de polinômios numa indeterminada X com coeficientes em A. Se $f \in A[X]\backslash\{0\}$, então o grau de f é denotado por gr(f). Se f é um polinômio numa ou duas indetermimadas e com coeficientes em A, então o ideal de A gerado pelos coeficientes de f é chamado o conteúdo de f e é denotado por $C_A(f)$ (ou simplesmente por C(f) se não existe perigo de confusão). Dizemos que $f \in A[X]$ é primitivo se e só se os únicos divisores comuns dos coeficientes de f são as unidades de A. A família de todos os ideais maximais de A é denotada por Max(A).

Em geral adota-se a terminologia e notação do livro "Multiplicative Ideal Theory" de R. Gilmer, com as seguintes exceções:

(1) A diferença de dois conjuntos A e B é denotada por $A\setminus B$.

(2) Todos os anéis considerados têm identidade.

(3) O conteúdo de um polinômio f é denotado por C(f).

(4) Dizemos que um ideal P do anel A é primo se e só se $P \subset A$ (P é um subconjunto próprio de A) e $A\setminus P$ é um sistema multiplicativo de A (subconjunto multiplicativamente fechado de A).

(5) Dizemos que o anel A é local se e só se tem um único ideal maximal (A não é necessariamente noetheriano).

(6) Um anel B é chamado uma localização do anel A se e só se existe um sistema multiplicativo M de A tal que $B = A_M$, isto é, B é um anel de frações de A. Só consideram-se sistemas multiplicativos que contêm a identidade do anel A.

(7) Utiliza-se só o conceito de dimensão de Krull para um anel.

Denota-se por T(A) o anel total de frações do anel A, isto é, $T(A) = A_{Reg(A)}$.

Toda propriedade utilizada (que aparece em algum livro da "Bibliografia") será indicado citando o número dela seguido por um número entre parénteses, correspondente ao livro da "Bibliografia".

No capítulo II demonstram-se alguns resultados sobre conteúdos de polinômios e propriedades elementares dos anéis R⟨X⟩ e R(X).

Um primeiro resultado é o seguinte:

$f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ é um divisor de zero se e só se existe $c \in R\setminus\{0\}$ tal que $ca_i = 0$ para todo $i \in \{0,1,\ldots,n\}$.

Dito de outro modo, $f \in R[X]$ é um elemento regular de R[X] se e só se $0:C(f) = 0$.

Uma consequencia importante deste resultado é que $U \subseteq S \subseteq \subseteq Reg(R[X])$ e portanto R⟨X⟩ e R(X) são localizações regulares de R[X].

Outro resultado destacável é o seguinte:

Se $f \in R[X]$ tem conteúdo localmente principal, então para qualquer $g \in R[X]$, $C(fg) = C(f)C(g)$.

A extensão e contração de ideais entre R e R⟨X⟩e entre R e R(X) têm bom comportamento. De fato, R⟨X⟩ e R(X) são R-álgebras fielmente planas. Isto é consequência de ser R[X] um R-módulo livre, de ser a aplicação $I \longmapsto IR\langle X\rangle$, do reticulado dos ideais de R no reticulado dos ideais de R⟨X⟩, injetiva, e de ser a aplicação $M \longmapsto MR(X)$, de Max(R) em Max(R(X)), uma bijeção.

Demonstra-se que para cada ideal I de R, $R(X)/IR(X) = (R/I)(X)$. Uma consequência imediata deste resultado e da correspondência bijetiva entre Max(R) e Max(R(X)) é o seguinte fato: se K é um ideal maximal de R(X), então R(X)/K é um corpo infinito.

Um resultado simples, mas muito útil é o seguinte: se R é um anel local e $I = (a_1, a_2, \ldots, a_n)$ $(a_i \in R,\ 1 \leq i \leq n)$ é um ideal principal de R, então $I = (a_i)$ para algum $i \in \{1,2,\ldots,n\}$. Isto permite demonstrar , por exemplo, que para cada $f \in R[X]$,

C(f) é localmente principal se e só se $fR(X) = C(f)R(X)$. (Teorema 2.1 (3) de (1))

Demonstra-se que um ideal I de R é inversível se e só se é regular, localmente principal e finitamente gerado. Para cada ideal I de R, IR⟨X⟩ (ou IR(X)) é inversível se e só se I é localmente principal finitamente gerado e $0:I = 0$.

O resultado mais importante do capítulo II é o seguinte:

Todo ideal localmente principal finitamente gerado de R(X) é principal (teorema 2.1 (5) de (1)).

Disto resulta que (para um domínio de integridade R) R(X) tem uma propriedade de divisibilidade se e só se R tem esta propriedade "em relação a ideais inversíveis", como demonstra-se no capítulo V.

Também demonstram-se no capítulo II os seguintes fatos:
(a) R⟨X⟩ (ou R(X)) é um domínio de integridade se e só se R o é.
(b) R⟨X⟩ (ou R(X)) é um anel noetheriano se e só se R o é.

(c) Se R⟨X⟩ ou R(X) é integralmente fechado, então R também o é (Proposição 2.6 (1) de (1)).

(d) Seja R um domínio de integridade. Se R é integralmente fechado, então R⟨X⟩ e R(X) também são integralmente fechados (proposição 2.6 (2) de (1)).

No capítulo III determinam-se condições necessárias e suficientes (em termos do anel base R) para ser R⟨X⟩ e R(X) anéis aritméticos ou de Prüfer.

Demonstra-se que as seguintes afirmações são equivalentes:

(i) R é aritmético.

(ii) Os ideais de R_M estão totalmente ordenados, para todo M em Max(R).

(iii) $I \cap (J + K) = (I \cap J) + (I \cap K)$ para quaisquer ideais I, J, K de R.

(iv) Os ideais de R_P estão totalmente ordenados, para todo ideal primo P de R.

Portanto R é um domínio de Prüfer se e só se R é um domínio localmente de valorização, isto é, R é um domínio de integridade e R_M é um anel de valorização, para todo $M \in Max(R)$.

É fácil demonstrar que se R(X) (ou R⟨X⟩) é aritmético, então R é aritmético.

Por outro lado, se R é aritmético, então para cada f em R[X], C(f) é localmente principal, isto é, fR(X) = C(f)R(X). Isto permite demonstrar que se R é aritmético, então R(X) é de Bézout. Portanto as seguintes afirmações são equivalentes:

(1) R(X) é aritmético.

(2) R(X) é de Bézout.

(3) R é aritmético.

(Teorema 3.1 (1) de (1))

Seja R um domínio de integridade. Demonstram-se os seguintes fatos:

(i) Se Q é um ideal primo de R[X] tal que $(Q \cap R)[X] \subset Q$ e $R[X]_Q$ é um anel de valorização, então $Q \cap R = 0$ (lema 1 de (4)).

(ii) Se $a \in R\setminus\{0\}$, então $(aX + 1)R[X]$ é um ideal primo de $R[X]$.

Utilizando estas duas propriedades demonstra-se que se $R\langle X\rangle$ é aritmético, então $\dim R \leq 1$ e R_M é um corpo sempre que $M \subset P$ é uma cadeia de ideais primos de R.

Reciprocamente, se R é aritmético, $\dim R \leq 1$ e R_M é um corpo sempre que $M \subset P$ é uma cadeia de ideais primos de R, então $R\langle X\rangle$ é aritmético. Este fato demonstra-se sem dificuldade.

Utilizando propriedades de conteúdos de polinômios, consegue-se estabelecer uma condição necessária e suficiente para que R(X) seja um anel de Prüfer:

R(X) é um anel de Prüfer se e só se R é um anel fortemente de Prüfer (teorema 3.2 (1) de (1)).

Estabelece-se também a seguinte propriedade:

Para que $R\langle X\rangle$ seja um anel de Prüfer é necessário e suficiente que seja R um anel fortemente de Prüfer com $\dim R \leq 1$ e tal que R_M seja um corpo para cada cadeia $M \subset P$ de ideais primos de R (teorema 3.2 (2) de (1)).

Os ideais regulares de um anel R formam um reticulado. De fato, é claro que se I e J são ideais regulares de R, então $I + J$ é um ideal regular de R. Se I e J são ideais regulares de R, então existe $a \in I \cap Reg(R)$ e existe $b \in J \cap Reg(R)$. Logo $ab \in (I \cap J) \cap Reg(R)$ e portanto $I \cap J$ é um ideal regular de R.

Um ideal I de R é chamado semi-regular se e só se existe um ideal finitamente gerado J de R tal que $0:J = 0$ e $J \subseteq I$.

Os ideais semi-regulares de R ordenados pela inclusão formam um reticulado. De fato, se K e L são ideais semi-regulares de R, então existem ideais finitamente gerados I e J de R tais que $0:I = 0$, $0:J = 0$, $I \subseteq K$ e $J \subseteq L$. Logo $I + J$ é finitamente gerado, $0:(I + J) = (0:I) \cap (0:J) = 0$ e $I + J \subseteq K + L$. Portanto $K + L$ é semi-regular. Por outro lado, IJ é finitamente gerado, $0:(IJ) = (0:I):J = 0:J = 0$ e $IJ \subseteq I \cap J \subseteq K \cap L$, donde $K \cap L$ é semi-regular.

Dizemos que um anel R satisfaz a condição (A) se e só se todo ideal finitamente gerado I de R, com $0:I = 0$, é regular.

Observamos que um anel R satisfaz a condição (A) se e só se todo ideal semi-regular de R é regular.

Finalmente no capítulo III considera-se a aplicação

$$\theta: L(R) \longrightarrow L(R(X))$$
$$I \longmapsto IR(X)$$

onde L(R) e L(R(X)) são os reticulados de ideais de R e R(X), respectivamente. Demonstram-se os seguintes fatos:

- A aplicação θ preserva somas e interseções arbitrárias e produtos finitos de ideais.
- θ é sobrejetiva se e só se R é aritmético.(teorema 3.3 (1) de (1)).
- As seguintes afirmações são equivalentes:

(i) θ é um isomorfismo de reticulados entre o sub-reticulado dos ideais semi-regulares de R e o sub-reticulado dos ideais regulares de R(X).

(ii) Todo ideal regular de R(X) é extensão de um ideal de R.

(iii) R é um anel fortemente de Prüfer.

(Teorema 3.3 (2) de (1)).

- As seguintes afirmações são equivalentes:

(i) θ é um isomorfismo de reticulados entre os sub-reticulados dos ideais regulares de R e R(X).

(ii) Todo ideal principal regular de R(X) é extensão de um ideal regular de R.

(iii) R é um anel de Prüfer que satisfaz a condição (A).

(Corolário 3.4 de (1)).

O objetivo do capítulo IV é estabelecer as condições necessárias e suficientes (em termos do anel base R) para que R(X) seja um anel de Hilbert, isto é, um anel no qual todo ideal primo seja interseção de ideais maximais.

Facilmente demonstra-se que R(X) é um anel de Hilbert se e só se todo ideal primo de R(X) é a extensão de um ideal de R e R é um anel de Hilbert.

Dizemos que R satisfaz a condição (*) se e só se para ca-

da ideal primo Q de R[X], com $Q \subseteq M[X]$ para algum $M \in Max(R)$, temos $Q = P[X]$ para algum idal primo P de R (necessariamente $P = Q \cap R$).

Demonstra-se que R satisfaz a condição (*) se e só se todo ideal primo de R(X) é a extensão de um ideal de R.

Consequentemente temos: R(X) é um anel de Hilbert se e só se R é um anel de Hilbert e satisfaz a condição (*).

Denotamos por $\bar{R}$ o fecho integral do anel R. Então $\bar{R}[X]$ é inteiro sobre R[X]. Utilizando a propriedade (de incomparabilidade) INC e o teorema do ascenso para os anéis R[X] e $\bar{R}[X]$, demonstra-se que R satisfaz a condição (*) se e só se $\bar{R}$ a satisfaz (lema 4.2 de (1)).

Se R é um domínio de Prüfer, então R(X) é aritmético. Logo a aplicação $I \longmapsto IR(X)$, do reticulado dos ideais de R no reticulado dos ideais de R(X), é sobrejetiva. Portanto todo ideal primo de R(X) é extensão de um ideal de R e consequentemente R satisfaz a condição (*).

Reciprocamente, se R é um domínio integralmente fechado que satisfaz a condição (*), então R é um domínio de Prüfer. Para demonstrar este fato consideramos algumas propriedades dos "places" e anéis de valorização sobre um corpo.

Finalmente obtem-se a propriedade mais importante do capítulo IV:

R(X) é um anel de Hilbert se e só se R é um anel de Hilbert e para cada ideal primo minimal P de R, o fecho integral de R/P é um domínio de Prüfer (teorema 4.3 de (1)).

No capítulo V estudam-se as propriedades de divisibilidade dos anéis R(X) e R(X). Demonstram-se os seguintes teoremas:

Teorema 1 - As seguintes afirmações são equivalentes:

(a) R(X) é um G-GCD domínio.

(b) R(X) é um G-GCD domínio.

(c) R(X) é um GCD-domínio.

(d) R é um G-GCD domínio.

(Teorema 5.1 (1) de (1)).

Teorema 2 - $R\langle X\rangle$ é um GCD-domínio se e só se R é um GCD-domínio.

(Teorema 5.1 (2) de (1)).

Teorema 3 - $R\langle X\rangle$ é um domínio fatorial se e só se R é um domínio fatorial (proposição 1.2 de (10)).

Teorema 4 - $R\langle X\rangle$ é um domínio de ideais principais se e só se R é um domínio de ideais principais (proposição 2.5 de (10)).

Teorema 5 - As seguintes afirmações são equivalentes:

(a) $R\langle X\rangle$ é um domínio de Dedekind.

(b) $R(X)$ é um domínio de Dedekind.

(c) $R(X)$ é um domínio de ideais principais.

(d) R é um domínio de Dedekind.

(Teorema 5.4 (1) de (1)).

Logo desenvolve-se a teoria dos domínios de Krull. Demonstra-se, por exemplo, que a única família de definição de um domínio de Krull R é $\{Rp;\ P \in X^{(1)}(R)\}$, onde $X^{(1)}(R)$ é o conjunto de todos os ideais primos minimais de R; toda localização de um domínio de Krull é um domínio de Krull; se R é um domínio de Krull, então $R[X]$ é um domínio de Krull.

Para os anéis $R\langle X\rangle$ e $R(X)$ obtemos o seguinte teorema:

Teorema 6 - As seguintes afirmações são equivalentes:

(a) $R\langle X\rangle$ é um domínio de Krull.

(b) $R(X)$ é um domínio de Krull.

(c) R é um domínio de Krull.

(Teorema 5.2 (1) de (1)).

Caracterizam-se os π-domínios da seguinte maneira:

R é um π-domínio se e só se R é um domínio de Krull e um G-GCD domínio (teorema 3 de (3)).

Após disto obtem-se o seguinte teorema:

Teorema 7 - As seguintes afirmações são equivalentes:

(a) $R\ X$ é um π-domínio.

(b) $R(X)$ é um π-domínio.

(c) $R(X)$ é um domínio fatorial.

(d) R é um π-domínio.

(Teorema 5.3 de (1)).

Define-se o semigrupo dos divisores de um domínio de integridade R da seguinte maneira:

Seja R um domínio de integridade. Denota-se por $\mathfrak{F}(R)$ o conjunto de todos os ideais fracionários não nulos de R. Em $\mathfrak{F}(R)$ define-se uma relação $\sim$ da seguinte maneira: $K \sim L$ se e só se $K_v = L_v$. Esta relação é de equivalencia e para cada $K \in \mathfrak{F}(R)$ denota-se por div(K) a classe de equivalencia de K. Escreve-se $\mathfrak{D}(R) = \{div(K);\ K \in \mathfrak{F}(R)\}$ e cada elemento de $\mathfrak{D}(R)$ é chamado um divisor de R. Define-se uma operação de adição em $\mathfrak{D}(R)$: $div(K) + div(L) = div(KL)$. Com esta operação, $\mathfrak{D}(R)$ é um semigrupo abeliano aditivo. Define-se uma ordem em $\mathfrak{D}(R)$: $div(K) \leq div(L)$ se e só se $L_v \subseteq K_v$. Esta ordem é compatível com a adição.

Demonstra-se que $\mathfrak{D}(R)$ é um grupo se e só se R é um domínio completamente integralmente fechado.

Da definição de domínio de Krull resulta que todo domínio de Krull é completamente integralmente fechado. Portanto, se R é um domínio de Krull, então $\mathfrak{D}(R)$ é um grupo.

Definem-se o grupo de classes de divisores e o grupo de Picard de um domínio completamente integralmente fechado da seguinte maneira:

Seja R um domínio completamente integralmente fechado. Os conjuntos $\mathfrak{P}(R) = \{div(x);\ x \in T(R)\setminus\{0\}\}$ e $\mathfrak{C}(R) =$ $= \{div(K);\ K$ é um ideal fracionário inversível de $R\}$ são subgrupos de $\mathfrak{D}(R)$. O grupo $Cl(R) = \mathfrak{D}(R)/\mathfrak{P}(R)$ é chamado o grupo de classes de divisores de R e o grupo $Pic(R) = \mathfrak{D}(R)/\mathfrak{C}(R)$ é chamado o grupo de Picard de R. Pic(R) é um subgrupo de Cl(R). O grupo $G(R) = Cl(R)/Pic(R)$ é chamado o grupo de classes local de R.

Demonstra-se que para um domínio de Krull R, valem as seguintes afirmações:

- $\mathfrak{D}(R)$, o grupo dos divisores de R, é um $\mathbb{Z}$-módulo livre com $\mathbb{Z}$-base $\{div(P);\ P$ é um ideal primo minimal de $R\}$.
- A v-operação sobre R e a w-operação sobre R induzida pela família de definição de R são iguais (teorema 44.2 de (7)).

- Se M é um sistema multiplicativo de R, então a aplicação $g: D(R) \longrightarrow D(R_M)$, dada por $g(div(K)) = div(KR_M)$ está bem definida e induz um epimorfismo de $Cl(R)$ sobre $Cl(R_M)$ (teorema 8.27 de (9)).
- $Cl(R[X])$ é canonicamente isomorfo a $Cl(R)$ (teorema 45.5 de (7)).
- $Cl(R\langle X\rangle)$ é canonicamente isomorfo a $Cl(R)$ e $pic(R\langle X\rangle)$ é canonicamente isomorfo a $Pic(R)$ (teorema 5.2 (2) de (1)).

Para relacionar os grupos $Cl(R(X))$ e $Cl(R)$ consideram-se vários resultados de Álgebra Homólogica, tais como o Lema dos Cinco, o Lema da Serpente, propriedades de R-módulos livres, projetivos, planos, fielmente planos e de apresentação finita.

Finalmente demonstra-se que se R é um domínio de Krull, então $Cl(R(X))$ é canonicamente isomorfo a $G(R) = Cl(R)/Pic(R)$ (corolário 6 de (5)).

CAPÍTULO II

PROPRIEDADES ELEMENTARES DE R⟨X⟩ E R(X)

Neste capítulo demonstraremos algumas propriedades elementares dos anéis R⟨X⟩ e R(X) que serão usadas através do resto do trabalho.

LEMA 1 - Seja $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$. São equivalentes:

(a) f é um divisor de zero.

(b) Existe $c \in R\setminus\{0\}$ tal que $ca_i = 0$, $0 \leqslant i \leqslant n$.

DEMONSTRAÇÃO - É claro que (b) implica (a).

(a) $\Longrightarrow$ (b). Suponhamos que f é um divisor de zero. Então existe $h \in R[X]\setminus\{0\}$ tal que $fh = 0$. Escolhamos um polinômio $g = b_0 + b_1X + \cdots + b_mX^m \in R[X]$ de grau mínimo tal que $fg = 0$. Como $a_nb_m = 0$, então $gr(a_ng) < gr(g)$; logo $a_ng = 0$, pois $f(a_ng) = a_nfg = 0$. Demonstraremos por indução sobre r que $a_{n-r}g = 0$ para todo $r \in \{0,1,\ldots,n\}$. Se $r = 0$, então o resultado é verdadeiro. Suponhamos que $r > 0$ e que o resultado é verdadeiro para cada $k \in \{0,1,\ldots,r-1\}$, isto é, $a_{n-k}b = 0$ para cada $k \in \{0,1,\ldots,r-1\}$ e para cada $j \in \{0,1,\ldots,m\}$. O coeficiente de X^{n+m-r} no polinômio fg é $c_{n+m-r} = a_{n-r}b_m + a_{n-r+1}b_{m-1} + \cdots + a_{n-r+s}b_{m-s}$ onde $s = \min\{m,r\}$. Como $fg = 0$, então $c_{m+n-r} = 0$. Pela hipótese indutiva $a_{n-r+1}b_{m-1} = \cdots = a_{n-r+s}b_{m-s} = 0$. Portanto $a_{n-r}b_m = 0$. Mas isto implica que $gr(a_{n-r}g) < gr(g)$; logo $a_{n-r}g = 0$, pois $f(a_{n-r}g) = a_{n-r}fg = 0$. Em consequência $a_ig = 0$ para todo i em $\{0,1,\ldots,n\}$, donde $a_ib_j = 0$, $0 \leqslant i \leqslant n$, $0 \leqslant j \leqslant m$. Em particular $b_ma_i = 0$, $0 \leqslant i \leqslant n$. Se $c = b_m \in R\setminus\{0\}$, então $ca_i = 0$, $0 \leqslant i \leqslant n$.

C.Q.D.

PROPOSIÇÃO 1 - (a) $U = \{ f \in R[X];\ f \text{ é mônico} \}$ é multiplicativamente fechado.

(b) $U \subseteq S = \{ f \in R[X] ;\ C(f) = R \} \subseteq Reg(R[X])$.

(c) $S = R[X] \setminus \bigcup \{ M[X] ;\ M \in Max(R) \}$.

(d) S é multiplicativamente fechado.

DEMONSTRAÇÃO - (a) É imediata.

(b) É claro que $U \subseteq S$. Seja $f = a_0 + a_1 X + \cdots\cdots + a_n X^n \in S$. Suponhamos que f não é regular. Então f é um divisor de zero e portanto existe $c \in R \setminus \{0\}$ tal que $ca_i = 0$ para todo $i \in \{0,1,\ldots,n\}$; logo $(c) = (c)R = (c)(a_0, a_1, \ldots, a_n) = (ca_0, ca_1, \ldots, ca_n) = (0)$. Isto implica que $c = 0$ o que é uma contradição. Em consequência f é regular, isto é, $f \in Reg(R[X])$.

(c) $f \in S$ se e só se $C(f) = R$

" $C(f) \not\subseteq M$ para todo $M \in Max(R)$

" $f \notin M[X]$ para todo $M \in Max(R)$

" $f \in R[X] \setminus \bigcup \{M[X] ;\ M \in Max(R)\}$.

(d) $fg \in R[X] \setminus S = \bigcup \{M[X] ;\ M \in Max(R)\} \Longrightarrow fg \in M[X]$ para algum $M \in Max(R) \Longrightarrow f \in M[X]$ ou $g \in M[X]$ para algum $M \in Max(R)$, pois $M[X]$ é um ideal primo de $R[X] \Longrightarrow f \in R[X] \setminus S$ ou $g \in R[X] \setminus S$. Em consequência $f \in S$ e $g \in S$ implica $fg \in S$.

C.Q.D.

OBSERVAÇÕES - (1) $R[X] \subseteq R\langle X \rangle \subseteq R(X) \subseteq T(R[X]) = R[X]_{Reg(R[X])}$.

(2) Se R é um corpo, então $S = R[X] \setminus \{0\}$ e portanto $R(X) = R[X]_S = \{ f/g ;\ f,g \in R[X] ,\ g \neq 0 \}$.

(3) Como na parte (c) da proposição 1, demonstra-se que $\{f \in R[X,Y];\ C(f) = R\} = R[X,Y] \setminus \bigcup \{MR[X,Y];\ M \in Max(R)\}$.

PROPOSIÇÃO 2 - Para todo $f \in R[X]$,

$$fR\langle X\rangle \subseteq C(f)R\langle X\rangle \text{ e } fR(X) \subseteq C(f)R(X)$$

DEMONSTRAÇÃO - Sejam $f = a_0 + a_1X + \cdots + a_nX^n$, $g \in R[X]$, $h \in U$. Temos

$$f(g/h) = \frac{a_0 g}{h} + \frac{a_1 Xg}{h} + \cdots + \frac{a_n X^n g}{h} \in C(f)R\langle X\rangle.$$

Similarmente demonstra-se que $fR(X) \subseteq C(f)R(X)$.

C.Q.D.

PROPOSIÇÃO 3 - Sejam $f, g \in R[X]\setminus\{0\}$. Se $m = gr(g)$, então

$$(C(f))^{m+1}C(g) = (C(f))^m C(fg)$$

DEMONSTRAÇÃO - Se f é um monômio, digamos $f = a_nX^n$, $a_n \neq 0$, então $(C(f))^{m+1}C(g) = (a_n^{m+1})C(g) = (a_n^m)(a_n)C(g) = (a_n^m)C(a_n g) = (C(f))^m C(fg)$. Se g é um monômio, digamos $g = b_mX^m$, $b_m \neq 0$, então $(C(f))^{m+1}C(g) = (C(f))^{m+1}(b_m) = (C(f))^m C(b_m f) = (C(f))^m C(fg)$.

Agora consideremos $f, g \in R[X]\setminus\{0\}$ quaisquer. Sejam

$$f = a_0 + a_1X + \cdots + a_nX^n,\ a_n \neq 0$$

$$g = b_0 + b_1X + \cdots + b_mX^m,\ b_m \neq 0.$$

Então $fg = c_0 + c_1X + \cdots + c_{n+m}X^{n+m}$, onde $c_\kappa = \sum_{i+j=\kappa} a_i b_j$. É claro que $C(fg) \subseteq C(f)C(g)$. Portanto $(C(f))^m C(fg) \subseteq (C(f))^{m+1}C(g)$. Demonstraremos que $(C(f))^{m+1}C(g) \subseteq (C(f))^m C(fg)$ por indução sobre os graus de f e g.

Se $gr(f) = 0$ ou $gr(g) = 0$, então o resultado é verdadeiro, pois neste caso f é um monômio ou g é um monômio.

Suponhamos que f e g não são monômios e consideremos as seguintes hipóteses indutivas:

(a) Se $p, q \in R[X]$, $gr(p) < n$ e $gr(q) = m$, então $(C(p))^{m+1}C(q) \subseteq$

$\subseteq (C(p))^m C(pq)$.

(b) Se $p, q \in R[X]$, $gr(p) = n$ e $gr(q) = s < m$, então $(C(p))^{s+1} C(q) \subseteq (C(p))^s C(pq)$.

Sejam $p = f - a_n X^n$, $q = g - b_m X^m$. Então

$$pg = (f - a_n X^n)g = fg - a_n X^n g$$
$$= c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} + (c_n - a_n b_0) X^n + \cdots + (c_{n+m-1} - a_n b_{m-1}) X^{n+m-1}$$

$$fq = f(g - b_m X^m) = fg - b_m X^m f$$
$$= c_0 + c_1 X + \cdots + c_{m-1} X^{m-1} + (c_m - a_0 b_m) X^m + \cdots + (c_{n+m-1} - a_{n-1} b_m) X^{n+m-1}$$

Logo $C(pg) = (c_0, c_1, \ldots, c_{n-1}, c_n - a_n b_0, \ldots, c_{n+m-1} - a_n b_{m-1})$
$\subseteq (c_0, c_1, \ldots, c_{n+m}) + a_n (b_0, b_1, \ldots, b_{m-1})$
$= C(fg) + a_n C(q)$.

Similarmente resulta que $C(fq) \subseteq C(fg) + b_m C(p)$.

Como $(C(f))^{m+1} C(g)$ é gerado por elementos da forma $a = a_0^{r_0} a_1^{r_1} \ldots a_n^{r_n} b_j$, onde $r_0 + r_1 + \cdots + r_n = m+1$, $0 \leq j \leq m$, então é suficiente demostrar que cada elemento desta forma está contido em $(C(f))^m C(fg)$. Se $r_n \neq 0$ e $j = m$, então $a = a_0^{r_0} a_1^{r_1} \ldots a_n^{r_n - 1} a_n b_m = a_0^{r_0} a_1^{r_1} \ldots a_n^{r_n - 1} c_{n+m} \in (C(f))^m C(fg)$. Se $r_n \neq 0$ e $j < m$, então $a \in (C(f))^m (a_n) C(q)$. Finalmente, se $r_n = 0$, então $a \in (C(p))^{m+1} C(g)$. Portanto

(1) $(C(f))^{m+1} C(g) \subseteq (C(f))^m C(fg) + (C(p))^{m+1} C(g) + (C(f))^m (a_n) C(q)$

Mas pela hipótese indutiva (a), $(C(p))^{m+1} C(g) \subseteq \subseteq (C(p))^m C(pg)$ e temos visto que $C(pg) \subseteq C(fg) + a_n C(q)$; logo

$$(C(p))^{m+1} C(g) \subseteq (C(p))^m C(fg) + (C(p))^m (a_n) C(q)$$
$$\subseteq (C(f))^m C(fg) + (C(f))^m (a_n) C(q).$$

Disto e de (1), temos

(2) $(C(f))^{m+1} C(g) \subseteq (C(f))^m C(fg) + (C(f))^m (a_n) C(q)$.

Seja $s = gr(q)$. Então $(C(f))^{s+1} C(q) \subseteq (C(f))^s C(fq)$ pela hipótese indutiva (b). Como $s \leq m-1$, então

$$(C(f))^m C(q) = (C(f))^{m-s-1} (C(f))^{s+1} C(q)$$
$$\subseteq (C(f))^{m-s-1} (C(f))^s C(fq)$$
$$= (C(f))^{m-1} C(fq).$$

Mas $C(fq) \subseteq C(fg) + b_m C(p)$; logo

(3) $(C(f))^m (a_n) C(q) \subseteq (C(f))^{m-1} (a_n) C(fg) + (C(f))^{m-1} (a_n) (b_m) C(p)$

$$\subseteq (C(f))^m C(fg) + c_{n+m}(C(f))^{m-1} C(p)$$
$$\subseteq (C(f))^m C(fg).$$

Como consequência de (2) e (3), temos

$$(C(f))^{m+1} C(g) \subseteq (C(f))^m C(fg).$$

C.Q.D.

DEFINIÇÃO - Seja I um ideal de R. Dizemos que I é localmente principal se IR_M é principal para todo ideal $M \in Max(R)$.

LEMA 2. Seja $f \in R[X]$. Se $C(f) = (a)$, então existe $h \in R[X]$ tal que $f = ah$ e $C(h) = R$.

DEMONSTRAÇÃO - Seja $f = a_0 + a_1 X + \cdots + a_n X^n$. Como $(a_0, a_1, \ldots, a_n) = C(f) = (a)$, então para cada $i \in \{0,1,\ldots,n\}$, existe $r_i \in R$ tal que $a_i = r_i a$ e existem $s_0, s_1, \ldots, s_n \in R$ tais que

$$a = s_0 a_0 + s_1 a_1 + \cdots + s_n a_n$$

Logo

$$a = s_0 r_0 a + s_1 r_1 a + \cdots + s_n r_n a$$
$$= ad$$

onde $d = s_0 r_0 + s_1 r_1 + \cdots + s_n r_n$.

Como

$$1 = d + (1-d)$$
$$= s_0 r_0 + s_1 r_1 + \cdots + s_n r_n + (1-d)$$

é um elemento de $(r_0, r_1, \ldots, r_n, 1-d)$, então

$$(r_0, r_1, \ldots, r_n, 1-d) = R.$$

Seja $h = r_0 + r_1 X + \cdots + r_n X^n + (1-d)X^{n+1}$. Como $a = ad$, então $a(1-d) = 0$ e portanto

$$ah = ar_0 + ar_1 X + \cdots + ar_n X^n + a(1-d)X^{n+1}$$
$$= a_0 + a_1 X + \cdots + a_n X^n = f$$

e $C(h) = (r_0, r_1, \ldots, r_n, 1-d) = R$.

C.Q.D.

PROPOSIÇÃO 4 - Seja $f \in R[X]$. Se $C(f)$ é localmente principal, então para todo $g \in R[X]$

$$C(fg) = C(f)C(g)$$

DEMONSTRAÇÃO - Por localização, podemos supor que R é local e $C(f)$ é principal. Seja $C(f) = (a)$. Então existe $h \in R[X]$ tal que $f = ah$ e $C(h) = R = (1)$. Se $f = 0$ ou $g = 0$, então $C(fg) = (0) = C(f)C(g)$. Se $f \neq 0$, $g \neq 0$ e $m = gr(g)$, então $h \neq 0$ e $C(hg) = (1)^m C(hg) = (C(h))^m C(hg) = (C(h))^{m+1} C(g) = (1)^{m+1} C(g) = (1)C(g) = C(h)C(g)$. Em consequência $C(fg) = C(ahg) = aC(hg) = aC(h)C(g) = C(ah)C(g) = C(f)C(g)$.

C.Q.D.

LEMA 3. Seja I um ideal de R. Se I é idempotente e finitamente gerado, então I é principal e gerado por um elemento idempotente.

DEMONSTRAÇÃO - Seja $I = (a_1, a_2, \ldots, a_n)$. É claro que $a_1 I + \cdots + a_n I \subseteq I$. Sejam $a, b \in I$. Então $a = r_1 a_1 + \cdots + r_n a_n$ para alguns $r_1, \ldots, r_n \in R$. Logo $ab = a_1(r_1 b) + \cdots + a_n(r_n b) \in a_1 I + \cdots + a_n I$. Como todo elemento de I^2 é uma soma finita de elementos da forma $c = ab$, com $a, b \in I$, então $I = I^2 \subseteq a_1 I + \cdots + a_n I$ e assim $I = a_1 I + \cdots + a_n I$.

Para cada $i \in \{1, 2, \ldots, n\}$, tem-se $a_i = e_{i1} a_1 + \cdots + e_{in} a_n$, onde $e_{ij} \in I$, $1 \leq i, j \leq n$. Portanto

$$\begin{aligned}
(e_{11} - 1)a_1 + e_{12} a_2 + \cdots + e_{1n} a_n &= 0 \\
e_{21} a_1 + (e_{22} - 1)a_2 + \cdots + e_{2n} a_n &= 0 \\
&\cdots\cdots\cdots\cdots \\
e_{n1} a_1 + e_{n2} a_2 + \cdots + (e_{nn} - 1)a_n &= 0
\end{aligned}$$

Seja d o determinante deste sistema linear. Então $da_i = 0$, $1 \leq i \leq n$, pela regra de Cramer. Logo $da = 0$ para todo $a \in I$, pois $a_1, a_2, \ldots, a_n$ geram I. Mas d é da forma $d = e - 1$, onde $e \in I$.

Em consequência $(e-1)a = da = 0$ para todo $a \in I$, isto é, $a = ae$ para todo $a \in I$. Em particular $e = e^2$. Resulta assim que o elemento e é idempotente e $I = (e)$.

C.Q.D.

TEOREMA 1 - Todo elemento idempotente de R(X) é um elemento de R.

DEMONSTRAÇÃO - Seja $f/g \in R(X)$ idempotente, com $C(g) = R$. Como $f/g = f^2/g^2$, então $fg^2 = gf^2$ e portanto $fg = f^2$, pois g é regular. Sendo C(g) principal, temos que $C(f)C(g) = C(fg)$. Logo $C(f) = C(f)R = C(f)C(g) = C(fg) = C(f^2) \subseteq (C(f))^2$ e portanto $(C(f))^2 = C(f)$, isto é, C(f) é idempotente e finitamente gerado. Então, pelo lema 3, existe $e \in R$ idempotente tal que $C(f) = (e)$. Segundo o lema 2 existe $h \in R[X]$ tal que $f = eh$ e $C(h) = R$. Então $eh^2/g^2 = e^2h^2/g^2 = f^2/g^2 = eh/g$ e portanto $f/g = eh/g = e \in R$, pois h e g são regulares.

C.Q.D.

PROPOSIÇÃO 5 - (1) Se I é um ideal de R, então

$$IR\langle X\rangle \cap R = I = IR(X) \cap R$$

(2) Sejam I e J ideais de R. São equivalentes:

(a) $IR\langle X\rangle = JR\langle X\rangle$.

(b) $IR(X) = JR(X)$.

(c) $I = J$.

DEMONSTRAÇÃO - (1) Como $IR[X] \cap R = I$, então para demonstrar que $IR(X) \cap R = I$, é suficiente demonstrar que $IR(X) \cap R[X] \subseteq IR[X]$. Se $f \in IR(X) \cap R[X]$, então existe $g \in S$ tal que $fg \in IR[X]$. Logo $C(f) = C(f)R = C(f)C(g) = C(fg) \subseteq I$ e portanto

$f \in I[R[X]]$. Em consequência $I \subseteq I[R(X)] \cap R = I[R(X)] \cap R[X] \cap R \subseteq$
$\subseteq I[R[X]] \cap R = I$, isto é, $I[R(X)] \cap R = I$.

Por outro lado, $I \subseteq I[R(X)] \cap R \subseteq I[R(X)] \cap R = I$, ou seja $I[R(X)] \cap R = I$.

(2) É uma consequência imediata de (1).

C.Q.D.

TEOREMA 2 - Existe uma correspondencia bijetiva entre os ideais maximais de R e de R(X), dada por $M \longmapsto MR(X)$.

DEMONSTRAÇÃO - Seja $M \in Max(R)$. Suponhamos que $f/g \in R(X) \setminus MR(X)$. Então $f \notin M[X]$. Se $f = a_0 + a_1X + \cdots + a_nX^n$, então existe $i \in \{0,1,\ldots,n\}$ tal que $a_i \notin M$. Como $M \in Max(R)$, então existem $m \in M$, $r \in R$ tais que $m + ra_i = 1$; logo o coeficiente de X^i no polinômio $mX^i + rf$ é 1 e portanto tal polinômio é um elemento de S. Em consequência $(mX^i + rf)/g \in U(R(X))$. Isto implica que $MR(X) + (f/g)R(X) = R(X)$, pois

$$\frac{mX^i + rf}{g} = \frac{mX^i}{g} + r\frac{f}{g} \in MR(X) + (f/g)R(X).$$

Portanto $MR(X) \in Max(R(X))$. Pela proposição anterior $M \longmapsto MR(X)$ é injetiva. Agora demonstraremos que também é sobrejetiva. Seja $Q \in Max(R(X))$. O conjunto

$M = \{a \in R;\ a$ é coeficiente de algum elemento de $Q \cap R[X]\}$

é um ideal de R. De fato, se $a, b \in M$, $r \in R$, então existem $f = a_0 + a_1X + \cdots + a_nX^n$, $g = b_0 + b_1X + \cdots + b_mX^m \in Q \cap R[X]$ tais que $a = a_i$ e $b = b_j$ para algum $i \in \{0,1,\ldots,n\}$ e algum $j \in \{0,1,\ldots,m\}$. Podemos supor que $i \leq j$. Então a-b é coeficiente de $X^{j-i}f - g \in Q \cap R[X]$ e ra é coeficiente de $rf \in Q \cap R[X]$. Portanto a-b, $ra \in M$. Se $M = R$, então 1 é elemento de M e portanto existe $f \in Q \cap R[X]$, com 1 como um de seus coeficientes; mas isto implica que $C(f) = R$ e assim $f \in U(R(X))$ e $f \in Q$, o que é

é uma contradição. Logo $M \neq R$ e portanto $MR(X) \neq R(X)$. Vejamos agora que $MR(X) = Q$ e que $M \in Max(R)$. Se $h/k \in Q$, então $h = (h/k)k \in Q \cap R[X] \subseteq M[X]$ e portanto $h/k \in MR(X)$. Logo $Q \subseteq MR(X)$. Como $Q \in Max(R(X))$, então $Q = MR(X)$. Se I é um ideal de R e $M \subsetneq I \subset R$, então $Q = MR(X) \subseteq IR(X) \subset R(X)$. Logo $MR(X) = IR(X)$ e portanto $M = I$. Em consequência $M \in Max(R)$.

C.Q.D.

PROPOSIÇÃO 6 - (a) Se P é um ideal primo de R, então

$$R_P[X] \cong R[X]_{R\setminus P}$$

$$R_P(X) = R_P[X]_{PR_P[X]} \cong R[X]_{P[X]} \cong R(X)_{PR(X)} \cong R\langle X\rangle_{PR\langle X\rangle}$$

(b) Se P é um ideal primo de R e Q é um ideal primo de $R[X]$, com $P \subsetneq Q$ e $Q \cap U = 0$, então $R[X]_Q \cong (R[X]_U)_{Q_U} \cong (R_P[X])_{Q_P}$.

(c) Se I é um ideal de R, então $R(X)/IR(X) = (R/I)(X)$.

DEMONSTRAÇÃO - (a) Definimos $\mu: R[X]_{R\setminus P} \longrightarrow R_P[X]$ por $\mu((a_0 + a_1X + \cdots + a_nX^n)/s) = (a_0/s) + (a_1/s)X + \cdots + (a_n/s)X^n$. Comprova-se sem dificuldade que μ está bem definida e é um isomorfismo de anéis.

Seja $A = R_P$. Para demonstrar que $R_P(X) = R_P[X]_{PR_P[X]}$ é suficiente demonstrar que $\{f \in A[X];\ C(f) = A\} = A[X]\setminus PA[X]$. Seja $f = a_0 + a_1X + \cdots + a_nX^n \in A[X]$. Então $C(f) = a_0A + a_1A + \cdots + a_nA$. Como A é local, então $C(f) = A$ se e só se $a_i \in U(A) = A\setminus PA$ para algum $i \in \{0,1,\ldots,n\}$; logo $C(f) = A$ se e só se $f \in A[X]\setminus PA[X]$.

Agora demonstraremos que $R_P[X]_{PR_P[X]} \cong R[X]_{P[X]}$. Dado $q = (b_0/s_0) + (b_1/s_1)X + \cdots + (b_n/s_n)X^n \in R_P[X]$, podemos escrever $q = (a_0/s) + (a_1/s)X + \cdots + (a_n/s)X^n$, onde $a_i = s_0s_1 \cdots s_{i-1}s_{i+1} \cdots s_nb_i$, $0 \leq i \leq n$, $s = s_0s_1 \cdots s_n \in R\setminus P$. Denotaremos o polinômio $(a_0/s) + (a_1/s)X + \cdots + (a_n/s)X^n$ por

$(a_0 + a_1X + \cdots + a_nX^n)/s$. Assim, todo elemento de $R_p[X]$ é da forma $q = f/s$, onde $f \in R[X]$, $s \in R\setminus P$. Com esta notação, observamos que se $f,g \in R[X]$ e $s,t \in R\setminus P$, então

$$\frac{f}{s}\,\frac{g}{t} = \frac{fg}{st} \quad \text{e} \quad \frac{f}{s} + \frac{g}{t} = \frac{tf}{st} + \frac{sg}{st} = \frac{tf + sg}{st}$$

Definimos $\theta: R_p[X]_{PR_p[X]} \longrightarrow R[X]_{P[X]}$ por $\theta((f/s)/(g/t)) = tf/(sg)$. É claro que θ está bem definida e que preserva produtos. Se f_1/s_1, $f_2/s_2 \in R_p[X]$, $g_1/t_1, g_2/t_2 \notin PR_p[X]$, então

$$\frac{f_1/s_1}{g_1/t_1} + \frac{f_2/s_2}{g_2/t_2} = \frac{f_1 g_2/(s_1 t_2) + f_2 g_1/(s_2 t_1)}{g_1 g_2/(t_1 t_2)}$$

$$= \frac{(s_2 t_1 f_1 g_2 + s_1 t_2 f_2 g_1)/(s_1 s_2 t_1 t_2)}{g_1 g_2/(t_1 t_2)}$$

Logo

$$\theta\left(\frac{f_1/s_1}{g_1/t_1} + \frac{f_2/s_2}{g_2/t_2}\right) = \frac{t_1 t_2 (s_2 t_1 f_1 g_2 + s_1 t_2 f_2 g_1)}{s_1 s_2 t_1 t_2 g_1 g_2}$$

$$= \frac{s_2 t_1 f_1 g_2 + s_1 t_2 f_2 g_1}{s_1 s_2 g_1 g_2}$$

$$= \frac{t_1 f_1 g_2}{s_1 g_1 g_2} + \frac{t_2 f_2 g_1}{s_2 g_1 g_2}$$

$$= \frac{t_1 f_1}{s_1 g_1} + \frac{t_2 f_2}{s_2 g_2}$$

$$= \theta\left(\frac{f_1/s_1}{g_1/t_1}\right) + \theta\left(\frac{f_2/s_2}{g_2/t_2}\right)$$

Portanto θ é um homomorfismo de anéis. Dado f/g em $R[X]_{P[X]}$, vemos que $\theta((f/1)/(g/1)) = f/g$. Em consequência θ é sobrejetivo. Se $\theta((f/s)/(g/t)) = 0$, então $tf/(sg) = 0$; logo existe $h \in R[X]\setminus P[X]$ tal que $tfh = 0$. Então $(f/s)(th/t) = 0$, onde $th/t \in R_p[X]\setminus PR_p[X]$; logo $(f/s)/(g/t) = 0$. Em consequência θ é injetivo. Assim temos demonstrado que θ é um isomorfismo de a-

néis.

