UMA ABORDAGEM NATURAL PARA ANÉIS DE DEDEKIND

CLEITON BATISTA VASCONCELOS

(37)

MONOGRAFIA SUBMETIDA À COORDENAÇÃO DO
CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA, COMO REQUISITO
PARCIAL PARA OBTENÇÃO DO GRAU DE MESTRE
UNIVERSIDADE FEDERAL DO CEARÁ

FORTALEZA

SUMÁRIO

AGRADECIMENTOS

"Foi uma luta chegar até aqui, mas cá estou, forte e mais do que nunca consciente do meu papel. Apesar de tudo acredito nesse projeto. As desilusões foram muitas, mas quase nada porque tinha a certeza de que vocês chegariam comigo.

Confesso que de início me assustou um pouco o preço da minha opção, mas em casa, na escola ou nas ruas vocês me acolhiam e, com o calor do corpo ou da palavra, me incentivaram apoiando-me sempre.

O dia de hoje não é como um dia qualquer, é a realização de uma etapa de meu projeto. As outras talvez sejam até mais árduas, mas estaremos juntos novamente, numa comunhão de sonhos e realizações.

Aos meus companheiros no lar, na escola e nas ruas, eu agradeço por este trabalho."

INTRODUÇÃO

Neste trabalho, baseado em notas, não publicadas do professor HERMÍNIO BORGES NETO [1] e no artigo DEDEKIND DOMAINS AND RINGS OF QUOTIENTS, de Luther Claborn [2], nós estudamos, de uma maneira natural, os anéis de Dedekind.

Estudamos a relação entre o grupo de classes de um anel de Dedekind R com o de $S^{-1}R$ onde S é um sistema multiplicativamente fechado de R. Construimos exemplos de um anel de Dedekind sem ideais primos principais. E obtemos, ainda, algumas informações sobre o número de ideais primos não principais de um anel de Dedekind qualquer.

No final do primeiro capítulo damos um exemplo de um anel de Dedekind que não é o fecho integral de um domínio principal, provando que a conjectura, no livro Commutative Algebra [3], não é verdadeira.

No último capítulo provamos, sob forma de exemplo, que se R é um anel de Dedekind, S é o conjunto de todos os polinômios mônicos e T é o conjunto de todos os polinômios primitivos de $R[x]$ então $S^{-1}(R[x])$ e $T^{-1}(R[x])$ são, ambos, anéis de Dedekind. Para finalizar, obtemos o grupo de classes destes novos anéis de Dedekind em termos do de R.

A explicação de todos os termos matemáticos usados aqui, bem como a dos que aparecem no decorrer deste trabalho, podem ser encontrados no capítulo 0.

0. CONCEITOS BÁSICOS

(0.1) - Introdução

Para uma melhor compreensão deste trabalho daremos, agora, alguns resultados básicos que serão usados nos capítulos posteriores.

Neste capítulo, por anel entenderemos anel comutativo com unidade. Por ideais próprios entenderemos ideais não triviais, isto é, diferentes de 0 e do anel.

(0.2) - Resultados

(0.2.01) - Lema de Zorn - Seja S um conjunto não vazio, parcialmente ordenado. Se toda cadeia ascendente de S é estacionária, então S tem pelo menos um elemento maximal.

(0.2.02) - Lema - Se R é um anel e A é um ideal de R, então existe um ideal maximal de R que contém A.

(0.2.03) - Definição - Sejam R um anel e A e B ideais de R. A e B são ditos ideais co-máximais se, e somente se, $A + B = R$.

(0.2.04) - Lema - Se R é um anel e $A_1, A_2, \ldots, A_n$ são ideais de R, dois a dois co-maximais, então

$$\prod_{i=i}^{n} A_i = \bigcap_{i=1}^{n} A_i$$

Prova - A prova será feita por indução sobre o número n de fatores.

Para n = 2.

é claro que $A_1A_2 \subset A_1 \cap A_2$.

Como

$$(A_1 + A_2)(A_1 \cap A_2) = A_1(A_1 \cap A_2) + A_2(A_1 \cap A_2) \subseteq A_1A_2,$$

e desde que $A_1 + A_2 = (1)$, teremos

$$A_1 \cap A_2 \subseteq A_1 A_2.$$

Logo $A_1A_2 = A_1 \cap A_2$.

Suponha que o resultado é válido para um produto com n-1 fatores, com $n > 2$.

Para n fatores.

Seja

$$B = \prod_{i=1}^{n-1} A_i$$

Por hipótese de indução

$$B = \prod_{i=1}^{n-1} A_i = \bigcap_{i=1}^{n-1} A_i$$

Como $A_i + A_n = (1)$, para cada i existem $x_i \in A_i$ e $y_i \in A_n$, tais que

$$x_i + y_i = 1$$

e, portanto,

$$\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1-y_i) \equiv 1 \text{ mód } (A_n)$$

Logo $A_n + B = (1)$

E assim

$$B \cap A_n = B.A_n,$$

ou seja:

$$(\bigcap_{i=1}^{n-1} A_i) \cap A_n = (\prod_{i=1}^{n-1} A_i)\, A_n$$

O que nos dá:

$$\bigcap_{i=1}^{n} A_i = \prod_{i=1}^{n} A_i$$

(0.2.05) - Lema - i) Sejam R um anel e $P_1, P_2, \ldots, P_r$ ideais primos de R. e seja A um ideal de R, tal que $A \subset \bigcup_{i=1}^{r} P_i$. Então $A \subset P_{io}$ para algum io.

ii) Sejam R um anel e $A_1, A_2, \ldots, A_r$ ideais de R e P um ideal primo de R tal que $P \supset \bigcap_{i=1}^{r} A_i$. Então $P \supset A_{io}$ para algum io. Se $P = \bigcap_{i=1}^{r} A_i$ então $P = A_{io}$ para algum io.