Similarmente demonstra-se que

$$\varphi : R(X)_{PR(X)} \longrightarrow R[X]_{P[X]}$$
$$\frac{f/h}{g/k} \longmapsto \frac{kf}{hg}$$

$$\lambda : R(X)_{PR(X)} \longrightarrow R[X]_{P[X]}$$
$$\frac{f/h}{g/k} \longmapsto \frac{kf}{hg}$$

são isomorfismos de anéis.

(b) Definimos $\theta: R[X]_Q \longrightarrow (R[X]_U)_{Q_U}$ por $\theta(f/g) = (f/1)/(g/1)$. Se $f/g = h/k \in R[X]_Q$ (aqui $f, h \in R[X]$, $g, k \in R[X]\setminus Q$), então existe $p \in R[X]\setminus Q$ tal que $pkf = pgh$. Logo $(p/1)(k/1)(f/1) = (pkf)/1 = (pgh)/1 = (p/1)(g/1)(h/1)$ em $R[X]_U$. Se $p/1 \in Q_U$, então $p/1 = q/u$ para algum $q \in Q$ e algum $u \in U$. Portanto $tup = tq \in Q$ para algum $t \in U$. Como Q é um ideal primo de $R[X]$, então $tu \in Q$ ou $p \in Q$. Mas $tu \in U$ e $Q \cap U = \emptyset$; logo $tu \notin Q$ e portanto $p \in Q$, o que é uma contradição. Consequentemente $p/1$ é um elemento de $R[X]_U\setminus Q_U$. Então $(f/1)/(g/1) = (h/1)/(k/1)$ e θ está bem definida. Comprova-se sem deficuldade que θ é um homomorfismo de anéis. Se $\theta(f/g) = 0$, então $(f/1)/(g/1) = 0$. Logo $(h/k)(f/1) = 0$ para algum $h \in R[X]\setminus Q$ e algum $k \in U$. Portanto $hf/k = 0$ em $R[X]_U$. Então $hf = 0$, donde $f/g = hf/(hg) = 0$. Em consequência θ é injetivo. Se $(f/g)/(h/k) \in (R[X]_U)_{Q_U}$ (aqui $f \in R[X]$, $h \in R[X]\setminus Q$, $g, k \in U$), então $(f/g)/(h/k) = (kf/1)/(gh/1)$, pois $(gh/1)(f/g) = ghf/g = hf/1 = khf/k = (kf/1)(h/k)$ em $R[X]_U$. Como $g \in U$, então $g \notin Q$, pois $Q \cap U = \emptyset$. Logo $gh \in R[X]\setminus Q$ e portanto $kf/(gh) \in R[X]_Q$ e $(f/g)/(h/k) = (kf/1)/(gh/1) = \theta(kf/(gh))$. Consequentemente θ é sobrejetivo.

Similarmente demonstra-se que a aplicação $\varphi: R[X]_Q \longrightarrow (R[X]_P)_{Q_P}$ dada por $(f/g) = (f/1)/(g/1)$ está bem definida e é um isomorfismo de anéis. Como $R[X]_P \cong R_P[X]$, então $R[X]_Q \cong (R_P[X])_{Q_P}$.

(c) Consideremos o isomorfismo de anéis
$\lambda: R[X]/IR[X] \longrightarrow (R/I)[X]$ definido por $\lambda(\sum_{i=0}^{n} a_i X^i + IR[X]) = \sum_{i=0}^{n} (a_i + I)X^i$. Seja $A = R/I$. Observamos que $C_R(\sum_{i=0}^{n} a_i X^i) = R$, isto é, $\sum_{i=0}^{n} a_i X^i \in S$, implica $C_A(\lambda(\sum_{i=0}^{n} a_i X^i + IR[X])) = C_A(\sum_{i=0}^{n} (a_i + I)X^i) = \sum_{i=0}^{n} (a_i + I)A = A$.

Definimos $\varphi: R(X)/IR(X) \longrightarrow (R/I)(X)$ por $\varphi((f/g) + IR(X)) = \lambda(f + IR[X])/\lambda(g + IR[X])$. É claro que φ está bem definida e é um homomorfismo de anéis. Se $(f/g) + IR(X)$ é um elemento arbitrário de $Ker(\varphi)$ (aqui $f \in R[X]$, $g \in S$), então $\lambda(f + IR[X])/\lambda(g + IR[X]) = 0$ em $(R/I)(X) = A(X)$. Como $A(X)$ é uma localização regular de $A[X]$ (proposição 1 do capítulo II), então $\lambda(f + IR[X]) = 0$ e portanto $f + IR[X] = 0$ em $R[X]/IR[X]$, pois λ é injetivo. Logo $f \in IR[X]$, donde $f/g \in IR(X)$. Consequentemente $(f/g) + IR(X) = 0$ em $R(X)/IR(X)$ e φ é injetivo. Seja f'/g' um elemento arbitrário de $A(X)$ (aqui $f' \in A[X]$, $g' \in A[X]$ e $C_A(g') = A$). É claro que existe $f \in R[X]$ tal que $\lambda(f + IR(X)) = f'$. Seja $g' = (a_0 + I) + (a_1 + I)X + \cdots + (a_n + I)X^n$. Como $(a_0 + I)A + (a_1 + I)A + \cdots + (a_n + I)A = C_A(g') = A$, então $a_0R + a_1R + \cdots + a_nR + I = R$. Logo existe $c \in I$ e existem $r_0, r_1, \ldots, r_n \in R$ tais que $a_0r_0 + a_1r_1 + \cdots + a_nr_n + c = 1$. Portanto $a_0R + a_1R + \cdots + a_nR + cR = R$. Seja $g = a_0 + a_1X + \cdots + a_nX^n + cX^{n+1}$. Então $C_R(g) = R$, isto é, $g \in S$. Como $\lambda(g + IR[X]) = (a_0 + I) + (a_1 + I)X + \cdots + (a_n + I)X^n + (c + I)X^{n+1} = (a_0 + I) + (a_1 + I)X + \cdots + (a_n + I)X^n = g'$, então $\varphi((f/g) + IR(X)) = \lambda(f + IR[X])/\lambda(g + IR[X]) = f'/g'$. Segue-se que φ é sobrejetivo.

Consequentemente φ é um isomorfismo de anéis.

C.Q.D.

PROPOSIÇÃO 7 - Seja I um ideal de R. São equivalentes:

(a) $IR\langle X\rangle$ é finitamente gerado.

(b) $IR(X)$ é finitamente gerado.

(c) I é finitamente gerado.

DEMONSTRAÇÃO - É claro que (c) implica (a).
(a) $\Rightarrow$ (b). Suponhamos que $IR(X)$ é finitamente gerado. Como $R(X)$ é uma localização regular de $R(X)$, então $IR(X)$ é a extensão de $IR(X)$ a $R(X)$. Portanto $IR(X)$ também é finitamente gerado.

(b) $\Rightarrow$ (c). Suponhamos que $IR(X) = f_1R(X) + \cdots + f_nR(X)$, onde $f_i \in IR[X]$, $1 \leq i \leq n$. Como $f_iR(X) \subseteq C(f_i)R(X)$ e $C(f_i) \subseteq I$, $1 \leq i \leq n$, então $IR(X) = C(f_1)R(X) + \cdots + C(f_n)R(X) =$
$= (C(f_1) + \cdots + C(f_n))R(X)$. Logo $I = C(f_1) + \cdots + C(f_n)$ pela proposição 5. Portanto I é finitamente gerado.

C.Q.D.

Agora consideraremos um resultado muito útil.

LEMA 4 - Seja R um anel local. Se $I = (a_1, a_2, \ldots, a_n)$ é um ideal principal de R, então $I = (a_k)$ para algum $k \in \{1,2,\ldots,n\}$.

DEMONSTRAÇÃO - Podemos supor que $I \neq 0$, porque se $I = 0$, então o resultado é trivialmente verdadeiro. Ponhamos $I = (d)$ e suponhamos que M é o único ideal maximal de R. Como $(a_1, a_2, \ldots, a_n) =$
$= (d)$, então existem $s_1, s_2, \ldots, s_n \in R$ tais que $d = s_1a_1 +$
$+ s_2a_2 + \cdots + s_na_n$ e para cada $i \in \{1,2,\ldots,n\}$ existe $r_i \in R$ tal que $a_i = r_id$; logo $a_i = r_i(s_1a_1 + s_2a_2 + \cdots + s_na_n) =$
$= r_is_1a_1 + r_is_2a_2 + \cdots + r_is_na_n$ Para cada $i \in \{1,2,\ldots,n\}$.

Suponhamos que $r_i \in M$ para todo $i \in \{1,2,\ldots,n\}$. Como $a_n = r_ns_1a_1 + r_ns_2a_2 + \cdots + r_ns_na_n$, então $(1-r_ns_n)a_n = r_ns_1a_1 +$
$+ r_ns_2a_2 + \cdots + r_ns_{n-1}a_{n-1}$; logo $a_n \in (a_1, a_2, \ldots, a_{n-1})$, pois $1-r_ns_n \in U(R)$ (o radical de Jacobson de R é M neste caso). Então $(d) = (a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, a_{n-1})$.

Por repetição do mesmo raciocínio obtem-se $(d) =$
$= (a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, a_{n-1}) = \cdots\cdots = (a_1, a_2) = (a_1)$. Então existe $s \in R$ tal que $d = sa_1$ e portanto $a_1 = r_1d = r_1sa_1$. Lo

go $(1-r_i s)a_i = 0$ e portanto $a_i = 0$, pois $1-r_i s \in U(R)$. Então $I = (a_1, a_2, \ldots, a_n) = (a_i) = 0$, o que é uma contradição.

Então existe $k \in \{1,2,\ldots,n\}$ tal que $r_k \in R \setminus M = U(R)$ e portanto $d = a_k r_k^{-1} \in (a_k)$. Em consequência existe $k \in \{1,2,\ldots,n\}$ tal que $I = (d) = (a_k)$.

C.Q.D.

PROPOSIÇÃO 8 - Seja $f \in R[X]$. São equivalentes:

(a) $C(f)$ é localmente principal.

(b) $fR(X) = C(f)R(X)$.

(c) $fR(X) = IR(X)$ para algum ideal I de R.

(d) $C(f)R(X)$ é principal.

(e) $C(f)R(X)$ é localmente principal.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Por localização podemos supor que R é local e que $C(f)$ é um ideal principal de R. Seja $C(f) = (a)$. Pelo lema 2 existe $h \in R[X]$ tal que $f = ah$ e $C(h) = R$, isto é, $h \in S$. Portanto $hR(X) = R(X)$, pois $h \in U(R(X))$; logo $C(f)R(X) = (a)R(X) = (a)hR(X) = ahR(X) = fR(X)$.

(b) $\Rightarrow$ (c). É suficiente tomar $I = C(f)$.

(c) $\Rightarrow$ (a). Por localização podemos supor que R é local. Devemos demonstrar que $C(f)$ é principal. Como $IR(X) = fR(X)$, então $IR(X)$ é gerado por um número finito de elementos de I, pela demonstração da proposição 7. Logo $IR(X) = aR(X)$ para algum $a \in I$ pelo lema 4. Portanto $f = a(g/h)$ para alguns $g, h \in R[X]$, com $C(h) = R$. Então $hf = ag$ e $C(f) = C(f)R = C(f)C(h) = C(ag) = aC(g) \subseteq (a) \subseteq C(f)$, pois $IR(X) = fR(X) \subseteq C(f)R(X)$ e portanto $I = IR(X) \cap R \subseteq C(f)R(X) \cap R = C(f)$. Em consequência $C(f) = (a)$ é principal.

É claro que (b) implica (d) e que (d) implica (e).

(e) $\Rightarrow$ (a). Podemos assumir que R é local e C(f)R(X) é principal (R(X) é local pelo teorema 2). Então C(f)R(X) = aR(X) = = (a)R(X) para algum a $\in$ C(f), pela proposição 7 e o lema 4. Portanto C(f) = (a), pela proposição 5. Consequentemente C(f) é principal.

C.Q.D.

COROLÁRIO - Se $I = (a_0, a_1, \ldots, a_n)$ é um ideal localmente principal de R, então IR(X) é principal. De fato, IR(X) = fR(X), onde $f = a_0 + a_1X + \cdots + a_nX^n$.

PROPOSIÇÃO 9 - Seja I um ideal de R. São equivalentes:

(a) IR(X) é localmente principal.

(b) IR(X) é localmente principal.

(c) I é localmente principal.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que IR(X) é localmente principal. Por localização podemos assumir que R(X) é local. Então IR(X) é principal. Como IR(X) é a extensão de IR(X) a R(X), então IR(X) é principal.

(b) $\Rightarrow$ (c). Por localização podemos supor que R é local e IR(X) é principal (R(X) é local pelo teorema 2). Então IR(X) = fR(X) para algum f $\in$ IR[X]. Logo I = C(f) é principal, pelas proposições 5 e 8.

(c) $\Rightarrow$ (a). Suponhamos que I é localmente principal. Seja $K \in \mathrm{Max}(R(X))$ qualquer e ponhamos $Q = K \cap R[X]$ e $P = Q \cap R$. Então $Q \cap U = \emptyset$ e P é um ideal primo de R. Logo $R(X)_K = R[X]_Q = R_P[X]_{Q_P}$, pela parte (b) da proposição 6. Como I_P é principal, então $IR(X)_K = IR[X]_Q = I_PR_P[X]_{Q_P}$ é principal. Consequentemente

$IR\langle X\rangle$ é localmente principal.

C.Q.D.

COROLÁRIO - Seja I um ideal de R. São equivalentes:

(a) $IR\langle X\rangle$ é localmente principal finitamente gerado.

(b) $IR(X)$ é localmente principal finitamente gerado.

(c) I é localmente principal finitamente gerado.

Agora consideraremos o anel $R(X,Y) = R[X,Y]_W$, onde $W = \{f \in R[X,Y];\ C_R(f) = R\} = R[X,Y] \setminus \cup\{M[X,Y];\ M \in Max(R)\}$. Demonstraremos que $R(X,Y) = R(X)(Y)$. Este fato permite demonstrar facilmente que todo ideal localmente principal finitamente gerado de $R(X)$ é principal.

PROPOSIÇÃO 10 - $R(X,Y) = R(X)(Y)$.

DEMONSTRAÇÃO - Se $M \in Max(R)$, então $MR[X]_S[Y] = MR[X,Y]_S$; logo $MR(X)[Y] \cap R[X,Y] = MR[X]_S[Y] \cap R[X,Y] = MR[X,Y]_S \cap R[X,Y] = MR[X,Y]$, pois $MR[X,Y]$ é um ideal primo de $R[X,Y]$ disjunto de S (teorema 4.5 de (7)). Portanto $g \in R[X,Y]$ e $g \in \cup\{MR(X)[Y];\ M \in Max(R)\}$ implica que $g \in \cup\{MR[X,Y];\ M \in Max(R)\}$. Segue-se que $g \in R[X,Y] \setminus \cup\{MR[X,Y];\ M \in Max(R)\}$ implica que $g \in R(X)[Y] \setminus \cup\{MR(X)[Y];\ M \in Max(R)\}$. Em consequência $R(X,Y) = \{f/g;\ f, g \in R[X,Y],\ g \notin \cup\{MR[X,Y];\ M \in Max(R)\}\} \subseteq \{f/g;\ f, g \in R(X)[Y],\ g \notin \cup\{MR(X)[Y];\ M \in Max(R)\}\} = R(X)(Y)$.

Por outro lado, se $f/g \in R(X)(Y)$, onde $f, g \in R(X)[Y]$, $g \notin \cup\{MR(X)[Y];\ M \in Max(R)\}$, então $f = f'/h$, $g = g'/k$, onde $f', g' \in R[X,Y]$, $h,k \notin \cup\{MR[X];\ M \in Max(R)\}$ e $g' \notin \cup\{MR[X,Y];\ M \in Max(R)\}$. Logo $f/g = (f'k)/(g'h)$, onde $f'k, g'h \in R[X,Y]$ e $g'h \notin \cup\{MR[X,Y];\ M \in Max(R)\}$ e portanto $f/g \in R(X,Y)$.

C.Q.D.

TEOREMA 3 - Todo ideal localmente principal finitamente gerado de R(X) é principal.

DEMONSTRAÇÃO - Seja $K = f_0R(X) + f_1R(X) + \cdots + f_nR(X)$ um ideal localmente principal de R(X), onde $f_i \in R[X]$, $0 \leq i \leq n$. Seja $f = f_0 + f_1X^{r_1} + f_2X^{r_2} + \cdots + f_nX^{r_n}$, onde $r_i = gr(f_0) + gr(f_1) + \cdots + gr(f_{i-1}) + i$, $1 \leq i \leq n$. Então $C_R(f) = C_R(f_0) + C_R(f_1) + \cdots + C_R(f_n)$. Seja $A = R(X)$. Se $g = f_0 + f_1Y + \cdots + f_nY^n \in A[Y]$, então $C_A(g) = K$. Como K é localmente principal, então $KA(Y) = C_A(g)A(Y) = gA(Y)$, pela proposição 8. Logo $KR(X,Y) = KR(X)(Y) = KA(Y) = gA(Y) = gR(X)(Y) = gR(X,Y)$. Por outro lado $fR(X,Y) = fR(X)(Y) \subseteq KR(X)(Y) = KR(X,Y) = gR(X,Y)$. Portanto $f = (h/k)g$ para alguns $h, k \in R[X,Y]$, onde $C_R(k) = R$. Além disto $C_R(f) = C_R(f_0) + C_R(f_1) + \cdots + C_R(f_n) = C_R(g)$ (aqui g é considerado como um elemento de R[X,Y]). Segue-se que $C_R(f) = RC_R(f) = C_R(k)C_R(f) = C_R(kf) = C_R(hg) \subseteq C_R(h)C_R(g) = C_R(h)C_R(f) \subseteq C_R(f)$, isto é, $C_R(f) = C_R(f)C_R(h)$. Seja $M \in Max(R)$ arbitrário. Então $C_R(f)_M = (0)_M$ ou $C_R(h)_M = R_M$, pelo Lema de Nakayama. No primeiro caso resulta $KR_M(X) = 0 = fR_M(X)$. No segundo caso temos $C_R(h)_M = R_M$ e portanto a imagem de h em $R_M(X,Y)$ é uma unidade; logo $fR_M(X,Y) = gR_M(X,Y)$, donde $fR_M(X) = fR_M(X)(Y) \cap R_M(X) = gR_M(X)(Y) \cap R_M(X) = KR_M(X)(Y) \cap R_M(X) = KR_M(X)$. Consequentemente (globalizando) $K = fR(X)$ é principal.

C.Q.D.

O próximo resultado a ser demonstrado é o seguinte: um ideal de R é inversível se e só se é regular, localmente principal e finitamente gerado. Em primeiro lugar consideramos um lema.

LEMA 5 - Seja R um anel local. Se I é um ideal (inteiro) inversível de R, então I é principal.

DEMONSTRAÇÃO - Seja M o único ideal maximal de R. Como I é inversível, então $I \not\subseteq IM$; logo existe $a \in I \setminus IM$. Pelo teorema 7.2 de (7), existe um ideal J de R tal que $(a) = IJ$, pois $(a) \subseteq I$ e I é inversível. Se $J \neq R$, então $J \subseteq M$ e portanto $(a) = IJ \subseteq IM$, o que é uma contradição. Em consequência $J = R$, donde $I = IR = IJ = (a)$ é principal.

C.Q.D.

PROPOSIÇÃO 11 - Se I é um ideal (inteiro) inversível de R, então I é regular, localmente principal e finitamente gerado.

DEMONSTRAÇÃO - Suponhamos que I é um ideal (inteiro) inversível de R. Seja K o inverso de I. Como $KI = R$, então $K \subseteq [R:I]_{T(R)}$. Logo $R = KI \subseteq [R:I]_{T(R)}I \subseteq R$, isto é, $KI = R = [R:I]_{T(R)}I$. Portanto $[R:I]_{T(R)} = K$ e $[R:I]_{T(R)}$ é o único inverso de I. Como $[R:I]_{T(R)}I = R$, então existem $x_1, x_2, \ldots, x_n \in [R:I]_{T(R)}$ e $a_1, a_2, \ldots, a_n \in I$ tais que $1 = x_1a_1 + x_2a_2 + \cdots + x_na_n$. Seja $a \in I$ arbitrário, então $a = a1 = a(x_1a_1 + x_2a_2 + \cdots + x_na_n) = (ax_1)a_1 + (ax_2)a_2 + \cdots + (ax_n)a_n$, onde $ax_i \in R$ para cada i em $\{1,2,\ldots,n\}$. Logo $a \in (a_1,a_2,\ldots,a_n)$. Segue-se que $I = (a_1,a_2,\ldots,a_n)$ é finitamente gerado. Por outro lado, como $x_i \in [R:I]_{T(R)} \subseteq T(R) = R_{Reg(R)}$, então existe $r_i \in Reg(R)$ tal que $r_ix_i \in R$, $1 \leq i \leq n$. Seja $r = r_1r_2 \cdots r_n \in Reg(R)$. Então rx_i está em R para cada $i \in \{1,2,\ldots,n\}$ e portanto $r = r(x_1a_1 + x_2a_2 + \cdots + x_na_n) = (rx_1)a_1 + \cdots + (rx_n)a_n$ está em $(a_1,a_2,\ldots,a_n) = I$. Consequentemente I é regular. Vejamos agora que I é localmente principal. Seja $M \in Max(R)$ arbitrário. Então IR_M é um ideal inversível de R_M. Como R_M é local, então IR_M é principal, pelo lema 5. Em consequência I é localmente principal.

C.Q.D.

DEFINIÇÃO - Seja I um ideal de R. Dizemos que I é localmente inversível se IR_M é inversível para todo $M \in Max(R)$.

PROPOSIÇÃO 12 - Seja I um ideal de R. Se I é regular, localmente inversível e finitamente gerado, então I é inversível.

DEMONSTRAÇÃO - Suponhamos que I é regular, localmente inversível e finitamente gerado. Então existe $a \in I \cap Reg(R)$; Seja $M \in Max(R)$ arbitrário. Como I é finitamente gerado, então $((a):I)_M = (a)_M:I_M$, pela parte (4) do teorema 4.4 de (7). Por outro lado, $(a)_M(I_M)^{-1} \subseteq R_M$, pois I_M é inversível e $(a)_M \subseteq I_M$. Também temos $((a)_M(I_M)^{-1})I_M = (a)_M$ e $((a)_M:I_M)I_M \subseteq (a)_M$. Logo $(a)_M(I_M)^{-1} \subseteq (a)_M:I_M$ e portanto $(a)_M \subseteq ((a)_M:I_M)I_M \subseteq (a)_M$, isto é, $((a)_M:I_M)I_M = (a)_M$. Segue-se que $(((a):I)I)_M = ((a):I)_M I_M = ((a)_M:I_M)I_M = (a)_M$ para todo $M \in Max(R)$. então $((a):I)I = (a)$ pela proposição 3.13 de (9). Em consequência I é inversível (teorema 7.2 de (7)).

C.Q.D.

Todo ideal fracionário regular principal de R é inversível. De fato, se $x \in T(R)$ e x é um elemento regular de T(R), então x é uma unidade de T(R), pela proposição 2.7 de (7). Como $(x)(x^{-1}) = R$, então (x) é um ideal fracionário inversível. Segundo este resultado, temos o seguinte corolário.

COROLÁRIO - Seja I um ideal de R. Se I é regular, localmente principal e finitamente gerado, então I é inversível.

OBSERVAÇÕES - (1) Segundo este corolário e a proposição 11, um ideal de R é inversível se e só se é regular, localmente principal e finitamente gerado.

(2) Segundo o lema 1, $f \in Reg(R[X])$ se e só se $0:C(f) = 0$.

(3) Se I é um ideal regular de R, então $0:I = 0$. De fato, se x é um elemento arbitrário de $0:I$ e $a \in I \cap Reg(R)$, então $xI \subseteq 0$ e portanto $xa = 0$. Logo $x = 0$. Consequentemente $0:I = 0$.

PROPOSIÇÃO 13 - Seja I um ideal de R. São equivalentes:

(a) $IR\langle X\rangle$ é inversível.

(b) $IR(X)$ é inversível.

(c) I é localmente principal finitamente gerado e $0:I = 0$.

Em particular, se I é regular, então são equivalentes:

(d) $IR\langle X\rangle$ é inversível.

(e) $IR(X)$ é inversível.

(f) I é inversível.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que $IR\langle X\rangle$ é inversível. Então sua localização $IR(X)$ é também inversível.

(b) $\Rightarrow$ (c). Suponhamos que $IR(X)$ é inversível. Então $IR(X)$ é localmente principal finitamente gerado e portanto I também é localmente principal finitamente gerado (corolário da proposição 9). Seja $I = (a_0, a_1, \ldots, a_n)$. Se $f = a_0 + a_1X + \cdots + a_nX^n$, então $IR(X) = fR(X)$, pois $C(f) = I$ é localmente principal (proposição 8). Logo f é regular e portanto $0:I = 0:C(f) = 0$.

(c) $\Rightarrow$ (a). Suponhamos que I é localmente principal finitamente gerado e $0:I = 0$. Então $IR\langle X\rangle$ é localmente principal finitamente gerado (corolário da proposição 9). Seja $I = (a_0, a_1, \ldots, a_n)$. Então $f = a_0 + a_1X + \cdots + a_nX^n$ é um elemento regular de $IR\langle X\rangle$, pois $0:C(f) = 0:I = 0$. Logo $IR\langle X\rangle$ é regular, localmente principal e finitamente gerado e em consequência $IR\langle X\rangle$ é inversível.

Para demonstrar a equivalencia de (d), (e) e (f), é suficiente observar que se I é regular, então I é inversível se e somente se I é localmente principal finitamente gerado e 0:I = 0.

C.Q.D.

PROPOSIÇÃO 14 - Se I é um ideal principal de R, então IR⟨X⟩ e IR(X) são ideais principais de R⟨X⟩ e R(X), respectivamente.

DEMONSTRAÇÃO - Se I = (a), então IR⟨X⟩ = (a/1)R⟨X⟩ e IR(X) = = (a/1)R(X).

C.Q.D.

PROPOSIÇÃO 15 - Sejam R um domínio de integridade e I um ideal de R. São equivalentes:

(a) IR⟨X⟩ é principal.

(b) I é principal.

DEMONSTRAÇÃO - (a) $\Longrightarrow$ (b). Suponhamos que IR⟨X⟩ é principal. Então IR⟨X⟩ = fR⟨X⟩ para algum f $\in$ R[X]. Seja $f = a_0 + a_1X + \cdots + a_nX^n$, onde $a_n \neq 0$. Como f $\in$ IR⟨X⟩, então existe g $\in$ U tal que gf $\in$ IR[X]; logo $a_n \in I$, pois g é mônico. Portanto $(a_n) \subseteq I$. Seja a $\in$ I qualquer. Então a $\in$ IR⟨X⟩=fR⟨X⟩. Portanto a = f(k/h), para algum k $\in$ R[X] e algum h $\in$ U; logo ah = fk. Como h é mônico, então a é o coeficiente líder de ah e como R é um domínio de integridade, então a é o coeficiente líder de fk. Portanto a = $= a_nb_m$, onde b_m é o coeficiente líder de k. Em consequência, $a \in (a_n)$ e assim $I = (a_n)$.

Pela proposição anterior (b) implica (a).

C.Q.D.

TEOREMA 4 - São equivalentes:

(a) $R\langle X\rangle$ é um domínio de integridade.

(b) $R(X)$ é um domínio de integridade.

(c) R é um domínio de integridade.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que $R\langle X\rangle$ é um domínio de integridade. Como $R(X)$ é uma localização de $R\langle X\rangle$, então $R(X)$ é um domínio de integridade.

(b) $\Rightarrow$ (c). Suponhamos que $R(X)$ é um domínio de integridade. Então R é um domínio de integridade, pois R é um subanel de $R(X)$.

(c) $\Rightarrow$ (a). Suponhamos que R é um domínio de integridade. Então $R[X]$ é um domínio de integridade. Como toda localização de um domínio de integridade é um domínio de integridade, então $R\langle X\rangle$ é um domínio de integridade.

C.Q.D.

TEOREMA 5 - São equivalentes:

(a) $R\langle X\rangle$ é noetheriano.

(b) $R(X)$ é noetheriano.

(c) R é noetheriano.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que $R(X)$ é noetheriano. Então sua localização $R(X)$ é um anel noetheriano.

(b) $\Rightarrow$ (c). Suponhamos que $R(X)$ é noetheriano. Seja $I_1 \subseteq I_2 \subseteq \subseteq \ldots \subseteq I_n \subseteq \ldots$ uma cadeia ascendente de ideais de R. Então $I_1R(X) \subseteq I_2R(X) \subseteq \ldots \ldots I_nR(X) \subseteq \ldots$ é uma cadeia ascendente de ideais de $R(X)$. Logo existe um inteiro positivo m tal que $I_nR(X) = I_mR(X)$ para todo $n \geq m$, donde $I_n = I_nR(X) \cap R =$

$= I_m R(X) \cap R = I_m$ para todo $n \geq m$. Em consequência, R é noetheriano.

(c) $\Rightarrow$ (a). Suponhamos que R é noetheriano. Então R[X] é noetheriano, pelo teorema da base de Hilbert. Portanto R(X) é noetheriano, pois toda localização de um anel noetheriano é um anel noetheriano.

C.Q.D.

DEFINIÇÃO - Dizemos que R é radicalmente fechado se $q \in T(R)$ e $q^n \in R$ para algum $n \in \mathbb{N}$ implica que $q \in R$.

LEMA 5 - $R\langle X\rangle \cap T(R) = R = R(X) \cap T(R)$.

DEMONSTRAÇÃO - É claro que $R \subseteq R\langle X\rangle \cap T(R) \subseteq R(X) \cap T(R)$. Se $q \in R(X) \cap T(R)$, então $q = a/b$, para algum $a \in R$ e algum $b \in Reg(R)$. Como $a/b \in R(X)$, então $Rb = R$ e portanto $b \in U(R)$. Logo $q \in R$. Consequentemente $R\langle X\rangle \cap T(R) = R = R(X) \cap T(R)$.

C.Q.D.

TEOREMA 6 - Se $R\langle X\rangle$ ou R(X) é radicalmente fechado, então R é radicalmente fechado.

DEMONSTRAÇÃO - Suponhamos que $R\langle X\rangle$ é radicalmente fechado. Seja $q \in T(R)$. Se $q^n \in R$ para algum $n \in \mathbb{N}$, então $q \in T(R\langle X\rangle) = T(R[X])$ e $q^n \in R\langle X\rangle$ para algum $n \in \mathbb{N}$; logo $q \in R\langle X\rangle$, pois $R\langle X\rangle$ é radicalmente fechado. Portanto $q \in R\langle X\rangle \cap T(R) = R$. Em consequência R é radicalmente fechado. Similarmente demonstra-se que R é radicalmente fechado, se R(X) o é.

C.Q.D.

TEOREMA 7 - Se $R\langle X\rangle$ ou $R(X)$ é integralmente fechado, então R é integralmente fechado.

DEMONSTRAÇÃO - Suponhamos que $R\langle X\rangle$ é integralmente fechado. Se $q \in T(R)$ é inteiro sobre R, então $q \in T(R\langle X\rangle) = T(R[X])$ e q é inteiro sobre $R\langle X\rangle$; logo $q \in R\langle X\rangle$. Portanto $q \in R\langle X\rangle \cap T(R) = R$. Em consequência R é integralmente fechado. Similarmente demonstra-se que R é integralmente fechado se $R(X)$ o é.

C.Q.D.

TEOREMA 8 - Seja R um domínio de integridade. Se R é integralmente fechado, então $R\langle X\rangle$ e $R(X)$ são integralmente fechados.

DEMONSTRAÇÃO - Suponhamos que R é um domínio integralmente fechado. Então $R[X]$ é integralmente fechado (corolário 10.8 de (7)) e portanto suas localizações $R\langle X\rangle$ e $R(X)$ são integralmente fechados (proposição 10.2 de (7)).

C.Q.D.

CAPÍTULO III

ANÉIS ARITMÉTICOS E ANÉIS DE PRUFER

Aqui consideram-se os domínios de Prüfer e suas generalizações. Ve-se a grande utilidade do lema 4 do capítulo II. Também utiliza-se o seguinte resultado formal: todo ideal I de um anel R é a soma de todos os ideais principais de R contidos em I.

DEFINIÇÃO - Seja R um domínio de integridade. Dizemos que R é um domínio de Prüfer se todo ideal não nulo finitamente gerado de R é inversível.

DEFINIÇÃO - Dizemos que R é um anel aritmético se todo ideal finitamente gerado de R é localmente pricipal.

OBSERVAÇÃO - Como um ideal de R é inversível se e só se é regular, localmente principal e finitamente gerado, então temos o seguinte resultado: R é um domínio de Prüfer se e só se R é um domínio de integridade e R é aritmético.

LEMA 1 - Seja R um anel. Se os ideais principais de R estão totalmente ordenados, então os ideais de R estão totalmente ordenados.

DEMONSTRAÇÃO - Suponhamos que os ideais principais de R estão totalmente ordenados. Sejam I e J ideais de R quaisquer. Se $I \nsubseteq J$, então existe $a \in I$ tal que $a \notin J$. Seja $x \in J$ qualquer. Então $(a) \nsubseteq (x) \subseteq J$. Logo $(x) \subseteq (a)$, pela hipótese. Portanto $x \in (a) \subseteq I$. Consequentemente $J \subseteq I$.

C.Q.D.

PROPOSIÇÃO 1 - São equivalentes:

(a) R é aritmético.

(b) Os ideais de R_M estão totalmente ordenados, para todo $M \in Max(R)$.

(c) $I \cap (J + K) = (I \cap J) + (I \cap K)$ para quaisquer ideais I, J, K de R.

(d) Os ideais de R_P estão totalmente ordenados, para todo ideal primo P de R.

DEMONSTRAÇÃO - (a) $\Longrightarrow$ (b). Suponhamos que R é um anel aritmético. Seja $M \in Max(R)$ qualquer. Todo ideal principal de R_M é da forma $(a)_M$ para algum $a \in R$. Pelo lema 1 é suficiente demonstrar que $(a)_M \subseteq (b)_M$ ou $(b)_M \subseteq (a)_M$ para quaisquer $a, b \in R$. Como R_M é local e $(a,b)_M$ é principal, então podemos supor que $(a,b)_M = (a)_M$ (lema 4 do capítulo II). Logo $(b)_M \subseteq (a)_M$.

(b) $\Longrightarrow$ (c). Suponhamos que os ideais de R_M estão totalmente ordenados, para todo $M \in Max(R)$. Então dados quaisquer ideais I, J, K de R, podemos supor que $J_M \subseteq K_M$; logo $(I \cap (J + K))_M = I_M \cap (J_M + K_M) = I_M \cap K_M = (I_M \cap J_M) + (I_M \cap K_M)$, pois $I_M \cap J_M \subseteq I_M \cap K_M$. Portanto $(I \cap (J + K))_M = ((I \cap J) + (I \cap K))_M$ para qualquer $M \in Max(R)$. Globalizando resulta $I \cap (J + K) = (I \cap J) + (I \cap K)$.

(c) $\Longrightarrow$ (d). Suponhamos que $I \cap (J + K) = (I \cap J) + (I \cap K)$ para quaisquer ideais I, J, K de R. Sejam P um ideal primo de R e $a, b \in R$ quaisquer. Como $a \in (b) + (a-b)$, então $(a) = (a) \cap ((b) + (a-b)) = ((a) \cap (b)) + ((a) \cap (a-b))$; logo $a = c + r(a-b)$, onde $c \in (a) \cap (b)$, $r \in R$ e $r(a-b) \in (a)$. Portanto $rb \in (a)$ e $(1-r)a = c-rb \in (b)$. Se $r \in R\backslash P$, então $b/1 = rb/r \in (a)_P$ e se $r \in P$, então $1-r \in R\backslash P$ e portanto $a/1 = (1-r)a/(1-r) = (c-rb)/(1-r) \in (b)_P$. Então $(b)_P \subseteq (a)_P$ ou $(a)_P \subseteq (b)_P$ e conse-

quentemente os ideais de R_p estão totalmente ordenados.

(d) $\Longrightarrow$ (a). Suponhamos que os ideais de R_p estão totalmente ordenados, para todo ideal primo P de R. Para demonstrar que R é aritmético é suficiente demonstrar que (a,b) é localmente principal, para quaisquer a, b $\in$ R. Seja M $\in$ Max(R) e a, b $\in$ R quaisquer. Pela hipótese, podemos supor que $(a)_M \subseteq (b)_M$. Logo $(a,b)_M = (a)_M + (b)_M = (b)_M$, isto é, (a,b) é localmente principal.

C.Q.D.

LEMA 2 - Para quaisquer ideais I, J de R,

(a) $(I \cap J)R\langle X\rangle = IR\langle X\rangle \cap JR\langle X\rangle$.

(b) $(I \cap J)R(X) = IR(X) \cap JR(X)$.

DEMONSTRAÇÃO - (a) Como $(I \cap J)R[X] = IR[X] \cap JR[X]$, então $(I \cap J)R\langle X\rangle = (I \cap J)R[X]_U = (IR[X] \cap JR[X])_U = IR[X]_U \cap JR[X]_U = IR\langle X\rangle \cap JR\langle X\rangle$.

(b) É similar à anterior.

TEOREMA 1 - São equivalentes:

(a) R(X) é aritmético.

(b) R é aritmético.

DEMONSTRAÇÃO - (a) $\Longrightarrow$ (b). Suponhamos que R(X) é aritmético. Sejam I, J, K ideais de R quaisquer. Então

$$\begin{aligned}(I \cap (J + K))R(X) &= IR(X) \cap (J + K)R(X) \\ &= IR(X) \cap (JR(X) + KR(X)) \\ &= (IR(X) \cap JR(X)) + (IR(X) \cap KR(X))\end{aligned}$$

$$= (I \cap J)R(X) + (I \cap K)R(X)$$
$$= ((I \cap J) + (I \cap K))R(X).$$

Logo $I \cap (J + K) = (I \cap J) + (I \cap K)$ (proposição 5 do capítulo II) e portanto R é aritmético, pela proposição 1.

(b) $\Longrightarrow$ (a). Suponhamos que R é aritmético. Demonstraremos que $R(X)$ é de Bézout. Sejam $f, g \in R[X]\setminus\{0\}$. Definimos $h = f + X^n g$, onde $n = 1 + gr(f)$. Então $C(h) = C(f) + C(g)$. Como $C(f)$, $C(g)$ e $C(h)$ são localmente principais, então (pela proposição 8 do capítulo II) temos $fR(X) + gR(X) = C(f)R(X) + C(g)R(X)$

$$= (C(f) + C(g))R(X)$$
$$= C(h)R(X)$$
$$= hR(X).$$

C.Q.D.

PROPOSIÇÃO 2 - Se $R\langle X\rangle$ é aritmético, então R é aritmético.

DEMONSTRAÇÃO - Suponhamos que $R\langle X\rangle$ é aritmético. Seja P um ideal maximal de R. Como $P[X]$ é um ideal primo de $R[X]$ e $P[X] \cap U = \emptyset$, então $PR\langle X\rangle$ é um ideal primo de $R\langle X\rangle$. Logo os ideais de $R\langle X\rangle_{PR\langle X\rangle}$ estão totalmente ordenados. Mas $R\langle X\rangle_{PR\langle X\rangle} \cong R_P[X]_{PR_P[X]}$ e $R_P \subseteq R_P[X]_{PR_P[X]} = R_P(X)$, pela proposição 6 do capítulo II. Sejam $a, b \in R_P$. Então podemos supor que $bR_P[X]_{PR_P[X]} \subseteq aR_P[X]_{PR_P[X]}$. Logo existem $f \in R_P[X]$, $h \in R_P[X]\setminus PR_P[X]$ tais que $b = (f/h)a$ e portanto $bh = af$. Sejam $f = p_0 + p_1X + \cdots + p_nX^n$ e $h = q_0 + q_1X + \cdots + q_mX^m$. Como $h \notin PR_P[X]$, então existe $k \in \{0,1,\ldots,m\}$ tal que $q_k \in R_P\setminus PR_P = U(R_P)$. Se $b = 0$, então $bR_P \subseteq aR_P$ obviamente. Se $b \neq 0$, então $bq_k = ap_k \neq 0$; logo $b = ap_kq_k^{-1} \in aR_P$ e portanto $bR_P \subseteq aR_P$. Então os ideais de R_P estão totalmente ordenados e consequentemente R é aritmético.

C.Q.D.

LEMA 3 - Seja R um domínio de integridade. Se Q é um ideal primo de R[X] tal que $R[X]_Q$ é um anel de valorização e $(Q \cap R)[X] \subset Q$, então $Q \cap R = 0$.

DEMONSTRAÇÃO - Como $R[X]_Q$ é um anel de valorização e $R_{Q \cap R} = R[X]_Q \cap T(R)$, então $R_{Q \cap R}$ é um anel de valorização, pelo teorema 19.16 de (7). Portanto não existe perda de generalidade em assumir que R é um anel de valorização e $Q \cap R$ é seu único ideal maximal. Como $R/(Q \cap R)$ é um corpo e $R[X]/(Q \cap R)[X] = (R/(Q \cap R))[X]$, então $Q/(Q \cap R)[X]$ é principal. Logo Q é gerado módulo $(Q \cap R)[X]$ por um polinômio mónico $f \in Q$. Seja $a \in Q \cap R$ e suponhamos que $a \neq 0$. Como $R[X]_Q$ é uma anel de valorização e $f \notin (Q \cap R)[X]_Q$, então f divide a em $R[X]_Q$ e portanto existem $g \in R[X]$, $h \in R[X] \setminus Q$ tais que $a = (g/h)f$. Logo $h = (1/a)gf$ em $F[X]$, onde $F = T(R)$. Sejam $f = a_n X^n + \cdots + a_1 X + a_0$, $n \geq 1$, $(1/a)g = b_m X^m + \cdots + b_1 X + b_0$ e $h = c_{n+m} X^{n+m} + \cdots + c_1 X + c_0$, onde $a_n = 1$, $a_i \in R$, $0 \leq i \leq n$, $b_j \in F$, $0 \leq j \leq m$, $b_m \neq 0$ e $c_k \in R$, $0 \leq k \leq m+n$. Então

$c_{n+m} = b_m$

$c_{n+m-1} = b_{m-1} + b_m a_{n-1}$

.....

$c_{n+m-r} = b_{m-r} + b_{m-r+1} a_{n-1} + \cdots + b_{m-r+s} a_{n-s}$, $s = \min\{n,r\}$

.....

$c_{n+1} = b_1 + b_2 a_{n-1} + \cdots + b_{s+1} a_{n-s}$, $s = \min\{n,m-1\}$

$c_n = b_0 + b_1 a_{n-1} + \cdots + b_s a_{n-s}$, $s = \min\{n,m\}$.

Logo $b_m = c_{n+m} \in R$, $b_{m-1}, \ldots, b_1, b_0 \in R$. Portanto $h \in fR[X] \subseteq Q$, o que é absurdo. Consequentemente $a = 0$ e $Q \cap R = 0$.

C.Q.D.

Seja R um anel. Se M é um subconjunto multiplicativamente fechado de R[X] e K é um ideal primo de $R[X]_M$, então existe um ideal primo Q de R[X], com $Q \cap M = \emptyset$, tal que $K = Q_M = QR[X]_M$. Comprova-se sem dificuldade que a aplicação

$H:R[X]_Q \longrightarrow (R[X]_M)_{Q_M}$ dada por $H(f/g) = (f/1)/(g/1)$ está bem definida e é um isomorfismo de anéis. Também pode demonstrar-se que se $M \subseteq R$, então $R_M[X]$ e $R[X]_M$ são anéis isomorfos.

LEMA 4 - Seja R um domínio de integridade. Se $a \in R\setminus\{0\}$, então $aX + 1 \in R[X]$ é primo, isto é, $(aX + 1)R[X]$ é um ideal primo de $R[X]$.

DEMONSTRAÇÃO - Consideremos o homomorfismo de anéis $H:R[X] \longrightarrow T(R)$ tal que $H(X) = -1/a$ e $H(r) = r$ para cada $r \in R$. É claro que $(aX + 1)R[X] \subseteq Ker(H)$. Seja $f = a_nX^n + \cdots + a_1X + a_0 \in Ker(H)$ qualquer. Então

$$a_n(-1/a)^n + a_{n-1}(-1/a)^{n-1} + \cdots + a_1(-1/a) + a_0 = H(f) = 0.$$

Logo

$$a_n = (-1)^{n+1}a^n(a_{n-1}(-1/a)^{n-1} + \cdots + a_1(-1/a) + a_0)$$
$$= a((-1)^{2n}a_{n-1} + \cdots + (-1)^{n+2}a^{n-2}a_1 + (-1)^{n+1}a^{n-1}a_0).$$

Seja $g = b_{n-1}X^{n-1} + \cdots + b_1X + b_0$, onde

$$b_{n-1} = (-1)^{2n}a_{n-1} + (-1)^{2n-1}aa_{n-2} + \cdots + (-1)^{n+1}a^{n-1}a_0$$
$$b_{n-2} = (-1)^{2n}a_{n-2} + (-1)^{2n-1}aa_{n-3} + \cdots + (-1)^{n+2}a^{n-2}a_0$$

$\cdots\cdots$

$$b_1 = (-1)^{2n}a_1 + (-1)^{2n-1}aa_0$$
$$b_0 = (-1)^{2n}a_0 = a_0$$

Então $g(aX + 1) = b_{n-1}aX^n + (b_{n-1} + ab_{n-2})X^{n-1} + \cdots + (b_1 + b_0a)X + b_0 = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = f$. Logo $f \in (aX + 1)R[X]$. Portanto $Ker(H) = (aX + 1)R[X]$. Consequentemente $R[X]/((aX + 1)R[X])$ é um domínio de integridade, isto é, $(aX + 1)R[X]$ é um ideal primo de $R[X]$.

C.Q.D.

PROPOSIÇÃO 3 - Se R(X) é aritmético, então $\dim R \leq 1$.

DEMONSTRAÇÃO - Suponhamos que $R\langle X\rangle$ é aritmético e que dim $R > 1$. Consideremos em primeiro lugar o caso em que R é um domínio de integridade. Então existe uma cadeia $0 \subset M \subset P$ de ideais primos de R. Seja $a \in P \setminus M$. O ideal $Q = M[X] + (aX + 1)R[X]$ não contém polinômios mônicos, isto é, $Q \cap U = \emptyset$, e $M[X] \subset Q$. em $R[X]/M[X] \cong (R/M)[X]$ o ideal $Q/M[X]$ é gerado por $(a + M)X + (1 + M)$. Como R/M é um domínio de integridade, então $(a + M)X + (1 + M)$ é primo, pelo lema 4. Logo $Q/M[X]$ é um ideal primo de $R[X]/M[X]$ e portanto Q é um ideal primo de R[X]. Por outro lado $aX + 1 \in Q$ e $aX + 1 \notin (Q \cap R)[X]$, pois $1 \notin Q \cap R$; também $M \subset Q$. Logo $(Q \cap R)[X] \subset Q$ e $Q \cap R \neq 0$. Então (pelo lema 3) $R[X]_Q$ não é um anel de valorização. Seja K a extensão de Q a $R\langle X\rangle$, isto é, $K = Q_U = QR\langle X\rangle$. Então K é um ideal primo de $R\langle X\rangle$ e $R\langle X\rangle_K = (R[X]_U)_{Q_U} \cong R[X]_Q$ não é um anel de valorização, o que contradiz o fato de ser $R\langle X\rangle$ um anel aritmético.

Consideremos agora um anel R qualquer. Seja $M \subset N \subset P$ uma cadeia de ideais primos de R. Então $0 \subset N/M \subset P/M$ é uma cadeia de ideais primos do domínio de integridade R/M e portanto $\dim(R/M) > 1$. Segundo o caso anterior existe um ideal primo Q de R[X], com $M[X] \subsetneq Q$ e $Q \cap U = \emptyset$, tal que $Q/M[X]$ é um ideal primo de $(R/M)[X] \cong R[X]/M[X]$ e $(R[X]/M[X])_{Q/M[X]}$ não é um anel de valorização. Seja $W = R[X]\setminus Q$. Como $M[X] \subsetneq Q$ e Q é um ideal de R[X], então $M[X] \cap W = \emptyset$ e $(M[X] + W)/M[X] = (R[X]/M[X]) \setminus (Q/M[X])$. Logo $(R[X]/M[X])_{Q/M[X]} \cong R[X]_Q/M[X]_Q$, pela proposição 5.8 de (7). Portanto os ideais de $R[X]_Q$ não estão totalmente ordenados, o que é uma contradição, como no caso anterior. Consequentemente se $R\langle X\rangle$ é aritmético, então $\dim R \leq 1$.

C.Q.D.

TEOREMA 2 - São equivalentes:

(a) $R\langle X\rangle$ é aritmético.

(b) R é aritmético, $\dim R \leq 1$ e R_M é um corpo sempre que $M \subset P$ é uma cadeia de ideais primos de R.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que $R\langle X\rangle$ é aritmético. Então R é aritmético e $\dim R \leq 1$, pelas proposições 2 e 3, respectivamente. Seja $M \subset P$ uma cadeia de ideais primos de R. Se $a \in P\backslash M$, então (pelo lema 4) $(a + M)X + (1 + M)$ é um elemento primo de $(R/M)[X]$. Seja $Q = M[X] + (aX + 1)R[X]$. Então $Q/M[X]$ é um ideal primo de $R[X]/M[X] \cong (R/M)[X]$, pois seu gerador $(a + M)X + (1 + M)$ é primo. Portanto Q é um ideal primo de $R[X]$ e não contém polinômios mônicos, isto é, $Q \cap U = \emptyset$. Então $R[X]_Q \cong R\langle X\rangle_{Q_U}$ é uma localização de $R\langle X\rangle$ e portanto os ideais de $R[X]_Q$ estão totalmente ordenados. Como $aX + 1 \notin M[X]$, então $((aX + 1)R[X])_Q \not\subseteq M[X]_Q$. Logo $M[X]_Q \subseteq ((aX + 1)R[X])_Q$. Seja $m \in M$ qualquer. Então $m/1 = (aX + 1)f/g$, para algum $f \in R[X]$ e algum $g \in R[X]\backslash Q$; logo $mgh = (aX + 1)fh$ para algum $h \in R[X]\backslash Q$. Como $C(aX + 1) = R$, então $C(fh) = C(aX + 1)C(fh) = C((aX + 1)fh) =$ $= C(mgh) = (m)C(gh) \subseteq (m)$ e portanto $fh = mk$ para algum $k \in R[X]$. Então

$$\frac{m}{1} = \frac{(aX + 1)f}{g} = \frac{(aX + 1)fh}{gh} = \frac{m(aX + 1)k}{gh}$$

Consequentemente $(m)_Q = Q_Q(m)_Q$, donde $(m)_Q = (0)_Q$, pelo Lema de Nakayama. Portanto $M[X]_Q = (0)_Q$; logo $R[X]_{M[X]} \cong$ $\cong (R[X]_Q)_{M[X]_Q} = (R[X]_Q)_{(0)_Q}$ é um domínio de integridade. Então $R_M \subseteq R[X]_{M[X]}$ é um domínio de integridade. Mas $MR_M = 0$ em R_M, pois em caso contrário obteriamos uma cadeia $0 \subset M \subset P$ de ideais primos de R, o que implicaria que $\dim R > 1$. Portanto R_M é um corpo.

(b) $\Rightarrow$ (a). Suponhamos que R é aritmético, $\dim R \leq 1$ e R_M é um corpo sempre que $M \subset P$ é uma cadeia de ideais primos de R. Seja Q um ideal primo de $R[X]$, com $Q \cap U = \emptyset$, e seja $M = Q \cap R$. Se M é maximal, então $(R/M)[X] \cong R[X]/M[X]$ é um domínio de ideais principais e portanto $Q/M[X] = 0$ ou $Q/M[X]$ é gerado por algum $f \in U \cap Q$. A segunda possibilidade implica que $Q \cap U \neq \emptyset$, o que é absurdo; logo devemos ter $Q = M[X]$. Como os ideais de R_M estão totalmente ordenados, então R_M é de Bézout e portanto aritmético. Logo $R\langle X\rangle_{Q_U} \cong R[X]_{M[X]} \cong R_M(X)$ é aritmético (teorema 1). Mas R_M

é local; logo $R_M(X)$ é local, pelo teorema 2 do capítulo II. Portanto os ideais de $R\langle X\rangle_{Q_U}$ estão totalmente ordenados, pela proposição 1. Se M não é maximal, então R_M é um corpo, pela hipótese. Logo $R\langle X\rangle_{Q_U} \cong R[X]_Q \cong R_M[X]_{Q_M}$ é uma localização do domínio de ideais principais $R_M[X]$ e portanto é um anel aritmético local. Então os ideais de $R\langle X\rangle_{Q_U}$ estão totalmente ordenados, pela proposição 1. Consequentemente $R\langle X\rangle$ é aritmético.

C.Q.D.

DEFINIÇÃO - Dizemos que R é um anel de Prüfer se todo ideal regular finitamente gerado de R é inversível.

DEFINIÇÃO - Dizemos que R é um anel fortemente de Prüfer se todo ideal finitamente gerado I de R, com $0:I = 0$, é localmente principal.

OBSERVAÇÕES - (1) Todo anel aritmético é um anel fortemente de Prüfer.
(2) Todo anel fortemente de Prüfer é um anel de Prüfer.

TEOREMA 3 - São equivalentes:
(a) R(X) é um anel de Prüfer.
(b) R é um anel fortemente de Prüfer.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que R(X) é um anel de Prüfer. Seja $I = (a_0, a_1, \ldots, a_n)$ um ideal finitamente gerado de R, com $0:I = 0$. Seja $f = a_0 + a_1X + \cdots + a_nX^n$. Se $c \in R$ e $ca_i = 0$, $0 \leq i \leq n$, então $cI = 0$; logo $c \in 0:I$ e portanto $c = 0$. Então f é regular e portanto $IR(X) = C(f)R(X)$ é um ideal regular finitamente gerado de R(X), pois $f \in fR(X) \subseteq C(f)R(X) = IR(X)$. Como R(X) é um anel de Prüfer, então IR(X) é inversível. Logo I é localmente principal, pela proposição 13 do capítulo II. Conse

quentemente R é um anel fortemente de Prüfer.

(b) $\Rightarrow$ (a). Suponhamos que R é um anel fortemente de Prüfer. Seja K um ideal regular finitamente gerado de R(X). Então $K = Q_S$ para algum ideal regular finitamente gerado Q de R[X]. Seja $Q = f_1R[X] + f_2R[X] + \cdots + f_nR[X]$. Se $g = f_1 + f_2X^{n_2} + \cdots + f_nX^{n_n}$, onde $r_i = gr(f_1) + gr(f_2) + \cdots + gr(f_{i-1}) + i-1$, $2 \leq i \leq n$, então $C(g) = C(f_1) + C(f_2) + \cdots + C(f_n)$ é um ideal finitamente gerado de R e $0:C(g) = 0$, pois Q contém um elemento regular. Logo C(g) é localmente principal e portanto $C(g)R(X) = gR(X)$ (proposição 8, cap. II). Mas $gR(X) \subseteq QR(X) = K \subseteq C(g)R(X) = gR(X)$, pois $f_iR(X) \subseteq C(f_i)R(X)$, $1 \leq i \leq n$. Então $K = gR(X)$ é principal e portanto inversível. Consequentemente R(X) é um anel de Prüfer.

C.Q.D.

COROLÁRIO - São equivalentes:

(a) R(X) é um domínio de Prüfer.

(b) R é um domínio de Prüfer.

TEOREMA 4 - São equivalentes:

(a) R(X) é um anel de Prüfer.

(b) R é um anel fortemente de Prüfer, $\dim R \leq 1$ e R_M é um corpo sempre que $M \subset P$ é uma cadeia de ideais primos de R.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que R(X) é um anel de Prüfer. Então sua localização R(X) é um anel de Prüfer. Logo R é um anel fortemente de Prüfer, pelo teorema anterior. Seja $M \subset P$ uma cadeia de ideais primos de R. Sejam $m \in M$ e $a \in P \setminus M$. Então $I = mR[X] + (aX + 1)R[X]$ é um ideal regular finitamente gerado de R[X]. Portanto IR(X) é inversível. Como $M[X] + (aX + 1)R[X]$ não contém polinômios mônicos, então existe um ideal primo Q de R[X] tal que Q não contém polinômios mônicos e $M[X] +$

$+ (aX + 1)R[X] \subseteq Q$. Logo $I_Q = IR\langle X\rangle_{Q_U}$ é principal, pois $IR\langle X\rangle$ é inversível. Portanto $I_Q = ((aX + 1)R[X])_Q$, porque não podemos ter $((aX + 1)R[X])_Q \subseteq (mR[X])_Q$. Então, como no teorema 2, resulta que R_M é um corpo. Consequentemente dim $R \leqslant 1$ e R_M é um corpo sempre que $M \subset P$ é uma cadeia de ideais primos de R.

(b) $\Longrightarrow$ (a). Suponhamos que R é um anel fortemente de Prüfer, dim $R \leqslant 1$ e R é um corpo sempre que $M \subset P$ é uma cadeia de ideais primos de R. Seja K um ideal regular finitamente gerado de $R\langle X\rangle$. Para demonstrar que K é inversível é suficiente demonstrar que K_L é um ideal principal para todo ideal maximal L de $R\langle X\rangle$ que contém K. Sejam $K = J_U$, onde J é um ideal regular finitamente gerado de R[X], $L = Q_U$, onde Q é um ideal primo de R[X] e $M = Q \cap R$. Demonstraremos que $J_Q = (J_U)_{Q_U} = K_L$ é principal. Se M não é maximal, então R_M é um corpo, pela hipótese. Logo J_Q é um ideal principal no anel de valorização discreta $R[X]_Q \cong R_M[X]_{Q_M}$. Se M é maximal, então $Q = M[X]$ ou $Q = M[X] + fR[X]$ para algum $f \in R[X]$ mônico. Como Q não contém polinômios mônicos, pois sua localização L é maximal, então devemos ter $Q = M[X]$. Logo $R[X]_Q = R[X]_{M[X]} \cong R_M(X)$. Sejam $J = f_1R[X] + f_2R[X] + \cdots + f_nR[X]$, onde $f_i \in R[X]$, $1 \leqslant i \leqslant n$, e $g = f_1 + f_2X^{r_2} + \cdots + f_nX^{r_n}$, onde $r_i = gr(f_1) + gr(f_2) + \cdots + gr(f_{i-1}) + i-1$, $2 \leqslant i \leqslant n$. Então, como na demonstração de teorema 3, $J_Q = JR_M(X) = gR_M(X)$ é principal.

C.Q.D.

Agora consideremos os reticulados de ideais, L(R) e L(R(X)), de R e R(X), respectivamente, e a aplicação

$$\begin{aligned} \theta : L(R) &\longrightarrow L(R(X)) \\ I &\longmapsto IR(X) \end{aligned}$$

OBSERVAÇÃO - É claro que θ é injetiva (proposição 5, cap. II).

PROPOSIÇÃO 4 - A aplicação θ preserva somas e interseções arbitrárias e produtos finitos de ideais.

DEMONSTRAÇÃO - Seja I uma soma de ideais de R, digamos $I = \sum_{\alpha \in \Lambda} I_\alpha$. Se $q \in IR(X)$, então $q = f/h$, para alguns $f \in IR[X]$, $h \in S$. Portanto existem $\alpha_1, \ldots, \alpha_n \in \Lambda$ tais que $f = a_1 f_1 + \cdots + a_n f_n$, onde $a_i \in I_{\alpha_i}$, $f_i \in R[X]$, $1 \leq i \leq n$. Logo $q = a_1(f_1/h) + \cdots + a_n(f_n/h) \in \sum_{\alpha \in \Lambda} I_\alpha R(X)$. Reciprocamente, se $q \in \sum_{\alpha \in \Lambda} I_\alpha R(X)$, então existem $\alpha_1, \ldots, \alpha_n \in \Lambda$ tais que $q = a_1(f_1/h_1) + \cdots + a_n(f_n/h_n)$, onde $a_i \in I_{\alpha_i}$, $f_i \in R[X]$, $h_i \in S$, $1 \leq i \leq n$. Logo podemos escrever $q = (a_1 g_1 + \cdots + a_n g_n)/h$, onde $g_i \in R[X]$, $1 \leq i \leq n$, $h \in S$. Portanto $q \in IR(X)$. Consequentemente $(\sum_{\alpha \in \Lambda} I_\alpha)R(X) = IR(X) = \sum_{\alpha \in \Lambda} I_\alpha R(X)$. Similarmente demonstra-se que θ preserva interseções arbitrárias e produtos finitos.

C.Q.D.

TEOREMA 5 - São equivalentes:

(a) θ é sobrejetiva.

(b) θ é um isomorfismo de reticulados que preserva a multiplicação de ideais.

(c) R é aritmético.

DEMONSTRAÇÃO - É claro que (a) implica (b).

(b) $\Longrightarrow$ (c). Suponhamos que θ é um isomorfismo de reticulados. Seja $I = (a_0, a_1, \ldots, a_n)$ um ideal finitamente gerado de R. Se $f = a_0 + a_1 X + \cdots + a_n X^n$, então $fR(X) = JR(X)$ para algum ideal J de R, pois θ é sobrejetiva. Então $I = C(f)$ é localmente principal pela proposição 8 do capítulo II. Consequentemente R é aritmético.

(c) $\Longrightarrow$ (a). Suponhamos que R é aritmético. Seja K um ideal de

R(X). É suficiente considerar o caso em que K é principal, pois todo ideal é a soma de todos os ideais principais que contém e θ preserva somas arbitrárias. Seja K = fR(X), onde $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$. Como R é aritmético, então C(f) é localmente principal. Logo K = fR(X) = C(f)R(X), pela proposição 8 do capítulo II. Portanto K = θ(C(f)) e θ é sobrejetiva.

C.Q.D.

DEFINIÇÃO - Seja J um ideal de R. Dizemos que J é semi-regular se existe um ideal finitamente gerado I de R tal que $I \subseteq J$ e 0:I = 0.

É claro que o conjunto dos ideais semi-regulares de R é um sub-reticulado de L(R).

DEFINIÇÃO - Dizemos que R satisfaz a condição (A) se todo ideal finitamente gerado I de R com 0:I = 0 é regular.

OBSERVAÇÃO - R satisfaz a condição (A) se e somente se todo ideal semi-regular de R é regular.

TEOREMA 6 - São equivalentes:
(a) θ é um isomorfismo de reticulados entre o sub-reticulado dos ideais semi-regulares de R e o sub-reticulado dos ideais regulares de R(X).
(b) Todo ideal regular de R(X) é extensão de um ideal de R.
(c) R é fortemente de Prüfer.

DEMONSTRAÇÃO - É claro que (a) implica (b).
(b) $\Rightarrow$ (c). Suponhamos que todo ideal regular de R(X) é extensão de um ideal de R. Seja $I = (a_0, a_1, \ldots, a_n)$ um ideal finita-

mente gerado de R com 0:I = 0. Então $f = a_0 + a_1X + \cdots + a_nX^n$ é um elemento regular de R(X) e portanto fR(X) é um ideal regular de R(X). Logo fR(X) = JR(X) para algum ideal J de R. Então I = C(f) é localmente principal, pela proposição 8 do capítulo II. Consequentemente R é um anel fortemente de Prüfer.

(c) $\Rightarrow$ (a). Suponhamos que R é fortemente de Prüfer. Seja J um ideal semi-regular de R. Então existe um ideal finitamente gerado de R, $I = (a_0, a_1, \ldots, a_n) \subseteq J$, com 0:I = 0. Se $f = a_0 + a_1X + \cdots + a_nX^n$, então $f \in JR(X)$ é regular e portanto $\theta(J) = JR(X)$ é um ideal regular de R(X). Por outro lado, se K é um ideal regular de R(X), então existe $f \in K \cap R[X]$ regular. Demonstraremos que K é extensão de um ideal de R, isto é, demonstraremos que todo ideal regular de R(X) é um elemento de $\theta(L(R))$. Como K = K + fR(X), então K é a soma de todos os ideais da forma gR(X) +fR(X), com $g \in K$. Para $g \in K$, gR(X) + fR(X) é um ideal regular finitamente gerado de R(X). Então gR(X) + fR(X) é inversível, pois R(X) é de Prüfer pelo teorema 3. Logo gR(X) + fR(X) é um ideal principal de R(X) pelo teorema 3 do capítulo II. Portanto existe $h \in R[X]$ regular tal que gR(X) + fR(X) = hR(X). Como C(h) é finitamente gerado e 0:C(h) = 0, então C(h) é localmente principal. Portanto gR(X) + fR(X) = hR(X) = C(h)R(X). Disto resulta que K é extensão de um ideal de R. Seja K = JR(X), onde J é um ideal de R. Como fR(X) é um ideal regular de R(X), então fR(X) = IR(X) para algum ideal I de R, segundo o que acabamos de demonstrar. Então C(f) é localmente principal e I = C(f). Logo I é um ideal finitamente gerado de R, 0:I = 0:C(f) = 0 e $I \subseteq J$. Portanto J é um ideal semi-regular de R e consequentemente K = $\theta(J)$, onde J é semi-regular.

C.Q.D.

COROLÁRIO - São equivalentes:

(a) θ é um isomorfismo de reticulados entre os sub-reticulados dos ideais regulares de R e R(X).

(b) Todo ideal principal regular de R(X) é extensão de um ideal regular de R.

(c) R é um anel de Prüfer que satisfaz a condição (A).

DEMONSTRAÇÃO - É claro que (a) implica (b).

(b) $\Rightarrow$ (c). Suponhamos que todo ideal principal regular de R(X) é extensão de um ideal regular de R. Seja $I = (a_0, a_1, \ldots, a_n)$ um ideal regular de R. Então $f = a_0 + a_1X + \cdots + a_nX^n$ é um elemento regular de R(X) e portanto fR(X) é um ideal principal regular de R(X). Logo $fR(X) = JR(X)$ para algum ideal regular J de R. Mas isto implica que $I = C(f)$ é localmente principal, pela proposição 8 do capítulo II. Portanto I é um ideal regular localmente principal finitamente gerado. Consequentemente I é inversível e R é de Prüfer. Agora suponhamos que $I = (a_0, a_1, \ldots, a_n)$ é um ideal de R e que $0:I = 0$. Seja $f = a_0 + a_1X + \cdots + a_nX^n$. Então $fR(X) = JR(X)$ para algum ideal regular J de R, pois f é um elemento regular de R(X). Logo $I = C(f)$ é localmente principal e $JR(X) = fR(X) = C(f)R(X)$ e portanto $I = C(f) = J$ é regular. Em consequência R satisfaz a condição (A).

(c) $\Rightarrow$ (a). Suponhamos que R é um anel de Prüfer que satisfaz a condição (A). Então R é um anel fortemente de Prüfer e todo ideal semi-regular de R é regular. Logo θ é um isomorfismo de reticulados entre os sub-reticulados de ideais regulares de R e R(X), pelo teorema 6.

C.Q.D.

CAPITULO IV

ANÉIS DE HILBERT

Neste capítulo, $\bar{A}$ denota o fecho integral de um anel A. Utilizaremos os resultados do capítulo anterior para estabelecer condições necessárias e suficientes para ser R(X) um anel de Hilbert.

DEFINIÇÃO - Dizemos que R é um anel de Hilbert se todo ideal primo de R é uma interseção de ideais maximais de R.

PROPOSIÇÃO 1 - São equivalentes:
(a) R(X) é um anel de Hilbert.
(b) R é um anel de Hilbert e todo ideal primo de R(X) é a extensão de um ideal de R.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que R(X) é um anel de Hilbert. Seja P um ideal primo de R. Então PR(X) é um ideal primo de R(X). Logo existe um conjunto $\{M_\alpha ; \alpha \in \Lambda\}$ de ideais maximais de R tal que $PR(X) = \bigcap \{M_\alpha R(X) ; \alpha \in \Lambda\}$. Logo $P = PR(X) \cap R = (\bigcap \{M_\alpha R(X) ; \alpha \in \Lambda\}) \cap R = \bigcap \{M_\alpha R(X) \cap R; \alpha \in \Lambda\} = \bigcap \{M_\alpha ; \alpha \in \Lambda\}$ é uma interseção de ideais maximais de R e portanto R é um anel de Hilbert. Seja Q um ideal primo de R(X). Então $Q = \bigcap \{M_\alpha R(X) ; \alpha \in \Lambda\}$ para algum conjunto $\{M_\alpha ; \alpha \in \Lambda\}$ de ideais maximais de R. Logo $Q = (\bigcap_{\alpha \in \Lambda} M_\alpha)R(X)$, onde $\bigcap_{\alpha \in \Lambda} M_\alpha = Q \cap R$ é um ideal primo de R, e portanto Q é a extensão de um ideal de R.

(b) $\Rightarrow$ (a). Suponhamos que R é um anel de Hilbert e que todo ideal primo de R(X) é a extensão de um ideal de R. Seja Q um i-

deal primo de R(X). Então Q = PR(X) para algum ideal P de R. Como P = Q ∩ R e Q é primo, então P é um ideal primo de R. Logo $P = \bigcap \{M_\alpha ; \alpha \in \Lambda\}$ para algum conjunto $\{M_\alpha ; \alpha \in \Lambda\}$ de ideais maximais de R, pois R é de Hilbert. Portanto Q = PR(X) = $= (\bigcap_{\alpha \in \Lambda} M_\alpha)R(X) = \bigcap_{\alpha \in \Lambda} M_\alpha R(X)$ é uma interseção de ideais maximais de R(X). Consequentemente R(X) é um anel de Hilbert.

C.Q.D.

DEFINIÇÃO - Dizemos que R satisfaz a condição (*) se para cada ideal primo Q de R[X] com $Q \subseteq M[X]$ para algum ideal maximal M de R, temos Q = P[X] para algum ideal primo P de R (necessariamente P = Q ∩ R).

PROPOSIÇÃO 2 - São equivalentes:

(a) Todo ideal primo de R(X) é a extensão de um ideal de R.

(b) R satisfaz a condição (*).

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que todo ideal primo de R(X) é a extensão de um ideal de R. Seja Q um ideal primo de R[X] com $Q \subseteq M[X]$ para algum $M \in Max(R)$. Então Q ∩ S = Ø (lembramos que $S = \{f \in R[X] ; C(f) = R\}$). Logo Q_S é um ideal primo de R(X) e portanto $Q_S = PR(X)$ para algum ideal (primo) P de R (P = = Q ∩ R). Então $Q = Q_S \cap R[X] = PR(X) \cap R[X] = P[X]$. Consequentemente R satisfaz a condição (*).

(b) $\Rightarrow$ (a). Suponhamos que R satisfaz a condição (*). Seja K um ideal primo de R(X). Então $K = Q_S$, onde Q = K ∩ R[X] é um ideal primo de R[X] com Q ∩ S = Ø. O ideal $N = \{a \in R ; a$ é coeficiente de algum polinômio em $Q\}$ está propriamente contido em R, pois Q ∩ S = Ø. Logo existe $M \in Max(R)$ tal que $N \subseteq M$ e portanto $Q \subseteq$ $\subseteq N[X] \subseteq M[X]$. Então existe um ideal P de R tal que Q = P[X] , pela hipótese. Consequentemente $K = Q_S = P[X]_S = PR(X)$ é a exten

são de um ideal de R.

C.Q.D.

PROPOSIÇÃO 3 - São equivalentes:

(a) R(X) é um anel de Hilbert.

(b) R é um anel de Hilbert e satisfaz a condição (*).

DEMONSTRAÇÃO - Imediata.

PROPOSIÇÃO 4 - São equivalentes:

(a) R satisfaz a condição (*).

(b) $\bar{R}$ satisfaz a condição (*).

DEMONSTRAÇÃO - (a) $\Longrightarrow$ (b). Suponhamos que R satisfaz a condição (*). Seja $\bar{Q}$ um ideal primo de $\bar{R}[X]$ com $\bar{Q} \subseteq \bar{M}[X]$ para algum ideal $\bar{M} \in Max(\bar{R})$. Como $\bar{Q} \cap R[X] \subseteq \bar{M}[X] \cap R[X] = (\bar{M} \cap R)[X]$ e $\bar{M} \cap R$ é um ideal primo de R , então existe $N \in Max(R)$ tal que $\bar{Q} \cap R[X] \subseteq N[X]$ e portanto $\bar{Q} \cap R[X]$ P[X] para algum ideal primo P de R. Logo $\bar{Q} \cap R = P$. Seja $\bar{P} = \bar{Q} \cap \bar{R}$. Então $\bar{P}$ é um ideal primo de $\bar{R}$ e $\bar{P}[X]$ é um ideal primo de $\bar{R}[X]$. Como $\bar{R}[X]$ é inteiro sobre R[X] e $\bar{P}[X] \cap R[X] = (\bar{Q} \cap \bar{R})[X] \cap R[X] = (\bar{Q} \cap \bar{R} \cap R)[X] =$ $= (\bar{Q} \cap R)[X] = P[X] = \bar{Q} \cap R[X]$ e $\bar{P}[X] \subseteq \bar{Q}$, então $\bar{Q} = \bar{P}[X]$ .Consequentemente, $\bar{R}$ satisfaz a condição (*).

(b) $\Longrightarrow$ (a). Suponhamos que $\bar{R}$ satisfaz a condição (*). Seja Q um ideal primo de R[X] com $Q \subseteq M[X]$ para algum $M \in Max(R)$. Como $\bar{R}[X]$ é inteiro sobre R[X], então pelo Teorema do Ascenso, existem ideais primos $\bar{K}$, $\bar{Q}$ em $\bar{R}[X]$ tais que $\bar{Q} \subseteq \bar{K}$, $\bar{Q} \cap R[X] = Q$ e $\bar{K} \cap R[X] =$ $= M[X]$. Observamos que $\bar{K} \cap R = (\bar{K} \cap R[X]) \cap R = M[X] \cap R = M$. Seja $K = \bar{K} \cap \bar{R}$. Então $K \cap R = \bar{K} \cap R = M$. Como $K[X] \subseteq \bar{K}$ e

$K[X] \cap R[X] = (K \cap R)[X] = M[X] = \bar{K} \cap R[X]$,então por INC , $K[X] = \bar{K}$. Como $\bar{R}$ satisfaz a condição (*) e $\bar{Q} \subsetneq K[X]$, onde K é um ideal primo de $\bar{R}$, então $\bar{Q} = (\bar{Q} \cap \bar{R})[X]$. Portanto $Q = \bar{Q} \cap R[X] = (\bar{Q} \cap \bar{R})[X] \cap R[X] = (\bar{Q} \cap R)[X]$ onde $\bar{Q} \cap R$ é um ideal primo de R. Consequentemente R satisfaz a condição (*).

C.Q.D.

DEFINIÇÃO - Seja F um corpo arbitrário. Um "place" de F é um homomorfismo não nulo L de um subanel F_L de F num corpo F' tal que se $x \in F \setminus F_L$, então $1/x \in F_L$ e $L(1/x) = 0$.

CONVENÇÃO - Se $x \in F \setminus F_L$, então escrevemos $L(x) = \infty$. Dizemos que x tem L-valor finito se $L(x) \neq \infty$, isto é, se $x \in F_L$. O anel F_L será chamado de anel de valorização do "place" L .

OBSERVAÇÃO - Um subanel R do corpo F é un anel de valorização de um "place" L de F se e somente se R é um anel de valorização de F.

De fato, se $R = F_L$ é o anel de valorização de um "place" L de F , então da definição, F_L resulta ser um anel de valorização.Recíprocamente, se R é um anel de valorização de F, então R tem um único ideal maximal $M = R \setminus U(R)$. Seja L o homomorfismo canónico de R sobre o corpo R/M . Então é claro que L é um "place" de F e R é o anel de valorização de L.

DEFINIÇÃO - Sejam R um domínio de integridade, F um corpo contendo R e L um "place" de F. Dizemos que L é finito sobre R se todo elemento de R tem L-valor finito, isto é, se R está contido no anel de valorização de L.

LEMA 1. Seja A um subanel de um corpo F e J um ideal próprio de A. Se $x \in F \setminus \{0\}$, então $JA[x] \neq A[x]$ ou $JA[1/x] \neq A[1/x]$.

DEMONSTRAÇÃO - Suponhamos que $JA[x] = A[x]$ e $JA[1/x] = A[1/x]$. Então

$$(a) \quad 1 = a_0 + a_1 x + \cdots + a_n x^n$$

$$(b) \quad 1 = b_0 + b_1(1/x) + \cdots + b_m(1/x)^m$$

para alguns $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m \in J$.

Podemos supor que as equações (a) e (b) são de grau mínimo e que $m \leq n$. Multiplicando (a) por $1-b_0$ e (b) por $a_n x^n$, obtemos

$$1-b_0 = (1-b_0)a_0 + \cdots + (1-b_0)a_n x^n$$

$$(1-b_0)a_n x^n = a_n b_1 x^{n-1} + \cdots + a_n b_m x^{n-m}$$

donde

$$1 = b_0 + (1-b_0)a_0 + \cdots + (1-b_0)a_{n-1}x^{n-1} + a_n b_1 x^{n-1} + \cdots + a_n b_m x^{n-m}$$

o que contradiz a minimalidade de n.

Consequêntemente, $JA[x] \neq A[x]$ ou $JA[1/x] \neq A[1/x]$.

C.Q.D.

PROPOSIÇÃO 5 - Seja R um subanel de um corpo F e I um ideal próprio de R. Então existe um "place" L de F com anel de valorização F_L tal que $R \subseteq F_L$ e $I \subseteq M_L$, onde $M_L = F \setminus U(F_L)$.

DEMONSTRAÇÃO - Seja $\mathcal{R} = \{A;\ A$ é subanel de F, $R \subseteq A$ e $IA \neq A\}$. Então $\mathcal{R} \neq \emptyset$, pois $R \in \mathcal{R}$. Uma ordem parcial em $\mathcal{R}$ está dada pela inclusão de conjuntos. Se $\{A_\alpha;\ \alpha \in \Lambda\}$ é uma cadeia em $\mathcal{R}$, então $A = U\{A_\alpha;\ \alpha \in \Lambda\} \in \mathcal{R}$ é uma cota superior de $\{A_\alpha;\ \alpha \in \Lambda\}$. Logo $\mathcal{R}$ tem elementos maximais. Demonstraremos que todo elemento maximal de $\mathcal{R}$ é um anel de valorização de F. Seja A um elemento maximal de $\mathcal{R}$. Então A satisfaz as seguintes condições:

(1) $R \subseteq A$ e $IA \neq A$.

(2) Se B é um subanel de F e $A \subset B$, então $IB = B$.

Seja $J = IA$. Então $J \neq A$. Se $x \in F \setminus \{0\}$, então $JA[x] \neq A[x]$ ou $JA[1/x] \neq A[1/x]$, pelo lema anterior. Logo $IA[x] \neq A[x]$ ou $IA[1/x] \neq A[1/x]$; portanto $A = A[x]$ ou $A = A[1/x]$,

pela maximalidade de A. Então $x \in A$ ou $1/x \in A$, isto é, A é um anel de valorização de F. Portanto existe um "place" L de F tal que $F_L = A$ é o anel de valorização de L. Se $M_L = A \setminus U(A)$ é o único ideal maximal de A , então $I \subseteq IA \subseteq M_L$. Também temos $R \subseteq F_L$.

C.Q.D.

DEFINIÇÃO - Sejam R um domínio de integridade, F um corpo contendo R e L um "place" de F com anel de valorização F_L. O centro de L em R é o ideal primo $P = M_L \cap R$, onde M_L é o (único) ideal maximal de F_L.

PROPOSIÇÃO 6 - Se D é um domínio de integridade contido num corpo F e se P é um ideal primo de D, então existe um "place" L de F, com anel de valorização $F_L \supseteq D$, cujo centro em D é P.

DEMONSTRAÇÃO - Sejam $R = D_P$ e $I = R \setminus U(R)$. Então $I \neq R$ e $R \subseteq F$. Logo existe um "place" L de F com anel de valorização F_L tal que $R \subseteq F_L$ e $I \subseteq M_L \cap R$, onde M_L é o ideal maximal de F_L. Como I é maximal e $1 \notin M_L$, então $I = M_L \cap R$. Portanto $P = M_L \cap D$, pois $I \cap D = P$. Consequentemente $D \subseteq F_L$ e o centro de L em D é P.

C.Q.D.

PROPOSIÇÃO 7 - Seja R um domínio integralmente fechado. Se P é um ideal primo de R , $f \in R[X] \setminus P[X]$ e $c \in T(R) \setminus \{0\}$ é raíz de f , então $c \in R_P$ ou $1/c \in R_P$.

DEMONSTRAÇÃO - Seja $f = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$. Como $a_0c^n + a_1c^{n-1} + \cdots + a_{n-1}c + a_n = 0$, então $a_0 + a_1(1/c) + \cdots + a_{n-1}(1/c^{n-1}) + a_n(1/c^n) = 0$; logo $1/c$ é raíz de $a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + a_nX^n \in R[X] \setminus P[X]$ e portanto nossas hipóteses são

simétricas em c e 1/c. Sabemos que existe um "place" L_0 tal que o centro de L_0 é P. Demonstraremos que $c \in R_P$ ou $1/c \in R_P$ segundo $L_0(c) \neq \infty$ ou $L(1/c) \neq \infty$, respectivamente. Suponhamos que $L_0(c) \neq \infty$ e que $a_0, a_1, \ldots, a_{K-1} \in P$, $a_K \in R \setminus P$, onde $0 \leq k \leq n$. Se $k = 0$, então c é inteiro sobre R_P; logo $c \in R_P$. Não podemos ter $k = n$, pois em caso contrário, a existencia de um "place" L_0 com centro P e tal que $L_0(c) \neq \infty$ implicaria que $L_0(a_n) = 0$ e portanto $a_n \in P$, o que é uma contradição. Então assumiremos que $0 < k < n$. Sejam

$$x = a_0 c^K + a_1 c^{K-1} + \cdots + a_{K-1} c + a_K$$

$$y = a_{K+1} + a_{K+2} c^{-1} + \cdots + a_n c^{K+1-n}$$

Seja L qualquer "place" finito sobre R. Se $L(c) \neq \infty$, então também $L(x) \neq \infty$ e $L(y) \neq \infty$, pois $cx + y = 0$. Se $L(c) = \infty$, então $L(y) \neq \infty$ e portanto $L(x) = 0$, pois $x + c^{-1}y = 0$. Logo em todos os casos temos $L(x) \neq \infty$ e $L(y) \neq \infty$. Como isto vale para todos os "places" que são finitos sobre R, então x e y são elementos de $\cap\{A;\ A$ é anel de valorização de $T(R)$ e $R \subseteq A\} = R$ (por ser R integralmente fechado). Agora, pelo assumido, existe um "place" L_0 com centro P e tal que $L_0(c) \neq \infty$. Para este "place" L_0 temos $L_0(x) \neq 0$, pois $L_0(a_i) = 0$, $0 \leq i \leq k-1$, e $L_0(a_K) \neq 0$ (em vista do suposto sobre $a_0, a_1, \ldots, a_{K-1}$ e a_K). Então $x \in R \setminus P$ e portanto $c = -y/x \in R_P$.

C.Q.D.

LEMA 2. Seja R um domínio de integridade que satisfaz a condição (*). Se Q é um ideal primo não nulo de R[X] tal que $Q \subseteq \cup\{M[X];\ M \in Max(R)\}$, então $Q \cap R \neq 0$.

DEMONSTRAÇÃO - Como $Q \subseteq \cup\{M[X];\ M \in Max(R)\} = R[X] \setminus S$ então $Q \cap S = \emptyset$; logo Q_S é um ideal primo de R(X) e portanto $Q_S = PR(X)$ para algum ideal primo não nulo P de R, pela proposição 2. Então $Q = Q_S \cap R[X] = PR(X) \cap R[X] = P[X]$, donde $Q \cap R =$

$= P[X] \cap R = P \neq 0.$

C.Q.D.

PROPOSIÇÃO 8 - Seja R um domínio integralmente fechado. São equivalentes:

(a) R satisfaz a condição (*).

(b) R é um domínio de Prüfer.

DEMONSTRAÇÃO - (a) $\Longrightarrow$ (b). Suponhamos que R satisfaz a condição (*). Sejam P um ideal primo de R e $c \in T(R) \setminus \{0\}$. Seja Q o núcleo do R-homomorfismo canónico φ de R[X] sobre R[c] tal que $\varphi(X) = c$. Então Q é um ideal primo não nulo de R[X]. Como $\varphi(a) = a$ para todo $a \in R$, então $Q \cap R = 0$; logo $Q \nsubseteq \cup\{M[X]; M \in Max(R)\}$, pelo lema acima. Mas $P[X] \subseteq \cup\{M[X]; M \in Max(R)\}$; portanto existe $f(X) \in Q \setminus P[X]$, isto é, existe $f(X) \in R[X]$ tal que $f(c) = 0$ e $f(X) \notin P[X]$. Então $c \in R_P$ ou $1/c \in R_P$, pela proposição 7. Logo R_P é um anel de valorização para cada ideal primo P de R e consequentemente R é um domínio de Prüfer.

(b) $\Longrightarrow$ (a). Suponhamos que R é um domínio de Prüfer. Então R é aritmético. Logo todo ideal de R(X) é a extensão de um ideal de R. Em particular todo ideal primo de R(X) é a extensão de um ideal de R. Consequentemente R satisfaz a condição (*), pela proposição 2.

C.Q.D.

TEOREMA 1 - São equivalentes:

(a) R(X) é um anel de Hilbert.

(b) R é um anel de Hilbert e $\overline{R/P}$ é um domínio de Prüfer para todo ideal primo minimal P de R.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que $R(X)$ é um anel de Hilbert. Então R é um anel de Hilbert, pela proposição 1. Seja P um ideal primo minimal de R. $R(X)/PR(X)$ é um domínio de Hilbert pelo teorema 31.8 de (7). Mas $R(X)/PR(X) \cong (R/P)(X)$ pela proposição 6 do capítulo II; logo R/P satisfaz a condição (*) (proposição 3). Portanto $\overline{R/P}$ satisfaz a condição (*) pela proposição 4. Em consequência $\overline{R/P}$ é um domínio de Prüfer, pela proposição anterior.

(b) $\Rightarrow$ (a). Suponhamos que R é um anel de Hilbert e que $\overline{R/P}$ é um domínio de Prüfer, para todo ideal primo minimal P de R. Para demonstrar que $R(X)$ é um anel de Hilbert é suficiente demonstrar que $R(X)/Q$ é um domínio de Hilbert, para todo ideal primo minimal Q de $R(X)$. Seja Q um ideal primo minimal de $R(X)$. Então $Q = PR(X)$, onde $P = Q \cap R$ é um ideal primo minimal de R. Logo R/P é um domínio de Hilbert. Como $\overline{R/P}$ é um domínio de Prüfer, então $\overline{R/P}$ satisfaz a condição (*) e portanto R/P satisfaz a condição (*). Segue-se que $(R/P)(X)$ é um domínio de Hilbert, pela proposição 3. Consequentemente $R(X)/Q = R(X)/PR(X) \cong (R/P)(X)$ é um domínio de Hilbert.

C.Q.D.

CAPÍTULO V

PROPRIEDADES DE DIVISIBILIDADE DE R(X) E R(X)

Neste capítulo, L(R) denota o reticulado de ideais do anel R e Inv(R) denota o conjunto dos ideais (integrais) inversíveis de R. Para um domínio de Krull R, Cl(R) denota o grupo de classes de divisores, isto é, o grupo de ideais divisoriais de R módulo os ideais principais; Pic(R) denota o subgrupo dos ideais inversíveis de R módulo os ideais principais e é chamado o grupo de Picard de R.

DEFINIÇÃO - Seja R um domínio de integridade. Dizemos que R é um GCD-domínio generalizado (G-GCD domínio) se $I \cap J \in Inv(R)$ para quaisquer $I, J \in Inv(R)$.

PROPOSIÇÃO 1 - Seja R um domínio de integridade. São equivalentes:

(a) R é um G-GCD domínio.

(b) $(a) \cap (b) \in Inv(R)$ para quaisquer $a, b \in R \setminus \{0\}$.

(c) $(a) : (b) \in Inv(R)$ para quaisquer $a, b \in R \setminus \{0\}$.

(d) $I : J \in Inv(R)$ para quaisquer $I, J \in Inv(R)$.

(e) Inv(R) é um reticulado-grupo ordenado, com a ordem dada por $I \leqslant J$ se e só se $J \subseteq I$.

(f) Todo v-ideal de R finitamente gerado é inversível.

DEMONSTRAÇÃO - (a) $\Leftrightarrow$ (b). É claro que (a) implica (b). Reciprocamente, se $I = (a_1, a_2, \ldots, a_n)$ e $J = (b_1, b_2, \ldots, b_m)$ são ideais (integrais) inversíveis de R, então $I \cap J = \sum_{i,j} (a_i) \cap (b_j)$. De fato, se $M \in Max(R)$, então existem $k \in \{1, 2, \ldots, n\}$ e $l \in \{1, 2, \ldots, m\}$ tais que $I_M = (a_k)_M$ e $J_M = (b_l)_M$; logo $(I \cap J)_M =$

$= I_M \cap J_M = (a_k)_M \cap (b_l)_M = ((a_k) \cap (b_l))_M \subseteq (\sum_{i,j} (a_i) \cap (b_j))_M \subseteq$
$\subseteq (I \cap J)_M$. Então $(I \cap J)_M = ((a_k) \cap (b_l))_M$ é principal, pois $(a_k) \cap (b_l) \in Inv(R)$. Além disto, $I \cap J = \sum_{i,j} (a_i) \cap (b_j)$ é uma soma finita de ideais inversíveis de R e portanto é um ideal finitamente gerado; logo $I \cap J \in Inv(R)$.

(b) $\Longleftrightarrow$ (c). Sejam $a, b \in R \setminus \{0\}$ quaisquer. É claro que $((a) : (b))(b) \subseteq (a) \cap (b)$. Por outro lado, se $x \in (a) \cap (b)$, então existe $r \in R$ tal que $x = rb \in (a)$; logo $r \in (a) : (b)$ e portanto $x = rb \in ((a) : (b))(b)$. Temos, assim, que $(a) \cap (b) =$
$= ((a) : (b))(b)$ (localizando, demonstra-se que $I \cap J =$
$= (I : J)J$ para quaisquer $I, J \in Inv(R)$). Como consequência disto, $(a) \cap (b) \in Inv(R)$ se e só $(a) : (b) \in Inv(R)$.