(0.2.06) - Definição - Se R é um anel e A e B são ideais de R, seu ideal quociente é denotado por (A:B) e é definido

por:

$$(A:B) = \{x \in R \ ; \ xB \subseteq A\}.$$

O anulador de B se indica por Ann(B) e é o conjunto (0:B)

(0.2.07) - Definição - Se R é um anel e A é um ideal de R, o radical de A é denotado por r(A) e é definido por:

$$r(A) = \{x \in R \ ; \ x^n \in A \text{ para algum } n > 0\}$$

(0.2.08)- Lema - Sejam R um anel e A e B ideais de R. Então valem:

i) $r(A) = R$ se, e somente se, $A = R$

ii) $r(A+B) = r(r(A) + r(B))$

Prova - i) Se $r(A) = R$ então $1 \in r(A)$. Assim existe $n > 0$ tal que $1^n \in A$. Mas $1^n = 1$. Logo $1 \in A$ e portanto $A = R$. A recíproca é obvia.

ii) Como $A \subseteq r(A)$ e $B \subseteq r(B)$ então $A+B \subseteq r(A)+r(B)$. Logo $r(A+B) \subseteq r(r(A)+r(B))$. Reciprocamente, seja $x \in r(r(A) + r(B))$. Assim existe $n > 0$ tal que $x^n \in r(A)+r(B)$. Portanto $x^n = a + b$, onde $a \in r(A)$ e $b \in r(B)$. Então existem $n_1 > 0$ e $n_2 > 0$ tais que $a^{n_1} \in A$ e $b^{n_2} \in B$.

Logo

$$(x^n)^{n_1+n_2} = (a+b)^{n_1+n_2} \in A + B,$$

seguindo-se o resultado.

(0.2.09) - Definição - Sejam R_1 e R_2 anéis. Se f é um homomorfismo de R_1 em R_2 e A é um ideal de R_1, a extensão de A a R_2 (A^e) é o ideal de R_2 gerado por f(A), isto é,

$$A^e = \{\Sigma\, a_i b_i \text{ onde } a_i \in f(A) \text{ e } b_i \in R_2\} .$$

Se B é um ideal de R_2 o ideal $f^{-1}(B)$ é chamado a contração de B em R_1 e é denotado B^c.

(0.2.10) - Lema - Sejam R_1 e R_2 anéis e f um homomorfismo de R_1 em R_2. Se A e B são ideais de R_1 e R_2, respectivamente, valem:

i) $A \subset A^{ec}$

ii) $B \supseteq B^{ce}$.

(0.2.11) - Definição - Seja R um anel. Um R-módulo é um grupo abeliano M tal que para todos x e y em M e todos a e b em R, valem,

i) $ax \in M$

ii) $a(x+y) = ax + ay$

iii) $(a+b)x = ax + bx$

iv) $(a.b)x = a(bx)$

v) $1.x = x$, onde $1 \in R$.

(0.2.12) - Definição - Um R-módulo M é dito um R-módulo fini

to (ou um R-módulo finitamente gerado) se, e somente se, existem $x_1, x_2, \ldots, x_n$ em M tais que para cada x em M vale:

$$x = \sum_{i=1}^{n} a_i x_i \quad \text{onde} \quad a_i \in R$$

(0.2.13) - Definição - Sejam M e N dois R-módulos. Uma aplicação $f : M \to N$ é um homomorfismo de R-módulos se, e somente se, para todos x e y em M e a em R, tem-se:

i) $f(x+y) = f(x) + f(y)$

ii) $f(ax) = a\, f(x)$

(0.2.14) - Lema - M é um R-módulo finitamente gerado se, e somente se, M é isomorfo a um quociente de A^n para algum $n > 0$.

Prova - Sejam $x_1, x_2, \ldots, x_n$ geradores de M como R-módulo. Defina:

$$\phi : R^n \longrightarrow M$$

$$(a_1, a_2, \ldots, a_n) \longmapsto a_1x_1 + a_2x_2 + \ldots + a_nx_n .$$

ϕ é um homomorfismo sobrejetor. Logo $M \simeq R^n/Ker$.

Reciprocamente se M é isomorfo a R^n/E, existe um homomorfismo sobrejetivo de R^n em M.

Assim como $\{e_i = (0,0,\ldots,1,\ldots,0)\}$ gera R^n . $\phi(e_i)$ gera M. Logo M é finitamente gerado (como R-módulo)

(0.2.15) - Definição - Seja R um anel comutativo com uni

dade. Um sistema multiplicativamente fechado de R é um subconjunto S de R tal que:

i) $1 \in S$.

ii) S é fechado com respeito a multiplicação de A.

Se definirmos em R X S uma relação de equivalência $\equiv$ por:

$(a, s) \equiv (b,t)$ se, e somente se, $(at - bs)n = 0$ para algum $n \in S$,

e denotarmos por a/s a classe de equivalência de (a,s), então o conjunto $S^{-1}R$ de todas as classes de equivalência com as operações:

$$+ : \frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

$$. : \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

é um anel, chamado ANEL DE FRAÇÕES de R COM RESPEITO a S.

(0.2.16) - Observação - Se P é um ideal primo de R então $S = R - P$ é sistema multiplicativamente fechado de R e, neste caso, $S^{-1}R$ será denotado por R_p.

(0.2.17) - Definição - Um anel R é dito um anel local se, e somente se, R possui um único ideal maximal.

(0.2.18) - Lema - R_p é um anel local.

(0.2.19) - Definição - Sejam R um anel e M um R-módulo. O conjunto de todos os elementos x de R tais que x M = 0 é um ideal de R, chamado o anulador de M e denotado por Ann(M).

(0.2.20) - Lema - Sejam R um anel, M um R-módulo e P (resp M) um ideal primo (resp. maximal) de R. Denote por M_p. (resp M_M) o R_p-módulo (resp. R_M-módulo) $S^{-1}M$ onde S = R - P (resp. R-M). As seguintes afirmações são equivalentes:

i) M = 0

ii) M_p = 0 para todo ideal primo P de R.

iii) M_M = 0 para todo ideal maximal M de R.

Prova - É claro que i) $\longrightarrow$ ii) $\longrightarrow$ iii).

Suponha que vale iii) e que M seja diferente de 0.

Sejam x um elemento não nulo de M e A = Ann(x)

A é um ideal próprio de R e, portanto, pelo lema (0.2.02) A está contido em um ideal maximal M de R.

Assim $\frac{x}{1}$ está em M_M. Como M_M = 0, $\frac{x}{1}$ = 0. Portanto existe u em R - M tal que ux = 0. Neste caso u $\in$ Ann(x). Mas Ann(x) $\subset$ M. Absurdo! Logo M = 0.

(0.2.21) - Lema - i) Cada ideal de $S^{-1}R$ é um ideal extendido.

ii) Se A é um ideal de R, então $A^{ec} = \bigcup_{s \in S} (A:s)$.

Portanto $A^e = S^{-1}R$ se, e somente se, $A \cap S \neq \emptyset$.

iii) Os ideais primos de $S^{-1}R$ estão em correspondência biunívoca ($P - S^{-1}P$) com os ideais primos de R que não interceptam S.

Prova - i) Sejam B um ideal em $S^{-1}R$ e $x/s \in B$. Então $x/1 \in B$, portanto $x \in B^c$ e, consequentemente, $x/s \in B^{ce}$. Assim $B \subseteq B^{ce}$. Como $B \supseteq B^{ce}$, segue-se que $B = B^{ce}$.

ii) Temos que $A^{ec} = (S^{-1}A)^c$.

Assim $x \in A^{ec}$ se, e somente se, $x/1 = a/s$ para algum $a \in A$ e algum $s \in S$. Mas termos

$$x/1 = a/s.$$

é equivalente a existir $t \in S$ tal que

$$(xs - a)t = 0$$

Isto nos dá que $xst \in A$. Logo $x \in \bigcup_{s \in S} (A:s)$.

A recíproca se faz seguindo o sentido contrário ao que foi feito.

iii) Se Q é um ideal primo de $S^{-1}R$ então Q^c é um ideal primo de R. Reciprocamente se P é um ideal primo de R então R/P é um domínio de integridade. Se $\bar{S}$ é a imagem de S em R/P tem-se $S^{-1}R/S^{-1}P = \bar{S}^{-1}(R/P)$

Mas $S^{-1}R/S^{-1}P$ ou é zero ou está contido no corpo de frações de R/P e portanto é um domínio de integridade.

Assim $S^{-1}P$ ou é um ideal primo de $S^{-1}R$ ou é $S^{-1}R$. Mas por ii) $S^{-1}P = S^{-1}R$ se, e somente se, $P \cap S \neq \emptyset$.

(0.2.22) - Definição - Sejam R_1 um anel comutativo com unidade e R um subanel de R_1 tal que $1_{R_1} \in R$. Um elemento $x \in R_1$ é dito inteiro sobre R se, e somente se, existem $a_1, a_2, \ldots, a_n$ em R, tais que:

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0.$$

O conjunto C dos elementos de R_1 que são inteiros sobre R é um anel chamado fecho inteiro de R em R_1. Se $C = R$ dizemos que R é INTEGRALMENTE FECHADO em R_1. Se $C = R_1$ dizemos que R_1 é INTEIRO sobre R.

Se R é um domínio de integridade que é integralmente fechado em seu corpo de frações então dizemos apenas que R é integralmente fechado.

(0.2.23) - Exemplos - i) O fecho integral de $\mathbb{Z}$ em Q é $\mathbb{Z}$. Logo $\mathbb{Z}$ é integralmente fechado. De fato, seja $x \in Q$ inteiro sobre $\mathbb{Z}$. Assim existem $a_1, a_2, \ldots, a_n$ em $\mathbb{Z}$, tais que:

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

Como $x \in Q$ então podemos tomar $x = a/b$, $a, b \in \mathbb{Z}$, $b \neq 0$, com $(a,b) = 1$.

Assim:

$$\left(\frac{a}{b}\right)^n + a_1\left(\frac{a}{b}\right)^{n-1} + \ldots + a_o = 0.$$

O que nos dá:

$$a^n + a_1 b a^{n-1} + \ldots + b^n a_o = 0$$

Então b/a e assim $b = \pm 1$

Logo $x \in Z/$.

(0.2.24) - Lema - Sejam R_1 um anel comutativo com unidade e R um subanel de R_1 tal que $1_{R_1} \in R$. As seguintes afirmações são equivalentes:

i) $x \in R_1$ é inteiro sobre R

ii) $R[x]$ é um R-módulo com geração finita

iii) $R[x]$ está contido em um subanel C de R_1 tal que C é um R-módulo com geração finita.

iv) Existe um $R[x]$ - módulo fiel M que é de geração finita como R-módulo.

(0.2.25) - Lema - Sejam $R \subset R_1 \subset R_2$ anéis comutativos com unidade. Se R_1 é inteiro sobre R e R_2 é inteiro sobre R_1 então R_2 é inteiro sobre R.

Prova - Seja $x \in R_2$. Então existem $b_1, b_2, \ldots, b_n \in R_1$ tais que:

$$x^n + b_1 x^{n-1} + \ldots + b_n = 0$$

Pelo lema (0.2.24), o anel $R' = R[b_1, \ldots, b_n]$ é um R-módulo com geração finita e $R'[x]$ é um R_1-módulo com

geração finita pois x é inteiro sobre R_1. Assim $R'[x]$ é um R-módulo com geração finita. Pelo lema anterior, x é inteiro sobre R.

(0.2.26) - Lema - Sejam $R \subset R_1$ anéis e seja C o fecho inteiro de R em R_1. Então C é integralmente fechado R_1.

(02.27) - Lema - Sejam $R \subseteq R_1$ domínios de integridade. Suponha que R_1 é inteiro sobre R. Então R_1 é um corpo se, e somente se, R é um corpo.

(0.2.28) - Lema - Sejam $R \subseteq R_1$ anéis comutativos com unidade. Suponha que R_1 é inteiro sobre R. Se S é um sistema multiplicativamente fechado de R, então $S^{-1}R_1$ é inteiro sobre $S^{-1}R$.

(0.2.29) - Lema - Seja R um domínio de integridade. As seguintes afirmações são equivalentes:

i) R é integralmente fechado

ii) R_p é integralmente fechado para cada ideal primo P, de R.

iii) R_m é integralmente fechado para cada ideal maximal m de R.

Prova - Sejam K o corpo de frações de R e C o

fecho integral de R em K. Considere a aplicação.

$$f : R \longrightarrow C$$

$$x \longmapsto x$$

Então R é integralmente fechado se, e somente se, f é sobrejetiva. Pelo lema anterior R_p é integralmente fechado se, e somente se:

$$f_p : R_p \longrightarrow S^{-1}C \quad , \qquad (S = R - P)$$

$$\frac{x}{s} \longmapsto \frac{x}{s}$$

é sobrejetiva.