(a) $\Longleftrightarrow$ (d). É similar à anterior.

(a) $\Longleftrightarrow$ (e). Para quaisquer $I, J \in Inv(R)$, $\sup(I,J)$ existe se e só se $I \cap J \in Inv(R)$ e neste caso $\sup(I,J) = I \cap J$.

(a) $\Longrightarrow$ (f). Suponhamos que R é um G-GCD domínio. Seja $(a_1,a_2,\ldots,a_n)_v = ((a_1,a_2,\ldots,a_n)^{-1})^{-1}$, um v-ideal de R finitamente gerado. Como $(a_1,a_2,\ldots,a_n)^{-1} = a_1^{-1}R \cap \cdots \cap a_n^{-1}R \in Inv(R)$, então $(a_1,a_2,\ldots,a_n)_v \in Inv(R)$.

(f) $\Longrightarrow$ (e). Suponhamos que todo v-ideal de R finitamente gerado é inversível. Sejam $I, J \in Inv(R)$. Como $(I + J)_v$ é um v-ideal de R finitamente gerado, então $(I + J)_v \in Inv(R)$; logo existe $\inf(I,J) = (I + J)_v$.

C.Q.D.

PROPOSIÇÃO 2 - Se R é um G-GCD domínio, então R é integralmente fechado.

DEMONSTRAÇÃO - Suponhamos que R é um G-GCD domínio. É suficiente demonstrar que R é localmente integralmente fechado. Seja $M \in Max(R)$ e sejam $(a)_M$ e $(b)_M$ ideais principais de R_M. Então $(a)_M \cap (b)_M = ((a) \cap (b))_M$ é um ideal principal de R_M; logo R_M é um GCD-domínio e portanto integralmente fechado.

C.Q.D.

Seja R um domínio de integridade. Denotaremos por F o corpo de frações de R, isto é, F = T(R). Dados os ideais fracionários não nulos K, L de R, escreveremos $K \equiv L$ $(\mathfrak{R})$ se e só se $[R:K]_F = [R:L]_F$. Observa-se que $K \equiv L$ $(\mathfrak{R})$ se e só se $K_v = L_v$. Se $f \in F[X]$, então c(f) denotará o ideal fracionário de R gerado pelos coeficientes de f.

PROPOSIÇÃO 3 (LEMA DE DEDEKIND-MERTENS) - Se $f, g \in F[X] \setminus \{0\}$, então existe um inteiro positivo n tal que $(c(f))^{n+1}c(g) = (c(f))^n c(fg)$.

DEMONSTRAÇÃO - Podemos escrever f = p/a e g = q/b, onde $p, q \in R[X]$, $a, b \in R\setminus\{0\}$. Então c(f) = C(p)/a e c(g) = C(q)/b. Pela proposição 3 do capítulo II, $(C(p))^{n+1}C(q) = (C(p))^n C(pq)$, onde n = gr(q). Logo

$$\begin{aligned}(c(f))^{n+1}c(g) &= (C(p)/a)^{n+1}C(q)/b \\ &= ((C(p))^{n+1}/a^{n+1})C(q)/b \\ &= (C(p))^{n+1}C(q)/(a^{n+1}b) \\ &= (C(p))^n C(pq)/(a^{n+1}b) \\ &= (C(p)/a)^n C(pq)/(ab) \\ &= (c(f))^n c(fg).\end{aligned}$$

C.Q.D.

PROPOSIÇÃO 4 - Se R é um domínio integralmente fechado e f,

$g \in F[X]$, então $c(f)c(g) \equiv c(fg)$ (R), isto é, $(c(f)c(g))_v = (c(fg))_v$.

DEMONSTRAÇÃO - É claro que o resultado é verdadeiro se $f = 0$ ou $g = 0$. Suponhamos que $f \neq 0$ e $g \neq 0$. Pelo lema de Dedekind-Mertens, existe um inteiro positivo n tal que $(c(f))^{n+1}c(g) = (c(f))^n c(fg)$. Então, escrevendo $h = fg$, temos $c(f)c(g) \subseteq [(c(f))^{n+1}c(g):(c(f))^n]_F = [(c(f))^n c(h):(c(f))^n]_F$. Portanto $[c(f)c(g):c(h)]_F \subseteq [(c(f))^n c(h):((c(f))^n c(h))]_F = R$, pois R é integralmente fechado. Mas $c(h) \subseteq c(f)c(g)$; logo $R = [c(h):c(h)]_F \subseteq [c(f)c(g):c(h)]_F$. Consequentemente $[c(f)c(g):c(h)]_F = R$ e portanto $[c(f)c(g):(c(h)c(f)c(g))]_F = [R:(c(f)c(g))]_F$. Finalmente resulta $[R:c(fg)]_F = [R:(c(f)c(g))]_F$, isto é, $c(f)c(g) \equiv c(fg)(R)$.

C.Q.D.

PROPOSIÇÃO 5 - Se R é um domínio integralmente fechado e $f \in R[X]\setminus\{0\}$, então $fF[X] \cap R[X] = f[R:C(f)]_F R[X]$.

DEMONSTRAÇÃO - Se $h \in fF[X] \cap R[X]$, então existe $g \in F[X]$ tal que $h = fg \in R[X]$; logo $c(h) = C(h) \subseteq R$. Portanto $(c(h))_v \subseteq R$. Segue-se que $c(f)c(g) \subseteq (c(f)c(g))_v \subseteq R$, pela proposição 4. Então $c(g) \subseteq [R:C(f)]_F$, isto é, $g \in [R:C(f)]_F R[X]$ e portanto $h \in f[R:C(f)]_F R[X]$. Reciprocamente, se $h \in f[R:C(f)]_F R[X]$, então existe $g \in F[X]$ tal que $h = fg$ e $g \in [R:C(f)]_F R[X]$; logo $c(f)c(g) \subseteq R$. Como $c(h) = c(fg) \subseteq c(f)c(g)$, então $h = fg \in R[X]$. Consequentemente $fF[X] \cap R[X] = f[R:C(f)]_F R[X]$.

C.Q.D.

PROPOSIÇÃO 6 - Seja R um domínio de integridade. Se J é um v-ideal de $R[X]$ e $I = J \cap F \neq 0$, então

$I = \cap\{a[R:C(g)]_F;\ J \subseteq R[X](a/g),\ a \in R\setminus\{0\},\ g \in R[X]\setminus\{0\}\}$
e portanto é um v-ideal de R.

DEMONSTRAÇÃO - Observamos que se $f, h \in R[X]\setminus\{0\}$ são tais que $(f/h)R[X] \cap F \neq 0$, então existem $a \in R\setminus\{0\}$, $g \in R[X]\setminus\{0\}$ tais que $(f/h)R[X] = (a/g)R[X]$. De fato, se $a/b \in (f/h)R[X] \cap F$, onde $a, b \in R\setminus\{0\}$, então $a/b = (f/h)k$ para algum $k \in R[X]\setminus\{0\}$, donde $f/h = a/(bk)$, isto é, $(f/h)R[X] = (a/g)R[X]$, onde $g = bk$. Logo

$$J = \cap\{(f/h)R[X];\ J \subseteq (f/h)R[X],\ f, h \in R[X]\setminus\{0\}\}$$
$$= \cap\{(a/g)R[X];\ J \subseteq (a/g)R[X],\ a \in R\setminus\{0\},\ g \in R[X]\setminus\{0\}\}.$$

Seja

$$K = \cap\{a[R:C(g)]_F;\ J \subseteq (a/g)R[X],\ a \in R\setminus\{0\},\ g \in R[X]\setminus\{0\}\}.$$

Se $x \in I$, então para quaisquer $a \in R\setminus\{0\}$, $g \in R[X]\setminus\{0\}$ tais que $J \subseteq (a/g)R[X]$, tem-se $xg \in aR[X]$ e portanto $xC(g) \subseteq Ra$, isto é, $x \in [Ra:C(g)]_F = a[R:C(g)]_F$. Logo $x \in K$. Consequentemente $I \subseteq K$. Reciprocamente, se $x \in K$, então $x \in a[R:C(g)]_F = [Ra:C(g)]_F$ para quaisquer $a \in R\setminus\{0\}$, $g \in R[X]\setminus\{0\}$, com $J \subseteq (a/g)R[X]$. Logo $xC(g) \subseteq Ra$ e portanto $C(g) \subseteq R(a/x)$, isto é, $g \in R[X](a/x)$. Segue-se que $x \in R[X](a/g)$ e portanto

$$x \in \cap\{(a/g)R[X];\ J \subseteq (a/g)R[X],\ a \in R\setminus\{0\},\ g \in R[X]\setminus\{0\}\} = J.$$

Mas $x \in F$; logo $x \in J \cap F = I$ e consequentemente $K = I$.

C.Q.D.

PROPOSIÇÃO 7 - Seja R um domínio integralmente fechado e seja J um v-ideal inteiro de R[X].

(a) Se $J \cap F = I \neq 0$, então $IR[X] = J$.

(b) Se $J \cap F = 0$, então existe $f \in R[X]\setminus\{0\}$ e existe um v-ideal inteiro K de R tal que $J = fKR[X]$.

DEMONSTRAÇÃO - (a) Segundo a proposição anterior, temos $I =$
$= J \cap F = \cap\{a[R:C(g)]_F;\ J \subseteq R[X](a/g),\ a \in R\setminus\{0\},\ g \in R[X]\setminus\{0\}\}$.

Se $f \in J$, então $fg \in R[X]a$ para quaisquer $a \in R\setminus\{0\}$ e $g \in R[X]\setminus\{0\}$, com $J \subseteq R[X](a/g)$. Logo $C(fg) \subseteq Ra$. Como R é integralmente fechado, então $C(f)C(g) \subseteq (C(fg))_v \subseteq Ra$, pela proposição 4. Logo $C(f) \subseteq [Ra:C(g)]_F$ e portanto

$C(f) \subseteq \bigcap \{a[R:C(g)]_F;\ J \subseteq R[X](a/g),\ a \in R\setminus\{0\},\ g \in R[X]\setminus\{0\}\} =$
$= I$. Então $f \in IR[X]$ e assim $J \subseteq IR[X]$. Mas $IR[X] \subseteq J$; logo $J =$
$= IR[X]$.

(b) Suponhamos que $J \cap F = 0$ Como $JF[X] = fF[X]$ para algum $f \in R[X]$, então $J \subseteq fF[X] \cap R[X] = f[R:C(f)]_F R[X]$, pela proposição 5. Seja $L = ((1/f)C(f)J)_v$. Como $(1/f)C(f)J \subseteq R[X]$, então L é um v-ideal inteiro de R[X]. Além disto, $(1/f)C(f)JF[X] = LF[X]$; logo $L \cap F \neq 0$. Então existe um v-ideal inteiro I de R tal que $L = IR[X]$, pela parte (a). Portanto $IR[X] \equiv (1/f)C(f)J\ (R)$ e mais ainda $fIR[X] \equiv C(f)J\ (R)$. Por outro lado, C(f) é inversível módulo (R). Então, de $fIR[X] \equiv C(f)J\ (R)$, resulta $f(C(f))^{-1}IR[X] \equiv$
$\equiv J\ (R)$ e se $K = ((C(f))^{-1}I)_v$, então $J = fKR[X]$.

C.Q.D.

PROPOSIÇÃO 8 - Se R é um G-GCD domínio, então R[X] é um G-GCD domínio.

DEMONSTRAÇÃO - Suponhamos que R é um G-GCD domínio. Seja J um v-ideal inteiro de tipo finito de R[X]. Como R é integralmente fechado, então $J = fKR[X]$ para algum $f \in R[X]$ e algum v-ideal inteiro K de R, pela proposição 7. Como J é de tipo finito, então K também é de tipo finito. Logo $K \in Inv(R)$ e portanto $J \in Inv(R[X])$. Consequentemente R[X] é um G-GCD domínio.

C.Q.D.

PROPOSIÇÃO 9 - Toda localização de um G-GCD domínio é um G-GCD

domínio.

DEMONSTRAÇÃO - Suponhamos que R é um G-GCD domínio. Seja M um subconjunto multiplicativamente fechado de R. Se $p, q \in R_M$, então $(p) = IR_M$ e $(q) = JR_M$ para alguns ideais principais I e J de R. Como $I \cap J \in Inv(R)$, então $(p) \cap (q) = IR_M \cap JR_M = (I \cap J)R_M$ pertence a $Inv(R_M)$. Consequentemente R_M é um G-GCD domínio.

C.Q.D.

TEOREMA 1 - Seja R um domínio de integridade. São equivalentes:

(a) R⟨X⟩ é um G-GCD domínio.

(b) R(X) é um G-GCD domínio.

(c) R(X) é um GCD-domínio.

(d) R é um G-GCD domínio.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que R⟨X⟩ é um G-GCD domínio. Então sua localização R(X) é um G-GCD domínio.

(b) $\Rightarrow$ (c). Suponhamos que R(X) é um G-GCD domínio. Sejam p, q elementos arbitrários de $R(X)\setminus\{0\}$. Então $(p) \cap (q) \in Inv(R(X))$. Logo $(p) \cap (q)$ é localmente principal finitamente gerado e portanto é principal, pelo teorema 3 do capítulo II. Consequentemente R(X) é um LCM-domínio e portanto um GCD-domínio.

(c) $\Rightarrow$ (d). Suponhamos que R(X) é um GCD-domínio. Sejam I, J elementos arbitrários de Inv(R). Então $IR(X), JR(X) \in Inv(R(X))$. Logo $IR(X) \cap JR(X)$ é principal e portanto é um ideal inversível do domínio de integridade R(X). Mas $IR(X) \cap JR(X) = (I \cap J)R(X)$ e $I \cap J$ é regular. Então $I \cap J \in Inv(R)$, pela proposição 13 do capítulo II. Em consequência R é um G-GCD domínio.

(d) $\Rightarrow$ (a). Suponhamos que R é um G-GCD domínio. Então R[X] é um G-GCD domínio e portanto R(X) é um G-GCD domínio, pois R(X) é uma localização de R[X].

C.Q.D.

PROPOSIÇÃO 10 - Seja R um GCD-domínio com corpo de frações F.
(a) Se $f \in R[X] \setminus R$ é irredutível em R[X], então f é primo em F[X] e em R[X].
(b) Cada polinômio primitivo não constante em R[X] é um produto finito de polinômios primos em R[X].

DEMONSTRAÇÃO - (a) Seja f = gh uma fatoração de f em F[X]. Escrevemos $g = ag_1$, $h = bh_1$, onde $a, b \in F$ e g_1, h_1 são polinômios primitivos em R[X]. Então $f = abg_1h_1$ e como f é irredutível em R[X], com R um GCD-domínio, resulta que f é primitivo em R[X]. Logo $f = ug_1h_1$ para alguma unidade u de R. Portanto g_1 ou h_1 é uma unidade de R[X]. Então g ou h é uma unidade de F[X]. Consequentemente f é irredutível em F[X], isto é, f é primo em F[X].

Por outro lado, $fF[X] \cap R[X] = f[R:C(f)]_F R[X]$ pela proposição 5. Mas $[R:C(f)]_F = [R:R]_F = R$; logo $fF[X] \cap R[X] = fR[X]$. Como fF[X] é um ideal primo de F[X], então fR[X] é um ideal primo de R[X], isto é, f é primo em R[X].

(b) Seja $f \in R[X] \setminus R$ primitivo. Podemos escrever f como um produto finito $f_1 f_2 \cdots f_n$ de elementos irredutíveis de R[X] de grau positivo. Como $R = (C(f))_v = (C(f_1 f_2 \cdots f_n))_v =$
$= (C(f_1)C(f_2) \cdots C(f_n))_v \subseteq (C(f_i))_v$ para cada $i \in \{1,2,\ldots,n\}$, então cada f_i é primitivo em R[X]. Logo cada f_i é primo em R[X], pela parte (a).

C.Q.D.

PROPOSIÇÃO 11 - Se R é um GCD-domínio, então R[X] é um GCD-domínio.

DEMONSTRAÇÃO - Sejam $f, g \in R[X]\setminus\{0\}$ não-unidades. Escrevemos $f = af_1$, $g = bg_1$, onde $a, b \in R$ e f_1, g_1 são polinômios primitivos em R[X]. Pela proposição anterior, f_1 e g_1 têm um (necessariamente primitivo) máximo comúm divisor h em R[X] e h é um máximo comúm divisor de f_1 e g_1 em F[X], onde F = T(R). Mais ainda a e b têm um máximo comúm divisor c em R. É claro que ch é um divisor comúm de f e g em R[X]. Provaremos que ch é o máximo comúm divisor de f e g em R[X]. Se k é um divisor comúm de f e g em R[X], então escrevemos $k = rk_1$, onde $r \in R$ e $k_1 \in R[X]$ é primitivo. Existe $p \in R[X]$ tal que $f = pk$. Escrevemos $p = sp_1$, onde s é um elemento de R e $p_1 \in R[X]$ é primitivo. Então $f = af_1 = pk = (sp_1)(rk_1) = rsp_1k_1$, onde p_1k_1 é um polinômio primitivo de R[X]. Então, pela unicidade de representação, r divide a em R e k_1 divide f_1 em R[X]. Similarmente, r divide b em R e k_1 divide g_1 em R[X]. Logo r divide c = MCD(a, b) e k_1 divide h em R[X] e portanto $k = rk_1$ divide ch em R[X]. Em consequência ch = MCD(f, g).

C.Q.D.

PROPOSIÇÃO 12 - Toda localização de um GCD-domínio é um GCD-domínio.

DEMONSTRAÇÃO - Suponhamos que R é um GCD-domínio. Seja M um subconjunto multiplicativamente fechado de R. Sejam $p, q \in R_M$ quaisquer. Então $(p) = IR_M$ e $(q) = JR_M$, para alguns ideais principais I e J de R. Como $I \cap J$ é um ideal principal de R, então $(p) \cap (q) = IR_M \cap JR_M = (I \cap J)R_M$ é um ideal principal de R_M. Em consequência R_M é um LCM-domínio e portanto um GCD-domínio.

C.Q.D.

TEOREMA 2 - Seja R um domínio de integridade. São equivalentes:
(a) $R\langle X\rangle$ é um GCD-domínio.
(b) R é um GCD-domínio.

DEMONSTRAÇÃO - (a) $\Longrightarrow$ (b). Suponhamos que $R\langle X\rangle$ é um GCD-domínio. Sejam $a, b \in R$ quaisquer. Então $((a) \cap (b))R\langle X\rangle =$
$= ((a)R\langle X\rangle \cap ((b)R\langle X\rangle)$ é principal. Logo $(a) \cap (b)$ é um ideal principal de R, pela proposição 15 do capítulo II. Em consequência R é um LCM-domínio e portanto um GCD-domínio.

(b) $\Longrightarrow$ (a). Suponhamos que R é um GCD-domínio. Então $R[X]$ é um GCD-domínio; logo $R\langle X\rangle = R[X]_U$ é um GCD-domínio.

C.Q.D.

PROPOSIÇÃO 13 - Toda localização de um domínio fatorial é um domínio fatorial.

DEMONSTRAÇÃO - Suponhamos que R é um domínio fatorial. Seja M um subconjunto multiplicativamente fechado de R. Se $t \in R_M$ é não nulo e não unidade, então $t = a/m$, onde $a \in R\setminus\{0\}$ não é unidade de R e $m \in M$. Logo $a = p_1 p_2 \cdots p_n$ para alguns elementos primos $p_1, p_2, \ldots, p_n$ de R. Portanto $a/m = (1/m)(p_1/1)\cdots(p_n/1)$, onde $1/m$ é uma unidade de R_M. Se $(p_i) \cap M \neq \emptyset$, então $(p_i/1)R_M =$
$= (p_i)_M = R_M$, isto é, $p_i/1$ é uma unidade de R_M. Se $(p_i) \cap M = \emptyset$, então $(p_i/1)R_M = (p_i)_M$ é um ideal primo de R_M, isto é, $p_i/1$ é um elemento primo de R_M. Consequentemente $t = (1/m)(p_1/1)\cdots(p_n/1)$ é um produto finito de unidades de R_M e elementos primos de R_M. Agora demonstraremos que a representação de t como um produto finito de elementos primos é única, a menos de fator inversível. Suponhamos que $q_1 q_2 \cdots q_n = t = t_1 t_2 \cdots t_r$, onde q_i e t_j são primos em R_M, $1 \leq i \leq n$, $1 \leq j \leq r$. Sejam $q_i = p_i/m_i$ e $t_j = x_j/k_j$,

onde p_i, $x_j \in R$ e m_i, $k_j \in M$, $1 \leq i \leq n$, $1 \leq j \leq r$. Como q_iR_M é um ideal primo de R_M e $q_iR_M = (p_i/m_i)R_M = (p_i)_M$, então (p_i) é um ideal primo de R (a contração de q_iR_M) e $(p_i) \cap M = \emptyset$ para cada $i \in \{1, 2, \ldots, n\}$. Similarmente, (x_j) é um ideal primo de R e $(x_j) \cap M = \emptyset$ para cada $j \in \{1, 2, \ldots, r\}$. Logo podemos escrever $p_1p_2 \cdots p_n/m = t = x_1x_2 \cdots x_r/k$, onde $m = m_1m_2 \cdots m_n$ e $k = k_1k_2 \cdots k_r$. Observamos que $MCD(m, p_1p_2 \cdots p_n) = 1 = MCD(k, x_1x_2 \cdots x_r)$, pois $(p_i) \cap M = \emptyset = (x_j) \cap M$, $1 \leq i \leq n$, $1 \leq j \leq r$. Como $kp_1p_2 \cdots p_n = mx_1x_2 \cdots x_r$, então m/k e k/m, isto é, existe $u \in U(R)$ tal que $m = ku$. Logo $kp_1p_2 \cdots p_n = kux_1x_2 \cdots x_r$ e portanto $p_1p_2 \cdots p_n = ux_1x_2 \cdots x_r$, onde p_i e x_j são elementos primos de R, $1 \leq i \leq n$, $1 \leq j \leq r$. Então $n = r$ e, se necessário reenumerando, $p_i = x_i$, $1 \leq i \leq n$. Logo $q_iR_M = (p_i)_M = (x_i)_M = t_iR_M$, isto é, q_i e t_i são associados, $1 \leq i \leq n = r$. Portanto a representação $t = q_1q_2 \cdots q_n$ é única, a menos de fator inversível. Em conclusão R_M é um domínio fatorial.

C.Q.D.

TEOREMA 3 - Seja R um domínio de integridade. São equivalentes:

(a) $R\langle X\rangle$ é um domínio fatorial.

(b) R é um domínio fatorial.

DEMONSTRAÇÃO - (a) $\Longrightarrow$ (b). Suponhamos que $R\langle X\rangle$ é um domínio fatorial. Então $R\langle X\rangle$ é um GCD-domínio. Logo R é um GCD-domínio, pelo teorema 2. Seja $I_1 \subseteq I_2 \subseteq \ldots$ uma cadeia ascendente de ideais principais de R. Então $I_1R\langle X\rangle \subseteq I_2R\langle X\rangle \subseteq \ldots$ é uma cadeia ascendente de ideais principais de $R\langle X\rangle$. Logo existe m tal que $I_mR\langle X\rangle = I_nR\langle X\rangle$ para todo $n \geq m$, pois um domínio de integridade é um domínio fatorial se e só se é um GCD-domínio e satisfaz a condição de cadeia ascendente para ideais principais (proposição 16.4 de (7)). Portanto $I_n = I_nR\langle X\rangle \cap R = I_mR\langle X\rangle \cap R = I_m$ para todo $n \geq m$. Em consequência, R é um domínio fatorial.

(b) $\Rightarrow$ (a). Suponhamos que R é um domínio fatorial. Então R[X] é um domínio fatorial. Logo $R\langle X\rangle = R[X]_U$ é um domínio fatorial, pela proposição 13.

C.Q.D.

Agora relacionaremos as dimensões (de Krull) de R e R⟨X⟩ e usaremos esta relação para demonstrar que R⟨X⟩ é um domínio de ideais principais (respectivamente um domínio de Dedekind) se e só se R é um domínio de ideais principais (respectivamente um domínio de Dedekind).

PROPOSIÇÃO 14 - Se R é um anel de dimensão finita e Q é um ideal maximal de R[X] com altura maximal, então $M = Q \cap R$ é um ideal maximal de R.

DEMONSTRAÇÃO - Pelo corolário 30.19 de (7), existe uma cadeia de ideais primos de comprimento maximal terminando em M[X]. Suponhamos que M não é maximal em R. Então existe um ideal maximal P de R tal que $M \subset P$. Logo existe uma cadeia $M[X] \subset P[X] \subset K$ de R[X], onde K é um ideal maximal de R[X], pelo corolário 30.2 de (7). Portanto Q não tem altura maximal. Em consequência deve ser M um ideal maximal de R.

C.Q.D.

PROPOSIÇÃO 15 - Se R é um anel de dimensão finita, então $\dim R\langle X\rangle = \dim R[X] - 1$.

DEMONSTRAÇÃO - Se Q é um ideal maximal de R[X] com altura maximal, então $M = Q \cap R$ é um ideal maximal de R tal que $M[X] \subset Q$, pela proposição anterior. Logo existe $f \in Q \setminus M[X]$ e podemos su-

por que o coeficiente líder de f não está em M. Se $f = a_n X^n + \cdots + a_1 X + a_0$, então $M + a_n R = R$, pois M é maximal; Logo existem $r \in R$ e $m \in M$ tais que $m + a_n r = 1$. Portanto $mX^n + rf$ é um polinômio mônico em Q. Então $Q \cap U \neq \emptyset$ e $M[X] \cap U = \emptyset$. Logo não existem ideais primos próprios entre M[X] e Q, pelo teorema 37 de (8). Em consequência a dimensão de $R\langle X\rangle = R[X]_U$ diminui exatamente em 1, isto é, dim $R\langle X\rangle$ = dim R[X] - 1.

C.Q.D.

PROPOSIÇÃO 16 - Se R é um anel noetheriano, então dim $R\langle X\rangle$ = dim R.

DEMONSTRAÇÃO - Se R é um anel noetheriano, então dim R[X] = dim R + 1, pelo teorema 30.5 de (7). Logo dim $R\langle X\rangle$ = dim R[X] - 1 = dim R.

C.Q.D.

PROPOSIÇÃO 17 - Se R é um domínio fatorial e dim R = 1, então R é um domínio de ideais principais.

DEMONSTRAÇÃO - Seja P um ideal primo não nulo. Então existe $a \in P \setminus \{0\}$. Suponhamos que $a = p_1 p_2 \cdots p_n$, onde $p_1, p_2, \ldots, p_n$ são elementos primos de R. Então $p_1 p_2 \cdots p_n \in P$. Logo existe $i \in \{1,2,\ldots,n\}$ tal que $p_i \in P$ e portanto $(p_i) \subseteq P$. Como (p_i) é primo e dim R = 1, então (p_i) é maximal; Logo $P = (p_i)$ é principal. Portanto todo ideal primo de R é principal e em consequência R é um domínio de ideais principais, pelo corolário 37.9 de (7).

C.Q.D.

TEOREMA 4 - Seja R um domínio de integridade. São equivalentes:
(a) R⟨X⟩ é um domínio de ideais principais.
(b) R é um domínio de ideais principais.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que R⟨X⟩ é um domínio de ideais principais. Como R⟨X⟩ é noetheriano, então R é noetheriano, pelo teorema 5 do capítulo II. Se dim R⟨X⟩ = 0, então dim R = = dim R⟨X⟩ = 0, pela proposição 16. Logo R é um corpo e portanto um domínio de ideais principais. Se dim R⟨X⟩ = 1, então dim R = = 1. Além disto, R é um domínio fatorial, pois R⟨X⟩ é um domínio fatorial (teorema 3). Portanto R é um domínio de ideais principais, pela proposição 17.

(b) $\Rightarrow$ (a). Similar a (a) $\Rightarrow$ (b).

TEOREMA 5 - Seja R um domínio de integridade. São equivalentes:
(a) R⟨X⟩ é um domínio de Dedekind.
(b) R(X) é um domínio de Dedekind.
(c) R(X) é um domínio de ideais principais.
(d) R é um domínio de Dedekind.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que R⟨X⟩ é um domínio de Dedekind. Então R⟨X⟩ é um domínio de Prüfer noetheriano. Logo R(X) é um domínio de Prüfer noetheriano, pois R(X) é uma localização de R⟨X⟩. Portanto R(X) é um domínio de Dedekind, pelo teorema 37.1 de (7).

(b) $\Rightarrow$ (c). Suponhamos que R(X) é um domínio de Dedekind. Seja K um ideal não nulo de R(X). Então K é um ideal inversível de R(X). Logo K é um ideal principal de R(X), pelo teorema 3 do capítulo II. Em consequência R(X) é um domínio de ideais princi-

pais.

(c) $\Rightarrow$ (d). Suponhamos que R(X) é um domínio de ideais principais. Então R(X) é um domínio de Prüfer noetheriano. Logo R é um domínio de Prüfer noetheriano, pelo teorema 5 do capítulo II e o corolário do teorema 3 do capítulo III. Portanto R é um domínio de Dedekind.

(d) $\Rightarrow$ (a). Suponhamos que R é um domínio de Dedekind. Então R é um domínio noetheriano integralmente fechado com dim R = 1. Logo R⟨X⟩ é um domínio noetheriano com dim R⟨X⟩ = dim R = 1, pela proposição 16. Além disto, R⟨X⟩ é integralmente fechado, pelo teorema 8 do capítulo II. Portanto R⟨X⟩ é um domínio de Dedekind.

C.Q.D.

Seja R um domínio de integridade com corpo de frações F. Denotamos por $\mathcal{F}(R)$ o conjunto dos ideais fracionários não nulos de R. Se K, L $\in \mathcal{F}(R)$, então escrevemos $K \sim L$ se e só se $K_v = L_v$. A relação $\sim$ é uma relação de equivalencia. Denotamos por div(K) a classe de equivalencia de $K \in \mathcal{F}(R)$. Cada classe de equivalencia div(K) contem um único v-ideal: o v-ideal K_v. O conjunto $\mathcal{D}(R) = \{div(K);\ K \in \mathcal{F}(R)\}$ é um semigrupo abeliano aditivo com a adição definida por div(K) + div(L) = div(KL). Os elementos de $\mathcal{D}(R)$ são chamados os divisores de R. O zero de $\mathcal{D}(R)$ é div(R). Obtemos uma relação de ordem sobre $\mathcal{D}(R)$ compatível com a adição se, para div(K), div(L) $\in \mathcal{D}(R)$, definimos $div(K) \leq div(L)$ para significar $L_v \subseteq K_v$. O conjunto de elementos positivos de $\mathcal{D}(R)$ é o conjunto de classes que contém ideais inteiros de R.

Observação - $K \sim L$ se e só se $[R:K]_F = [R:L]_F$. Segue isto do seguinte fato: $K \subseteq Rx$ se e só se $1/x \in [R:K]_F$, para qualquer x em $F\setminus\{0\}$.

Denotemos por $\mathcal{V}(R)$ a família de todos os v-ideais de R.

Se $\pi: \mathcal{F}(R) \longrightarrow \mathcal{D}(R)$ é a aplicação canónica $K \longmapsto div(K)$, então π restrita a $\mathcal{V}(R)$ é uma bijeção sobre $\mathcal{D}(R)$. Definimos $K_v * L_v = (KL)_v$ para $K, L \in \mathcal{F}(R)$. Observamos que $\mathcal{V}(R)$ com a operação $*$ é um semigrupo abeliano isomorfo a $\mathcal{D}(R)$.

PROPOSIÇÃO 18 - (a) Se $div(K)$ é cancelativo em $\mathcal{D}(R)$, então $[K:K]_F = R$.
(b) Se K é um v-ideal de R e se $[K:K]_F = R$, então $div(K)$ tem um inverso em $\mathcal{D}(R)$.
(c) Se $div(K)$ é cancelativo em $\mathcal{D}(R)$, então $div(K)$ tem um inverso em $\mathcal{D}(R)$.

DEMONSTRAÇÃO - (a) É claro que $R \subseteq [K:K]_F$. Seja $x \in [K:K]_F$ qualquer. Então $K = K + K(x)$ e $div(K) = div(K) + div(R) = div(KR) = div((K + K(x))R) = div(K(R + Rx)) = div(K) + div(R + Rx)$. Como $div(K)$ é cancelativo em $\mathcal{D}(R)$, então $div(R + Rx) = div(R)$. Logo $(R + Rx)_v = R_v = R$ e portanto $x \in R$. Em consequência $R \subseteq [K:K]_F \subseteq R$, isto é, $[K:K]_F = R$.

(b) Como $K^{-1} = [R:K]_F$, então $K^{-1}K = [R:K]_F K \subseteq R$; logo $(KK^{-1})_v \subseteq R_v = R$. Seja Rx um ideal fracionário principal de R contendo KK^{-1}. Então $(1/x)KK^{-1} \subseteq R$. Logo $(1/x)K \subseteq (K^{-1})^{-1} = K_v = K$ e portanto $1/x \in [K:K]_F = R$. Então $R(1/x) \subseteq R$, isto é, $R \subseteq Rx$ e assim $R \subseteq (KK^{-1})_v \subseteq R$. Em consequência, $div(K) + div(K^{-1}) = div(KK^{-1}) = div((KK^{-1})_v) = div(R)$, isto é, $div(K^{-1})$ é o inverso de $div(K)$ em $\mathcal{D}(R)$.

(c) Se $div(K)$ é cancelativo, então a parte (a) demonstra que $[L:L]_F = R$ para cada ideal fracionário L de R tal que $L_v = K_v$. Em particular, $[K_v:K_v]_F = R$. Logo $div(K) = div(K_v)$ é um elemento inversível em $\mathcal{D}(R)$, pela parte (b).

C.Q.D.

DEFINIÇÃO - Seja R um subanel de um anel T. Dizemos que $t \in T$ é quase-inteiro sobre R se existe um R-submódulo finitamente gerado M de T tal que $t^n \in M$ para todo inteiro positivo n.

O conjunto $R_0 = \{t \in T;\ t$ é quase-inteiro sobre $R\}$ é chamado o fecho integral completo de R em T. Se $R_0 = R$, então dizemos que R é completamente integralmente fechado em T. Se $R_0 = T$, então dizemos que T é quase inteiro sobre R. Se $T = T(R)$, o anel total de frações de R, então R_0 é chamado o fecho integral completo de R. Dizemos que R é completamente integralmente fechado se R é completamente integralmente fechado em T(R).

OBSERVAÇÕES - (1) Uma interseção arbitrária de domínios completamente integralmente fechados é um domínio completamente integralmente fechado.
(2) Seja R um subanel de um anel T. É claro que todo elemento de T inteiro sobre R é quase-inteiro sobre R. Portanto todo anel completamente integralmente fechado é integralmente fechado.
(3) Como todo módulo finitamente gerado sobre um anel noetheriano é um módulo noetheriano, então todo anel noetheriano integralmente fechado é completamente integralmente fechado.

Caracterizaremos os domínios completamente integralmente fechados e daremos algumas de suas propriedades.

PROPOSIÇÃO 19 - Sejam R um domínio de integridade com corpo de frações F, $\mathfrak{F}(R)$ o conjunto dos ideais fracionários não nulos de R e $\mathfrak{D}(R)$ o semigrupo dos divisores de R. São equivalentes:
(a) R é completamente integralmente fechado.
(b) $\mathfrak{D}(R)$ é um grupo.
(c) $[K:K]_F = R$ para cada v-ideal K de R.
(d) $[K:K]_F = R$ para cada $K \in \mathfrak{F}(R)$;

DEMONSTRAÇÃO - (a) $\Rightarrow$ (d). Suponhamos que R é completamente integralmente fechado. Seja $K \in \mathcal{F}(R)$ qualquer. Então existem um ideal inteiro I de R e um $r \in R \setminus \{0\}$ tais que $K = I/(r)$. É claro que $R \subseteq [K:K]_F$. Seja $y \in [K:K]_F$ qualquer. Como $[K:K]_F = [I:I]_F$, então $yI \subseteq I$. Logo $y^2I \subseteq yI \subseteq I, \ldots$ e $y^nI \subseteq I \subseteq R$ para todo inteiro positivo n. Seja a um elemento de I não nulo. Portanto $y^na \in R$ para todo inteiro positivo n, isto é, $y^n \in R(1/a) \subseteq F$. Então y é quase-inteiro sobre R. Logo $y \in R$ e portanto $[K:K]_F \subseteq R$. Consequêntemente $[K:K]_F = R$.

(d) $\Rightarrow$ (a). Suponhamos que $[K:K]_F = R$ para cada $K \in \mathcal{F}(R)$. Seja $y \in F$ quase-inteiro sobre R. Então $K = R[y]$ é um anel que é um ideal fracionário de R, pois R[y] está contido num ideal fracionário de R. Logo $[K:K]_F = R$. Como K é um anel, então $KK \subseteq K$. Segue-se que $K \subseteq [K:K]_F = R$ e portanto $y \in R$. Em consequência R é completamente integralmente fechado.

(b) $\Rightarrow$ (c). Suponhamos que $\mathcal{D}(R)$ é um grupo. Seja K um v-ideal de R qualquer. Como div(K) é cancelativo em $\mathcal{D}(R)$, então $[K:K]_F = R$, pela parte (a) da proposição 18.

(c) $\Rightarrow$ (d). Suponhamos que $[K:K]_F = R$ para cada v-ideal K de R. Seja $K \in \mathcal{F}(R)$ qualquer. Como K_v é um v-ideal de R e $[K_v: K_v]_F = R$, então $div(K) = div(K_v)$ tem um inverso em $\mathcal{D}(R)$, pela parte (b) da proposição 18. Logo div(K) é cancelativo no semigrupo $\mathcal{D}(R)$ e portanto $[K:K]_F = R$.

(d) $\Rightarrow$ (b). Suponhamos que $[K:K]_F = R$ para cada $K \in \mathcal{F}(R)$. Seja $div(K) \in \mathcal{D}(R)$ qualquer. Como K_v é um v-ideal de R e $[K_v:K_v]_F = R$, então $div(K) = div(K_v)$ tem um inverso em $\mathcal{D}(R)$, pela parte (b) da proposição 18.

C.Q.D.

OBSERVAÇÃO - .Se R é completamente integralmente fechado, então

$\mathcal{V}(R)$, o conjunto dos v-ideais de R, com a operação $*$ definida anteriormente, é um grupo isomorfo a $\mathcal{D}(R)$.

PROPOSIÇÃO 20 - Seja R um domínio completamente integralmente fechado. Se $M \in Max(R)$ e $M^{-1} \neq R$, então M é inversível.

DEMONSTRAÇÃO - Seja $F = T(R)$. Como R é completamente integralmente fechado, então $[M:M]_F = R$. Pela hipótese $R \subset M^{-1}$. Logo $M^{-1} \quad R = [M:M]_F$ e portanto $MM^{-1} \nsubseteq M$. Então $M = MR \subset MM^{-1} = M[R:M]_F \subseteq R$. Consequêntemente $MM^{-1} = R$, isto é, M é inversível.

C.Q.D.

PROPOSIÇÃO 21 - Seja R um domínio noetheriano integralmente fechado (portanto completamente integralmente fechado). Se $d \in R\setminus\{0\}$ é não-unidade e P é um ideal primo de R que pertence a (d), então $h(P) = 1$. Se este ideal P é maximal, então P é inversível.

DEMONSTRAÇÃO - Suponhamos que P é um ideal primo pertencente a (d) e que $P \in Max(R)$. Então $(d) \subset (d):P$, pelo teorema 11 da página 214 de (14). Escolhamos $x \in ((d):P)\setminus(d)$. Então $x/d \in [R:P]_F = P^{-1}$, onde $F = T(R)$. Mas $x/d \notin R$. Então $P^{-1} \neq R$. Como R é completamente integralmente fechado, então P é inversível, pela proposição anterior.

Agora suponhamos que P é um ideal primo (não necessáriamente maximal) pertencente a (d). Como PR_P é um ideal maximal de R_P pertencente a dR_P e R_P é noetheriano integralmente fechado (portanto completamente integralmente fechado), então PR_P é inversível. Logo PR_P é um ideal primo minimal de R_P, pelo teorema 7.6 de (7) e o corolário 1 da página 216 de (14). Portanto $h(P) = \dim(R_P) = 1$.

C.Q.D.

DEFINIÇÃO - Seja R um domínio de integridade com corpo de frações R, isto é, F = T(R). Dizemos que R é um domínio de Krull se existe uma família $\mathcal{F} = (V_\lambda)_{\lambda \in \Lambda}$ de sobreanéis de valorização de R satisfazendo as seguintes condições:

(K1) $R = \cap\{V_\lambda ;\ \lambda \in \Lambda\}$.

(K2) Cada V_λ é discreto de pôsto um.

(K3) A família $\mathcal{F}$ tem carácter finito, isto é, se $x \in F\backslash\{0\}$, então x é não-unidade só em um número finito de elementos de $\mathcal{F}$.

(K4) Cada V_λ é essencial para R.

A família $\mathcal{F}$ é chamada uma família de definição para R.

OBSERVAÇÃO - Como um anel de valorização de pôsto um é completamente integralmente fechado, então um domínio de Krull é completamente integralmente fechado.

Demonstraremos que todo domínio noetheriano integralmente fechado é um domínio de Krull. Antes damos um resultado preliminar.

PROPOSIÇÃO 22 - Seja R um domínio noetheriano integralmente fechado. Se P é um ideal primo minimal de R, então R_P é um anel de valorização discreto de pôsto um. Se $d \in R\backslash\{0\}$ e $d \in R\backslash U(R)$, então as componentes na única representação minimal de (d) são potencias simbólicas de ideais primos minimais de R.

DEMONSTRAÇÃO - Seja P um ideal primo minimal de R. Então h(P) = = 1. Logo R_P é noetheriano integralmente fechado e $\dim(R_P) = 1$. Portanto R_P é um domínio de Dedekind local, isto é, um anel de valorização discreto de pôsto um.

Se $(d) = Q_1 \cap \cdots \cap Q_n$ é uma representação minimal de (d), onde cada Q_i é P_i-primário, então cada P_i é minimal em R,

pela proposição 21. Logo $dR_{P_i} = Q_i R_{P_i}$ para cada i. Como R_{P_i} é um anel de valorização discreto de pôsto um, então $Q_i R_{P_i} = P^{e_i} R_{P_i}$ para algum inteiro positivo e_i. Portanto $Q_i = (P^{e_i} R_{P_i}) \cap R = P^{(e_i)}$. Segue-se que $(d) = P_1^{(e_1)} \cap \ldots \cap P^{(e)}$ é a única representação minimal de (d), pois (d) não tem componentes imersas.

C.Q.D.

PROPOSIÇÃO 23 - Se R é um domínio noetheriano integralmente fechado e se $\mathcal{P}$ é o conjunto de todos os ideais primos minimais de R, então R é um domínio de Krull e $\mathcal{F} = \{R_P;\ P \in \mathcal{P}\}$ é uma família de definição para R.

DEMONSTRAÇÃO - Pela proposição anterior, cada elemento da família $\mathcal{F}$ é um sobreanel de valorização (essencial para R) discreto de pôsto um. Seja $d \in R \setminus U(R)$, $d \neq 0$. Pela proposição anterior, $(d) = Q_1 \cap \ldots \cap Q_n$, onde cada Q_i é uma potencia simbólica de um elemento $P_i \in \mathcal{P}$. Logo $dR_P = R_P$ para cada $R \in \mathcal{P} \setminus \{P_1, \ldots, P_n\}$. Portanto d é não-unidade só em um número finito de elementos de $\mathcal{F}$. Segue-se que $\mathcal{F}$ tem carácter finito.

É claro que $R \subseteq \cap \{R_P;\ P \in \mathcal{P}\}$. Suponhamos que $x \in F \setminus R$, onde $F = T(R)$. Seja $x = a/b$, onde $a, b \in R \setminus \{0\}$. Então $b \in R \setminus U(R)$ e $a \in R \setminus (b)$. Logo $(b) = \cap \{bR\ ;\ P \in \mathcal{P}\}$, pela proposição anterior. Portanto existe $P_1 \in \mathcal{P}$ tal que $a \notin bR_{P_1}$. Segue-se que $x = a/b$ não pertence a R_{P_1}. Em consequência $R = \cap \{R_P;\ P \in \mathcal{P}\}$.

Em conclusão R é um domínio de Krull e $\mathcal{F}$ é uma família de definição para R.

C.Q.D.

PROPOSIÇÃO 24 - Toda localização de um domínio de Krull é um domínio de Krull.

DEMONSTRAÇÃO - Seja R um domínio de Krull com corpo de frações F. Suponhamos que $\mathcal{F} = (V_\lambda)_{\lambda \in \Lambda}$ é uma família de definição para R. Seja M um subconjunto multiplicativamente fechado de R. Demonstraremos que R_M é um domínio de Krull e que $((V_\lambda)_M)_{\lambda \in \Lambda}$ é uma família de definição para R_M.