Assim, para provarmos o lema, basta provarmos que as três afirmações abaixo são equivalentes:

i) $f : R \to C$ é sobrejetiva

ii) $f_p : R_p \to S^{-1}C$ é sobrejetiva $(S = R - P)$

iii) $f_m : R_m \to S^{-1}C$ é sobrejetiva $(S_1 = R-m)$

Provaremos estas equivalências provando o lema mais geral:

(0.2.30) - Lema - Sejam R um anel, M e N dois R-módulos e $\phi : M \to N$ um homomorfismo de R-módulo. As seguintes proposições são equivalentes:

i) ϕ é sobrejetiva

ii) $\phi_p : M_p \to N_p$ é sobrejetiva para cada ideal primo P.

iii) $\phi_m : M_m \to M_m$ é sobrejetiva para cada ideal maxi-

mal m.

Prova - i) $\longrightarrow$ ii)

Seja $y \in N_p$. Assim $y = y_1/p$ onde $y_1 \in M$ e $p \in R-P$. Como $\phi: M \to N$ é sobrejetiva existe $x_1 \in M$ tal que $\phi(x_1) = y_1$. Tome $x_1/p \in M_p$. Então $\phi_p(x_1/p) = \frac{\phi(x_1)}{p} = \frac{y_1}{p} = y$. Logo ϕ_p é sobrejetiva

ii) $\longrightarrow$ iii)

É óbvio.

iii) $\longrightarrow$ i)

Como $\phi_m : M_m \quad N_m$ é sobrejetiva, temos que $N_m/\phi_m(M_m) = 0$.

Mas

$$\frac{N_m}{\phi_m(M_m)} = \frac{N_m}{\phi(M)_m} = \left(\frac{N}{\phi(M)}\right)_m .$$

Assim $(N/\phi(M))_m = 0$, para cada m.

Pelo lema (0.2.20) $N/\phi(M) = 0$. Logo $N = \phi(M)$ e, consequentemente, ϕ é sobrejetiva.

(0.2.31) - Definição - Sejam K e L dois corpos. Nós dizemos que L é uma extensão de K se L K.

(0.2.32) - Definição - A dimensão de L sobre K(como espaço vetorial) é chamada o grau de L sobre K e é denotada por $[L:K]$. Se $[L:K]$ é finito então dizemos que L é uma extensão finita de K. Caso contrário dizemos que L é uma extensão infinita de K.

(0.2.33) - Definição - Sejam L e K dois corpos tais que L é uma extensão de K. Dizemos que $a \in L$ é algébrico sobre K se, e somente se, existem $a_0, a_1, \ldots, a_n$ em K, nem todos nulos, tais que:

$$a_n a^n + a_{n-1} a^{n-1} + \ldots + a_0 = 0.$$

Se todo elemento de L é algébrico sobre K, dizemos que L/K é uma extensão algébrica.

(0.2.34) - Definição - Se L é uma extensão de K e $x \in L$, então o polinômio mínimo de x em $K[X]$ é o único polinômio mônico em $K[X]$ que se anula em x.

0.2.35) - Definição - Dois elementos x e y de uma mesma extensão L de um corpo K são ditos conjugados sobre K se e somente se, eles são algébricos sobre K e têm o mesmo polinômio mínimo sobre K.

(0.2.36) - Definição - Se K é um corpo, um polinômio irredu

tível f(X) em K [X] é separável se f'(X) ≠ 0. Um polinômio qualquer é separável se todos os seus fatores irredutíveis o são.

(0.2.37) - Definição - Sejam L uma extensão do corpo K e x um elemento de L algébrico sobre K, x é separável sobre K se seu polinômio minimal é separável em K [X] . Se L é uma extensão algébrica de K e todo elemento de L é separável sobre K dizemos que L/K é separável.

(0.2.38) - Definição - Sejam K um corpo de características p ≠ 0 e L uma extensão algébrica de K. Um elemento x em L é dito puramente inseparável sobre K se existe n ∈ ℕ tal que x^{p^n} pertence a K. L é uma extensão puramente inseparável de K se, e somente se, todo elemento de L é puramente inseparável sobre K.

(0.2.39) - Lema - Se L é uma extensão finita e puramente inseparável de K então o grau [L:K] é uma potência de p (p = característica de K).

(0.2.40) - Lema - Se x é separável e puramente inseparável sobre K, então x ∈ K.

(0.2.41) - Definição - Seja L uma extensão do corpo K. Então

o fecho separável de K em L é o conjunto K_S de todos os elementos de L que são separáveis sobre K.

(0.2.42) - Lema - Seja L uma extensão algébrica de K.Então L pode ser obtido como uma extensão separável seguida de uma extensão puramente inseparável.

(0.2.43) - Definição - Uma extensão L de K é dita uma extensão normal de K se L é algébrica sobre K e se todo polinômio irredutível de $K[x]$ que tem uma raiz em L, tem todas as raízes em L.

(0.2.44) - Lema - Seja L uma extensão finita de K. Então existe uma extensão finita e normal F de K que contém L e que é a menor extensão normal de K que contém L.

(0.2.45) - Lema - Sejam R um domínio integralmente fechado,K seu corpo de frações, L uma extensão algébrica finita e separável de K e R' o fecho integral de R em L. Então existe uma base $v_1,\ldots,v_n$ de L sobre K tal que $R' \subset \sum_{i=1}^{n} R_{vi}$.

Prova - Se v é um elemento de L, então v é algébrico sobre K e portanto existem $a_o,\ldots,a_r$ em R tais que

$a_o v^r + a_1 v^{r-1} + \ldots + a_r = 0$.

Multiplicando esta equação por a_o^{r-1} teremos

$$a_o^r v^r + a_1 a_o^{r-1} v^{r-1} + \ldots + a_o^{r-1} a_r = 0,$$

o que nos dá:

$$(a_o v)^r + a_1 (a_o v)^{r-1} + \ldots + a_o^{r-1} a_r = 0$$

Assim $a_o v$ é inteiro sobre R, e portanto pertence a R'.

Então se $v_1, v_2, \ldots, v_n$ é uma base de L sobre K, podemos multiplicar cada v_i por um a_i, conveniente, para obter uma base $u_1, u_2, \ldots, u_m$ de L sobre K tal que u_i esteja em R' para cada i.