É claro que $R_M \subseteq \cap\{(V_\lambda)_M;\ \lambda \in \Lambda\}$. Seja $x \in \cap\{(V_\lambda)_M;\ \lambda \in \Lambda\}$ qualquer. Suponhamos que $\{\lambda_1, \ldots, \lambda_n\} = \{\lambda \in \Lambda;\ x$ é não-unidade de $V_\lambda\}$. Como $x \in (V_{\lambda_i})_M$ para cada $i \in \{1,2,\ldots,n\}$, então existe $m \in M$ tal que $mx \in V_{\lambda_i}$ para cada $i \in \{1,2,\ldots n\}$. Logo $mx \in \cap\{V_\lambda;\ \lambda \in \Lambda\} = R$ e portanto $x = mx/m \in R_M$. Em consequência $R_M = \cap\{(V_\lambda)_M;\ \lambda \in \Lambda\}$.

Seja $x \in F \setminus \{0\}$. Então x é unidade em V_λ para todo λ em $\Lambda \setminus \{\lambda_1, \ldots, \lambda_n\}$. Logo existe $\Lambda_1 \subseteq \{\lambda_1, \ldots, \lambda_n\}$ tal que x é unidade em $(V_\lambda)_M$ para todo $\lambda \in \Lambda \setminus \Lambda_1$. Portanto a família $((V_\lambda)_M)_{\lambda \in \Lambda}$ tem carácter finito.

Por outro lado, como V_λ é um anel de valorização, então $(V_\lambda)_M$ é um anel de valorização. Além disto, $(V_\lambda)_M = V_\lambda$ ou $(V_\lambda)_M = F$, pois V_λ é de pôsto um.

Em conclusão R_M é um domínio de Krull e $((V_\lambda)_M)_{\lambda \in \Lambda}$ é uma família de definição para R_M.

C.Q.D.

COROLÁRIO - Sejam R um domínio de Krull e $\mathcal{F}$ uma família de definição para R. Se M é um subconjunto multiplicativamente fechado de R, então $\mathcal{F}$ contém uma subfamília $\mathcal{F}'$ tal que $\mathcal{F}'$ é uma família de definição para R_M.

PROPOSIÇÃO 25 - Seja R um domínio de Krull. Se $\mathcal{F}$ é uma família de definição para R e se V é um sobreanel de valorização essencial não-trivial de R, então $V \in \mathcal{F}$ e portanto V é discreto de pôsto um e $V = R_P$ para algum ideal primo minimal P de R. Reciprocamente, R_P é um anel de valorização para cada ideal primo mini-

mal P de R.

DEMONSTRAÇÃO - Seja $V = R_M$, onde M é um subconjunto multiplicativamente fechado de R. Podemos supor que M é saturado. Demonstraremos que $M = R\setminus(K \cap R)$, onde K é o único ideal maximal de V. Se $m \in M$, então m é uma unidade em $R_M = V$. Logo $m \notin K$ e portanto $m \in R\setminus(K \cap R)$. Seja $P = K \cap R$. Segue-se que $M \subseteq R\setminus P$. Como M é saturado, então $M = R\setminus P$. Portanto $V = R_M = R_P$, onde $P = K \cap R$ é um ideal primo de R. O corolário acima implica que existe uma subfamília $\mathcal{F}'$ de $\mathcal{F}$ tal que $R_P = \cap\{W;\ W \in \mathcal{F}'\}$. Como R_P é um anel de valorização, então R_P tem no máximo um sobreanel de valorização de pôsto um, pelo teorema 22.8 de (7). Logo $\mathcal{F}'$ tem um único elemento W e portanto $V = R_P = W \in \mathcal{F}$. Como R_P tem pôsto um, então P é minimal em R.

Reciprocamente, se P é um ideal primo minimal de R, então existe uma subfamília $(V_\alpha)_{\alpha \in A}$ de $\mathcal{F}$ tal que $R_P = \cap\{V_\alpha;\ \alpha \in A\}$. Como P é minimal, então cada V_α deve ser centrado sobre PR_P em R_P. Logo $(V_\alpha)_{\alpha \in A}$ é finita. Se $(V_\alpha)_{\alpha \in A} = \{V_1, \ldots, V_n\}$, então $R_P = V_1 \cap \cdots \cap V_n$ tem n ideais maximais, pelo teorema 22.8 de (7). Portanto $n = 1$ e $R_P = V_1$ é um anel de valorização.

C.Q.D.

COROLÁRIO - Se R é um domínio de Krull e se $\mathcal{P}$ é o conjunto de todos os ideais primos minimais de R, então $\mathcal{F} = \{R_P;\ P \in \mathcal{P}\}$ é a única família de definição para R.

OBSERVAÇÃO - Em vista deste corolário podemos falar da família de definição de um domínio de Krull.

PROPOSIÇÃO 26 - Se R é um domínio de Krull, então R[X] é um do-

mínio de Krull.

DEMONSTRAÇÃO - Sejam F o corpo de frações de R e $\mathcal{F} = (V_\lambda)_{\lambda \in \Lambda}$ a família de definição de R. Para cada $\lambda \in \Lambda$, seja V_λ^* a extensão trivial de V_λ a F(X) e seja $(W_\sigma)_{\sigma \in \Sigma}$ a família de todos os sobreanéis de valorização não triviais de F[X]. Demonstraremos que R[X] é um domínio de Krull e que $\mathcal{F}' = (V_\lambda^*)_{\lambda \in \Lambda} \cup (W_\sigma)_{\sigma \in \Sigma}$ é a família de definição de R[X].

Como F[X] é um domínio de ideais principais, então F[X] é um domínio de Krull, pela proposição 23. Logo cada W_σ é discreto de pôsto um e essencial para F[X], pela proposição 25 e seu corolário. Por outro lado, F[X] é um anel de frações de R[X], F[X] = $= (R[X])_M$, onde $M = R\setminus\{0\}$, e portanto cada W_σ é também essencial para R[X], pelo teorema 2.6 de (7).

Para cada $\lambda \in \Lambda$, seja v_λ uma valorização associada com V_λ. Denotemos por v_λ^* a extensão trivial de v_λ a F(X). Como F[X] = $= \cap\{W_\sigma;\ \sigma \in \Sigma\}$, então $R[X] \subseteq (\cap\{V_\lambda^*;\ \lambda \in \Lambda\}) \cap F[X] =$ $= (\cap\{V_\lambda^*;\ \lambda \in \Lambda\}) \cap (\cap\{W_\sigma;\ \sigma \in \Sigma\})$. Se $f = f_0 + f_1X + \cdots + f_nX^n$ é um elemento de $(\cap\{V_\lambda^*;\ \lambda \in \Lambda\}) \cap F[X]$, então para cada coeficiente f_i não nulo e para cada $\lambda \in \Lambda$, temos: $v_\lambda(f_i) \geq v_\lambda^*(f) \geq 0$. Logo $f_i \in \cap\{V_\lambda;\ \lambda \in \Lambda\} = R$ e portanto $f \in R[X]$. Em consequência $R[X] = (\cap\{V_\lambda^*;\ \lambda \in \Lambda\}) \cap (\cap\{W_\sigma;\ \sigma \in \Sigma\})$.

Como v_λ e v_λ^* tem o mesmo grupo de valores, então V_λ e V_λ^* tem o mesmo pôsto e são simultaneamente discretos. Logo cada V_λ^* é discreto de pôsto um. Além disto, cada V_λ^* é essencial para R[X], pela proposição 18.7 de (7). Em consequência, cada elemento de $\mathcal{F}'$ é discreto de pôsto um e essencial para R[X].

Seja $f = f_0 + f_1X + \cdots + f_nX^n \in R[X]\setminus\{0\}$. Como F[X] é um domínio de Krull, então f é não-unidade só em um número finito de elementos da família $(W_\sigma)_{\sigma \in \Sigma}$. Se f_i é um coeficiente não nulo de f, então existe só um número finito de valorizações v_1, $v_2, \ldots, v_r$ na família $(v_\lambda)_{\lambda \in \Lambda}$ tais que $v_1(f_i) \neq 0$, $v_2(f_i) \neq 0$, $\ldots, v_n(f_i) \neq 0$. Segue-se da definição de v_λ^* que $v_\lambda^*(f) = 0$ pa-

ra todo $\lambda \in \Lambda\setminus\{1,2,\ldots,r\}$, isto é, $f \in U(V^*)$ para todo λ em $\Lambda\setminus\{1,2,\ldots,r\}$. Consequêntemente $\mathcal{F}'$ tem carácter finito.

Em resumo R[X] é um domínio de Krull e $\mathcal{F}'$ é a família de definição de R[X].

C.Q.D.

TEOREMA 6 - Seja R um domínio de integridade. São equivalentes:
(a) R(X) é um domínio de Krull.
(b) R(X) é um domínio de Krull.
(c) R é um domínio de Krull.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que R(X) é um domínio de Krull. Então R(X) é um domínio de Krull, pela proposição 24.

(b) $\Rightarrow$ (c). Suponhamos que R(X) é um domínio de Krull. Então $R(X) \cap T(R)$ é um domínio de Krull, pela proposição 1.2 de (6). Mas $R(X) \cap T(R) = R$, como demonstramos no capítulo II. Logo R é um domínio de Krull.

(c) $\Rightarrow$ (a). Suponhamos que R é um domínio de Krull. Então R[X] é um domínio de Krull, pela proposição 26. Logo $R\langle X\rangle = R[X]_U$ é um domínio de Krull.

C.Q.D.

DEFINIÇÃO - Seja R um domínio de integridade. Dizemos que R é um π-domínio se todo ideal principal não nulo de R é um produto finito de ideais primos de R.

São π-domínios, por exemplo, os domínios fatoriais e os domínios de Dedekind.

Demonstraremos que um domínio de integridade R é um π-domínio se e somente se R é um domínio de Krull e um G-GCD domínio.

Para isto damos algumas propriedades adicionais dos domínios de Krull e dos π-domínios.

Sejam R um domínio de Krull com corpo de frações F, $\mathcal{F}(R)$ a família de todos os ideais fracionários não nulos de R, $\mathcal{V}(R)$ a família de todos os v-ideais de R e $\mathcal{D}(R)$ o grupo dos divisores de R. Se $\mathcal{F} = (V_\lambda)_{\lambda \in \Lambda}$ é a família de definição de R, então para cada $V_\lambda \in \mathcal{F}$ existe uma valorização v_λ associada. Podemos assumir que o grupo de valores de v_λ é $\mathbb{Z}$ para cada $\lambda \in \Lambda$.

Se $K \in \mathcal{F}(R)$, então definimos $v_\lambda(K) = \max\{v_\lambda(x);\ x \in F\setminus\{0\}$ e $K \subseteq Rx\}$. Este máximo sempre existe, porque se $y \in K\setminus\{0\}$, então $v_\lambda(x) \leq v_\lambda(y)$ sempre que $K \subseteq Rx$.

OBSERVAÇÕES - (1) O conjunto $\{\lambda \in \Lambda;\ v_\lambda(K) \neq 0\}$ é finito. De fato, se $x \in F\setminus\{0\}$ e $K \subseteq Rx$, então $v_\lambda(x) \leq v_\lambda(K)$. Se $y \in K\setminus\{0\}$, então $v_\lambda(K) \leq v_\lambda(y)$. Como os conjuntos $\{\lambda \in \Lambda;\ v_\lambda(y) \neq 0\}$ e $\{\lambda \in \Lambda;\ v_\lambda(x) \neq 0\}$ são finitos, então segue-se a afirmação.
(2) É claro que $v_\lambda(R) = 0$ para todo $\lambda \in \Lambda$.

Para cada $\lambda \in \Lambda$, seja $Z_\lambda = \mathbb{Z}$, o grupo aditivo de números inteiros. Consideremos a soma direta de grupos $\mathbb{Z}^{(\Lambda)} = \oplus\{Z_\lambda;\ \lambda \in \Lambda\}$. Definimos uma aplicação $\theta: \mathcal{D}(R) \longrightarrow \mathbb{Z}^{(\Lambda)}$ por $\theta(\mathrm{div}(K)) = (v_\lambda(K))_{\lambda \in \Lambda}$. Observa-se que $\theta(\mathrm{div}(K)) = \theta(\mathrm{div}(K_v))$ pela definição de $v_\lambda(K)$. Segundo isto e a observação acima, segue-se que θ está bem definida.

AFIRMAÇÃO - Se $K, L \in \mathcal{V}(R)$, isto é, K e L são v-ideais de R, então $K \subseteq L$ se e somente se $v_\lambda(L) \leq v_\lambda(K)$ para todo $\lambda \in \Lambda$.

PROVA - É claro que se $K \subseteq L$, então $v_\lambda(L) \leq v_\lambda(K)$ para todo $\lambda \in \Lambda$. Reciprocamente, se $v_\lambda(L) \leq v_\lambda(K)$ para todo $\lambda \in \Lambda$, então para qualquer $x \in K$ temos $v_\lambda(K) \leq v_\lambda(x)$ para todo $\lambda \in \Lambda$. Seja $\lambda \in \Lambda$ qualquer. Se $z \in F\setminus\{0\}$ e $L \subseteq Rz$, então $v_\lambda(z) \leq v_\lambda(L)$. Logo $v_\lambda(z) \leq v_\lambda(x)$ e portanto $v_\lambda(x/z) \geq 0$, isto é, $x/z \in V_\lambda$. Como is-

to vale para todo $\lambda \in \Lambda$, então $x/z \in \cap\{V_\lambda;\ \lambda \in \Lambda\} = R$ e disto segue-se que $x \in Rz$. Consequentemente $x \in \cap\{Rz;\ L \subseteq Rz\} = L$ e $K \subseteq L$.

Uma consequência imediata deste resultado é que a aplicação θ: $(R) \longrightarrow Z^{(\Lambda)}$ é injetiva.

PROPOSIÇÃO 27 - Se R é um domínio de Krull, então toda família não vazía de v-ideais inteiros de R tem um elemento maximal.

DEMONSTRAÇÃO - Seja A uma família não vazía de v-ideais inteiros de R. Com a notação anterior, definimos a aplicação $\varphi: V(R) \quad Z^{(\Lambda)}$ por $\varphi = \theta \circ \pi$, onde $\pi: K \longrightarrow div(K)$ é a bijeção de V(R) sobre D(R). Seja $B = \varphi(A)$. Então $B \neq \emptyset$. Definimos uma ordem em $Z^{(\Lambda)}$ da seguinte maneira: se $m = (m_\lambda)_{\lambda \in \Lambda}$, $n = (n_\lambda)_{\lambda \in \Lambda} \in Z^{(\Lambda)}$, então escrevemos $m \leqslant n$ se e só se $m_\lambda \leqslant n_\lambda$ para todo $\lambda \in \Lambda$. Com esta ordem $Z^{(\Lambda)}$ é um reticulado-grupo ordenado. Observamos que φ é injetiva e inverte a ordem, onde a ordem de V(R) é a inclusão. Se $m = (m_\lambda)_{\lambda \in \Lambda} \in B$, então $m_\lambda \geqslant 0$ para todo $\lambda \in \Lambda$ e existe um subconjunto finito $\Lambda_1 \subseteq \Lambda$ tal que $m_\lambda > 0$ para todo $\lambda \in \Lambda_1$ e $m_\lambda = 0$ para todo $\lambda \in \Lambda \backslash \Lambda_1$. Se $n \in B$ e $n \leqslant m$, então $n_\lambda = 0$ para todo λ em $\Lambda \backslash \Lambda_1$ e $0 \leqslant n_\lambda \leqslant m_\lambda$ para todo $\lambda \in \Lambda$. Portanto o conjunto $C = \{n \in B;\ n \leqslant m\}$ é finito e existe $r \in C \cap B$ tal que r é um elemento minimal de B. Consequentemente A tem um elemento maximal.

C.Q.D.

PROPOSIÇÃO 28 - Sejam I e J ideais do anel R, onde J é próprio, finitamente gerado e regular. Suponhamos que $\{P_1, \ldots, P_m\}$ e $\{Q_1, \ldots, Q_n\}$ são duas famílias de ideais primos de R tais que $J = P_1^{s_1} \cdots P_m^{s_m} = Q_1^{t_1} \cdots Q_n^{t_n}$ para alguns $s_i, t_j \in Z^+$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$. Então cada elemento minimal da família

$\{P_1,\ldots,P_m, Q_1,\ldots, Q_n\}$ aparece simultaneamente como um P_i e um Q_j, e os expoentes s_i e t_j são iguais.

DEMONSTRAÇÃO - Podemos supor que P_1 é um elemento minimal da família $\{P_1,\ldots, P_m, Q_1,\ldots, Q_n\}$. Seja $T = R_{P_1}$. Então $JT = (IT)(P_1T)^{s_1} = (IT)(Q_jT)^{wt_j}$, onde $w = 0$ se $P_1 \notin \{Q_1,\ldots,Q_n\}$ e $w = 1$ se $P_1 \in \{Q_1,\ldots, Q_n\}$ e $P_1 = Q_j$. Suponhamos que $w = 0$. Neste caso temos: $JT = (IT)(P_1T)^{s_1} = (IT)T = IT$. Logo $JT = (JT)(P_1T)^{s_1}$, onde JT é próprio, finitamente gerado e regular e $(P_1T)^{s_1}$ é próprio em T. Mas isto é impossível pelo corolário 6.4 de (7). Portanto $w = 1$ e $JT = (IT)(P_1T)^{s_1} = (IT)(P_1T)^{t_j}$. Se fosse $s_1 < t_j$, então teríamos $JT = (JT)(P_1T)^{t_j - s_1}$, o que é impossível como já vimos. Também não pode ser $t_j < s_1$. Em consequência temos $s_1 = t_j$.

C.Q.D.

PROPOSIÇÃO 29 - Seja J um ideal próprio, finitamente gerado e regular do anel R. Se J é um produto finito de ideais primos de R, então a representação de J como um produto finito de ideais primos de R é única.

DEMONSTRAÇÃO - Sejam $J = P_1^{s_1} \cdots P_m^{s_m}$ e $J = Q_1^{t_1} \cdots Q_n^{t_n}$ duas representações de J como produto finito de ideais primos de R. Segue-se da proposição anterior que a família

$\mathcal{P} = \{P_i;\ 1 \leq i \leq m,\ P_i = Q_j$ para algum $j \in \{1,\ldots,n\}$ e $s_i = t_j\}$

é não vazia. Seja $\mathcal{P} = \{P_1,\ldots,P_r\}$, onde $r \leq m$ e $P_i = Q_i$, $1 \leq i \leq r$. Escrevendo $I = P_1^{s_1} \cdots P_r^{s_r}$, temos $J = IP_{r+1}^{s_{r+1}} \cdots P_m^{s_m} = IQ_{r+1}^{t_{r+1}} \cdots Q_n^{t_n}$. Se fosse $r < m$ ou $r < n$, então isto estaría em contradição com a proposição anterior. Consequentemente $r = m = n$.

C.Q.D.

COROLÁRIO - Se R é um π-domínio, então todo ideal principal não nulo e próprio tem uma representação única como produto finito de ideais primos.

PROPOSIÇÃO 30 - Seja R un anel. (a) Se I é um ideal inversível de R e Q é um ideal P-primário de R tal que $I \not\subseteq P$, então $I \cap Q = IQ$.

(b) Se $\{P_1,\ldots,P_n\}$ é uma família finita de ideais primos inversíveis de R e se $\{Q_1,\ldots,Q_n\}$ é uma família finita de ideais primários de R, com $\sqrt{Q_i} = P_i$, $1 \leq i \leq n$, então $Q_1 \cap \cdots \cap Q_n = Q_1 \cdots Q_n$.

DEMONSTRAÇÃO - (a) Como I é inversível, então existe um ideal J de R tal que $I \cap Q = IJ$. Logo $IJ \subseteq Q$, Q é P-primário e $I \not\subseteq P$. Portanto $J \subseteq Q$. Consequentemente $I \cap Q = IJ \subseteq IQ \subseteq I \cap Q$ e assim $I \cap Q = IQ$.

(b) Ordenemos a família $\{P_1,\ldots,P_n\}$ de modo que $P_i \not\subseteq P_j$ para $i < j$. Como P_1 é inversível, então Q_1 é uma potencia de P_1 (e portanto inversível), pelo teorema 7.6 de (7). Logo $Q_1 \cap Q_2 = Q_1Q_2$, pela parte (a). Suponhamos que $I_K = Q_1 \cap Q_2 \cap \cdots \cap Q_K = Q_1Q_2 \cdots Q_K$, onde $k < n$. Então I_K é inversível, pois cada Q_i é inversível. Como $P_i \not\subseteq P_{K+1}$ para cada $i \leq k$, então $I_K \not\subseteq P_{K+1}$. Logo $Q_1 \cap Q_2 \cap \cdots Q_K \cap Q_{K+1} = I_K \cap Q_{K+1} = I_KQ_{K+1} = Q_1Q_2 \cdots Q_KQ_{K+1}$. Segue-se por indução que $Q_1 \cap Q_2 \cap \cdots \cap Q_n = Q_1Q_2 \cdots Q_n$.

C.Q.D.

PROPOSIÇÃO 31 - Se R é um π-domínio, então R é um G-GCD domínio e um domínio de Krull.

DEMONSTRAÇÃO - Suponhamos que R é um π-domínio. Sejam a, b elementos quaisquer de $R\setminus\{0\}$. Então existem ideais primos $P_1, P_2, \ldots, P_m, Q_1, Q_2, \ldots, Q_n$ de R tais que $(a) = P_1P_2 \cdots P_m$ e $(b) = Q_1Q_2 \cdots Q_n$. Como os ideais (a) e (b) são inversíveis, então P_i e Q_j são inversíveis, $1 \leq i \leq m$, $1 \leq j \leq n$. Logo $P_1P_2 \cdots P_m = P_1 \cap P_2 \cap \cdots \cap P_m$ e $Q_1Q_2 \cdots Q_n = Q_1 \cap Q_2 \cap \cdots \cap Q_n$, pela proposição 30. Portanto $(a) \cap (b) = (\cap_{i=1}^{m} P_i) \cap (\cap_{j=1}^{n} Q_j)$. Mas $(\cap_{i=1}^{m} P_i) \cap (\cap_{j=1}^{n} Q_j) = P_1P_2 \cdots P_mQ_1Q_2 \cdots Q_n$, também pela proposição 30. Então $(a) \cap (b)$ é um ideal inversível de R. Consequentemente R é um G-GCD domínio.

Seja $\mathcal{P} = \{P;\ P$ é um ideal primo minimal de $R\}$. Demonstraremos que R é um domínio de Krull e que $\mathcal{F} = \{R_P;\ P \in \mathcal{P}\}$ é sua família de definição. Se $P \in \mathcal{P}$, então existe $a \in P\setminus\{0\}$. Logo $(a) = P_1P_2 \cdots P_m$, para alguns ideais primos (necessariamente inversíveis) $P_1, P_2, \ldots, P_m$ de R. Portanto $P = P_i$ para algum i em $\{1,2,\ldots,m\}$, pois $P_1P_2 \cdots P_m = (a) \subseteq P$ e P é um ideal primo minimal de R. Segue-se que todo $P \in \mathcal{P}$ é inversível. Então para cada $P \in \mathcal{P}$, R_P é um anel de valorização discreto de posto um, pelo teorema 7.6 e a proposição 19.2 de (7). Como cada elemento não nulo de R pertence só a um número finito de ideais primos minimais de R, então a família $\mathcal{F}$ tem carácter finito. Suponhamos que $x \in F\setminus R$, onde $F = T(R)$. Escrevemos $x = a/b$, onde $a, b \in R\setminus\{0\}$, $a \notin Rb$ e $b \notin U(R)$. Seja $Rb = P^{e_1}P^{e_2} \cdots P^{e_r}$ a representação de Rb como produto finito de ideais primos de R (única, pela proposição 29), onde $P_1, P_2, \ldots, P_r$ são distintos e necessariamente inversíveis. Provaremos que $P_i \in \mathcal{P}$ para todo $i \in \{1,2,\ldots,r\}$. Suponhamos que existe $i \in \{1,2,\ldots,r\}$ tal que $P_i \notin \mathcal{P}$. Como P_i é inversível, então $P_0 = \cap\{P_i^n;\ n \in \mathbb{Z}^+\}$ é um ideal primo de R, $P_0 \subset P_i$ e cada ideal primo de R propriamente contido em P_i, está contido em P_0. Logo $P_0 \neq 0$, pois estamos supondo que P_i não é minimal. Seja $c \in P_0\setminus\{0\}$. Então P_0 contem algum fator primo Q (necessariamente inversível) de Rc. Logo Q e P_i são ideais inversíveis de R tais que $Q \subset P_i \subset R$. Mas isto é impossível, pelo teorema 7.6 de (7). Portanto $P_1, P_2, \ldots, P_r \in \mathcal{P}$, isto é, $P_1, P_2, \ldots$

..., P_r são minimais (inversíveis). Como $P_i^{e_i}$ é P_i-primário, $1 \leq i \leq r$, pelo teorema 7.6 de (7), então $Rb = P_1^{e_1} P_2^{e_2} \ldots P^{e_r} = P_1^{e_1} \cap P_2^{e_2} \cap \ldots \cap P_r^{e_r}$ é uma representação minimal (única) de Rb, pela proposição 30. Mais ainda $P_i^{e_i} = bR_{P_i} \cap R$ para cada i. Logo $Rb = (\cap_{i=1}^{r} bR_{P_i}) \cap R$. Segue-se que $a \notin bR_{P_k}$ para algum k em $\{1,2,\ldots,r\}$, desde que $a \notin Rb$. Então $x = a/b \notin R_{P_k}$. Isto implica que $\cap\{R_P; P \in \mathcal{P}\} \subseteq R$. Em consequência $R = \cap\{R_P; P \in \mathcal{P}\} = \cap\{V; V \in \mathcal{F}\}$. Temos demonstrado assim que R é um domínio de Krull.

C.Q.D.

COROLÁRIO - Todo domínio fatorial e todo domínio de Dedekind é um domínio de Krull.

PROPOSIÇÃO 32 - Seja R um G-GCD domínio. São equivalentes:

(a) R é um π-domínio.

(b) R é um domínio de Krull.

(c) Toda família não vazía de v-ideais inteiros de R tem um elemento maximal.

(d) Todo ideal inteiro inversível de R é um produto de ideais inversíveis irredutíveis de R.

DEMONSTRAÇÃO - (a) $\Longrightarrow$ (b). Segue-se da proposição anterior.

(b) $\Longrightarrow$ (c). É a proposição 27.

(c) $\Longrightarrow$ (d). Suponhamos que toda família não vazía de v-ideais inteiros de R tem um elemento maximal. Consideremos a família $\mathcal{J} \subseteq Inv(R)$, onde $I \in \mathcal{J}$ se e só se I não é um produto finito de ideais inteiros inversíveis irredutíveis de R. Suponhamos que $\mathcal{J} \neq \emptyset$. Então $\mathcal{J}$ tem um elemento maximal J. Como J não é irredutí-

vel, então existem ideais inteiros K e L em R tais que $J \subset K$, $J \subset L$ e $J = K \cap L$. Logo, em particular, $K \in Inv(R)$, pois $K \notin \mathcal{J}$. Portanto existe um ideal inteiro H (necessariamente inversível) tal que $J = HK$. Como J é inversível e $K \cap L = J \subset L$, então $J \subset H$ e portanto $H \notin \mathcal{J}$. Logo existem ideais inteiros inversíveis irredutíveis $H_1, H_2, \ldots, H_r, K_1, K_2, \ldots, K_s$ tais que $H = H_1H_2 \cdots H_r$ e $K = K_1K_2 \cdots K_s$. Portanto $J = H_1H_2 \cdots H_rK_1K_2 \cdots K_s$, o que é absurdo, pois $J \in \mathcal{J}$. Consequentemente $\mathcal{J} = \emptyset$, isto é, todo ideal inteiro inversível de R é um produto finito de ideais inteiros inversíveis irredutíveis de R.

(d) $\Rightarrow$ (a). Suponhamos que todo ideal inteiro inversível de R é um produto finito de ideais inteiros inversíveis irredutíveis de R. Para demonstrar que R é um π-domínio é suficiente demonstrar que todo ideal inteiro inversível irredutível de R é primo. Seja P um ideal inteiro inversível irredutível de R. Suponhamos que $a, b \in R$, $ab \in P$ e $b \notin P$. Se $a = 0$, então $a \in P$. Se $a \neq 0$, então $(a) \in Inv(R)$. Como $b \in P:(a)$, então $P \subset P:(a)$. Mas $P:(a) \in Inv(R)$ pois R é um G-GCD domínio. Logo existe um ideal inteiro I de R tal que $P = I(P:(a))$. Como $I = P(P:(a))^{-1} \subseteq P$, então $P = I(P:(a)) \subseteq I \cap (P:(a)) \subseteq I \subseteq P$, isto é, $P = I \cap (P:(a))$. Logo $I = P$, pois P é irredutível. Portanto $P = I(P:(a)) = P(P:(a))$. Então $P:(a) = R$ e disto segue-se que $a \in P$. Consequentemente P é um ideal primo de R.

C.Q.D.

Como consequência das proposições 31 e 32, temos a seguinte caracterização de um π-domínio.

PROPOSIÇÃO 33 - Seja R um domínio de integridade. São equivalentes:

(a) R é um π-domínio.

(b) R é um domínio de Krull e um G-GCD domínio.

TEOREMA 7 - Seja R um domínio de integridade. São equivalentes:

(a) R(X) é um π-domínio.

(b) R(X) é um π-domínio.

(c) R(X) é um domínio fatorial.

(d) R é um π-domínio.

DEMONSTRAÇÃO - (a) $\Longrightarrow$ (b). Suponhamos que R(X) é um π-domínio. Então R(X) é um G-GCD domínio e um domínio de Krull, pela proposição 33. Logo R(X) é um G-GCD domínio e um domínio de Krull, pelos teoremas 1 e 6. Portanto R(X) é um π-domínio, pela proposição 33.

(b) $\Longrightarrow$ (c). Suponhamos que R(X) é um π-domínio. Então R(X) é um G-GCD domínio e um domínio de Krull. Seja $K_1 \subseteq K_2 \subseteq K_3 \subseteq \ldots$ uma cadeia de ideais (inteiros) principais de R(X). Podemos assumir que $K_n \neq 0$ para todo $n \in \mathbb{Z}^+$. A família $\mathcal{J} = (K_n)_{n \in \mathbb{Z}^+}$ tem um elemento maximal K_m, pela proposição 32. Se $n \geq m$, então $K_m \subseteq K_n$. Logo $K_n = K_m$ para todo $n \geq m$, pela maximalidade de K_m. Portanto R(X) satisfaz a condição de cadeia ascendente para ideais principais. Além disto, R(X) é um GCD-domínio, pelo teorema 1. Consequentemente R(X) é um domínio fatorial, pela proposição 16.4 de (7).

(c) $\Longrightarrow$ (d). Suponhamos que R(X) é um domínio fatorial. Então R(X) é um π-domínio. Logo R(X) é um G-GCD domínio e um domínio de Krull. Portanto R é um G-GCD domínio e um domínio de Krull, pelos teoremas 1 e 6. Consequentemente R é um π-domínio.

(d) $\Longrightarrow$ (a). É consequência dos teoremas 1 e 6.

C.Q.D.

O objetivo seguinte é demonstrar que se R é um domínio de Krull, então Pic(R(X)) é isomorfo a Pic(R) e Cl(R(X)) é isomorfo

a Cl(R).

Utilizaremos a seguinte notação. Se A é um domínio de Krull, então denotaremos por $X^{(1)}(A)$ o conjunto dos ideais primos minimais de A. Para $x \in T(A)\setminus\{0\}$, escreveremos div(x) em lugar de div(Ax). O conjunto dos ideais fracionários não nulos principais de A será denotado por Prin(A) e sua imagem em $\mathcal{D}(A)$, o grupo dos divisores de A, será denotada por $\mathcal{P}(A)$, isto é, $\mathcal{P}(A) = \{div(x);\ x \in T(A)\setminus\{0\}\}$. Os elementos de $\mathcal{P}(A)$ serão chamados divisores principais de A. Observa-se que $\mathcal{P}(A)$ é um subgrupo de $\mathcal{D}(A)$. O grupo dos ideais (fracionários) inversíveis de A será denotado por Cart(A) e será chamado de o grupo de Cartier de A. A imagem de Cart(A) em $\mathcal{D}(A)$ será denotada por $\mathcal{C}(A)$, isto é, $\mathcal{C}(A) = \{div(K);\ K \in Cart(A)\}$. Os elementos de $\mathcal{C}(A)$ serão chamados de divisores inversíveis de A.

OBSERVAÇÃO - $\mathcal{D}(A)$ é um reticulado, isto é, existe o ínfimo e o supremo de $\{div(K), div(L)\}$ para quaisquer $div(K), div(L) \in \mathcal{D}(A)$. De fato, $inf(div(K),div(L)) = div(K + L)$ e $sup(div(K),div(L)) = div(K \cap L)$.

DEFINIÇÃO - Seja A um domínio de Krull. O grupo $\mathcal{D}(A)/\mathcal{P}(A)$ é denotado por Cl(A) e é chamado o grupo de classes de divisores de A.

Se K é um ideal fracionário não nulo de A, então sua imagem em Cl(A) será denotada por [K], isto é, $[K] = div(K) + \mathcal{P}(A)$.

DEFINIÇÃO - Seja A um domínio de Krull. O grupo $\mathcal{C}(A)/\mathcal{P}(A)$ é denotado por Pic(A) e é chamado o grupo de Picard de A.

DEFINIÇÃO - Seja A um domínio de Krull. O grupo Cl(A)/Pic(A) é denotado por G(A) e é chamado o grupo de classes local de A.

Condideraremos a seguir alguns resultados sobre R-módulos,

onde R é um anel comutativo com identidade.

Se $f:L \longrightarrow M$ é um homomorfismo de R-módulos, então o submódulo $f^{-1}(0)$ é denotado por Ker(f) e é chamado o núcleo de f. O submódulo f(L) é denotado por Im(f) e é chamado a imagem de f. O módulo quociente M/Im(f) é denotado por Coker(f) e é chamado o conúcleo de f.

PROPOSIÇÃO 34 (LEMA DOS QUATRO) - Consideremos o seguinte diagrama de homomorfismos de R-módulos

$$\begin{array}{ccccccc} K & \xrightarrow{f} & L & \xrightarrow{g} & M & \xrightarrow{h} & P \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} \\ K' & \xrightarrow{f'} & L' & \xrightarrow{g'} & M' & \xrightarrow{h'} & P' \end{array}$$

onde as duas filas são exatas e os tres quadrados são comutativos. Se α é um epimorfismo e δ é um monomorfismo, então

(a) $$Im(\beta) = g'^{-1}(Im(\gamma))$$

(b) $$Ker(\gamma) = g(Ker(\beta)).$$

Portanto, se γ é um epimorfismo, então β também é um epimorfismo, e se β é um monomorfismo, então γ também é um monomorfismo.

DEMONSTRAÇÃO - (a) Seja $y' \in Im(\beta)$ qualquer. Então existe $y \in L$ tal que $\beta(y) = y'$. Pela comutatividade do quadrado central, temos $g'(y') = g'(\beta(y)) = \gamma(g(y)) \in Im(\gamma)$. Logo $y' \in g'^{-1}(Im(\gamma))$. Portanto $Im(\beta) \subseteq g'^{-1}(Im(\gamma))$.

Seja $y' \in g'^{-1}(Im(\gamma))$ qualquer. Então o elemento $z' = g'(y')$ pertence a $Im(\gamma)$. Logo existe $z \in M$ tal que $\gamma(z) = z'$. Pela exatidão da fila inferior temos $h'(z') = h'(g'(y')) = 0$. Pela comutatividade do quadrado da direita, temos $\delta(h(z)) = h'(\gamma(z)) = h'(z') = 0$. Como δ é um monomorfismo, então $h(z) = 0$. Portanto $z \in Ker(h) = Im(g)$. Então existe $y \in L$ tal que $g(y) = z$.

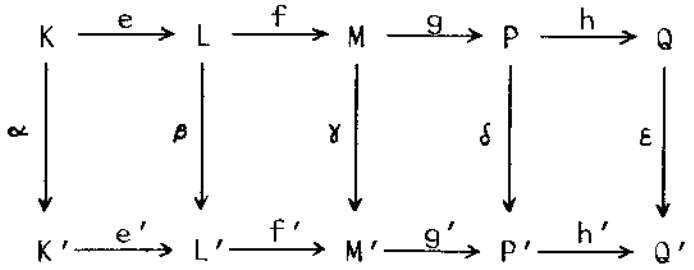
Consideremos o elemento $y' - \beta(y) \in L'$. Como $g'(y' - \beta(y)) = g'(y') - g'(\beta(y)) = z' - z' = 0$, então $y' - \beta(y) \in Ker(g') = Im(f')$. Segue-se que existe $x' \in K'$ tal que $f'(x') = y' - \beta(y)$. Por outro lado, como α é um epimorfismo, então existe $x \in K$ tal que $\alpha(x) = x'$. Agora consideremos o elemento $f(x) + y \in L$. Pela comutatividade do quadrado da esquerda, temos $\beta(f(x) + y) = \beta(f(x)) + \beta(y) = f'(\alpha(x)) + \beta(y) = f'(x') + \beta(y) = y' - \beta(y) + \beta(y) = y'$. Isto implica que $y' \in Im(\beta)$. Consequentemente $g'^{-1}(Im(\gamma)) \subseteq Im(\beta)$. Temos assim demonstrado (a).

(b) Seja $z \in Ker(\gamma)$ qualquer. Então $\gamma(z) = 0$. Pela comutatividade do quadrado da direita, temos $\delta(h(z)) = h'(\gamma(z)) = h'(0) = 0$. Como δ é um monomorfismo, então $h(z) = 0$. Logo $z \in Ker(h) = Im(g)$. Portanto existe $y \in L$ tal que $g(y) = z$. Consideremos o elemento $y' = \beta(y) \in L'$. Pela comutatividade do quadrado central, temos $g'(y') = g'(\beta(y)) = \gamma(g(y)) = \gamma(z) = 0$. Isto implica que $y' \in Ker(g') = Im(f')$. Então existe $x' \in K'$ tal que $f'(x') = y'$. Como α é um epimorfismo, então existe $x \in K$ tal que $\alpha(x) = x'$. Agora consideremos o elemento $y - f(x) \in L$. Pela comutatividade do quadrado da esquerda, temos $\beta(y - f(x)) = \beta(y) - \beta(f(x)) = \beta(y) - f'(\alpha(x)) = y' - y' = 0$. Segue-se que $y - f(x) \in Ker(\beta)$. Por outro lado, também temos $g(y - f(x)) = g(y) - g(f(x)) = z - 0 = z$. Isto implica que $z \in g(Ker(\beta))$. Consequentemente $Ker(\gamma) \subseteq g(Ker(\beta))$.

Seja $z \in g(Ker(\beta))$ qualquer. Então existe $y \in Ker(\beta)$ tal que $g(y) = z$. Pela comutatividade do quadrado central, temos $\gamma(z) = \gamma(g(y)) = g'(\beta(y)) = g'(0) = 0$. Isto implica que $z \in Ker(\gamma)$. Consequêntemente $g(Ker(\beta)) \subseteq Ker(\gamma)$.

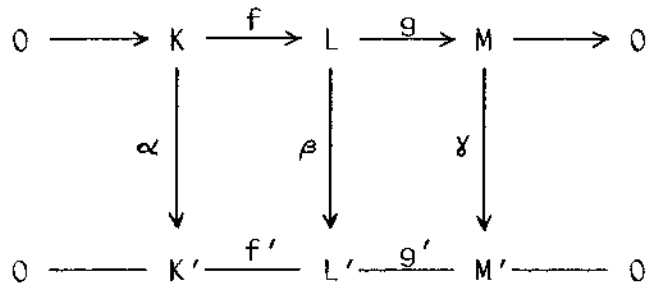
C.Q.D.

COROLÁRIO 1 (LEMA DOS CINCO) - Consideremos o seguinte diagrama de homomorfismos de R-módulos



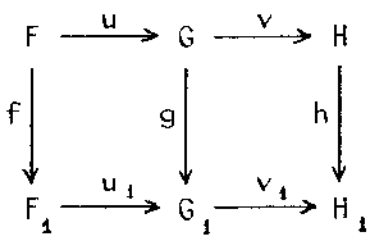
onde as filas são exatas e os quatro quadrados são comutativos. Se α, β, δ, ε são isomorfismos, então o homomorfismo central γ também é um isomorfismo.

COROLÁRIO 2 - Consideremos o seguinte diagrama de homomorfismos de R-módulos



onde as filas são exatas e os dois quadrados são comutativos.
(a) Se α e γ são monomorfismos, então β também é um monomorfismo.
(b) Se α e γ são epimorfismos, então β também é um epimorfismo.
Portanto se α e γ são isomorfismos, então o homomorfismo central β é um isomorfismo.

PROPOSIÇÃO 35 - Condideremos o diagrama comutativo de grupos abelianos e homomorfismos



onde as filas são exatas.

(a) Se h é injetivo, então $Im(g) \cap Im(u_1) = Im(u_1 \circ f) = Im(g \circ u)$.

(b) Se f é sobrejetivo, então $Ker(g) + Im(u) = Ker(v_1 \circ g) = Ker(h \circ v)$.

DEMONSTRAÇÃO - (a) É claro que $Im(u_1 \circ f) = Im(g \circ u) \subseteq Im(g) \cap Im(u_1)$. Seja $x \in Im(g) \cap Im(u_1)$ qualquer. Então existe $y \in G$ tal que $x = g(y)$. Como $v_1 \circ u_1 = 0$, então $0 = v_1(x) = v_1(g(y)) = h(v(y))$ e portanto $v(y) = 0$, pois h é injetivo. Pela exatidão da fila superior, existe $z \in F$ tal que $y = u(z)$ e assim $x = g(u(z))$, isto é, $x \in Im(g \circ u)$.

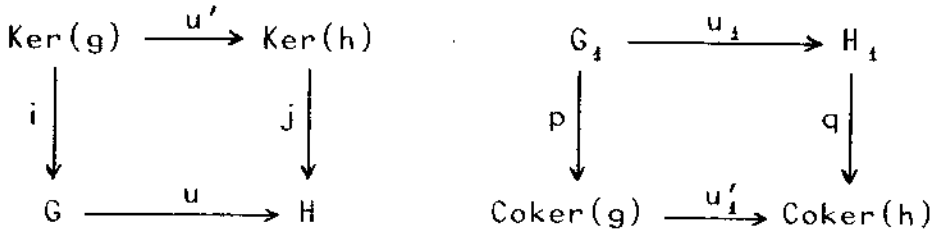
(b) Como $v \circ u = 0$ e $v_1 \circ u_1 = 0$, então é claro que $Ker(g) + Im(u) \subseteq Ker(v_1 \circ g) = Ker(h \circ v)$. Seja $x \in Ker(v_1 \circ g)$. Então $g(x) \in Ker(v_1)$ e portanto existe $y' \in F_1$ tal que $u_1(y') = g(x)$, pela exatidão da fila inferior. Por outro lado, como f é sobrejetivo, então existe $y \in F$ tal que $f(y) = y'$. Logo $g(x) = u_1(f(y)) = g(u(y))$. Portanto $x - u(y) \in Ker(g)$, isto é, $x \in Ker(g) + Im(u)$.

C.Q.D.

PROPOSIÇÃO 36 - Consideremos o seguinte diagrama comutativo de grupos abelianos e homomorfismos

$$\begin{array}{ccc} G & \xrightarrow{u} & H \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ G_1 & \xrightarrow{u_1} & H_1 \end{array}$$

Então existe um único homomorfismo $u' : Ker(g) \longrightarrow Ker(h)$ e um único homomorfismo $u' : Coker(g) \longrightarrow Coker(h)$ tais que os seguintes diagramas

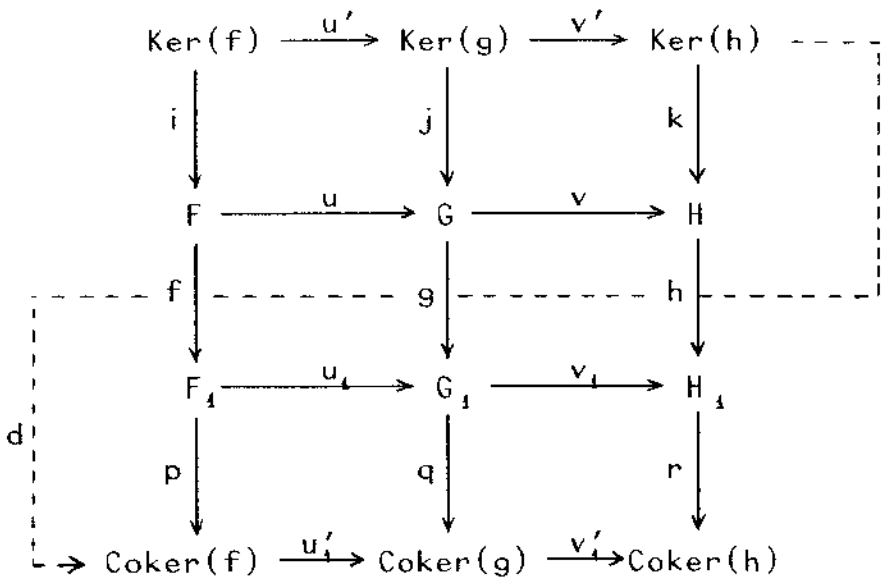


(onde i e j são os monomorfismos canónicos e p e q os epimorfismos canónicos) são comutativos.

DEMONSTRAÇÃO - Se $x \in Ker(g)$, então $g(x) = 0$ e portanto $h(u(x)) = u_1(g(x)) = 0$, isto é, $u(x) \in Ker(h)$. Consequentemente definindo $u'(x) = u(x)$ para cada $x \in Ker(g)$, temos que u' é o único homomorfismo de Ker(g) em Ker(h) tal que o diagrama acima comuta. Similarmente, como $u_1(g(G)) = h(u(G)) \subseteq h(H)$, então existe um único homomorfismo $u': Coker(g) \longrightarrow Coker(h)$ tal que o diagrama acima comuta.

C.Q.D.

PROPOSIÇÃO 37 (LEMA DA SERPENTE) - Consideremos o seguinte diagrama comutativo de grupos abelianos e homomorfismos



onde $Im(u) = Ker(v)$ e $Im(u_1) = Ker(v_1)$.

(a) $v' \circ u' = 0$; se u_1 é injetivo, então a fila superior é exata, isto é, $Im(u') = Ker(v')$.

(b) $v_1' \circ u_1' = 0$; se v é sobrejetivo, então a fila inferior é exata, isto é, $Im(u_1') = Ker(v_1')$.

(c) Se u_1 é injetivo e v é sobrejetivo, então existe um homomorfismo $d: Ker(h) \longrightarrow Coker(f)$ tal que a sequência

(*)
$$Ker(f) \xrightarrow{u'} Ker(g) \xrightarrow{v'} Ker(h) \xrightarrow{} \ldots$$
$$\ldots \xrightarrow{d} Coker(f) \xrightarrow{u'} Coker(g) \xrightarrow{v'} Coker(h)$$

é exata.

DEMONSTRAÇÃO - (a) Como $u'(x) = u(x)$, $v'(y) = v(y)$ para quaisquer $x \in Ker(f)$, $y \in Ker(g)$ e $v \circ u = 0$, então $v' \circ u' = 0$. Isto implica que $Im(u') \subseteq Ker(v')$. Observamos que $Ker(v') = Ker(g) \cap Ker(v) = Ker(g) \cap Im(u)$. Suponhamos que u_1 é injetivo. Seja $y \in Ker(v')$ qualquer. Então $y \in Ker(g)$ e $y \in Im(u)$. Logo existe $x \in F$ tal que $y = u(x) \in Ker(g)$. Portanto $u_1(f(x)) = g(u(x)) = 0$. Segue-se que $f(x) = 0$, pois u_1 é injetiva. Então $x \in Ker(f)$ e consequentemente $y = u(x) = u'(x) \in Im(u')$.

(b) Como $u_1'(x' + Im(f)) = u_1(x') + Im(g)$ e $v_1'(y' + Im(g)) = v_1(y') + Im(h)$ para quaisquer $x' \in F_1$, $y' \in G_1$ e $v_1 \circ u_1 = 0$, então $v_1' \circ u_1' = 0$. Portanto $Im(u_1') \subseteq Ker(v_1')$. Suponhamos que v é sobrejetivo. Se $y' + Im(g) \in Ker(v_1')$, então $v_1(y') \in Im(h)$. Logo existe $z \in H$ tal que $v_1(y') = h(z)$. Como v é sobrejetivo, então $z = v(y)$ para algum $y \in G$. Portanto $v_1(y') = h(z) = h(v(y)) = v_1(g(y))$. Segue-se disto que $y' - g(y) \in Ker(v_1) = Im(u_1)$. Então existe $x' \in F_1$ tal que $y' - g(y) = u_1(x')$. Mas isto implica que $y' - u_1(x') \in Im(g)$. Portanto $y' + Im(g) = u_1(x') + Im(g) = u_1'(x' + Im(f))$, isto é, $y' + Im(g) \in Im(u_1')$. Consequentemente $Ker(v_1') \subseteq Im(u_1')$.

(c) Seja $z \in Ker(h)$ qualquer. Então existe $y \in G$ tal que $v(y) = z = k(z)$, pois v é sobrejetivo. Mas $v_1(g(y)) = h(v(y)) =$

$= h(z) = 0$; logo $g(y) \in Ker(v_1) = Im(u_1)$. Portanto existe um único $x' \in F_1$ tal que $u_1(x') = g(y)$, pois u_1 é injetivo. Definimos $d: Ker(h) \longrightarrow Coker(f)$ por $d(z) = p(x')$. Vejamos que d está bem definida. Suponhamos que $y' \in G$ e que $v(y') = z$. Então $v(y') = z = v(y)$, isto é, $y' - y \in Ker(v) = Im(u)$. Segue-se disto que $y' = y + u(x)$ para algum $x \in F$. Como $v_1(g(y')) = h(v(y')) = h(z) = 0$, então existe $x'' \in F_1$ tal que $u_1(x'') = g(y')$. Logo $u_1(x') - u_1(x'') \in Im(g)$, donde $u_1'(x' - x'') = 0$, isto é, $x' - x''$ pertence a $Im(f)$. Portanto $x'' = x' + f(r)$ para algum $r \in F$. Consequentemente $p(x'') = p(x') + p(f(r)) = p(x')$. Agora demonstraremos que d é um homomorfismo. Sejam $z_1, z_2 \in Ker(h)$. Escrevemos $z = z_1 + z_2$. Escolhemos $y_1, y_2 \in G$ tais que $v(y_1) = z_1$ e $v(y_2) = z_2$. Escrevemos $y = y_1 + y_2$. Então $v(y) = v(y_1 + y_2) = z_1 + z_2 = z$. Logo $d(z) = p(x')$, $d(z_1) = p(x_1')$ e $d(z_2) = p(x_2')$, onde $u_1(x') = g(y)$, $u_1(x_1') = g(y_1)$ e $u_1(x_2') = g(y_2)$. Como $u_1(x_1' + x_2') = g(y_1 + y_2) = g(y) = u_1(x')$, então $x' = x_1' + x_2'$ e portanto $d(z_1 + z_2) = d(z) = p(x') = p(x_1' + x_2') = p(x_1') + p(x_2') = d(z_1) + d(z_2)$.

Finalmente demonstraremos que a sequência (*) é exata. Se $z = v'(y)$ para algum $y \in Ker(g)$, então $g(y) = 0$. Logo $d(z) = 0$, isto é, $z \in Ker(d)$. Por outro lado, se $d(z) = 0$, onde $z = v(y)$ para algum $y \in G$ e $u_1(x') = g(y)$ para algum $x' \in F_1$, então $p(x') = 0$, isto é, $x' \in Im(f)$. Portanto existe $x \in F$ tal que $x' = f(x)$. Segue-se que $g(y) = u_1(x') = u_1(f(x)) = g(u(x))$, isto é, $y - u(x) \in Ker(g)$. Então $y = u(x) + n$ para algum $n \in Ker(g)$. Logo $k(z) = v(y) = v(u(x) + n) = v(u(x)) + v(n) = v(j(n)) = k(v_1(n))$ e portanto $z = v_1(n) \in Im(v_1)$. Consequentemente $Im(v') = Ker(d)$.

Seja $z \in Ker(h)$ qualquer. Escolhemos $y \in G$ e $x' \in F_1$ tais que $z = v(y)$ e $u_1(x') = g(y)$. Então $d(z) = p(x')$ e $u_1'(d(z)) = u_1'(p(x')) = q(u_1(x')) = q(g(y)) = 0$. Logo $u_1' \circ d = 0$ e portanto $Im(d) \subseteq Ker(u_1')$. Se $u_1'(p(x')) = 0$, onde $x' \in F_1$, então $q(u_1(x')) = 0$. Logo $u_1(x') = g(y)$ para algum $y \in G$. Como $v_1(u_1(x')) = 0$, então $v_1(g(y)) = 0$ e portanto $h(v(y)) = 0$, isto é, $v(y) = z$ para

algum $z \in Ker(h)$. Segue-se da definição de d que $p(x') = d(z)$, isto é, $p(x') \in Im(d)$. Consequentemente $Ker(u_1') = Im(d)$. Pelas partes (a) e (b), a sequência (*) é exata também em Ker(g) e Coker(g). Em conclusão (*) é uma sequência exata.

C.Q.D.

PROPOSIÇÃO 38 - Sejam $f:K \longrightarrow L$ e $g:L \longrightarrow M$ homomorfismos de R-módulos. Se $g \circ f$ é um isomorfismo, então

$$L = Im(f) \oplus Ker(g).$$

DEMONSTRAÇÃO - Sejam $L_1 = Im(f)$ e $L_2 = Ker(g)$. Seja $y \in L$ qualquer. Escrevemos $z = g(y) \in M$. Como $g \circ f$ é um isomorfismo, então existe $x \in K$ tal que $g(f(x)) = z$. Sejam $s = f(x)$ e $t = y - s$. Então $g(t) = g(y - s) = g(y) - g(s) = z - g(f(x)) = z - z = 0$. Logo $t \in L_2$ e portanto $y = s + t \in L_1 + L_2$. Consequentemente $L = L_1 + L_2$. Por outro lado, se $y \in L_1 \cap L_2$, então existe $x \in K$ tal que $y = f(x) \in Ker(g) = L_2$. Logo $(g \circ f)(x) = g(f(x)) = 0$ e portanto $x = 0$, pois $g \circ f$ é um isomorfismo. Segue-se que $y = f(x) = f(0) = 0$ e $L_1 \cap L_2 = 0$. Em conclusão $L = L_1 \oplus L_2 = Im(f) \oplus Ker(g)$.

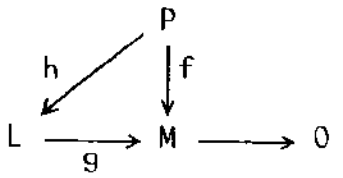
C.Q.D.

DEFINIÇÃO - Seja P um R-módulo. Dizemos que P é projetivo se para todo homomorfismo $f:P \longrightarrow M$ e todo epimorfismo $g:L \longrightarrow M$ de R-módulos, existe um homomorfismo $h:P \longrightarrow L$ tal que $g \circ h = f$.

Na linguagem de diagramas, isto significa o seguinte: um R-módulo P é projetivo se e só se todo diagrama

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow f & & \\ L & \xrightarrow[g]{} & M & \longrightarrow & 0 \end{array}$$

de homomorfismos de R-módulos, onde a fila é exata, pode ser imerso num diagrama comutativo:



PROPOSIÇÃO 39 - Seja P um R-módulo. São equivalentes:

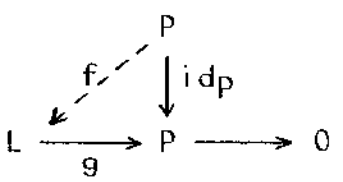
(a) P é projetivo.

(b) Existe um R-módulo livre L e homomorfismos $f:P \longrightarrow L$ e $g:L \longrightarrow P$ tais que $g \circ f = id_P$.

(c) Existe um subconjunto C de P e para cada $y \in C$ existe um homomorfismo $h_y:P \longrightarrow R$ tais que para cada $x \in P$, o conjunto $\{y \in C;\ h_y(x) \neq 0\}$ é finito e $x = \sum_{y \in C} (h_y(x))y$.

(d) P é somando direto de um R-módulo livre.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que P é projetivo. Seja $g:L \longrightarrow P$ um epimorfismo, onde L é um R-módulo livre. Então temos o seguinte diagrama:

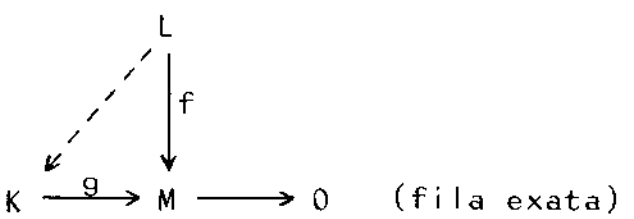


Portanto existe um homomorfismo $f:P \longrightarrow L$ tal que $g \circ f = id_P$.

(b) $\Rightarrow$ (c). Suponhamos que existem um R-módulo livre L e homomorfismos $f:P \longrightarrow L$ e $g:L \longrightarrow P$ tais que $g \circ f = id_P$. Sejam B uma base de L e $C = g(B)$. Para cada $x \in P$, escrevemos $f(x) = \sum_{z \in B} (f_z(x))z$. Obtemos assim para cada $z \in B$ um homomorfismo $f_z:P \longrightarrow R$. Para cada $y \in C$, seja $h_y = f_z$, onde $g(z) = y$. Observamos que $\{y \in C;\ h_y(x) \neq 0\}$ é finito para cada $x \in P$. Além disto $x = g(f(x)) = \sum_{z \in B} (f_z(x))g(z) = \sum_{y \in C} (h_y(x))y$ para cada x em P.

(c) $\Rightarrow$ (d). Suponhamos que existe um subconjunto C de P e para cada $y \in C$ existe um homomorfismo $h_y: P \longrightarrow R$ tais que para cada $x \in P$, o conjunto $\{y \in C;\ h_y(x) \neq 0\}$ é finito e $x = \sum_{y \in C} (h_y(x))y$. Seja $h: L \longrightarrow P$ um epimorfismo, onde L é um R-módulo livre. Sejam $B = h^{-1}(C)$ e K o R-módulo livre com base B. Definimos um homomorfismo $g: K \longrightarrow P$ por $g(z) = h(z)$, para cada elemento básico $z \in B$. Como P é gerado por C, então g é sobrejetivo. Definimos $f: P \longrightarrow K$ por $f(x) = \sum_{z \in B} (h_y(x))z$, para cada $x = \sum_{y \in C} (h_y(x))y \in P$, onde $h(z) = y$ se $h_y(x) \neq 0$. Então f é um homomorfismo e $g \circ f = id_P$. Portanto K é isomorfo a $P + Ker(g)$, pela proposição 38. Consequentemente P é somando direto de um R-módulo livre.

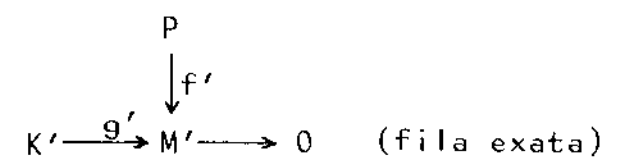
(d) $\Rightarrow$ (a). Suponhamos que P é somando direto de um R-módulo livre L. Então $L = P \oplus Q$, para algum R-módulo Q. Em primeiro lugar demonstraremos que L é projetivo. Seja B uma base de L. Consideremos o seguinte diagrama de R-módulos e homomorfismos



(fila exata)

Para cada $x \in B$, existe um elemento $k(x) \in K$ tal que $g(k(x)) = f(x)$, pois g é sobrejetivo. Obtemos assim uma aplicação $k: B \longrightarrow K$ tal que $g \circ k = f$. Extendendo linearmente k a L, obtemos um homomorfismo $h: L \longrightarrow K$ tal que $g \circ h = f$. Portanto L é projetivo.

Agora consideremos o seguinte diagrama de R-módulos e homomorfismos



(fila exata)

Sejam $i:P \longrightarrow L$ e $p:L \longrightarrow P$ o monomorfismo e o epimorfismo canónicos, respectivamente. Como L é projetivo, então existe um homomorfismo $k:L \longrightarrow K'$ tal $g' \circ k = f' \circ p$. Seja $h' = k \circ i : P \longrightarrow K'$. Como $p \circ i = id_P$, então $g' \circ h' = g' \circ k \circ i = f' \circ p \circ i = f'$. Consequentemente P é projetivo.

C.Q.D.

COROLÁRIO - Todo R-módulo livre é projetivo.

PROPOSIÇÃO 40 - Seja R um domínio de integridade. Um ideal não nulo I de R é inversível se e só se I é um R-módulo projetivo.

DEMONSTRAÇÃO - Suponhamos que I é inversível. Então $I[R:I]_F = R$, onde $F = T(R)$. Logo existem $q_1, q_2, \ldots, q_n \in [R:I]_F$ e $a_1, a_2, \ldots, a_n \in I$ tais que $q_1a_1 + q_2a_2 + \cdots + q_na_n = 1$. Definimos $h_i : I \longrightarrow R$ por $h_i(x) = q_ix$, $x \in I$, para cada i em $\{1, 2, \ldots, n\}$. Então para cada $x \in I$, $h_1(x)a_1 + h_2(x)a_2 + \cdots + h_n(x)a_n = q_1xa_1 + q_2xa_2 + \cdots + q_nxa_n = x(q_1a_1 + q_2a_2 + \cdots + q_na_n) = x$. Seja $C = \{a_1, a_2, \ldots, a_n\}$. Então C satisfaz a condição (c) da proposição 39. Portanto I é um R-módulo projetivo.

Reciprocamente, se I é um R-módulo projetivo, então existe um subconjunto C de I e para cada $y \in C$ existe um homomorfismo $h_y : I \longrightarrow R$ tais que para cada $x \in I$, o conjunto $\{y \in C; h_y(x) \neq 0\}$ é finito e $x = \sum_{y \in C} (h_y(x))y$. Logo para cada $y \in C$ e para quaisquer $x, z \in I$ temos: $xh_y(z) = h_y(xz) = zh_y(x)$. Escolhemos $x \in I \setminus \{0\}$ e escrevemos $q_y = h_y(x)/x \in T(R)$. Então $h_y(z) = q_yz \in R$ para quaisquer $y \in C$, $z \in I$. Logo $q_y \in [R:I]_F$, onde $F = T(R)$. Seja $z \in I \setminus \{0\}$. Então $h_y(z) = q_yz$ e $\{y \in C; q_yz \neq 0\}$ é finito. Segue-se que $\{y \in C; q_y \neq 0\}$ é finito. Além disto $z = \sum_{y \in C} (h_y(z))y = \sum_{y \in C} (q_yz)y = z \sum_{y \in C} yq_y$ e portanto $\sum_{y \in C} yq_y = 1$,

isto é, existem $y_1, y_2, \ldots, y_n \in I$, $q_1, q_2, \ldots, q_n \in [R:I]_F$ tais que $y_1q_1 + y_2q_2 + \cdots + y_nq_n = 1$. Então $I[R:I]_F = R$ e consequentemente I é inversível.

C.Q.D.

DEFINIÇÃO - Seja P um R-módulo. Dizemos que P é plano se para toda sequência exata de R-módulos e homomorfismos $K \xrightarrow{u} L \xrightarrow{v} M$, a sequência $P \otimes K \xrightarrow{id\otimes u} P \otimes L \xrightarrow{id\otimes v} P \otimes M$ é exata.

OBSERVAÇÃO - Se P é um R-módulo plano e L é um submódulo de um R-módulo M, então a aplicação canónica $P \otimes L \longrightarrow P \otimes M$ é injetiva, pois $0 \longrightarrow L \longrightarrow M$ é exata. Portanto podemos considerar $P \otimes L$ como um submódulo de $P \otimes M$.

PROPOSIÇÃO 41 - Seja P um R-módulo plano. Se $u:L \longrightarrow M$ é um homomorfismo de R-módulos, então $P \otimes (Ker(u))$ é isomorfo a $Ker(id_P \otimes u)$ e $P \otimes (Im(u))$ é isomorfo a $Im(id_P \otimes u)$.

DEMONSTRAÇÃO - Seja $K = Ker(u)$. Consideremos a sequência exata $0 \longrightarrow K \longrightarrow L \xrightarrow{u} M$. Como

$$0 \longrightarrow P \otimes K \longrightarrow P \otimes L \xrightarrow{id_P\otimes u} P \otimes M$$

é uma sequência exata, então $P \otimes K$ é isomorfo a $Ker(id_P \otimes u)$.

Seja $Q = Im(u)$. Definimos $v:L \longrightarrow Q$ por $v(x) = u(x)$ para cada $x \in L$. Se i é a aplicação inclusão de Q em M, então $u = i \circ v$. Logo $id_P \otimes u = (id_P \otimes i) \circ (id_P \otimes v)$, onde $id_P \otimes i$ é injetivo e $id_P \otimes v$ é sobrejetivo. Portanto $Im(id_P \otimes u) = (id_P \otimes i)(P \otimes Q)$ é isomorfo a $P \otimes Q$.

C.Q.D.

PROPOSIÇÃO 42 - Um R-módulo P é plano se e só se para qualquer

monomorfismo $u:L \longrightarrow M$ de R-módulos, $id_P \otimes u:P \otimes L \longrightarrow P \otimes M$ é também um monomorfismo.

DEMONSTRAÇÃO - Suponhamos que P é plano. Seja $u:L \longrightarrow M$ um monomorfismo de R-módulos qualquer. Então $0 \longrightarrow L \xrightarrow{u} M$ é uma sequência exata. Logo $0 \longrightarrow P \otimes L \xrightarrow{id_P \otimes u} P \otimes M$ é uma sequência exata e portanto $id_P \otimes u$ é injetivo.

Agora suponhamos que para qualquer monomorfismo $u:L \longrightarrow M$ de R-módulos, $id_P \otimes u$ é também um monomorfismo. Seja $K \xrightarrow{u} L \xrightarrow{v} M$ uma sequência exata qualquer. Se $J = Im(u)$ e $Q = Ker(v)$, então $0 \longrightarrow J \longrightarrow L \longrightarrow L/Q \longrightarrow 0$ é uma sequência exata curta. Como $P \otimes J \longrightarrow P \otimes L \longrightarrow P \otimes (L/Q) \longrightarrow 0$ é uma sequência exata e o homomorfismo canónico $P \otimes J \longrightarrow P \otimes L$ é injetivo, então $0 \longrightarrow P \otimes J \longrightarrow P \otimes L \longrightarrow P \otimes (L/Q) \longrightarrow 0$ é exata. Mas $Ker(P \otimes L \longrightarrow P \otimes (L/Q))$ é gerado pela imagem do monomorfismo canónico $P \otimes Q \longrightarrow P \otimes L$, pela proposição 1.21 de (9); logo $Ker(P \otimes L \longrightarrow P \otimes (L/Q)) = Ker(id_P \otimes v)$, pela proposição 41. Portanto $P \otimes (L/Q)$ é isomorfo a $(P \otimes L)/Ker(id_P \otimes v)$. Por outro lado $P \otimes J$ é isomorfo a $Im(id_P \otimes u)$, também pela proposição 41. Segue-se que

$$0 \longrightarrow Im(id_P \otimes u) \longrightarrow P \otimes L \longrightarrow (P \otimes L)/Ker(id_P \otimes v) \longrightarrow 0$$

é uma sequência exata. Consequentemente $Im(id_P \otimes u) = Ker(id_P \otimes v)$, isto é, $P \otimes K \xrightarrow{id_P \otimes u} P \otimes L \xrightarrow{id_P \otimes v} P \otimes M$ é exata. Portanto P é plano.

C.Q.D.

PROPOSIÇÃO 43 - Sejam M um sistema multiplicativo do anel P e Q um R-módulo. Então Q_M e $Q \otimes (R_M)$ são R-módulos isomorfos.

DEMONSTRAÇÃO - Definimos $u:Q_M \longrightarrow Q \otimes (R_M)$ por $u(x/m) = x \otimes (1/m)$ para cada $x/m \in Q_M$. Se $x/m = y/n \in Q_M$, então existe

$s \in M$ tal que $snx = smy$. Logo $x \otimes (1/m) = x \otimes (sn/snm)) =$
$= (snx) \otimes (1/(snm)) = (smy) \otimes (1/(snm)) = y \otimes (1/n)$ e portanto a aplicação u está bem definida. Sejam x/m, $z/t \in Q_M$ e $r \in R$ quaisquer. então $u(x/m + z/t) = u((tx + mz)/(mt)) =$
$= (tx + mz) \otimes (1/(mt)) = tx \otimes (1/(mt)) + (mz) \otimes (1/(mt)) =$
$= x \otimes (1/m) + z \otimes (1/t) = u(x/m) + u(z/t)$ e $u(r(x/m)) = u(rx/m) =$
$= (rx) \otimes (1/m) = r(x \otimes (1/m)) = ru(x/m)$. Portanto u é um homomorfismo de R-módulos.

Definimos $w: Q \times (R_M) \longrightarrow Q_M$ por $w(x, r/m) = rx/m$. Se $r/m = a/n \in R_M$, então $snr = sma$ para algum $s \in M$. Logo $snrx =$
$= smax$ e portanto $rx/m = ax/n$. Segue-se que w está bem definida. Sejam $c \in R$, $x, y \in Q$, r/m, $b/t \in R_M$ quaisquer. Então
$w(x + y, r/m) = r(x + y)/m = (rx + ry)/m = rx/m + ry/m =$
$= w(x, r/m) + w(y, r/m)$; $w(x, r/m + b/t) = w(x, (tr + mb)/(mt)) =$
$= (tr + mb)x/(mt) = trx/(mt) + mbx/(mt) = rx/m + bx/t =$
$= w(x, r/m) + w(x, b/t)$; $w(cx, r/m) = r(cx)/m = c(rx/m) = cw(x, r/m)$ e $w(x, c(r/m)) = w(x, cr/m) = crx/m = c(rx/m) = cw(x, r/m)$. Portanto w é bilinear. Segue-se que existe um homomorfismo $v: Q \otimes (R_M) \longrightarrow Q_M$ tal que $v(x \otimes (r/m)) = rx/m$ para qualquer tensor $x \otimes (r/m) \in Q \otimes (R_M)$. Como $u(v(x \otimes (r/m))) = u(rx/m) = ru(x/m) =$
$= r(x \otimes (1/m)) = x \otimes (r/m)$ e $v(u(x/m)) = v(x \otimes (1/m)) = x/m$, então u é um isomorfismo de R-módulos.

C.Q.D.

COROLÁRIO - Qualquer R-módulo Q é isomorfo a $Q \otimes R$. De fato, existe um isomorfismo de R-módulos $w: Q \otimes R \longrightarrow Q$ tal que $w(x \otimes r) = rx$ para cada tensor $x \otimes r \in Q \otimes R$.

PROPOSIÇÃO 44 - Se M é um sistema multiplicativo do anel R, então R_M é um R-módulo plano.

DEMONSTRAÇÃO - Seja $u:K \longrightarrow L$ um monomorfismo de R-módulos qualquer. Consideremos os isomorfismos

$$v:K_M \longrightarrow R_M \otimes K \qquad w:L_M \longrightarrow R_M \otimes L$$
$$x/m \longmapsto (1/m)\otimes x \qquad y/m \longmapsto (1/m)\otimes y$$

Definimos $t:K_M \longrightarrow L_M$ por $t(x/m) = u(x)/m$. Se $x/m = z/n \in K_M$, então $snx = smz$ para algum $s \in M$. Logo $u(x)/m = u(snx)/(snm) = u(smz)/(snm) = u(z)/n$ e portanto t está bem definida e é claro que é um homomorfismo de R-módulos. O seguinte diagrama

$$\begin{array}{ccc} K_M & \xrightarrow{\ t\ } & L_M \\ {\scriptstyle v}\downarrow & & \downarrow{\scriptstyle w} \\ R_M \otimes K & \xrightarrow{\ i\otimes u\ } & R_M \otimes L \end{array}$$

onde i é a aplicação identidade de R_M, é comutativo, pois para qualquer $x/m \in K_M$, $(i\otimes u)(v(x/m)) = (i\otimes u)((1/m)\otimes x) = (1/m)\otimes u(x) = w(u(x)/m) = w(t(x/m))$.

Seja $p \in \mathrm{Ker}(i\otimes u)$ qualquer. Então $p = v(x/m)$ para algum $x/m \in K_M$, pois v é sobrejetivo. Logo $w(t(x/m)) = (i\otimes u)(v(x/m)) = (i\otimes u)(p) = 0$. Portanto $t(x/m) = 0$, pois w é injetivo. Então $u(x)/m = t(x/m) = 0$, donde $su(x) = 0$ para algum $s \in M$. Logo $u(sx) = su(x) = 0$ e portanto $sx = 0$, pois u é injetivo. Segue-se que $x/m = sx/(sm) = 0$. Então $p = v(x/m) = v(0) = 0$. Portanto $\mathrm{Ker}(i\otimes u) = 0$, isto é, $i\otimes u:R_M \otimes K \longrightarrow R_M \otimes L$ é um monomorfismo. Consequentemente R_M é um R-módulo plano.

C.Q.D.

PROPOSIÇÃO 45 - Se M é um R-módulo e L é um R-módulo livre com base B, então todo elemento de $L\otimes M$ pode ser escrito de modo único na forma $\sum_{x\in B} x\otimes y_x$, onde $\{x \in B;\ y_x \neq 0\}$ é finito.

DEMONSTRAÇÃO - Consideremos um tensor $x\otimes y$ de $L\otimes M$. Como B é u-

ma base de L, então $x = a_1x_1 + \cdots + a_nx_n$ para alguns $a_1, \ldots, a_n \in R$ e alguns $x_1, \ldots, x_n \in B$. Logo $x \otimes y = x_1 \otimes (a_1y) + \cdots + x_n \otimes (a_ny) = \sum_{i=1}^{n} x_i \otimes y_i$, onde $y_i = a_iy$, $1 \leq i \leq n$. Logo $x \otimes y$ é da forma $\sum_{x \in B} x \otimes y_x$, com $\{x \in B;\ y_x \neq 0\}$ finito. Portanto qualquer elemento de $L \otimes M$ é também desta forma. Para demonstrar a unicidade, é suficiente demonstrar que $\sum_{x \in B} x \otimes y_x = 0$ implica $y_x = 0$ para todo $x \in B$. Suponhamos que $\sum_{x \in B} x \otimes y_x = 0$, onde $\{x \in B;\ y_x \neq 0\}$ é finito. Seja $\{x_1, x_2, \ldots, x_m\} = \{x \in B;\ y_x \neq 0\}$. Seja $z \in B$ qualquer. Se $z \in B \setminus \{x_1, \ldots, x_m\}$, então $y_z = 0$. Para $z \in \{x_1, x_2, \ldots, x_m\}$, definimos $u_z : L \longrightarrow Rz$ por $u_z(x) = z$ se $x = z$ e $u_z(x) = 0$ se $x \neq z$, para cada elemente básico $x \in B$. Então $0 = (u_z \otimes id_M)(\sum_{x \in B} x \otimes y_x) = \sum_{x \in B} (u_z \otimes id_M)(x \otimes y_x) = \sum_{x \in B} u_z(x) \otimes y_x = z \otimes y_z$. Para cada $x \in B$, definimos $v_x : Rx \longrightarrow R$ por $v_x(ax) = a$. É claro que v_x é um isomorfismo de R-módulos. Então $v_x \otimes id_M : Rx \otimes M \longrightarrow R \otimes M$ é um isomorfismo de R-módulos. Se $w : M \otimes R \longrightarrow M$ é o isomorfismo do corolário da proposição 43, então existe um isomorfismo de R-módulos $v : R \otimes M \longrightarrow M$ tal que $v(r \otimes y) = ry$ para cada tensor $r \otimes y \in R \otimes M$. Logo $0 = v((v_z \otimes id_M)(z \otimes y_z)) = v(v_z(z) \otimes y_z) = v(1 \otimes y_z) = 1y_z = y_z$. Portanto $\sum_{x \in B} x \otimes y_x = 0$, com $\{x \in B;\ y_x \neq 0\}$ finito, implica $y_x = 0$ para todo $x \in B$.

C.Q.D.

PROPOSIÇÃO 46 - Todo R-módulo livre é plano.

DEMONSTRAÇÃO - Suponhamos que K é um R-módulo livre. Seja $u : L \longrightarrow M$ um monomorfismo de R-módulos qualquer. Seja B uma base de K. Suponhamos que $t \in Ker(id_K \otimes u)$. Escrevemos $t = \sum_{x \in B} x \otimes y_x \in K \otimes L$, onde $\{x \in B;\ y_x \neq 0\}$ é finito. Então $0 = (id_K \otimes u)(\sum_{x \in B} x \otimes y_x) = \sum_{x \in B} x \otimes u(y_x)$. Logo $u(y_x) = 0$ para cada $x \in B$, pela unicidade mencionada na proposição anterior. Como u é injetivo, então $y_x = 0$ para cada $x \in B$. Logo $t = \sum_{x \in B} x \otimes y_x = 0$.

Portanto $Ker(id_K \otimes u) = 0$, isto é, $id_K \otimes u$ é injetivo. Consequentemente K é plano, pela proposição 42.

C.Q.D.

PROPOSIÇÃO 47 - Seja Q um R-módulo e sejam K e L dois submódulos de um R-módulo M tais que $M = K + L$. Então a interseção das imagens canónicas de $Q \otimes K$ e $Q \otimes L$ em $Q \otimes M$ é igual à imagem canónica de $Q \otimes (K \cap L)$ em $Q \otimes M$.

DEMONSTRAÇÃO - Consideremos o seguinte diagrama de R-módulos e homomorfismos canónicos:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K \cap L & \longrightarrow & K & \longrightarrow & K/(K \cap L) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow g & & \\ 0 & \longrightarrow & L & \longrightarrow & K + L & \longrightarrow & (K + L)/L & \longrightarrow & 0 \end{array}$$

onde g é o isomorfismo canónico $g(x + (K \cap L)) = x + L$. Este diagrama é comutativo e as filas são exatas. Como $M = K + L$, então temos o seguinte diagrama comutativo

$$\begin{array}{ccccc} Q \otimes (K \cap L) & \longrightarrow & Q \otimes K & \longrightarrow & Q \otimes (K/(K \cap L)) \\ \downarrow & & \downarrow & & \downarrow id \quad g \\ Q \otimes L & \longrightarrow & Q \otimes M & \longrightarrow & Q \otimes (M/L) \end{array}$$

onde as filas são exatas e $id_Q \otimes g$ é um isomorfismo. Logo $Im(Q \otimes K \longrightarrow Q \otimes M) \cap Im(Q \otimes L \longrightarrow Q \otimes M) = Im(Q \otimes (K \cap L) \longrightarrow Q \otimes M)$ pela parte (a) da proposição 35.

C.Q.D.

COROLÁRIO - Seja P um R-módulo plano e sejam K e L dois submódulos de um R-módulo M. Então

$$P \otimes (K \cap L) = (P \otimes K) \cap (P \otimes L).$$

DEMONSTRAÇÃO - Seja $M' = K + L$. Identificando $P \otimes K$, $P \otimes L$ e $P \otimes (K \cap L)$ com suas imagens canónicas em $P \otimes M'$, temos:

$$(P \otimes K) \cap (P \otimes L) = P \otimes (K \cap L)$$

comos submódulos de $P \otimes M'$, pela proposição anterior. Mas $P \otimes M'$ pode ser considerado como um submódulo de $P \otimes M$. Logo

$$P \otimes (K \cap L) = (P \otimes K) \cap (P \otimes L)$$

como submódulos de $P \otimes M$.

C.Q.D.

PROPOSIÇÃO 48 - Sejam R e T dois anéis tais que R é um subanel de T. Se M é um T-módulo e K é um R-módulo, então $M \otimes_T (T \otimes_R K)$ e $(M \otimes_T T) \otimes_R K$ são T-módulos isomorfos.

DEMONSTRAÇÃO - Seja $x \in M$ qualquer. Definimos

$$u_x : T \times K \longrightarrow (M \otimes_T T) \otimes_R K$$

por $u_x(t,y) = (x \otimes_T t) \otimes_R y$. É claro que u_x é R-bilinear. Logo existe um homomorfismo de R-módulos $f_x : T \otimes_R K \longrightarrow (M \otimes_T T) \otimes_R K$ tal que $f_x(t \otimes_R y) = (x \otimes_T t) \otimes_R y$ para cada $t \otimes_R y \in T \otimes_R K$. Mais ainda f_x é um homomorfismo de T-módulos. De fato, $f_x(s(t \otimes_R y)) =$
$= f_x((st) \otimes_R y) = (x \otimes_T (st)) \otimes_R y = (s(x \otimes_T t)) \otimes_R y =$
$= s((x \otimes_T t) \otimes_R y) = sf_x(t \otimes_R y)$ para qualquer $s \in T$ e qualquer $t \otimes_R y \in T \otimes_R K$. Definimos $u : M \times (T \otimes_R K) \longrightarrow (M \otimes_T T) \otimes_R K$ por $u(x,\alpha) = f_x(\alpha)$ para cada $(x,\alpha) \in M \times (T \otimes_R K)$. Observamos que u é T-bilinear. Logo existe um homomorfismo de T-módulos

$$f : M \otimes_T (T \otimes_R K) \longrightarrow (M \otimes_T T) \otimes_R K$$

tal que $f(x \otimes_T (t \otimes_R y)) = (x \otimes_T t) \otimes_R y$ para cada $x \otimes_T (t \otimes_R y)$ em $M \otimes_T (T \otimes_R K)$.

Similarmente obtemos um homomorfismo de T-módulos

$$g:(M \otimes_T T) \otimes_R K \longrightarrow M \otimes_T (T \otimes_R K)$$

tal que $g((x \otimes_T t) \otimes_R y) = x \otimes_T (t \otimes_R y)$ para cada $(x \otimes_T t) \otimes_R y$ em $(M \otimes_T T) \otimes_R K$.

É claro que $g \circ f$ e $f \circ g$ são as aplicações identidades de $M \otimes_T (T \otimes_R K)$ e $(M \otimes_T T) \otimes_R K$, respectivamente. Consequentemente $M \otimes_T (T \otimes_R K)$ e $(M \otimes_T T) \otimes_R K$ são T-módulos isomorfos.

C.Q.D.

PROPOSIÇÃO 49 - Sejam R e T dois anéis tais que R é um subanel de T. Se M é um T-módulo plano e T é um R-módulo plano, então M é um R-módulo plano.

DEMONSTRAÇÃO - Seja $u:K \longrightarrow L$ um monomorfismo de R-módulos qualquer. Como T é um R-módulo plano, então

$$id_T \otimes_R u:T \otimes_R K \longrightarrow T \otimes_R L$$

é um monomorfismo de R-módulos, pela proposição 42. Mas $(id_T \otimes_R u)(s(t \otimes_R y)) = (id_T \otimes_R u)((st) \otimes_R y) = (st) \otimes_R u(y) =$ $= s(t \otimes_R u(y)) = s(id_T \otimes_R u)(t \otimes_R y)$ para cada $s \in T$ e cada $t \otimes_R y$ em $T \otimes_R K$; logo $id_T \otimes_R u$ é um monomorfismo de T-módulos. Como M é um T-módulo plano, então $id_M \otimes_T (id_T \otimes_R u):M \otimes_T (T \otimes_R K) \longrightarrow M \otimes_T (T \otimes_R L)$ é um monomorfismo de T-módulos e portanto um monomorfismo de R-módulos. Pela proposição anterior, existe um isomorfismo de T-módulos $g:(M \otimes_T T) \otimes_R K \longrightarrow M \otimes_T (T \otimes_R K)$ tal que $g((x \otimes_T t) \otimes_R y) = x \otimes_T (t \otimes_R y)$ para cada $(x \otimes_T t) \otimes_R y \in (M \otimes_T T) \otimes_R K$.

Pelo corolário da proposição 43, existe um isomorfismo de T-módulos $v:M \longrightarrow M \otimes_T T$ tal que $v(x) = x \otimes_T 1$ para cada $x \in M$.

Como $v \otimes_R id_K:M \otimes_R K \longrightarrow (M \otimes_T T) \otimes_R K$ é um isomorfismo de R-módulos, então $g \circ (v \otimes_R id_K):M \otimes_R K \longrightarrow M \otimes_T (T \otimes_R K)$ é um isomorfismo de R-módulos. Seja $h = g \circ (v \otimes_R id_K)$. Observamos que

$$h(x \otimes_R y) = g((v \otimes_R id_K)(x \otimes_R y)) = g(v(x) \otimes_R y)$$
$$= g((x \otimes_T 1) \otimes_R y) = x \otimes_T (1 \otimes_R y)$$

para cada $x \otimes_R y \in M \otimes_R K$. Por outro lado, existe um isomorfismo de T-módulos $f: M \otimes_T (T \otimes_R L) \longrightarrow (M \otimes_T T) \otimes_R L$ tal que $f(x \otimes_T (t \otimes_R z)) = (x \otimes_T t) \otimes_R z$ para cada $x \otimes_T (t \otimes_R z) \in M \otimes_T (T \otimes_R L)$, pela proposição anterior. Também existe um isomorfismo de T-módulos $w: M \otimes_T T \longrightarrow M$ tal que $w(x \otimes_T t) = tx$ para cada $x \otimes_T t \in M \otimes_T T$, pelo corolário da proposição 43. Como $w \otimes_R id_L : (M \otimes_T T) \otimes_R L \longrightarrow M \otimes_R L$ é um isomorfismo de R-módulos, então $(w \otimes_R id_L) \circ f : M \otimes_T (T \otimes_R L) \longrightarrow M \otimes_R L$ é um isomorfismo de R-módulos. Seja $k = (w \otimes_R id_L) \circ f$. Observamos que

$$\begin{aligned} k(x \otimes_T (t \otimes_R z)) &= (w \otimes_R id_L)(f(x \otimes_T (t \otimes_R z))) \\ &= (w \otimes_R id_L)((x \otimes_T t) \otimes_R z) \\ &= (tx) \otimes_R z \end{aligned}$$

para cada $x \otimes_T (t \otimes_R z) \in M \otimes_T (T \otimes_R L)$. Como $id_M \otimes_T (id_T \otimes_R u)$ é um monomorfismo de R-módulos, então $k \circ (id_M \otimes_T (id_T \otimes_R u)) \circ h : M \otimes_R K \longrightarrow M \otimes_R L$ é um monomorfismo de R-módulos. Vejamos que $k \circ (id_M \otimes_T (id_T \otimes_R u)) \circ h = id_M \otimes_R u$. Se $x \otimes_R y$ é um elemento arbitrário de $M \otimes_R K$, então $(k \circ (id_M \otimes_T (id_T \otimes_R u)) \circ h)(x \otimes_R y) = (k \circ (id_M \otimes_T (id_T \otimes_R u)))(h(x \otimes_R y)) = (k \circ (id_M \otimes_T (id_T \otimes_R u)))(x \otimes_T (1 \otimes_R y)) = k(x \otimes_T (1 \otimes_R u(y))) = 1x \otimes_R u(y) = (id_M \otimes_R u)(x \otimes_R y)$. Logo $id_M \otimes_R u = k \circ (id_M \otimes_T (id_T \otimes_R u)) \circ h$ é um monomorfismo de R-módulos. Portanto M é um R-módulo plano, pela proposição 42.

C.Q.D.

DEFINIÇÃO - Seja P um R-módulo. Dizemos que P é fielmente plano se para quaisquer R-módulos K, L e M e quaisquer homomorfismos $u: K \longrightarrow L$ e $v: L \longrightarrow M$, a sequência $K \xrightarrow{u} L \xrightarrow{v} M$ é exata se e só se a sequência $P \otimes K \xrightarrow{i \otimes u} P \otimes L \xrightarrow{i \otimes v} P \otimes M$ é exata (i é a aplicação identidade de P).

PROPOSIÇÃO 50 - Seja P um R-módulo. São equivalentes:

(a) P é fielmente plano.

(b) P é plano e para qualquer R-módulo M, $P \otimes M = 0$ implica $M = 0$.

(c) P é plano e $id_P \otimes u = 0$ implica $u = 0$ para qualquer homomorfismo de R-módulos $u: L \longrightarrow M$.

(d) P é plano e $JP \neq P$ para qualquer $J \in Max(R)$.

DEMONSTRAÇÃO - (a) $\Rightarrow$ (b). Suponhamos que P é fielmente plano. Então é claro que P é plano. Seja M um R-módulo qualquer. Se $P \otimes M = 0$, então $0 \longrightarrow P \otimes M \longrightarrow 0$ é uma sequência exata. Logo $0 \longrightarrow M \longrightarrow 0$ é exata e portanto $M = 0$.

(b) $\Rightarrow$ (c). Suponhamos que P é plano e que para qualquer R-módulo M, $P \otimes M = 0$ implica $M = 0$. Seja $u: L \longrightarrow M$ um homomorfismo de R-módulos qualquer. Se $id_P \otimes u = 0$, então $Im(id_P \otimes u) = 0$. Logo $P \otimes Im(u) = 0$, pela proposição 41. Portanto $Im(u) = 0$, pela hipótese. Consequentemente $u = 0$.

(c) $\Rightarrow$ (a). Suponhamos que P é plano e que $id_P \otimes u = 0$ implica $u = 0$ para qualquer homomorfismo de R-módulos $u: L \longrightarrow M$. Seja $K \xrightarrow{u} L \xrightarrow{v} M$ uma sequência de homomorfismos de R-módulos arbitrária. Se esta sequência é exata, então a sequência $P \otimes K \xrightarrow{i \otimes u} P \otimes L \xrightarrow{i \otimes v} P \otimes M$ $(i = id_P)$ é exata, pois P é plano. Reciprocamente, se $P \otimes K \xrightarrow{i \otimes u} P \otimes L \xrightarrow{i \otimes v} P \otimes M$ é uma sequência exata, então $id_P \otimes (v \circ u) = (id_P \otimes v) \circ (id_P \otimes u) = 0$. Logo $v \circ u = 0$, pela hipótese. Portanto $Im(u) \subseteq Ker(v)$. Sejam $I = Im(u)$ e $J = Ker(v)$. Consideremos a sequência exata $0 \longrightarrow I \xrightarrow{j} J \xrightarrow{q} J/I \longrightarrow 0$, onde j e q são os homomorfismos canónicos. Como P é plano, então a sequência $0 \longrightarrow P \otimes I \xrightarrow{i \otimes j} P \otimes J \xrightarrow{i \otimes q} P \otimes (J/I) \longrightarrow 0$ é exata. Logo $P \otimes (J/I)$ é isomorfo a $(P \otimes J)/(P \otimes I)$ (aqui estamos identificando $P \otimes I$ com $(i \otimes j)(P \otimes I)$). Mas $P \otimes I$ é isomorfo a $Im(i \otimes u)$ e $P \otimes J$ é isomorfo a $Ker(i \otimes v) = Im(i \otimes u)$, pela proposição 41. Portanto $(P \otimes J)/(P \otimes I) = 0$. Segue-se que $P \otimes (J/I) = 0$, donde $i \otimes q = 0$. Logo $q = 0$, pela hipótese. Portanto $J/I = 0$. Consequentemente $Im(u) = I = J = Ker(v)$, isto é, a sequência $K \xrightarrow{u} L \xrightarrow{v} M$ é exata.