Seja T o traço de L sobre K. Posto que L é uma extensão separável de K, a forma bilinear:

$$(x,y) \longmapsto T(xy)$$

em L (considerado como um espaço vetorial sobre K) é não degenerada e portanto temos uma base dual $v_1', \ldots, v_n'$ de L sobre K, definida por:

$$T(u_i v_j') = \delta_{ij}$$

Seja $x \in R'$. Assim

$$x = \sum_{j=1}^{n} x_j v_j' \quad , \quad x_j \in K$$

Temos que $xu_i \in R'$ (posto que $u_i \in R'$) e, portanto, $T(xu_i) \in R$

Mas,

$$T(xu_i) = \sum_{j=1}^{n} T(x_j u_i v_j) = \sum_{j=1}^{n} x_j T(u_i v_j') = \sum_{j=1}^{n} x_j \delta_{ij} = x_i$$

Logo $x_i \in R$, pois $T(xu_i) \in R$. E assim

$$R' \subset \sum_{j=1}^{n} Rv_j .$$

(0.2.46) - Lema - Se R é um domínio integralmente fechado então $R[X]$ também o é.

Prova - Para tal, provaremos inicialmente que, se K é o corpo de frações de R, então $K[x]$ é integralmente fechado em $K(X)$ e então mostraremos que $R[X]$ é integralmente fechado em $K[X]$. E assim, pelo lema (0.2.25), $R[X]$ é integralmente fechado.

Para esta última parte mostraremos que se R' é o fecho integral de R em R_1, então $R'[X]$ é o fecho integral de $R[X]$ em $R_1[X]$.

Para tanto mostraremos, inicalmente, o seguinte:

(0.2.47) - Lema - Sejam $R \subset R_1$ domínios de integridade e R' o fecho integral de R em R_1. Se f e g são dois polinômios em $R_1[X]$, tais que o produto f.g está em $R'[X]$, então f e g estão em $R'[X]$.

Prova - Seja L um corpo contendo o corpo de raízes de f e g. Então, em L, podemos escrever

$$f(x) = \prod_{i=1}^{n} (x - a_i)$$

e

$$g(x) = \prod_{j=1}^{m} (x - b_j)$$

Cada a_i e cada b_j são raízes do polinômio f.g e portanto, são inteiros sobre R. Logo os coeficientes de f.g são inteiros sobre R' e, consequentemente, f e g são polinômios em R' $[X]$.

Continuação da Prova do Lema (0.2.46)

Seja $h \in K(x)$ inteiro sobre $K[X]$.

Então existem $a_1, a_2, \ldots a_n \in K[X]$ tais que

$$h^n + a_1 h^{n-1} + \ldots + a_n = 0$$

Como $h \in K(x)$ podemos escrever $h = f/g$ onde f e g estão em $K[X]$ e são tais que m.d.c. $(f,g) = 1$. Assim podemos escrever:

$$\frac{f^n}{g^n} + a_1 \frac{f^{n-1}}{g^{n-1}} + \ldots + a_n = 0$$

O que nos dá:

$$f^n + a_1 g f^{n-1} + \ldots + a_n g^n = 0$$

ou melhor:

$$f^n = -g(a_1 f^{n-1} + \ldots + a_n g^{n-1}).$$

E assim g/f^n o que é um absurdo, a menos que g seja constante.

Logo $h \in K[X]$

Tomemos, agora, h pertencente a $K[X]$ e inteiro sobre $R[X]$.

Então existem $b_1, b_2, \ldots, b_m$ em $R[X]$, tais que:

$$h^m + b_1 h^{m-1} + \ldots + b_m = 0$$

Seja r um inteiro maior que m e maior que o grau dos bi's, (observe que devemos ter r também maior que o grau de h, pois algum b_i deve ter grau maior do que ou igual ao grau de h)

Escreva $f_1 = h - x^r$.

Assim

$$(f_1 + x^r)^m + b_1(f_1 + x^r)^{m-1} + \ldots + b_m = 0.$$

O que nos dá:

$$f_1^m + h_1 f_1^{m-1} + \ldots h_m = 0$$

onde $h_m = (x^r)^m + b_1(x^r)^{m-1} + \ldots b_m \in R[X]$:

Mas

$$h_m = - f_1(f_1^{m-1} + h_1 f_1^{m-2} + \ldots + h_{m-1}) .$$

Comparando com o lema (0.2.48), teríamos $R = R$, $R_1 = K$, e como R é integralmente fechado $R' = R$.

Logo, como $-f_1$ e $f_1^{m-1} + h_1 f_1^{m-2} + \ldots + h_{m-1}$ são polinômios mônicos em $K[X]$, teremos, pelo lema (0.2.47), $-f_1$ pertencente a $R[X]$. E assim $h \in R[X]$. Seguindo-se o resultado.

(0.2.48) - Definição - Sejam R um domínio de integridade e K seu corpo de frações. R é um anel de valorização de K se, e

somente se, para cada $x \neq 0$, em K, tivermos x em R ou x^{-1} em R.

(0.2.49) - Definição - Um anel comutativo e com unidade R, é dito noetheriano se, e somente se, satisfaz às três condições equivalentes:

i) cada conjunto, não vazio, de ideais de R tem um elemento maximal.

ii) cada cadeia ascedente de ideais de R é estacionária.

iii) cada ideal de R é finitamente gerado.

(0.2.50) - Exemplos - i) Todo corpo é um anel noetheriano.

ii) Todo domínio principal é noetheriano

(0.2.51) - Contra-exemplo - Se K é um corpo e $x_1, x_2, \ldots$ são indeterminadas sobre K então o anel $K[x_1, x_2, \ldots]$ não é noetheriano, pois a cadeia

$$(x_1) \subset (x_1, x_2) \subset \ldots \subset (x_1, x_2, \ldots x_n) \subset \cdots$$

é uma cadeia ascedente de ideais que não é estacionária.

(0.2.52) - Lema - Sejam R_1 um anel e R um subanel de R_1. Se

R é noetheriano e R_1 é um R-módulo finitamente gerado então R_1 é um anel noetheriano.

(0.2.53) - Lema - Se R é noetheriano e S é um sistema multiplicativamente fechado de R então $S^{-1}R$ é noetheriano.

Prova - Todo ideal de $S^{-1}R$ é da forma $S^{-1}A$ onde A é um ideal de R. Como R é noetheriano. A é finitamente gerado. Sejam $x_1,\ldots,x_n$ geradores de A. É claro que $S^{-1}A$ é gerado por $x_1/1,\ldots, x_n/1$.

Assim todo ideal de $S^{-1}R$ é finitamente gerado. Logo $S^{-1}R$ é um anel noetheriano.

(0.2.54) - Lema - Se R é um anel noetheriano, então $R[X]$ também o é.

Prova - Dado um ideal A de $R[X]$,.denote por $d_n(A)$ o conjunto formado pelos coeficientes líderes dos polinômios de grau n pertencentes a A unido com o elemento 0 (zero). As seguintes propriedades são verificadas.

i) para todo inteiro $n \geq 0$ $d_n(A)$ é um ideal de R

Com efeito, sejam a e b dois elementos de $d_n(A)$. Ou $a + b = 0$ e neste caso pertence a $d_n(A)$ ou $a + b \neq 0$. Neste caso, sejam $f = ax^n + a_1x^{n-1}+\ldots+a_n$ e $g = bx^n+\ldots+b_n$ dois polinômios de A com coeficientes líderes a e b, respectivamente. Então f + g é um polinômio de A cujo coeficiente lí-

der é a + b. Assim a + b pertence a $d_n(A)$.

Se c pertence a R e a pertence a $d_n(A)$ então existe em A um polinômio f de grau n, com coeficiente líder a. Assim cf é um polinômio de grau n, em A, com coeficiente líder ca e, portanto, ca pertence a $d_n(A)$. Logo $d_n(A)$ é um ideal de R.

ii) fixando o ideal A , $d_n(A)$ é uma função crescente de n.

De fato, se $a \in d_n(A)$, então existe um polinômio f, em A, da forma $f = ax^n + \ldots + a_n$. Como A é um ideal, o polinômio xf(x) está em A, e seu coeficiente líder é a. Logo $a \in d_{n+1}(A)$.

iii) para um inteiro n , fixo, $d_n(A)$ é uma função crescente de A, isto é, se A e B são dois ideais de $R[X]$ tais que $A \subset B$, então $d_n(A) \subseteq d_n(B)$.

Isto é óbvio.

iv) se $A \subseteq B$ e se $d_n(A) = d_n(B)$ para todo inteiro $n \geq 0$ então A = B.

Seja $f \in B$. Provaremos que $f \in A$, por indução sobre o grau de f.

Se o grau de f for zero, teremos:

$$f \in B \cap R = d_o(B) = d_o(A) = A \cap R$$

E portanto $f \in A$.

Suponha que o resultado vale para todo polinômio com grau menor que n.

Se f é um polinômio de grau n, teremos

$$f = ax^n + a_1x^{n-1} + \ldots + a_n.$$

E assim

$$a \in d_n(B) = d_n(A).$$

Portanto existe um polinômio $g \in A$ tal que

$$g = ax^n + b_1x^{n-1} + \ldots + b_n.$$

Tome o polinômio $h = f - g$.

h pertence a B, pois f está em B e g está em A, e A B. Como o grau de h é menor do que ou igual a n-1, teremos, por hipótese de indução, h pertencente a A.

Logo

$$f = (f-g) + g \in A$$

Provemos, finalmente, que $R[X]$ é noetheriano.

Seja $A_1 \subset A_2 \subset \ldots \subset A_n \subset \ldots$, uma cadeia crescente de ideais de $R[X]$. Assim temos o seguinte diagrama:

$$\begin{array}{ccccccc}
d_o(A_1) & \subset & d_o(A_2) & \subset & \ldots & \subset & d_o(A_n) \quad \ldots \\
\cap & & \cap & & & & \cap \\
d_1(A_1) & \subset & d_1(A_2) & \subset & \ldots & \subset & d_1(A_n) \quad \ldots \\
 & & \cap & & & & \cap \\
\vdots & & \vdots & & & & \vdots \quad \vdots \\
\cap & & \cap & & & & \cap \\
d_p(A_1) & \subset & d_p(A_2) & \subset & \ldots & \subset & d_p(A_n) \quad \ldots \\
\vdots & & \vdots & & & & \vdots \quad \vdots \\
\vdots & & \vdots & & \ldots & & \vdots \quad \vdots \\
\vdots & & \vdots & & & & \vdots \quad \vdots
\end{array}$$

Como R é noetheriano, se considerarmos o conjunto de todos os $d_p(A_n)$, existe um elemento maximal $d_{po}(A_{no})$. Cada linha do diagrama, desde a primeira até a p_o-1 - ésima estaciona em um índice, digamos j_i. Seja $q = \max \{j_i , n_o\}$ Assim $d_{po}(A_{no}) = d_{po}(A_q)$. Considerando agora as colunas, desde a primeira até a q-ésima, encontramos um índice r a partir do qual todas estas colunas estacionam. Assim se $p \geq r$ e $n \geq q$ teremos $d_p(An) = d_r(A_q)$.

Pela observação iv) $A_n = A_q$ para todo $n \geq q$, e assim a cadeia $A_1 \subset A_2 \subset \ldots \subset A_n \subset \ldots$ é estacionária.

Logo $R[x]$ é noetheriano.

(0.2.55) Definição - Um ideal A em um anel R é dito primário se:

i) $A \neq R$

ii) se $xy \in A$ então $x \in A$ ou $y^n \in A$ para algum $n > 0$

(0.2.56) Definição - Um ideal A em um anel R é dito irredutível se, e somente se,

$A = B \cap C \longrightarrow A = B$ ou $A = C$.

(0.2.57) Lema - Em um anel noetheriano R todo ideal é uma interseção finita de ideais irredutíveis.

Prova - Suponha que não.

Seja Σ o conjunto dos ideais de R para os quais o lema é falso.

Desde que R é noetheriano e estamos supondo $\Sigma = \emptyset$, Σ tem elemento maximal. Seja A esse elemento e portanto teríamos A = B C com A B e A C. Pela maximalidade de A, B e C seriam interseção finita de ideais irredutíveis e portanto A também o seria.

Logo o lema é sempre verdadeiro.