Em conclusão, P é fielmente plano.

(b) $\Rightarrow$ (d). Suponhamos que P é plano e para qualquer R-módulo M, $P \otimes M = 0$ implica $M = 0$. Seja $J \in Max(R)$ qualquer. Como a sequência $0 \longrightarrow J \longrightarrow R \longrightarrow R/J \longrightarrow 0$ é exata e P é plano, então a sequência $0 \longrightarrow P \otimes J \longrightarrow P \otimes R \longrightarrow P \otimes (R/J) \longrightarrow 0$ é exata. Logo $P \otimes (R/J)$ é isomorfo a $(P \otimes R)/(P \otimes J)$, onde $P \otimes J$ é identificado com $Im(P \otimes J \longrightarrow P \otimes R)$. Consideremos a aplicação $u: P \times J \longrightarrow JP$ definida por $u(x,r) = rx$ para cada $(x,r) \in P \times J$. É claro que u é R-bilinear. Logo existe um homomorfismo $v: P \otimes J \longrightarrow JP$ tal que $v(x \otimes r) = rx$ para cada tensor $x \otimes r \in P \otimes J$. Observamos que v é um isomorfismo de R-módulos, com $v^{-1}(r_1 x_1 + \cdots + r_n x_n) = x_1 \otimes r_1 + \cdots + x_n \otimes r_n$ para cada $r_1 x_1 + \cdots + r_n x_n \in JP$, onde $r_i \in J$, $x_i \in P$, $1 \leqslant i \leqslant n$. Por outro lado, $P \otimes R$ é isomorfo a P. Logo $P/(JP)$ e $P \otimes (R/J)$ são isomorfos. Como $R/J \neq 0$, então $P \otimes (R/J) \neq 0$, pela hipótese. Logo $P/(JP) \neq 0$, isto é, $JP \neq P$.

(d) $\Rightarrow$ (b). Suponhamos que P é plano e $JP \neq P$ para qualquer $J \in Max(R)$. Seja M um R-módulo não nulo. Então existe $x \in M \setminus \{0\}$. Consideremos a aplicação $u: R \longrightarrow Rx$ definida por $u(r) = rx$. É claro que u é um epimorfismo de R-módulos. Seja $K = Ker(u)$. Então Rx é isomorfo a R/K. Como $Rx \neq 0$, então $K \neq R$. Logo existe $J \in Max(R)$ tal que $K \subseteq J$. Como $JP \neq P$, então $KP \neq P$. Como na demonstração de (b) $\Rightarrow$ (d) ($P/(JP)$ e $P \otimes (R/J)$ são isomorfos), temos: $P \otimes (R/K)$ é isomorfo a $P/(KP)$. Portanto $P \otimes (R/K) \neq 0$. Consequentemente $P \otimes (Rx) \neq 0$ e disto segue-se que $P \otimes M \neq 0$.

C.Q.D.

PROPOSIÇÃO 51 - Seja M um R-módulo. São equivalentes:

(a) M é finitamente gerado.

(b) Existe uma sequência exata $L \longrightarrow M \longrightarrow 0$ de R-módulos, onde L é livre de pôsto finito.

DEMONSTRAÇÃO - (a) $\Longrightarrow$ (b). Suponhamos que M é finitamente gerado. Seja $\{x_1, x_2, \ldots, x_n\}$ um sistema de geradores de M. Definimos $f: R^n \longrightarrow M$ por $f(r_1, r_2, \ldots, r_n) = r_1x_1 + r_2x_2 + \cdots + r_nx_n$. É claro que f é um epimorfismo de R-módulos. Seja $L = R^n$. Então $L \xrightarrow{f} M \longrightarrow 0$ é uma sequência exata, onde L é livre de pôsto finito.

(b) $\Longrightarrow$ (a). Suponhamos que existe uma sequência exata $L \longrightarrow M \longrightarrow 0$, onde L é um R-módulo livre de pôsto finito. Então $\mathrm{Im}(L \longrightarrow M) = M$. Como L é finitamente gerado, então M é finitamente gerado.

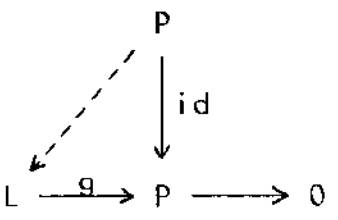
C.Q.D.

DEFINIÇÃO - Seja M um R-módulo. Dizemos que M é de apresentação finita se existe uma sequência exata de R-módulos $K \longrightarrow L \longrightarrow M \longrightarrow 0$, onde K e L são livres de pôsto finito.

É claro que todo R-módulo de apresentação finita é finitamente gerado.

PROPOSIÇÃO 52 - Se P é um R-módulo projetivo finitamente gerado, então P é de apresentação finita.

DEMONSTRAÇÃO - Como P é finitamente gerado, então existe uma sequência exata $L \xrightarrow{g} P \longrightarrow 0$, onde L é um R-módulo livre de pôsto finito. Consideremos o seguinte diagrama



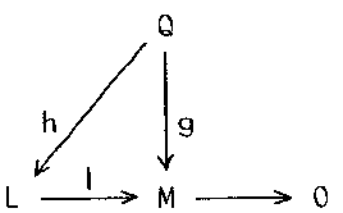
Como P é projetivo, então existe um homomorfismo

$f:P \longrightarrow L$ tal que $g \circ f = id_P$. Logo $L = Im(f) \oplus Ker(g)$, pela proposição 38. Portanto $Ker(g)$ é isomorfo a $L/Im(f)$. Segue-se que $Ker(g)$ é finitamente gerado. Então existe um epimorfismo de R-módulos $h:K \longrightarrow Ker(g)$, onde K é livre de pôsto finito, pela proposição 51. Seja $k = i \circ h$, onde i é a aplicação inclusão de $Ker(g)$ em L. Então a sequência $K \xrightarrow{k} L \xrightarrow{g} P \longrightarrow 0$ é exata, pois $Im(k) = Im(i \circ h) = (i \circ h)(K) = i(h(K)) = i(Ker(g)) = Ker(g)$. Consequentemente P é de apresentação finita.

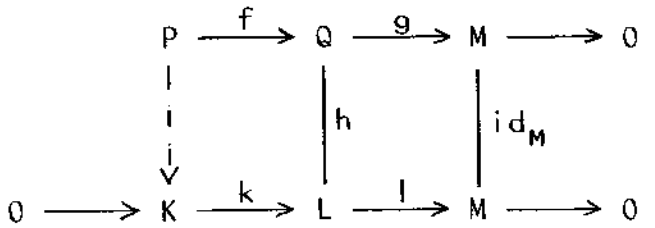
C.Q.D.

PROPOSIÇÃO 53 - Seja $0 \longrightarrow K \xrightarrow{k} L \xrightarrow{l} M \longrightarrow 0$ uma sequência exata de homomorfismos de R-módulos. Se L é finitamente gerado e M é de apresentação finita, então K é finitamente gerado.

DEMONSTRAÇÃO - Como M é de apresentação finita, então existe uma sequência exata $P \xrightarrow{f} Q \xrightarrow{g} M \longrightarrow 0$ de homomorfismos de R-módulos, onde P e Q são livres de pôsto finito. Como Q é projetivo (pelo corolário da proposição 39), então existe um homomorfismo $h:Q \longrightarrow L$ tal que o diagrama



comuta. Consideremos o seguinte diagrama comutativo



Como $l \circ h \circ f = g \circ f = 0$, então existe um homomorfismo $d:P \longrightarrow K$ tal que $k \circ d = h \circ f$. De fato, se $x \in P$, então $l(h(f(x))) = 0$, isto é, $h(f(x)) \in Ker(l) = Im(k)$. Logo existe $d(x) \in K$ tal que $k(d(x)) = h(f(x))$. Segue-se que existe uma sequência exata

$$0 = Ker(id_M) \longrightarrow Coker(d) \longrightarrow Coker(h) \longrightarrow Coker(id_M) = 0$$

pelo lema da serpente (proposição 37). Isto implica que Coker(d) é isomorfo a $Coker(h) = L/h(Q)$. Como L é finitamente gerado, então Coker(d) é finitamente gerado. Finalmente a sequência exata

$$0 \longrightarrow Im(d) \longrightarrow K \longrightarrow Coker(d) \longrightarrow 0$$

onde $Im(d) = d(P)$ e Coker(d) são finitamente gerados, mostram que K é finitamente gerado.

C.Q.D.

PROPOSIÇÃO 54 - Qualquer R-módulo X é isomorfo a Hom (R,X).

DEMONSTRAÇÃO - Definimos $u:Hom(R,X) \longrightarrow X$ por $u(f) = f(1)$. É claro que u é um homomorfismo de R-módulos. Se $u(f) = 0$, então $f(1) = 0$. Logo $f(r) = f(r1) = rf(1) = 0$ para qualquer $r \in R$ e portanto $f = 0$. Segue-se que u é injetivo. Seja $x \in X$ qualquer. Consideremos a função $h:\{1\} \longrightarrow X$ definida por $h(1) = x$. Como R é um R-módulo livre com base $\{1\}$, então existe $g \in Hom(R,X)$ tal que g restrita a $\{1\}$ é h. Logo $u(g) = g(1) = h(1) = x$. Portanto u é sobrejetivo.

Consequentemente Hom(R,X) e X são R-módulos isomorfos.

C.Q.D.

Sejam $f:L_1 \longrightarrow L$ e $g:M \longrightarrow M_1$ homomorfismos de R-módulos. A aplicação

$$\begin{aligned} Hom(L,M) &\longrightarrow Hom(L_1,M_1) \\ h &\longmapsto g \circ h \circ f \end{aligned}$$

é um homomorfismo de R-módulos e é denotado por Hom(f,g).

PROPOSIÇÃO 55 - Se $f:L_1 \longrightarrow L$, $g:M \longrightarrow M_1$, $f':L_2 \longrightarrow L_1$ e $g':M_1 \longrightarrow M_2$ são homomorfismos de R-módulos, então

$$\mathrm{Hom}(f \circ f', g' \circ g) = \mathrm{Hom}(f', g') \circ \mathrm{Hom}(f, g).$$

DEMONSTRAÇÃO - Seja $h \in \mathrm{Hom}(L,M)$ qualquer. Então

$\mathrm{Hom}(f',g')(\mathrm{Hom}(f,g)(h)) = \mathrm{Hom}(f',g')(g \circ h \circ f) =$

$= g' \circ (g \circ h \circ f) \circ f' = (g' \circ g) \circ h \circ (f \circ f') = \mathrm{Hom}(f \circ f', g' \circ g)(h).$

Portanto $\mathrm{Hom}(f \circ f', g' \circ g) = \mathrm{Hom}(f', g') \circ \mathrm{Hom}(f, g)$.

C.Q.D.

PROPOSIÇÃO 56 - Se $f:L_1 \longrightarrow L$ e $g:M \longrightarrow M_1$ são homomorfismos de R-módulos quaisquer, então

$$\mathrm{Ker}(\mathrm{Hom}(f,g)) = \{h \in \mathrm{Hom}(L,M);\ h(\mathrm{Im}(f)) \subseteq \mathrm{Ker}(g)\}.$$

DEMONSTRAÇÃO - Seja $K = \{h \in \mathrm{Hom}(L,M);\ h(\mathrm{Im}(f)) \subseteq \mathrm{Ker}(g)\}$. Se $h \in K$, então $h(f(x)) \in \mathrm{Ker}(g)$ para qualquer $x \in L_1$. Seja $x \in L_1$ qualquer. Então $\mathrm{Hom}(f,g)(h)(x) = (g \circ h \circ f)(x) = g(h(f(x))) = 0$. Logo $\mathrm{Hom}(f,g)(h) = 0$, isto é, $h \in \mathrm{Ker}(\mathrm{Hom}(f,g))$. Reciprocamente, se $h \in \mathrm{Ker}(\mathrm{Hom}(f,g))$, então $g \circ h \circ f = \mathrm{Hom}(f,g)(h) = 0$. Logo $\mathrm{Im}(h \circ f) \subseteq \mathrm{Ker}(g)$. Mas $\mathrm{Im}(h \circ f) = (h \circ f)(L_1) = h(f(L_1)) =$

$= h(\mathrm{Im}(f))$. Portanto $h(\mathrm{Im}(f)) \subseteq \mathrm{Ker}(g)$, isto é, $h \in K$.

Consequentemente

$$\mathrm{Ker}(\mathrm{Hom}(f,g)) = K = \{h \in \mathrm{Hom}(L,M);\ h(\mathrm{Im}(f)) \subseteq \mathrm{Ker}(g)\}.$$

C.Q.D.

COROLÁRIO - Se $f:L_1 \longrightarrow L$ é um epimorfismo de R-módulos e $g:M \longrightarrow M_1$ é um monomorfismo de R-módulos, então $\mathrm{Hom}(f,g)$ é um monomorfismo de R-módulos.

PROPOSIÇÃO 57 - Sejam M e Q R-módulos. Se M é a soma direta de n R-módulos M_1, M_2,..., M_n, isto é, $M = \bigoplus_{i=1}^{n} M_i$, então Hom(M,Q) é isomorfo a $\bigoplus_{i=1}^{n} \mathrm{Hom}(M_i,Q)$.

DEMONSTRAÇÃO - Seja $P = \bigoplus_{i=1}^{n} \mathrm{Hom}(M_i,Q)$. Definimos $u:\mathrm{Hom}(M,Q) \longrightarrow P$ por $u(f) = (\mathrm{Hom}(k_1,j)(f),\ldots,\mathrm{Hom}(k_n,j)(f))$, onde $k_i:M_i \longrightarrow M$ é o monomorfismo canónico, $1 \leqslant i \leqslant n$, e $j = id_Q$. É claro que u é um homomorfismo de R-módulos. Definimos $v:P \longrightarrow \mathrm{Hom}(M,Q)$ por $v(g)(x) = g_1(x_1) + \cdots + g_n(x_n)$ para cada $g = (g_1,\ldots,g_n) \in P$ e cada $x = (x_1,\ldots,x_n) \in M$. Também é claro que v é um homomorfismo de R-módulos. Como $v(u(f))(x) = \mathrm{Hom}(k_1,j)(f)(x_1) + \cdots + \mathrm{Hom}(k_n,j)(f)(x_n) = f(k_1(x_1)) + \cdots + f(k_n(x_n)) = f(k_1(x_1) + \cdots + k_n(x_n)) = f(x)$ para qualquer $f \in \mathrm{Hom}(M,Q)$ e qualquer $x = (x_1,\ldots,x_n) \in M$, então $v \circ u$ é a aplicação identidade de Hom(M,Q). Por outro lado, para cada i em $\{1,\ldots,n\}$, $\mathrm{Hom}(k_i,j)(v(g))(x_i) = v(g)(k_i(x_i)) = g_i(x_i)$ para qualquer $g = (g_1,\ldots,g_n) \in P$ e qualquer $x_i \in M_i$. Logo $u(v(g)) = (\mathrm{Hom}(k_1,j)(v(g)),\ldots,\mathrm{Hom}(k_n,j)(v(g))) = (g_1,\ldots,g_n) = g$ para qualquer $g = (g_1,\ldots,g_n) \in P$. Portanto $u \circ v$ é a aplicação identidade de P. Consequentemente u é um isomorfismo e Hom(M,Q) é isomorfo a $\bigoplus_{i=1}^{n} \mathrm{Hom}(M_i,Q)$.

C.Q.D.

PROPOSIÇÃO 58 - Se Q é um R-módulo qualquer e

$$K \xrightarrow{f} L \xrightarrow{g} M \longrightarrow 0$$

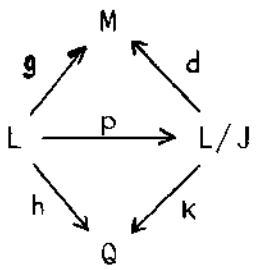
é uma sequência exata de R-módulos e homomorfismos, então

$$0 \longrightarrow \mathrm{Hom}(M,Q) \xrightarrow{g^*} \mathrm{Hom}(L,Q) \xrightarrow{f^*} \mathrm{Hom}(K,Q)$$

onde $f^* = \mathrm{Hom}(f,id_Q)$ e $g^* = \mathrm{Hom}(g,id_Q)$, também é um sequência exata.

DEMONSTRAÇÃO - Como g é um epimorfismo e id_Q é um monomorfismo,

então $g^* = Hom(g, id_Q)$ é um monomorfismo, pelo corolário anterior. Por outro lado, segundo a proposição 55 temos $f^* \circ g^* =$ $= Hom(f, id_Q) \circ Hom(g, id_Q) = Hom(g \circ f, id_Q \circ id_Q) = Hom(0, id_Q) = 0$. Logo $Im(g^*) \subseteq Ker(f^*)$. Seja $h \in Ker(f^*) = Ker(Hom(f, id_Q))$ qualquer e seja $J = Im(f) = Ker(g)$. Então $h(J) = h(Im(f)) \subseteq Ker(id_Q)$ pela proposição 56. Logo $h(J) = 0$ e portanto $h: L \longrightarrow Q$ induz um homomorfismo $k: L/J \longrightarrow Q$. Como $g: L \longrightarrow M$ é um epimorfismo com $Ker(g) = J$, então g induz um isomorfismo $d: L/J \longrightarrow M$. Seja $p: L \longrightarrow L/J$ o epimorfismo canónico. Então o diagrama



é comutativo. Como d é um isomorfismo, então podemos definir um homomorfismo $i = k \circ d^{-1}$ de M em Q. Logo $i \in Hom(M,Q)$ e $g^*(i) = Hom(g, id_Q)(i) = i \circ g = (k \circ d^{-1}) \circ g = k \circ (d^{-1} \circ g) = k \circ p = h$. Portanto $h \in Im(g^*)$. Segue-se que $Ker(f^*) \subseteq Im(g^*)$.

Consequentemente

$$0 \longrightarrow Hom(M,Q) \xrightarrow{g^*} Hom(L,Q) \xrightarrow{f^*} Hom(K,Q)$$

é uma sequência exata.

C.Q.D.

PROPOSIÇÃO 59 - Se Q é um R-módulo qualquer e $0 \longrightarrow K \xrightarrow{f} L \xrightarrow{g} M$ é uma sequência exata de homomorfismos de R-módulos, então a sequência $0 \longrightarrow Hom(Q,K) \xrightarrow{f_*} Hom(Q,L) \xrightarrow{g_*} Hom(Q,M)$, onde $f_* = Hom(id_Q, f)$ e $g_* = Hom(id_Q, g)$, é também exata.

DEMONSTRAÇÃO - Como id_Q é um epimorfismo e f é um monomorfismo,

então $f_* = \mathrm{Hom}(id_Q, f)$ é um monomorfismo, pelo corolário da proposição 56. Por outro lado, utilizando a proposição 55, temos $g_* \circ f_* = \mathrm{Hom}(id_Q, g) \circ \mathrm{Hom}(id_Q, f) = \mathrm{Hom}(id_Q, g \circ f) = \mathrm{Hom}(id_Q, 0) = 0$. Logo $\mathrm{Im}(f_*) \subseteq \mathrm{Ker}(g_*)$. Seja $h \in \mathrm{Ker}(g_*) = \mathrm{Ker}(\mathrm{Hom}(id_Q, g))$. Então $h(Q) = h(\mathrm{Im}(id_Q)) \subseteq \mathrm{Ker}(g) = \mathrm{Im}(f)$, pela proposição 56. Como $f: K \longrightarrow L$ é um monomorfismo, então existe um isomorfismo $k: \mathrm{Im}(f) \longrightarrow K$ tal que $f \circ k$ é o homomorfismo inclusão de $\mathrm{Im}(f)$ em L. Definimos um homomorfismo $j: Q \longrightarrow K$ por $j(x) = k(h(x))$ para cada $x \in Q$. Então $j \in \mathrm{Hom}(Q, K)$ e para qualquer $x \in Q$, $f_*(j)(x) = \mathrm{Hom}(id_Q, f)(j)(x) = (f \circ j)(x) = f(j(x)) = f(k(h(x))) = (f \circ k)(h(x)) = h(x)$, pois $h(x) \in \mathrm{Im}(f)$ e $f \circ k$ é o homomorfismo inclusão de $\mathrm{Im}(f)$ em L. Logo $f_*(j) = h$ e portanto $h \in \mathrm{Im}(f_*)$. Segue-se que $\mathrm{Ker}(g_*) \subseteq \mathrm{Im}(f_*)$.

Consequentemente a sequência

$$0 \longrightarrow \mathrm{Hom}(Q, K) \xrightarrow{f_*} \mathrm{Hom}(Q, L) \xrightarrow{g_*} \mathrm{Hom}(Q, M)$$

é exata.

C.Q.D.

PROPOSIÇÃO 60 - Seja P um R-módulo. São equivalentes:

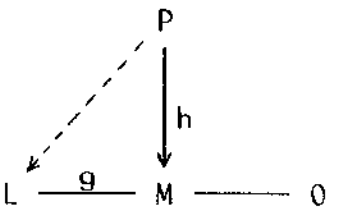
(a) P é projetivo.

(b) Para qualquer sequência exata curta de R-módulos $0 \longrightarrow K \xrightarrow{f} L \xrightarrow{g} M \longrightarrow 0$, a sequência $0 \longrightarrow \mathrm{Hom}(P, K) \xrightarrow{f_*} \mathrm{Hom}(P, L) \xrightarrow{g_*} \mathrm{Hom}(P, M) \longrightarrow 0$, onde $f_* = \mathrm{Hom}(id_P, f)$ e $g_* = \mathrm{Hom}(id_P, g)$, é também exata.

(c) Para qualquer epimorfismo de R-módulos $g: L \longrightarrow M$, $\mathrm{Hom}(id_P, g): \mathrm{Hom}(P, L) \longrightarrow \mathrm{Hom}(P, M)$ é também um epimorfismo.

DEMONSTRAÇÃO - (a) $\Longrightarrow$ (b). Suponhamos que P é projetivo. Seja $0 \longrightarrow K \xrightarrow{f} L \xrightarrow{g} M \longrightarrow 0$ uma sequência exata curta de R-módulos qualquer. Segundo a proposição anterior, a sequência $0 \longrightarrow \mathrm{Hom}(P, K) \xrightarrow{f_*} \mathrm{Hom}(P, L) \xrightarrow{g_*} \mathrm{Hom}(P, M)$ é exata. Vejamos que g_* é sobrejetivo. Seja $h \in \mathrm{Hom}(P, M)$ qualquer. Consideremos o

seguinte diagrama



Como P é projetivo, então existe um homomorfismo $f:P \longrightarrow L$ tal que $g \circ f = h$. Logo $f \in Hom(P,L)$ e $g_*(f) = Hom(id_P,g)(f) = g \circ f = h$. Portanto g_* é um epimorfismo. Segue-se que a sequência

$$0 \longrightarrow Hom(P,K) \xrightarrow{f_*} Hom(P,L) \xrightarrow{g_*} Hom(P,M) \longrightarrow 0$$

é exata.

(b) $\Longrightarrow$ (c). Suponhamos que para qualquer sequência exata curta $0 \longrightarrow K \xrightarrow{f} L \xrightarrow{g} M \longrightarrow 0$, a sequência $0 \longrightarrow Hom(P,K) \xrightarrow{f_*} Hom(P,L) \xrightarrow{g_*} Hom(P,M) \longrightarrow 0$, onde $f_* = Hom(id_P,f)$ e $g_* = Hom(id_P,g)$, é também exata. Seja $g:L \longrightarrow M$ um epimorfismo de R-módulos qualquer. Consideremos a sequência exata curta $0 \longrightarrow Ker(g) \xrightarrow{i} L \xrightarrow{g} M \longrightarrow 0$, onde i é o monomorfismo inclusão de Ker(g) em L. Segue-se da hipótese que a sequência

$$0 \longrightarrow Hom(P,Ker(g)) \xrightarrow{i_*} Hom(P,L) \xrightarrow{g_*} Hom(P,M) \longrightarrow 0$$

onde $i_* = Hom(id_P,i)$ e $g_* = Hom(id_P,g)$, é exata. Logo $g_* = Hom(id_P,g)$ é um epimorfismo.

(c) $\Longrightarrow$ (a). Suponhamos que para qualquer epimorfismo de R-módulos $g:L \longrightarrow M$, $g_* = Hom(id_P,g):Hom(P,L) \longrightarrow Hom(P,M)$ é também um epimorfismo. Seja $h:P \longrightarrow M$ um homomorfismo de R-módulos qualquer e $g:L \longrightarrow M$ um epimorfismo de R-módulos qualquer. Como $h \in Hom(P,M)$ e $g_*:Hom(P,L) \longrightarrow Hom(P,M)$ é sobrejetivo, então $h = g_*(f)$ para algum $f \in Hom(P,L)$. Logo $g \circ f = Hom(id_P,g)(f) = g_*(f) = h$. Portanto P é projetivo.

C.Q.D.

PROPOSIÇÃO 61 - Seja T uma R-álgebra plana. Se M é um R-módulo de apresentação finita, então o homomorfismo canónico

$$\chi : T \otimes \mathrm{Hom}_R(M,Q) \longrightarrow \mathrm{Hom}_T(T \otimes M, T \otimes Q)$$

tal que $\chi(t \otimes f)(s \otimes x) = ts \otimes f(x)$ para cada $t \otimes f \in T \otimes \mathrm{Hom}_R(M,Q)$ e cada $s \otimes x \in T \otimes M$, é um isomorfismo de T-módulos para qualquer R-módulo Q.

DEMONSTRAÇÃO - Se $M = R$, então, utilizando o corolário da proposição 43 e a proposição 54, temos $T \otimes \mathrm{Hom}_R(M,Q) = T \otimes \mathrm{Hom}_R(R,Q) \cong$ $\cong T \otimes Q \cong \mathrm{Hom}_T(T, T \otimes Q) \cong \mathrm{Hom}_T(T \otimes R, T \otimes Q) \cong \mathrm{Hom}_T(T \otimes M, T \otimes Q)$ como T-módulos. Se $M = R^n$ para algum $n \in \mathbb{Z}^+$, então, utilizando às proposições 54 e 57, temos $T \otimes \mathrm{Hom}_R(M,Q) = T \otimes \mathrm{Hom}_R(R^n,Q) \cong$ $\cong T \otimes ((\mathrm{Hom}\ (R,Q))^n) \cong T \otimes Q^n = (T \otimes Q)^n \cong (\mathrm{Hom}_T(T, T \otimes Q))^n \cong$ $\cong (\mathrm{Hom}_T(T \otimes R, T \otimes Q))^n \cong \mathrm{Hom}_T((T \otimes R)^n, T \otimes Q) \cong \mathrm{Hom}_T(T \otimes R^n, T \otimes Q) =$ $= \mathrm{Hom}_T(T \otimes M, T \otimes Q)$ como T-módulos. Logo o resultado vale se M é um R-módulo livre de pôsto finito.

Consideremos agora um R-módulo M de apresentação finita qualquer. Neste caso existe uma sequência exata de homomorfismos $K \xrightarrow{v} L \xrightarrow{w} M \longrightarrow 0$, onde K e L são R-módulos livres de pôsto finito. Então a sequência

$$T \otimes K \xrightarrow{id \otimes v} T \otimes L \xrightarrow{id \otimes w} T \otimes M \longrightarrow 0$$

onde id é a aplicação identidade de T, é exata. Escrevendo $FX = T \otimes \mathrm{Hom}_R(X,Q)$ e $GX = \mathrm{Hom}_T(T \otimes X, T \otimes Q)$ para cada R-módulo X e utilizando a proposição 58, obtemos as seguintes sequências exatas:
$0 \longrightarrow FM \xrightarrow{g} FL \xrightarrow{h} FK$, onde $g = id \otimes \mathrm{Hom}_R(w, id_Q)$ e $h = id \otimes \mathrm{Hom}_R(v, id_Q)$ são homomorfismos de T-módulos,
$0 \longrightarrow GM \xrightarrow{g'} GL \xrightarrow{h'} GK$, onde $g' = \mathrm{Hom}_T(id \otimes w, id_{T \otimes Q})$ e $h' = \mathrm{Hom}_T(id \otimes v, id_{T \otimes Q})$ são homomorfismos de T-módulos.

Para cada tensor simples $t \otimes f \in T \otimes \mathrm{Hom}_R(M,Q) = FM$, $g'(\chi(t \otimes f)) \in GL = \mathrm{Hom}_T(T \otimes L, T \otimes Q)$ e $g'(\chi(t \otimes f)) =$ $= \mathrm{Hom}_T(id \otimes w, id_{T \otimes Q})(\chi(t \otimes f)) = \chi(t \otimes f) \circ (id \otimes w)$. Seja $s \otimes z$ um

tensor simples qualquer em $T \otimes L$. Então $g'(\gamma(t \otimes f))(s \otimes z) =$ $= (\gamma(t \otimes f) \circ (id \otimes w))(s \otimes z) = \gamma(t \otimes f)(s \otimes w(z)) = ts \otimes f(w(z))$. Por outro lado, se $\delta : FL \longrightarrow GL$ é o homomorfismo canónico, então $\delta(g(t \otimes f)) = \delta((id \otimes \mathrm{Hom}_R(w, id_Q))(t \otimes f)) = \delta(t \otimes (f \circ w))$ e $\delta(g(t \otimes f))(s \otimes z) = \delta(t \otimes (f \circ w))(s \otimes z) = ts \otimes (f \circ w)(z) =$ $= ts \otimes (f(w(z)))$. Portanto $g' \circ \gamma = \delta \circ g$. Similarmente comprova-se que se $\varepsilon : FK \longrightarrow GK$ é o homomorfismo canónico, então $h' \circ \delta =$ $= \varepsilon \circ h$. Segue-se que os quadrados

$$\begin{array}{ccc} FM & \xrightarrow{g} & FL \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\delta} \\ GM & \xrightarrow{g'} & GL \end{array} \qquad \begin{array}{ccc} FL & \xrightarrow{k} & FK \\ {\scriptstyle\delta}\downarrow & & \downarrow{\scriptstyle\varepsilon} \\ GL & \xrightarrow{h'} & GK \end{array}$$

são comutativos. Consideremos o seguinte diagrama comutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & FM & \xrightarrow{g} & FL & \xrightarrow{h} & FK \\ \downarrow & & \downarrow & & {\scriptstyle\gamma}\downarrow & & {\scriptstyle\delta}\downarrow & & {\scriptstyle\varepsilon}\downarrow \\ 0 & \longrightarrow & 0 & \longrightarrow & GM & \xrightarrow{g'} & GL & \xrightarrow{h'} & GK \end{array}$$

Como L e K são R-módulos livres de pôsto finito, então δ e ε são isomorfismos. Portanto γ é um isomorfismo, pelo lema dos cinco (corolário 1 da proposição 34).

C.Q.D.

PROPOSIÇÃO 62 - Seja T uma R-álgebra fielmente plana e seja M um R-módulo.

(a) $T \otimes M$ é um T-módulo finitamente gerado se e só se M é finitamente gerado.

(b) Se $T \otimes M$ é um T-módulo de apresentação finita, então M é de apresentação finita.

(c) Se $T \otimes M$ é um T-módulo projetivo finitamente gerado, então M é projetivo finitamente gerado.

DEMONSTRAÇÃO - (a) Se $\{x_1, x_2, \ldots, x_n\} \subseteq M$ é um sistema de geradores de M, então comprova-se sem dificuldade que $T \otimes M$ é gerado sobre T pelos elementos $1 \otimes x_1$, $1 \otimes x_2, \ldots, 1 \otimes x_n$. Reciprocamente se $1 \otimes x_1$, $1 \otimes x_2, \ldots, 1 \otimes x_n$ geram $T \otimes M$ sobre T, então x_1, $x_2, \ldots, x_n$ geram M. De fato, se L é o submódulo de M gerado por $x_1, x_2, \ldots, x_n$ e $i: L \longrightarrow M$ é o monomorfismo de inclusão, então $id_T \otimes i: T \otimes L \longrightarrow T \otimes M$ é sobrejetivo. Logo

$$T \otimes L \xrightarrow{id_T \otimes i} T \otimes M \longrightarrow 0$$

é uma sequência exata. Como T é fielmente plano sobre R, então a sequência $L \xrightarrow{i} M \longrightarrow 0$ é exata. Portanto i também é sobrejetivo. Consequentemente M = L, isto é, M é finitamente gerado.

(b) Como $T \otimes M$ é um T-módulo de apresentação finita, então $T \otimes M$ é finitamente gerado sobre T. Logo M é finitamente gerado, pela parte (a). Portanto existe uma sequência exata de R-módulos $L \xrightarrow{u} M \longrightarrow 0$, onde L é livre de pôsto finito, pela proposição 51. Seja K = Ker(u). Então a sequência

$$0 \longrightarrow T \otimes K \xrightarrow{id_T \otimes i} T \otimes L \xrightarrow{id \otimes u} T \otimes M \longrightarrow 0$$

onde $i: K \longrightarrow L$ é a aplicação de inclusão, é exata. Como L é finitamente gerado, então $T \otimes L$ é um T-módulo finitamente gerado, pela parte (a). Portanto $T \otimes K$ é finitamente gerado sobre T, pela proposição 53. Segue-se, novamente pela parte (a), que K é finitamente gerado. Então existe um epimorfismo $v: J \longrightarrow K$, onde J é um R-módulo livre de pôsto finito. Seja $w = i \circ v$. Como $Im(w) = (i \circ v)(J) = i(v(J)) = i(K) = K = Ker(u)$, então a sequência $J \xrightarrow{w} L \xrightarrow{u} M \longrightarrow 0$ é exata, isto é, M é de apresentação finita.

(c) Se $T \otimes M$ é um T-módulo projetivo finitamente gerado, então $T \otimes M$ é um T-módulo de apresentação finita, pela proposição 52. Logo M é de apresentação finita (e portanto finitamente gerado), pela parte (b). Portanto o homomorfismo canónico $\aleph: T \otimes Hom_R(M,Q) \longrightarrow Hom_T(T \otimes M, T \otimes Q)$ é um isomorfismo para todo R-módulo Q, pela proposição anterior. Seja $g: K \longrightarrow L$ um epi

morfismo de R-módulos qualquer. Então $id_T \otimes g: T \otimes K \longrightarrow T \otimes L$ é um epimorfismo, pois T é um R-módulo plano. Consideremos o seguinte diagrama:

$$\begin{array}{ccc} T \otimes \mathrm{Hom}_R(M,K) & \xrightarrow{\beta} & \mathrm{Hom}_T(T \otimes M, T \otimes K) \\ \downarrow{\scriptstyle j \otimes \mathrm{Hom}(i,g)} & & \downarrow{\scriptstyle \mathrm{Hom}_T(j \otimes i, j \otimes g)} \\ T \otimes \mathrm{Hom}_R(M,L) & \xrightarrow{\gamma} & \mathrm{Hom}_T(T \otimes M, T \otimes L) \end{array}$$

onde $i = id_M$, $j = id_T$, β e γ são os isomorfismos . Vejamos que este diagrama é comutativo. Para cada tensor simples $t \otimes f$ em $T \otimes \mathrm{Hom}_R(M,K)$, $\gamma([j \otimes \mathrm{Hom}(i,g)](t \otimes f)) \in \mathrm{Hom}_T(T \otimes M, T \otimes L)$ e $\gamma([j \otimes \mathrm{Hom}(i,g)](t \otimes f)) = \gamma(t \otimes (g \circ f))$. Seja $s \otimes x \in T \otimes M$ um tensor simples arbitrário. Então $\gamma(t \otimes (g \circ f))(s \otimes x) = ts \otimes g(f(x))$. Por outro lado, $\mathrm{Hom}_T(j \otimes i, j \otimes g)(\beta(t \otimes f)) = (j \otimes g) \circ [\beta(t \otimes f)]$ e $(j \otimes g)(\beta(t \otimes f)(s \otimes x)) = (j \otimes g)(ts \otimes f(x)) = ts \otimes g(f(x))$. Segue-se que $\gamma([j \otimes \mathrm{Hom}(i,g)](t \otimes f)) = \mathrm{Hom}_T(j \otimes i, j \otimes g)(\beta(t \otimes f))$. Disto decorre que o diagrama acima comuta. Como $j \otimes g$ é sobrejetivo (Proposição 1.20 de (9)) e $T \otimes M$ é um T-módulo projetivo, então $\mathrm{Hom}_T(j \otimes i, j \otimes g)$ é sobrejetivo, pela proposição 60. Logo $j \otimes \mathrm{Hom}(i,g)$ é um epimorfismo, isto é, a sequência

$$T \otimes \mathrm{Hom}_R(M,K) \xrightarrow{j \otimes \mathrm{Hom}(i,g)} T \otimes \mathrm{Hom}_R(M,L) \longrightarrow 0$$

é exata. Portanto a sequência

$$\mathrm{Hom}_R(M,K) \xrightarrow{\mathrm{Hom}(i,g)} \mathrm{Hom}_R(M,L) \longrightarrow 0$$

também é exata, pois T é fielmente plano. Então $\mathrm{Hom}(i,g)$ é sobrejetivo. Consequentemente M é projetivo, pela proposição 60.

C.Q.D.

PROPOSIÇÃO 63 - Sejam R e T anéis tais que R é um subanel de T. Se I é um ideal de R, então IT e $T \otimes I$ são T-módulos isomorfos.

DEMONSTRAÇÃO - Definimos $u: T \times I \longrightarrow IT$ por $u(t,a) = at$. Claramente vemos que u é R-bilinear. Logo existe um homomorfismo de R-módulos $v: T \otimes I \longrightarrow IT$ tal que $v(t \otimes a) = at$ para todo tensor simples $t \otimes a \in T \otimes I$ e $v(t_1 \otimes a_1 + \cdots + t_n \otimes a_n) = a_1t_1 + \cdots + a_nt_n$, para qualquer $t_1 \otimes a_1 + \cdots + t_n \otimes a_n \in T \otimes I$. Observamos que v é um homomorfismo de T-módulos. De fato,
$v(s(t_1 \otimes a_1 + \cdots + t_n \otimes a_n)) = v((st_1) \otimes a_1 + \cdots + (st_n) \otimes a_n) =$
$= a_1(st_1) + \cdots + a_n(st_n) = s(a_1t_1 + \cdots + a_nt_n) =$
$= sv(t_1 \otimes a_1 + \cdots + t_n \otimes a_n)$ para qualquer $s \in T$ e qualquer $t_1 \otimes a_1 + \cdots + t_n \otimes a_n \in T \otimes I$. Definimos $w: IT \longrightarrow T \otimes I$ por $w(a_1t_1 + \cdots + a_nt_n) = t_1 \otimes a_1 + \cdots + t_n \otimes a_n$ para cada $a_1t_1 + \cdots + a_nt_n \in IT$, com $a_i \in I$, $t_i \in T$, $1 \leqslant i \leqslant n$. É claro que w é um homomorfismo de T-módulos e que $w \circ v$ e $v \circ w$ são as aplicações identidades de $T \otimes I$ e IT, respectivamente. Consequentemente u é um isomorfismo de T-módulos e IT e $T \otimes I$ são T-módulos isomorfos.

C.Q.D.

PROPOSIÇÃO 64 - Sejam T um domínio de integridade, R um subanel de T tal que T é um R-módulo fielmente plano, e I um ideal não nulo de R. Se IT é principal, então I é inversível.

DEMONSTRAÇÃO - Se IT é principal, então IT é um ideal inversível (e portanto finitamente gerado) de T. Logo IT é um T-módulo projetivo finitamente gerado, pela proposição 40. Portanto $T \otimes I$ é um T-módulo projetivo finitamente gerado, pela proposição anterior. Segue-se da parte (c) da proposição 62 que I é um R-módulo projetivo. Consequentemente I é um ideal inversível de R, pela proposição 40.

C.Q.D.

PROPOSIÇÃO 65 - Se R é um domínio de Krull e R não é um corpo, então o grupo dos divisores de R, $\mathcal{D}(R)$, é um $\mathbb{Z}$-módulo livre com base $\{div(P);\ P \in X^{(1)}(R)\}$.

DEMONSTRAÇÃO - Pela proposição 27 toda família não vazia de v-ideais inteiros de R tem um elemento maximal. Então toda família não vazia de elementos positivos de $\mathcal{D}(R)$ tem um elemento minimal. Seja $B = \{p_\lambda;\ \lambda \in \Lambda\}$ o conjunto de todos os elementos positivos não nulos minimais de $\mathcal{D}(R)$. Como R não é um corpo, então $B \neq \emptyset$. Para cada $\lambda \in \Lambda$, seja P_λ o v-ideal inteiro de R tal que $p_\lambda = div(P_\lambda)$. Então $\mathcal{P} = \{P_\lambda;\ \lambda \in \Lambda\}$ é a família de todos os v-ideais inteiros próprios maximais de R. Como $\mathcal{D}(R)$ é um grupo abeliano, então $\mathcal{D}(R)$ é um $\mathbb{Z}$-módulo. Demonstraremos que B é uma $\mathbb{Z}$-base de $\mathcal{D}(R)$. Seja $a \in \mathcal{D}(R)$ qualquer. Escrevendo $b = a \vee 0$, temos que $a = b - (b - a)$, onde $b \geqslant 0$ e $b - a \geqslant 0$. Logo, para demonstrar que B gera $\mathcal{D}(R)$, é suficiente demonstrar que todo elemento positivo não nulo de $\mathcal{D}(R)$ é uma combinação linear de elementos de B. Suponhamos que isto não é certo e que $a \in \mathcal{D}(R)$ é um elemento minimal do conjunto $A = \{c \in \mathcal{D}(R);\ c > 0$ e c não é uma combinação linear de elementos de $B\}$. Então $a \notin B$ e portanto existe $\lambda \in \Lambda$ tal que $0 < p_\lambda < a$. Logo $0 < a - p_\lambda < a$ e portanto $a - p$ é uma combinação linear de elementos de B. Mas $a = p_\lambda + (a - p_\lambda)$; logo $a \notin A$, o que é absurdo. Consequentemente B gera o $\mathbb{Z}$-módulo $\mathcal{D}(R)$, isto é, qualquer $a \in \mathcal{D}(R)$ é da forma $a = \sum_{\lambda \in \Lambda} n_\lambda p_\lambda$, onde $n_\lambda \in \mathbb{Z}$ para cada $\lambda \in \Lambda$ e $\{\lambda \in \Lambda;\ n_\lambda \neq 0\}$ é um conjunto finito.

Agora demonstraremos que se $p_\lambda \in B$, $a_1, a_2, \ldots, a_m \in \mathcal{D}(R)$ e $p_\lambda \leqslant a_1 + a_2 + \cdots + a_m$, então $p_\lambda \leqslant a_i$ para algum i no conjunto $\{1,2,\ldots,m\}$. É suficiente considerar o caso em que $m = 2$. Como p_λ é um elemento positivo minimal de $\mathcal{D}(R)$, então $p_\lambda \wedge a_1 = p_\lambda$ ou $p_\lambda \wedge a_1 = 0$. Se $p_\lambda \wedge a_1 = p_\lambda$, então $p_\lambda \leqslant a_1$. Se $p_\lambda \wedge a_1 = 0$, então $(p_\lambda + a_2) \wedge (a_1 + a_2) = a_2$. De fato, é claro que $a_2 \leqslant (p_\lambda + a_2) \wedge (a_1 + a_2)$ e se $a = (p_\lambda + a_2) \wedge (a_1 + a_2)$, então $a \leqslant p_\lambda + a_2$ e $a \leqslant a_1 + a_2$. Logo $a - a_2 \leqslant p_\lambda$ e $a - a_2 \leqslant a_1$ e por-

tanto $a - a_2 \leq p_\lambda \wedge a_1 = 0$. Segue-se que $(p_\lambda + a_2) \wedge (a_1 + a_2) = a \leq a_2$. Como $p_\lambda \leq p_\lambda + a_2$ e $p_\lambda \leq a_1 + a_2$, então $p_\lambda \leq (p_\lambda + a_2) \wedge (a_1 + a_2) = a_2$.

Do resultado anterior, segue-se que cada P_λ é um ideal primo de R, pois se $x, y \in R$ e $xy \in P_\lambda$, então $(x)(y) = (xy) \subseteq P_\lambda$ e portanto $div(x) + div(y) \geq div(P_\lambda) = p_\lambda$, donde $div(P_\lambda) = p_\lambda \leq div(x)$ ou $div(P_\lambda) = p_\lambda \leq div(y)$, isto é, $x \in P_\lambda$ ou $y \in P_\lambda$.

Vejamos que cada elemento de $\mathcal{D}(R)$ tem uma representação única como combinação linear de elementos de B. Suponhamos que $a \in \mathcal{D}(R)$ e $a = \sum_{\lambda \in \Lambda} n_\lambda p_\lambda = \sum_{\lambda \in \Lambda} n'_\lambda p_\lambda$, onde $n_\lambda - n'_\lambda > 0$ para algum $\lambda \in \Lambda$. Seja $\Lambda_1 = \{\lambda \in \Lambda;\ n_\lambda - n'_\lambda > 0\}$. Então $\Lambda_1 \neq \emptyset$. Escrevamos

$$m_\lambda = \begin{cases} n_\lambda - n'_\lambda, & \text{se } \lambda \in \Lambda_1 \\ n'_\lambda - n_\lambda, & \text{se } \lambda \notin \Lambda_1 \end{cases}$$

Então $\sum_{\lambda \in \Lambda} m_\lambda p_\lambda = \sum_{\alpha \in \Lambda \setminus \Lambda_1} m_\alpha p_\alpha \neq 0$, pois $\Lambda_1 \neq \emptyset$. Se $\lambda \in \Lambda$, então $p_\lambda \leq \sum_{\alpha \in \Lambda \setminus \Lambda_1} m_\alpha p_\alpha$. Logo existe $\alpha \in \Lambda \setminus \Lambda_1$ tal que $p_\lambda \leq p_\alpha$. Como p_α é um elemento positivo minimal de $\mathcal{D}(R)$, então $p_\lambda = p_\alpha$, o que é falso. Consequentemente cada elemento de $\mathcal{D}(R)$ tem uma representação única como combinação linear de elementos de B.

Finalmente demonstraremos que $\mathcal{P} = X^{(1)}(R)$. Para isto demonstraremos que $\{R_P;\ P \in \mathcal{P}\}$ é uma família de definição de R.

Se $x \in T(R) \setminus \{0\}$, então $div(x) = \sum_{\lambda \in \Lambda} n_\lambda p_\lambda$. Para cada $\lambda \in \Lambda$, definimos $v_\lambda : T(R) \longrightarrow \mathbb{Z} \cup \{\infty\}$ por $v_\lambda(x) = n_\lambda$ e $v_\lambda(0) = \infty$. Se $y \in T(R) \setminus \{0\}$, então $div(y) = \sum_{\lambda \in \Lambda} m_\lambda p_\lambda$ e $div(xy) = div(x) + div(y) = \sum_{\lambda \in \Lambda} (n_\lambda + m_\lambda) p_\lambda$. Logo $v_\lambda(xy) = n_\lambda + m_\lambda = v_\lambda(x) + v_\lambda(y)$. Por outro lado, $div(x) \wedge div(y) = div(Rx + Ry)$ e $R(x + y) \subseteq Rx + Ry$. Logo $div(x + y) \geq div(Rx + Ry)$. Como $(\sum_{\lambda \in \Lambda} n_\lambda p_\lambda) \wedge (\sum_{\lambda \in \Lambda} m_\lambda p_\lambda) = \sum_{\lambda \in \Lambda} (\min\{n_\lambda, m_\lambda\}) p_\lambda$, então $x + y = 0$ ou $div(x + y) = \sum_{\lambda \in \Lambda} k_\lambda p_\lambda \geq div(Rx + Ry) = div(x) \wedge div(y) = \sum_{\lambda \in \Lambda} (\min\{n_\lambda, m_\lambda\}) p_\lambda$. Logo $k_\lambda \geq \min\{n_\lambda, m_\lambda\}$ para cada $\lambda \in \Lambda$. Portanto $v_\lambda(x + y) \geq \min\{v_\lambda(x), v_\lambda(y)\}$, que vale também se $x + y = 0$. Consequentemente cada v_λ é uma valorização. Para cada $\lambda \in \Lambda$, seja V_λ o anel de valorização de v_λ. É claro que cada V_λ é um subanel de valorização discreto de pôsto um de R. Como o conjunto $\{\lambda \in \Lambda;\ v_\lambda(x) \neq 0\}$ é finito para qualquer $x \in T(R) \setminus \{0\}$, então

a família $\{V_\lambda;\ \lambda \in \Lambda\}$ tem carácter finito. Se $x \in T(R)\setminus\{0\}$ e $x \in V_\lambda$ para todo $\lambda \in \Lambda$, então $v_\lambda(x) \geqslant 0$ para todo $\lambda \in \Lambda$. Logo $div(x) \geqslant 0$. Portanto $Rx \subseteq R$, isto é, $x \in R$. Segue-se que $R = \cap\{V_\lambda;\ \lambda \in \Lambda\}$.

Seja $\lambda \in \Lambda$ qualquer. Se $x \in R$ e $v_\lambda(x) > 0$, então $div(x) \geqslant p_\lambda = div(P_\lambda)$. Logo $x \in P_\lambda$. Reciprocamente se $x \in P_\lambda$, então $div(x) \geqslant div(P_\lambda) = p_\lambda$. Logo $p_\lambda \leqslant v_\lambda(x)p_\lambda$ e portanto $v_\lambda(x) > 0$. Assim temos demonstrado que $x \in P_\lambda$ se e só se $x \in R, v_\lambda(x) > 0$, isto é, $P_\lambda = M_\lambda \cap R$, onde M_λ é o único ideal maximal de V_λ. Vejamos que $V_\lambda = R_{P_\lambda}$. Se $x \in V_\lambda$, então $v_\lambda(x) \geqslant 0$ e o conjunto $\Lambda_0 = \{\mu \in \Lambda;\ v_\mu(x) < 0\}$ é finito. Seja $\Lambda_0 = \{\mu_1, \mu_2, \ldots, \mu_m\}$. Como $v_\mu(x) < 0$ para qualquer $\mu \in \Lambda_0$, então $P_\mu \nsubseteq P_\lambda$ para cada $\mu \in \Lambda_0$. Logo para cada $i \in \{1,2,\ldots,m\}$, existe $s_i \in P_{\mu_i}\setminus P_\lambda$, isto é, existe $s_i \in R\setminus P_\lambda$ tal que $v_{\mu_i}(s_i) > 0$. Escolhamos $n \in \mathbb{Z}^+$ suficientemente grande de modo que $v_{\mu_i}(xs_i^n) \geqslant 0$ para qualquer $i \in \{1,2,\ldots,m\}$. Seja $s = (s_1 s_2 \cdots s_m)^n$. Então $v_\mu(xs) \geqslant 0$ para qualquer $\mu \in \Lambda$. Logo $xs \in R$ e portanto $x = xs/s \in R_{P_\lambda}$. Consequentemente $V_\lambda \subseteq R_{P_\lambda}$. Como V_λ é um anel de valorização de pôsto um, então $V_\lambda = R_{P_\lambda}$, pela parte (a) do teorema 17.6 de (7).

Em conclusão $\{R_P;\ P \in \mathcal{P}\} = \{R_P;\ P \in X^{(1)}(R)\}$ pelo corolário da proposição 25. Se $P \in \mathcal{P} = \{P_\lambda;\ \lambda \in \Lambda\}$, então $R_P = R_Q$ para algum $Q \in X^{(1)}(R)$. Logo $PR_P = QR_Q$ pela parte (c) do teorema 17.6 de (7). Portanto $P = PR_P \cap R = QR_Q \cap R = Q \in X^{(1)}(R)$. Em consequência $\mathcal{P} \subseteq X^{(1)}(R)$. Similarmente prova-se que $X^{(1)}(R) \subseteq \mathcal{P}$. Portanto $\{div(P);\ P \in X^{(1)}(R)\} = \{div(P_\lambda);\ \lambda \in \Lambda\} = \{p_\lambda;\ \lambda \in \Lambda\} = B$ é uma $\mathbb{Z}$-base de $\mathcal{D}(R)$.

C.Q.D.

COROLÁRIO - Seja R um domínio de Krull com $T(R) \neq R$. São equivalentes:

(a) P é um ideal primo minimal de R.

(b) P é um v-ideal inteiro maximal de R.

Seja R um domínio de Krull. Suponhamos que R não é um corpo. Se K é um ideal fracionário não nulo de R, então $K = I(1/r)$ para algum ideal inteiro não nulo I de R e algum $r \in R\setminus\{0\}$. Logo $div(K) + \mathcal{P}(R) = div(I(1/r)) + \mathcal{P}(R) = div(I) + div(1/r) + \mathcal{P}(R) = div(I) + \mathcal{P}(R)$, onde $div(I) \geq 0$. Quando consideremos um elemento arbitrário de $Cl(R)$, assumiremos que é da forma $div(I) + \mathcal{P}(R)$, onde I é um ideal inteiro não nulo de R.

Daqui para a frente $\mathcal{F}(R)$ denotará o conjunto de todos os ideais fracionários não nulos de R.

Seja R um domínio de Krull com corpo de frações $F \neq R$. Se $P \in X^{(1)}(R)$, então denotaremos por v_P a valorização determinada por R_P. Assumiremos que o grupo de valores de v_P é $\mathbb{Z}$ para cada $P \in X^{(1)}(R)$. Observamos que para cada $P \in X^{(1)}(R)$ e cada $n \in \mathbb{Z}^+$, $P^n R_P = \{x \in F;\ v_P(x) \geq n\}$ e $P^{(n)} = P^n R_P \cap R = \{x \in R;\ v_P(x) \geq n\}$. De fato, existe $a \in F\setminus\{0\}$ tal que $v_P(a) = 1$. Logo $a \in PR_P$ e mais ainda $PR_P = aR_P$. Segue-se que $P^n R_P = a^n R_P = \{x \in F;\ v_P(x) \geq v_P(a^n) = \{x \in F;\ v_P(x) \geq n\}$.

TEOREMA DE APROXIMAÇÃO PARA DOMÍNIOS DE KRULL - Seja R um domínio de Krull com corpo de frações $F \neq R$. Se $v_1, v_2, \ldots, v_n \in V = \{v_P;\ P \in X^{(1)}(R)\}$ e se $k_1, k_2, \ldots, k_n \in \mathbb{Z}$, então existe $t \in F$ tal que $v_i(t) = k_i$ para cada $i \in \{1,2,\ldots,n\}$ e tal que $v_P(t) \geq 0$ para cada $v_P \in V\setminus\{v_1, v_2, \ldots, v_n\}$.

DEMONSTRAÇÃO - Seja $v_i = v_{P_i}$ para cada $i \in \{1,2,\ldots,n\}$. É suficiente demonstrar que o resultado vale no caso em que no máximo um elemento de $\{k_1, k_2, \ldots, k_n\}$ é não nulo, porque se existem $t_1, t_2, \ldots, t_n \in F$ tais que $v_i(t_j) = \delta_{ij} k_i$ para quaisquer i, j em $\{1,2,\ldots,n\}$ e $v_P(t_j) \geq 0$ para cada $j \in \{1,2,\ldots,n\}$ e cada P em

$X^{(1)}(R)\setminus\{P_1,P_2,\ldots,P_n\}$, então $t = t_1t_2\cdots t_n \in F$ satisfaz as condições requeridas.

Seja $j \in \{1,2,\ldots,n\}$ qualquer. Suponhamos que $k_i = 0$ para cada $i \in \{1,2,\ldots,n\}\setminus\{j\}$. Podemos assumir que $j = 1$. Seja $P_1R_{P_1} = aR_{P_1}$, onde $a \in P_1$. Se $k_1 = 0$, então $t = 1$ satisfaz as condições requeridas. Se $k > 0$, então $P_1^{(k_1+1)} \subset P_1$, pois $v_1(a^{k_1}) = k_1 \neq k_1 + 1$. Logo $P_1^{(k_1)} \not\subseteq P_1^{(k_1+1)} \cup P_2 \cup \cdots \cup P_n$, pela proposição 4.9 de (7). Escolhemos $t \in P^{(k_1)}$ tal que $t \notin P_1^{(k_1+1)} \cup P_2 \cup \cdots \cup P_n$. Então $v_1(t) = k_1$, $v_i(t) = 0$ para cada $i \in \{2,3,\ldots,n\}$ e $v_P(t) \geq 0$ para cada $P \in \mathcal{P}_o$, onde $\mathcal{P}_o = X^{(1)}(R)\setminus\{P_1,P_2,\ldots,P_n\}$. Portanto o teorema vale se $k_i \geq 0$ para cada $i \in \{1,2,\ldots,n\}$. Se $k_1 < 0$ e $k_2 = k_3 = \cdots = k_n = 0$, então existe $y \in F\setminus\{0\}$ tal que $v_1(y) = -k_1$, $v_i(y) = 0$ para cada $i \in \{2,3,\ldots,n\}$ e $v_P(y) \geq 0$ para cada $P \in \mathcal{P}_o$. Se $u = 1/y$, então $v_1(u) = k_1$, $v_i(u) = 0$ para cada $i \in \{2,3,\ldots,n\}$. Seja $\{P_{n+1},P_{n+2},\ldots,P_r\} = \{P \in \mathcal{P}_o;\ v_P(u) < 0\}$. Seja $v_j = v_{P_j}$ para cada $j \in \{n+1, n+2,\ldots, r\}$. Escrevemos $v_j(u) = -h_j$ para cada $j \in \{n+1, n+2,\ldots, r\}$, onde $h_j > 0$. Então existe $t' \in F$ tal que $v_i(t') = 0$ para cada $i \in \{1,2,\ldots,n\}$, $v_j(t') = h_j$ para cada $j \in \{n+1,n+2,\ldots,r\}$ e $v_P(t') \geq 0$ para cada $P \in \mathcal{P}_o\setminus\{P_{n+1},P_{n+2},\ldots,P_r\}$. Se $t = ut'$, então $v_1(t) = k_1$, $v_i(t) = 0$ para cada $i \in \{2,3,\ldots,n,n+1,\ldots,r\}$ e $v_P(t) \geq 0$ para cada $P \in X^{(1)}(R)\setminus\{P_1,\ldots,P_n,P_{n+1},\ldots,P_r\}$. Portanto $v_1(t) = k_1$, $v_i(t) = 0$ para cada $i \in \{2,3,\ldots,n\}$ e $v_P(t) \geq 0$ para cada $P \in X^{(1)}(R)\setminus\{P_1,P_2,\ldots,P_n\}$.

C.Q.D.

PROPOSIÇÃO 66 - Seja R um domínio de Krull com $T(R) \neq R$. Suponhamos que $K \longmapsto K_w$ é a w-operação induzida sobre R pela família $\mathcal{F} = \{R_P;\ P \in X^{(1)}(R)\}$.

(a) Se $Q \in X^{(1)}(R)$ e $m \in \mathbb{Z}^+$, então $(Q^m)_w = Q^{(m)}$.

(b) Se I é um ideal não nulo de R tal que $I_w \neq R$, então existem $P_1, P_2,\ldots, P_n \in X^{(1)}(R)$ e $e_1, e_2,\ldots, e_n \in \mathbb{Z}^+$ tais que $I_w = P_1^{(e_1)} \cap P_2^{(e_2)} \cap \cdots \cap P^{(e_n)}$.

DEMONSTRAÇÃO - (a) Pela definição $(Q^m)_w = \cap\{Q^mR_P;\ P \in X^{(1)}(R)\} =$ $= \cap\{(QR_P)^m;\ P \in X^{(1)}(R)\} = \cap\{(QR_P)^m \cap R;\ P \in X^{(1)}(R)\}$. Se $P \in X^{(1)}(R)\setminus\{Q\}$, então $Q \notin P$. Logo $QR_P = R_P$ para cada P em $X^{(1)}(R)\setminus\{Q\}$. Portanto $(Q^m)_w = (QR_P)^m \cap R = Q^mR_P \cap R = Q^{(m)}$.

(b) Pela definição $I_w = \cap\{IR_P;\ P \in X^{(1)}(R)\} =$ $= \cap\{IR_P \cap R;\ P \in X^{(1)}(R)\}$. Se $IR_P = R_P$ para todo $P \in X^{(1)}(R)$, então $I_w = \cap\{IR_P;\ P \in X^{(1)}(R)\} = \cap\{R_P;\ P \in X^{(1)}(R)\} = R$, o que contradiz a hipótese. Logo o conjunto $\mathcal{P}_0 = \{P \in X^{(1)}(R);\ IR_P \neq R_P\}$ é não vazio. Vejamos que $\mathcal{P}_0$ é finito. Como $I \neq 0$, então existe $a \in I\setminus\{0\}$. O conjunto $\mathcal{P}_1 = \{P \in X^{(1)}(R);\ aR_P \neq R_P\}$ é finito. Se $P \in \mathcal{P}_0$, então $aR_P \subseteq IR_P \subset R_P$ e portanto $aR_P \neq R_P$, isto é, $P \in \mathcal{P}_1$. Logo $\mathcal{P}_0 \subseteq \mathcal{P}_1$, o que implica que $\mathcal{P}_0$ é finito. Seja $\mathcal{P}_0 =$ $= \{P_1, P_2, \ldots, P_n\}$. Para cada $i \in \{1,2,\ldots,n\}$, existe $e_i \in \mathbf{Z}^+$ tal que $IR_{P_i} = (P_iR_{P_i})^{e_i} = P^{e_i}R_{P_i}$. Consequentemente $I_w =$ $= (IR_{P_1} \cap R) \cap \cdots \cap (IR_{P_n} \cap R) = (P_1^{e_1}R_{P_1} \cap R) \cap \cdots \cap (P^{e_n}R_P \cap R) =$ $= P_1^{(e_1)} \cap \cdots \cap P^{(e_n)}$.

C.Q.D.

PROPOSIÇÃO 67 - Seja R um domínio de Krull com corpo de frações $F \neq R$. Se $K \longmapsto K_w$ é a w-operação sobre R induzida pela família $\mathcal{F} = \{R_P;\ P \in X^{(1)}(R)\}$, então $K_w = K_v$ para qualquer $K \in \mathcal{F}(R)$.

DEMONSTRAÇÃO - Seja $K \in \mathcal{F}(R)$ qualquer. Então $K = I(1/r)$ para algum ideal inteiro não nulo I de R e algum $r \in R\setminus\{0\}$. Como a w-operação $K \longmapsto K_w = \cap\{KR_P;\ P \in X^{(1)}(R)\}$ é uma $*$-operação sobre R, então $I_w \subseteq I_v$, pela parte (4) do teorema 34.1 de (7).

Se $I_w = R$, então $R = I_w \subseteq I_v \subseteq R$, isto é, $I_w = R = I_v$. Se $I_w \neq R$, então $I_w = P_1^{(e_1)} \cap \cdots \cap P^{(e_n)}$ para alguns $P_1, \ldots, P_n$ em $X^{(1)}(R)$ e alguns $e_1, \ldots, e_n \in \mathbf{Z}^+$. Seja $x \in I_v$ qualquer. Suponhamos que $x \notin I_w$. Então existe $k \in \{1,2,\ldots,n\}$, digamos $k = 1$, tal que $x \notin P_k^{(e_k)} = P_1^{(e_1)}$, isto é, $v_{P_1}(x) < e_1$. Pelo Teorema de Aproxi-

mação para Domínios de Krull, existe $t \in F$ tal que $v_{P_i}(t) = -e_i$ para cada $i \in \{1,2,\ldots,n\}$ e tal que $v_P(t) \geq 0$ para cada P em $X^{(1)}(R)\setminus\{P_1,P_2,\ldots,P_n\}$. Vejamos que $I \subseteq R(1/t)$. Seja $a \in I$ qualquer. Então $a \in I_w = P_1^{(e_1)} \cap \cdots \cap P_n^{(e_n)}$. Logo $v_{P_i}(a) \geq e_i$ para cada $i \in \{1,2,\ldots,n\}$. Por outro lado, $v_P(a) \geq 0$ para cada P em $X^{(1)}(R)\setminus\{P_1,P_2,\ldots,P_n\}$. Portanto $v_{P_i}(at) = v_{P_i}(a) + v_{P_i}(t) =$ $= v_{P_i}(a) - e_i \geq 0$ e $v_P(at) \geq 0$ para cada $i \in \{1,2,\ldots,n\}$ e cada $P \in X^{(1)}(R)\setminus\{P_1,P_2,\ldots,P_n\}$. Segue-se que $at \in R$, isto é, $a \in R(1/t)$. Portanto $I \subseteq R(1/t)$. Isto implica que $I_v \subseteq R(1/t)$. Então $x \in R(1/t)$, donde $xt \in R$. Logo $v_{P_1}(xt) \geq 0$ e portanto $0 > v_{P_1}(x) - e_1 = v_{P_1}(x) - v_{P_1}(t) = v_{P_1}(xt) \geq 0$, o que é absurdo. Consequentemente $x \in I_w$. Assim temos demonstrado que $I_v \subseteq I_w$.

Em conclusão temos $K_w = (I(1/r))_w = I_w(1/r) = I_v(1/r) =$ $= (I(1/r))_v = K_v$.

C.Q.D.

Se R é um domínio de Krull e M é um sistema multiplicativo de R, então demonstraremos que a aplicação $f:Cl(R) \longrightarrow Cl(R_M)$ dada por $f(div(I) + \mathcal{P}(R)) = div(IR_M) + \mathcal{P}(R_M)$, está bem definida e é um epimorfismo de grupos. Chamaremos a f de epimorfismo canônico.

PROPOSIÇÃO 68 - Seja R um domínio de Krull. Se M é um sistema multiplicativo de R, então a aplicação $g:\mathcal{D}(R) \longrightarrow \mathcal{D}(R_M)$, dada por $g(div(K)) = div(KR_M)$, está bem definida e induz um epimorfismo de $Cl(R)$ sobre $Cl(R_M)$.

DEMONSTRAÇÃO - Se R é um corpo, então $R_M = R$, $\mathcal{D}(R) = \{div(R)\} =$ $= \{div(R_M)\} = \mathcal{D}(R_M)$ e $Cl(R) = 0 = Cl(R_M)$. Este caso é trivial.

Suponhamos que $T(R) \neq R$. Então existe um subconjunto $\mathcal{P}$ de $X^{(1)}(R)$ tal que $\{R_P;\ P \in \mathcal{P}\}$ é a família de definição de R_M, pelo corolário da proposição 24. Seja $T = R_M$. Então $\{T_Q;\ Q \in X^{(1)}(T)\} =$

$= \{R_P;\ P \in \mathcal{P}\}$ pelo corolário da proposição 25. Vejamos que g está bem definida. Se $K, L \in \mathcal{F}(R)$ e $K_v = L_v$, então $K_w = L_w$, pela proposição 67. Logo $KR_P = K_wR_P = L_wR_P = LR$ para cada $P \in X^{(1)}(R)$, pelo teorema 32.5 de (7). Então, em particular, $KTR_P = LTR_P$ para cada $P \in \mathcal{P}$. Portanto $(KT)_v = (KT)_w = \cap\{KT_Q;\ Q \in X^{(1)}(T)\} =$
$= \cap\{KTR_P;\ P \in \mathcal{P}\} = \cap\{LTR_P;\ P \in \mathcal{P}\} = \cap\{LT_Q;\ Q \in X^{(1)}(T)\} =$
$= (LT)_w = (LT)_v$, isto é, $g(div(K)) = div(KT) = div(LT) =$
$= g(div(L))$. Segue-se que g está bem definida. É claro que g é um homomorfismo de grupos e que $g(\mathcal{P}(R)) \subseteq \mathcal{P}(T)$. Então g induz um homomorfismo de grupos $f: Cl(R) \longrightarrow Cl(T)$ definido por $f([K]) =$
$= [KT]$, para cada $[K] = div(K) + \mathcal{P}(R) \in Cl(R)$. Seja $B =$
$= \{div(Q);\ Q \in X^{(1)}(T)\}$. Então B é uma base de $\mathcal{D}(T)$. Seja Q um elemento arbitrário de $X^{(1)}(T)$. Então $Q = PT$ para algum P em $X^{(1)}(R)$, com $P \cap M = \emptyset$. Logo $div(Q) = div(PT) = g(div(P))$ está em $Im(g)$. Portanto $B \subseteq Im(g)$. Segue-se que $\mathcal{D}(T) \subseteq Im(g)$, isto é, $Im(g) = \mathcal{D}(T)$. Consequentemente o homomorfismo induzido f é sobrejetivo.

C.Q.D.

PROPOSIÇÃO 69 - Se R é um domínio de Krull com corpo de frações $F \neq R$, então
$X^{(1)}(R[X]) = \{PR[X];\ P \in X^{(1)}(R)\} \cup \{Q \cap R[X];\ Q \in X^{(1)}(F[X])\}$.

DEMONSTRAÇÃO - Seja $\mathcal{F} = (V_\lambda)_{\lambda \in \Lambda}$ a família de definição de R. Para cada $\lambda \in \Lambda$, seja V_λ^* a extensão trivial de V_λ a F(X) e seja $(W_\sigma)_{\sigma \in \Sigma}$ a família de todos os sobreanéis de valorização essenciais e não triviais de F[X]. Se $T = R[X]$, então $\mathcal{F}' =$
$= (V_\lambda^*)_{\lambda \in \Lambda} \cup (W_\sigma)_{\sigma \in \Sigma}$ é a família de definição de T, pela proposição 26. Logo $\mathcal{F}' = \{T_K;\ K \in X^{(1)}(T)\}$. Como $KT_K \cap T = K$ para cada $K \in X^{(1)}(T)$, então $K \in X^{(1)}(T)$ se e só se $K = M \cap T$, onde M é o ideal maximal de algum elemento de $\mathcal{F}'$. Seja P'_λ o ideal maximal de $V_\lambda^* \in \mathcal{F}'$. Então $P'_\lambda \cap V_\lambda$ é o ideal maximal de V_λ. Logo $P_\lambda =$

$= P'_\lambda \cap R = P'_\lambda \cap (V_\lambda \cap R) = (P'_\lambda \cap V_\lambda) \cap R \in X^{(1)}(R)$. Mas $P_\lambda R[X] \subseteq$ $\subseteq P'_\lambda \cap R[X]$ e se $f \in P'_\lambda \cap R[X]$, então $C(f) \subseteq P_\lambda$. Logo $f \in P_\lambda R[X]$. Segue-se que $P'_\lambda \cap R[X] = P_\lambda R[X]$, onde $P_\lambda \in X^{(1)}(R)$. Por outro lado, se M é o ideal maximal de $W \in (W_\sigma)_{\sigma \in \Sigma}$, então $M \cap T =$ $= M \cap (F[X] \cap T) = (M \cap F[X]) \cap T = Q \cap T$, onde $Q = M \cap F[X]$ é um ideal primo minimal de F[X]. Consequentemente $K \in X^{(1)}(R[X])$ se e só se $K = PR[X]$ para algum $P \in X^{(1)}(R)$ ou $K = Q \cap R[X]$ para algum $Q \in X^{(1)}(F[X])$.

C.Q.D.

PROPOSIÇÃO 70 - Seja R um domínio de Krull com $T(R) \neq R$. Se $P \in X^{(1)}(R)$ e $m \in \mathbb{Z}^+$, então $(PR[X])^{(m)} = P^{(m)}R[X]$.

DEMONSTRAÇÃO - Seja $T = R[X]$. É claro que $P^{(m)}T = (P^m R_P \cap R)T =$ $= P^m R_P T \cap T \subseteq (PT)^m T_{PT} \cap T = (PT)^{(m)}$. Seja $f \in (PT)^{(m)} = (PT)^m T_{PT} \cap T$ qualquer. Então $f \in T = R[X]$ e $fg \in (PT)^m = P^m T$ para algum g em $T \setminus (PT)$. Logo $C(fg) \subseteq P^m$ e portanto $C(f)C(g) \subseteq (C(f)C(g))_v =$ $= (C(fg))_v \subseteq (P^m)_v = (P^m)_w = P^{(m)}$, pelas proposições 4 e 66. Como $C(g) \not\subseteq P$ e $P^{(m)}$ é um ideal P-primário, então $C(f) \subseteq P^{(m)}$, isto é, $f \in P^{(m)}T$. Segue-se que $(PT)^{(m)} = P^{(m)}T$, isto é, $(PR[X])^{(m)} =$ $= P^{(m)}R[X]$.

C.Q.D.

PROPOSIÇÃO 71 - Seja I um ideal de um anel R. Se o conjunto $C \subseteq R[X]$ gera o ideal $IR[X]$, então o conjunto $B = \{f(0) \in I;$ $f(X) \in C\}$ gera o ideal I.

DEMONSTRAÇÃO - Seja $y \in I$ qualquer. Então $y \in IR[X]$ e portanto $y = f_1(X)g_1(X) + f_2(X)g_2(X) + \cdots + f_n(X)g_n(X)$ para alguns $f_1(X), f_2(X), \ldots, f_n(X) \in R[X]$ e alguns $g_1(X), g_2(X), \ldots\ldots$

$\ldots\ldots$, $g_n(X) \in C$. Como $y \in R$, então $y = f_1(0)g_1(0) + f_2(0)g_2(0) + \ldots\ldots + f_n(0)g_n(0)$, isto é, y pertence ao ideal de R gerado por B.

C.Q.D.

COROLÁRIO - Se I é um ideal de um anel R tal que $IR[X]$ é um ideal principal de $R[X]$, então I é principal.

PROPOSIÇÃO 72 - Seja R um domínio de Krull com corpo de frações $F \neq R$. Se I é um ideal não nulo de R, então $(IR[X])_v = I_vR[X]$.

DEMONSTRAÇÃO - Seja $T = R[X]$. Se $(W_\lambda)_{\lambda \in \Lambda}$ é a família de todos os sobreanéis de valorização essenciais não triviais de $F[X]$, então a família de definição de T é $\mathcal{F} = \{T_{PT};\ P \in X^{(1)}(R)\} \cup \{W_\lambda;\ \lambda \in \Lambda\}$.

Se $I_W = R$, então $I_vT = I_wT = RT = T$. Por definição $(IT)_w = (\cap\{IT_{PT};\ P \in X^{(1)}(R)\}) \cap (\cap\{IW_\lambda;\ \lambda \in \Lambda\}) = (\cap\{IT_{PT} \cap T;\ P \in X^{(1)}(R)\}) \cap (\cap\{IW_\lambda \cap T;\ \lambda \in \Lambda\})$. Como $I \neq 0$ e $F \subseteq W_\lambda$ para cada $\lambda \in \Lambda$, então $IW_\lambda = W_\lambda$ para cada $\lambda \in \Lambda$. Logo $(IT)_v = (IT)_w = \cap\{IT_{PT} \cap T;\ P \in X^{(1)}(R)\}$. Suponhamos que $(IT)_v \subset T$. Então $(IT)_w \neq T$. Logo $(IT)_w = \cap\{IT_{PT} \cap T;\ P \in X^{(1)}(R)\} = (P_1T)^{(e_1)} \cap (P_2T)^{(e_2)} \cap \ldots\ldots \cap (P_nT)^{(e_n)}$ para alguns $P_1, P_2, \ldots\ldots, P_n \in X^{(1)}(R)$ e alguns $e_1, e_2, \ldots\ldots, e_n \in \mathbb{Z}^+$, pela demonstração da parte (b) da proposição 66. Mas $(P_iT)^{(e_i)} = P_i^{(e_i)}T$ para cada $i \in \{1,2,\ldots\ldots,n\}$, pela proposição 70. Portanto $IT \subseteq (IT)_w = P_1^{(e_1)}T \cap P_2^{(e_2)}T \cap \ldots\ldots \cap P_n^{(e_n)}T = (P_1^{(e_1)} \cap P_2^{(e_2)} \cap \ldots\ldots \cap P_n^{(e_n)})T$. Pela parte (a) da proposição 66, $P_i^{(e_i)} = (P_i^{e_i})_w$ para cada i em $\{1,2,\ldots\ldots,n\}$. Segue-se que $0 \neq I \subseteq P_1^{(e_1)} \cap P_2^{(e_2)} \cap \ldots\ldots \cap P_n^{(e_n)} = (P_1^{e_1})_w \cap (P_2^{e_2})_w \cap \ldots\ldots \cap (P_n^{e_n})_w$. Em particular, $I \subseteq (P_1^{e_1})_w$. Logo $R = I_w \subseteq ((P_1^{e_1})_w)_w = (P_1^{e_1})_w \subseteq (P_1)_w = (P_1)_v$. Mas $(P_1)_v = P_1$ pelo corolário da proposição 65. Portanto $R \subseteq P_1$, o que é absur-

do. Consequentemente $(IR[X])_v = (IT)_v = T = I_wT = I_vT = I_vR[X]$.

Se $I_w \neq R$, então $I_w = Q_1^{(k_1)} \cap Q_2^{(k_2)} \cap \cdots \cap Q_m^{(k_m)}$ para alguns $Q_1, Q_2, \ldots, Q_m \in X^{(1)}(R)$ e alguns $k_1, k_2, \ldots, k_m \in \mathbb{Z}^+$. Por outro lado, $(IT)_v = (IT)_w = \cap\{IT_{PT} \cap T;\ P \in X^{(1)}(R)\}$ como vimos anteriormente. Observamos que $T_{PT} = R[X]_{P[X]} = R_P[X]_{P[X]}$ e $IT_{PT} = IR_P[X]_{P[X]}$, para cada $P \in X^{(1)}(R)$. Se $P \notin \{Q_1, Q_2, \ldots, Q_m\}$, então $IR_P = R_P$ e portanto $IT_{PT} \cap T = T$. Para cada $i \in \{1,2,\ldots,m\}$, $IR_{Q_i}[X]_{Q_i[X]} = Q_i^{k_i}R_{Q_i}[X]_{Q_i[X]} = Q_i^{k_i}R[X]_{Q_i[X]} = (Q_i[X])^{k_i}R[X]_{Q_i[X]}$. Então $IT_{Q_iT} \cap T = IR_{Q_i}[X]_{Q_i[X]} \cap R[X] = (Q_i[X])^{k_i}R[X]_{Q_i[X]} \cap R[X] = (Q_i[X])^{(k_i)}$ para cada $i \in \{1,2,\ldots,m\}$. Segue-se que $(IR[X])_v = (IT)_v = (IT)_w = (Q_1T)^{(k_1)} \cap (Q_2T)^{(k_2)} \cap \cdots \cap (Q_mT)^{(k_m)} = Q_1^{(k_1)}T \cap Q_2^{(k_2)}T \cap \cdots \cap Q_m^{(k_m)}T = (Q_1^{(k_1)} \cap Q_2^{(k_2)} \cap \cdots \cap Q_m^{(k_m)})T = I_wT = I_vT = I_vR[X]$.

C.Q.D.

PROPOSIÇÃO 73 - Se R é um domínio de Krull, então $Cl(R[X])$ é canonicamente isomorfo a $Cl(R)$.

DEMONSTRAÇÃO - Sejam $T = R[X]$ e $F = T(R)$. Se R é um corpo, então $\mathcal{D}(R) = 0$, $Cl(R) = \{[R]\} = 0$ e $Cl(R[X]) = 0$. Neste caso trivial a aplicação $[K] \longmapsto [KR[X]]$ de $Cl(R)$ em $Cl(R[X])$ é um isomorfismo de grupos. Suponhamos que R não é um corpo. Definimos $g: \mathcal{D}(R) \longrightarrow Cl(T)$ por $g(div(K)) = div(KT) + \mathcal{P}(T)$. Vejamos que g está bem definida. Se $K, L \in \mathcal{F}(R)$ e $K_v = L_v$, então $K = I(1/r)$ e $L = J(1/r)$ para alguns ideais inteiros não nulos I e J de R, com $I_v = J_v$, e algum $r \in R\backslash\{0\}$. Logo $(IT)_v = I_vT = J_vT = (JT)_v$ pela proposição 72. Portanto $(KT)_v = (IT)_vT(1/r) = (JT)_vT(1/r) = (LT)_v$, isto é, $div(KT) = div(LT)$. Segue-se que $g(div(K)) = g(div(L))$. É claro que g é um homomorfismo de grupos. Como $\{div(Q);\ Q \in X^{(1)}(T)\}$ gera $\mathcal{D}(T)$, então $\{div(Q) + \mathcal{P}(T);\ Q \in X^{(1)}(T)\}$ gera $Cl(T)$. Se $Q \in X^{(1)}(T)$, então $Q = PT$ para algum $P \in X^{(1)}(R)$ ou $Q = M \cap T$ para algum $M \in X^{(1)}(F[X])$. Se $Q = PT$ para algum P

em $X^{(1)}(R)$, então $div(Q) + P(T) = div(PT) + P(T) = g(div(P))$ está em $Im(g)$. Se $Q = (fF[X]) \cap T$ para algum $fF[X] \in X^{(1)}(F[X])$, então podemos assumir que $f \in T = R[X]$. Logo $fF[X] \cap T = f[R:C(f)]_F T$, pela proposição 5. Portanto $div(Q) + P(T) = div(fF[X] \cap T) + P(T) = div(f[R:C(f)]_F T) + P(T) = div([R:C(f)]_F T) + div(fT) + P(T) = div([R:C(f)]_F T) + P(T) = g(div([R:C(f)]_F)) \in Im(g)$. Consequentemente $Cl(T) \subseteq Im(g)$, isto é, $Im(g) = Cl(T)$.

Agora demonstraremos que $Ker(g) = P(R)$. É claro que $P(R) \subseteq Ker(g)$. Se K é um ideal fracionário não nulo e $g(div(K)) = P(T)$, então $div(KT) \in P(T)$. Como $K = I(1/r)$ para algum ideal inteiro não nulo I de R e algum $r \in R\setminus\{0\}$, então $div(IT) + P(T) = div(IT) + div((1/r)T) + P(T) = div(I(1/r)T) + P(T) = div(KT) + P(T) = P(T)$. Logo $div(IT) \in P(T)$ e portanto $I_v T = (IT)_v$ é um ideal principal de T. Segue-se que I_v é um ideal principal, pelo corolário da proposição 71. Então $div(K) = div(I(1/r)) = div(I) + div(1/r) = div(I_v) + div(1/r) \in P(R)$. Consequentemente $Ker(g) = P(R)$ e a aplicação $f: Cl(R) \longrightarrow Cl(T)$ definida por $f(div(I) + P(R)) = div(IT) + P(T)$ é um isomorfismo de grupos.

C.Q.D.

TEOREMA 8 - Se R é um domínio de Krull, então $Cl(R\langle X\rangle)$ é canonicamente isomorfo a $Cl(R)$ e $Pic(R\langle X\rangle)$ é canonicamente isomorfo a $Pic(R)$.

DEMONSTRAÇÃO - Consideremos os homomorfismos canónicos $f: Cl(R) \longrightarrow Cl(R[X])$ e $g: Cl(R[X]) \longrightarrow Cl(R\langle X\rangle)$. Seja $h = g \circ f$. Como f e g são sobrejetivos, então h é sobrejetivo. Observamos que $h(div(I) + P(R)) = div(IR\langle X\rangle) + P(R\langle X\rangle)$ para cada $div(I) + P(R) \in Cl(R)$. Suponhamos que $div(IR\langle X\rangle) + P(R\langle X\rangle) = P(R\langle X\rangle)$. Então $div(IR\langle X\rangle) = div(fR\langle X\rangle)$ para algum $f \in R[X]$. Podemos assumir que I é um v-ideal inteiro de R. Neste caso $IR\langle X\rangle$

é um v-ideal de R(X). Logo IR(X) = fR(X) e portanto I é principal, pela proposição 15 do capítulo II. Segue-se que div(I) + + P(R) = P(R) e consequentemente Ker(h) = 0. Temos assim demonstrado que h é um isomorfismo de grupos.

Consideremos agora o homomorfismo canónico k:Pic(R) ⟶ Pic(R(X)) induzido por h. Seja div(J) + P(R(X)) um elemento arbitrário de Pic(R(X)) (onde J é um ideal inteiro de R(X)). Como h é sobrejetivo, então div(J) + P(R(X)) = = h(div(I) + P(R)) = div(IR(X)) + P(R(X)) para algum v-ideal inteiro I de R. Logo IR(X) é um ideal inversível de R(X). Portanto I é um ideal inversível de R, pela proposição 13 do capítulo II. Consequentemente div(J) + P(R(X)) = k(div(I) + P(R)) e disto segue-se que k é sobrejetivo. Se div(I) + P(R) ∈ Ker(k) (aqui I é um ideal inversível de R), então h(div(I) + P(R)) = = k(div(I) + P(R)) = 0. Logo div(I) + P(R) = 0 em Pic(R). Portanto k é injetivo. Em consequência Pic(R(X)) é canonicamente isomorfo a Pic(R).

C.Q.D.

Finalmente queremos demonstrar que se R é um domínio de Krull, então Cl(R(X)) é canonicamente isomorfo a G(R) = = Cl(R)/Pic(R), o grupo de classes local de R.

OBSERVAÇÃO - Cl(R) e Pic(R) podem ser definidos para qualquer domínio completamente integralmente fechado.

PROPOSIÇÃO 74 - Seja R um domínio completamente integralmente fechado. Então Pic(R(X)) = 0.

DEMONSTRAÇÃO - Seja div(J) + P(R(X)) um elemento arbitrário de Pic(R(X)) (onde J é um ideal (inteiro) inversível de R(X)). Então J é principal, pelo teorema 3 do capítulo II. Logo

$div(J) + P(R(X)) = P(R(X))$. Portanto o único elemento de $Pic(R(X))$ é $P(R(X))$, isto é, $Pic(R(X)) = 0$.

C.Q.D.

PROPOSIÇÃO 75 - Seja R um anel qualquer. Então R(X) é um R-módulo fielmente plano.

DEMONSTRAÇÃO - É claro que R[X] é um R-módulo livre (com R-base $\{1,X,X^2,X^3,....\}$). Então R[X] é um R-módulo plano, pela proposição 46. R(X) é um R[X]-módulo plano, pela proposição 44. Logo R(X) é um R-módulo plano, pela proposição 49.

Seja $J \in Max(R)$ qualquer. Então $JR(X) \in Max(R(X))$ pelo teorema 2 do capítulo II. Logo $JR(X) \neq R(X)$. Portanto R(X) é um R-módulo fielmente plano, pela proposição 50.

C.Q.D.

TEOREMA 9 - Se R é um domínio de Krull, então o homomorfismo canónico

$$f: Cl(R) \longrightarrow Cl(R(X))$$
$$[I] \longmapsto [IR(X)]$$

está bem definido, é sobrejetivo e seu núcleo é Pic(R).

DEMONSTRAÇÃO - Seja $g: Cl(R) \longrightarrow Cl(R[X])$ o isomorfismo canónico da proposição 73. Segundo a proposição 68, a aplicação

$$h: Cl(R[X]) \longrightarrow Cl(R(X))$$
$$[J] \longmapsto [JR(X)]$$

está bem definida e é um epimorfismo de grupos. Seja $f = h \circ g$. Observamos que $f([I]) = [IR(X)]$ para cada $[I] = div(I) + P(R)$ em $Cl(R)$. É claro que f está bem definida e é um epimorfismo de grupos. Vejamos que $Ker(f) = Pic(R)$. Se $[I] \in Pic(R)$, onde I é um

ideal inteiro inversível de R, então IR(X) é um ideal inversível de R(X). Logo [IR(X)] ∈ Pic(R(X)). Mas Pic(R(X)) = 0, pela proposição 74. Portanto f([I]) = [IR(X)] = 0, isto é, [I] ∈ Ker(f). Reciprocamente, se [I] = div(I) + P(R) ∈ Ker(f), então [IR(X)] = = f([I]) = 0. Podemos assumir que I é um v-ideal inteiro de R. Logo IR(X) é um ideal principal de R(X). Portanto I é um ideal inversível de R, pelas proposições 64 e 75. Segue-se que [I] esta em Pic(R). Consequentemente Ker(f) = Pic(R).

C.Q.D.

COROLÁRIO - Se R é um domínio de Krull, então Cl(R(X)) é canonicamente isomorfo a G(R) = Cl(R)/Pic(R).

BIBLIOGRAFIA

(1) D. D. Anderson, D. F. Anderson e R. Markanda, The Rings R(X) and R⟨X⟩, Journal of Algebra, 95(1985) 96-115.

(2) D. D. Anderson, Multiplication Ideals, Multiplication Rings and the Ring R(X), Canad. J. Math. 28(1976) 760-768.

(3) D. D. Anderson e D. F. Anderson, Generalized GCD domains, Cmment. Math. Univ. St. Paul. 28(1979) 215-221.

(4) J. T. Arnold e J. W. Brewer, Kronecker Function Rings and Flat D[X]-modules, Proc. Amer. Math. Soc. 16(1971) 483-485.

(5) A. Bouvier, The Local Class Group of a Krull Domain, Canad. Math. Bull. 26(1)(1983) 13-19.

(6) R. M. Fossum, The Divisor Class Group of a Krull Domain, Springer-Verlag Berlin Heidelberg New York, 1973.

(7) R. Gilmer, Multiplicative Ideal Theory, Dekker, New York, 1972.

(8) I. Kaplansky, Commutative Rings, The University of Chicago Press, 1974.

(9) M. D. Larsen e P. J. McCarthy, Multiplicative Theory of Ideals, Academic Press, New York, 1971.

(10) L. R. Le Riche, The Ring R⟨X⟩, J. Algebra 67(1980) 327-341.

(11) M. Nagata, Local Rings, Interscience, New York, 1962.

(12) P. Samuel, Anneaux Factoriels, Sociedade de Matemática de São Paulo, 1963.

(13) J. Querré, Sur le Groupe des Classes de Diviseurs, C. R. Acad. Sci. Paris, 284(1977) 397-399.

(14) O. Zariski e P. Samuel, Commutative Algebra, Vol. I, Springer-Verlag Berlin Heidelberg New York, 1958.

(15) O. Zariski e P. Samuel, Commutative Algebra, Vol. II, Springer-Verlag Berlin Heidelberg New York, 1960.