(0.2.58) Lema - Em um anel noetheriano cada ideal irredutível é primário.

Prova - Seja A um ideal de R.

Passando ao anel quociente R/A é suficiente provar que se (0) é um ideal irredutível então é primário.

Seja xy = 0 com $y \neq 0$

Considere a cadeia $Ann(x) \subset Ann(x^2) \subset \ldots$. Como R é noetheriano esta cadeia é estacionária, isto é, existe n tal que $Ann(x^n) = Ann(x^{n+1}) = \ldots$.

Afirmo: $(x^n) \cap (y) = (0)$

De fato, se $a \in (y)$ então ax = 0. Por outro lado se $a \in (x^n)$ então $a = bx^n$, o que nos dá $ax = bx^{n+1} = 0$. Assim $b \in Ann(x^{n+1}) = Ann(x^n)$. Portanto $a = bx^n = 0$. Provando o resultado.

Como (0) é irredutível e $y \neq 0$ teremos $x^n = 0$.

Logo (0) é um ideal primário.

(0.2.59) - Lema - O radical de um ideal primário é primo.

(0.2.60) - Lema - Em um anel noetheriano R todo ideal contém uma potência de seu radical.

(0.2.61) - Definição - Seja R um Domínio de Integridade . Dizemos que a dimensão de Krull de R(Kim R) é 1 se todo ideal primo, não nulo, de R é maximal.

(0.2.32) - Definição - Sejam R um Domínio de Integridade e K seu corpo de frações. Um R submódulo M de K é um ideal fracionário de R se, e somente se, existe x em K' tal que $xM \subset R$. Assim se M é um ideal fracionário de R então $M=x^{-1}A$ onde A é um ideal próprio de R e x está em K.

(0.2.62) - Definição - Sejam R um domínio de integridade e K seu corpo de frações. Um R-submódulo M de K é um ideal inversível de R se, e somente se, existe um submódulo N de K tal que M . N = R.

(0.2.63) - Lema - Se M é um ideal inversível então M é finitamente gerado.

Estes são alguns dos resultados que devem ser

conhecidos para uma compreensão deste trabalho.

Todos os fatos relacionados com teoria dos números podem ser encontrados em [5] enquanto os outros podem ser encontrados em [3] ou [4].

1 - CARACTERIZAÇÕES PARA ANÉIS DE DEDEKIND

(1.1) - Introdução

Nosso objetivo, neste capítulo, é provar que em anéis de Dedekind é possível definir uma teoria de divisores e, como consequência, que estes são anéis de Krull.

Em todo este trabalho denotaremos por R um domínio de integridade e por K seu corpo de frações. Ideais próprios de R são, como no capítulo anterior, ideais diferentes de 0 e de R.

(1.2) - Definição e Exemplos

(1.2.01) - Definição - Um domínio de integridade R é um anel de Dedekind se, e somente se, todo ideal próprio de R se escreve como um produto finito de ideais primos.

(1.2.02) - Exemplos - i) O anel dos inteiros, $\mathbb{Z}$, é um anel de Dedekind.

ii) Mais geralmente todo Domínio Principal(D.P) é um anel de Dedekind.

iii) Se R é um anel de Dedekind e S é um sistema

multiplicativamente fechado de R, então $S^{-1}R$ é um anel de Dedekind. De fato, dado um ideal $\bar{A}$ de $S^{-1}R$ então $\bar{A} = S^{-1}A$, onde A é um ideal de R. Como R é um anel de Dedekind, $A = P_1 \ldots P_n$ onde, para cada i, é um P_i ideal primo de R. Assim $\bar{A} = S^{-1}(P_1 \ldots P_n) = (S^{-1}P_1)\ldots(S^{-1}P_n)$, onde $S^{-1}P_i$ ou é $S^{-1}R$ ou é um ideal primo de $S^{-1}R$.

iv) Será mostrado no capítulo II que se R é um anel de Dedekind e L é uma extensão finita do seu corpo de frações, então o fecho integral de R em L é também um anel de Dedekind.

v) No último capítulo deste trabalho daremos um exemplo menos elementar de anel de Dedekind.

(1.3) - Unicidade da Decomposição

Mostraremos, agora, que a decomposição na definição (1.2.01) é única e que todo ideal fracionário, de um anel de Dedekind é inversível. O que nos dá uma outra caracterização para anéis de Dedekind.

Para tanto basta nos atermos aos ideais próprios de R, já que se M é um ideal fracionário de R, então M=(xR)A onde A é um ideal próprio de R e x é um elemento do corpo de frações de R. Desde que (xR) é inversível, se A for inversível M também o será.

Estudemos os ideais inversíveis de R.

(1.3.01) - Lema - Em um domínio de integridade R, se um ideal A se decompõe em um produto de ideais primos inversíveis então esta decomposição é única.

Prova - A prova deste lema será feita por indução sobre o número n de ideais primos P que aparecem em uma certa decomposição de A.

Para n = 1. Neste caso A é um ideal primo e suponha que $\prod_{j=1}^{m} Q_j$ seja uma outra decomposição de A.

Assim existe j_o tal que $Q_{j_o} \subset A$. De fato, se $Q_j \neq A$ para todo j, existiria $x = x_1 \ldots x_n$ em A, com x_j em $Q_j - A$, o que não pode ocorrer pois A é um ideal primo. Logo existe j_o tal que $Q_{j_o} \subset A$. Como $A \subset Q_j$ para todo j segue-se que $A = Q_{j_o}$

Suponha, sem perda de generalidade, que $j_o = 1$

Assim $A = AQ_2 \ldots Q_m$

Usando a hipótese de A ser inversível e o fato de que $Q_2 \ldots Q_m \subset Q_j$ para todo $j = 2,3,\ldots, m$ temos que m=1. Valendo a unicidade da decomposção.

Suponha que o resultado vale para $n = k - 1$.

Para n = k, suponha que tenhamos

$$(1.3.02) \qquad A = \prod_{i=1}^{k} P_i = \prod_{j=1}^{m} Q_j$$

Seja P_{i_o} um elemento minimal de $\{P_1, P_2, \ldots, P_k\}$. Então existem j_o e i_1 tais que $Q_{j_o} \subset P_{i_o}$ e $P_{i_s} \subset Q_{j_o}$. Pela minimalidade de P_{i_o}, teremos $P_{i_1} = P_{i_o}$ e, consequentemente $Q_{j_o} = P_{i_o}$.

Assim cancelando na igualdade (1.3.02) P_{i_o} com Q_{j_o}, podemos, após uma reorganização nos índices, escrever:

$$(1.3.03) \qquad \prod_{i=1}^{k-1} P_i = \prod_{j=1}^{m-1} Q_j$$

Por hipótese de indução $k - 1 = m - 1$ e $P_i = Q_i$ para cada $i = 1,2,\ldots,k - 1$.

Logo $m = k$ e $P_i = Q_i$ para todo $i = 1,\ldots,K$, seguindo-se o resultado.

Se provarmos que em anéis de Dedekind todo ideal primo é inversível, teremos provado a unicidade da decomposição. Para tanto necessitaremos do seguinte:

(1.3.04) - Lema - Em um anel de Dedekind R todo ideal primo inversível é maximal.

Prova - Sejam P um ideal primo inversível de R e b pertencente a $R - P$. Sejam ainda os ideais:

$$A = (b) + P \quad e \quad B = (b^2) + P .$$

Como R é um domínio de Dedekind, teremos:

$$A = (b) + P = P_1 \ldots P_m \ , \ P_i \supsetneq B \text{ para cada } i$$

e

$$B = (b^2) + P = Q_1 \ldots . Q_n \ , \ Q_j \supsetneq P \text{ para cada } j.$$

Passando ao anel quociente R/P (que é ainda um

anel de Dedekind) teremos:

$$A/P = (\overline{b}) = \overline{P}_1 \ldots . \overline{P}$$

e

$$B/P = (\overline{b}^2) = \overline{Q}_1 \ldots . \overline{Q}_m$$

Desde que $(\overline{b})$ e $(\overline{b}^2)$ são ideais fracionários inversíveis, pois são ideais principais, os ideais $\overline{P}_i$ e $\overline{Q}_j$ também o são. Pelo lema (1.3.01) ocorre a unicidade da decomposição. Mas $(\overline{b}^2) = (\overline{b})^2$. Assim n = 2m e para cada i existem j_{i_o} e j_{i_1} tais que $\overline{Q}_{j_o} = \overline{Q}_{j_1} = \overline{P}_i$

Daí, pelo teorema da correspondência entre ideais de R e R/P, o mesmo acontece com os ideais P_i e Q_j.

Então

$$P \subset (b^2) + P = \left[(b) + P \right]^2 = (b)^2 + (b)\,P + P^2.$$

E como $P(\ (b) + P) \subset P$, basta-nos provar que $P \subset P((b)+P)$ pois neste caso haverá a igualdade $P = P((b) + P)$ e, desde que P é inversível, $(b) + P = R$. Assim P será maximal.

Provemos que $P \subset P\ (\ (b) + P)$

Temos que $P \subset (b)^2 + (b)\,P + P^2$. Então para todo p em P vale:

(1.3.05) $p = rb^2 + bp + \gamma$, onde $\gamma \in P^2$

Se $rb^2 \neq 0$, como P é um ideal primo e $rb^2 \in P$ (pois $rb^2 = p - p'b - \gamma$) devemos ter $r \in P$ ou $b \in P$. Isto nos dá que a componente de p em $(b)^2$, na expressão (1.3.05), pode

ser colocada em P(b) ou P^2. Assim $P \subset (b)\ P + P^2 = P((b)+P)$

Seguindo-se daí o resultado.

Passemos a tão falada unicidade.

(1.3.06) - Teorema - (Matusita) - Se R é um anel de Dedekind então todo ideal próprio de R se escreve, de maneira única, como um produto de ideais primos inversíveis.

Demonstração - Basta mostrarmos que cada ideal primo P de R é inversível.

Tome $b \in P$ e considere o ideal $(b) = P_1 \ldots P_n$.

Como (b) é inversível cada ideal P_i também o é.

Desde que $P \supset (b) = P_1 \ldots P_n$, temos que $P \supset P_{i_o}$ para algum i_o. Portanto pela maximalidade de P_{i_o} temos $P = P_{i_o}$

Logo P é inversível.

(1.3.07) - Observe que nós provamos que todo ideal primo de um anel de Dedekind R, é maximal. Em outras palavras, provamos que se R é um anel de Dedekind então a dimensão de Krull de R (Kdim R) é 1.

(1.3.08) - Corolário - Seja R um anel de Dedekind que não é corpo, então R é Noetheriano.

Prova - Seja A um ideal próprio de R. Provare - mos que A é finitamente gerado.

Como A é inversível existe o ideal fracionário A^{-1}, de R, tal que $A.A^{-1} = R$

Assim $1 = \sum_{i=1}^{n} a_i b_i$ com $a_i \in A$ e $b_i \in A^{-1}$

Então se $a \in A$ teremos:

$$a = \sum_{i=1}^{n} aa_i b_i = \sum_{i=1}^{n} (ab_i)a_i$$

Como $ab_i \in R$, pois $b_i \in A^{-1}$ e $a \in A$, teremos:

$$A = (a_1, \ldots, a_n)$$

Logo R é noetheriano.

O teorema (1.3.05) pode ser generalizado para:

(1.3.09) - Teorema - Seja R um anel de Dedekind. Então todo ideal fracionário M de R é inversível e pode ser escrito, de maneira única na forma:

(1.3.10)
$$M = \prod_{P = \text{primo}} P^{n_p(M)}$$

com $n_p(M)$ inteiro e quase todos nulos.

Para que tenhamos $M \subset N$ é necessário e suficiente que $n_p(M) \geq n_p(N)$ para todo ideal primo P , de R.

Além disso as relações

a) $n_p(M + N) = \min \{n_p(M), n_p(N)\}$

b) $n_p(M \cap N) = \max \{n_p(M) , n_p(N)\}$

são válidas para cada ideal primo P e mais os ideais (M : N) e $M \cdot N^{-1}$ são iguais e, consequentemente $n_p(M : N) = n_p(M) - n_p(N)$ para cada P.

Demonstração - Como todo ideal fracionário pode ser escrito na forma

$$M = A \cdot B^{-1}$$

onde A e B são ideais próprios de R, e como A e B podem ser escritos, de maneira única, como um produto de ideais primos inversíveis, M será inversível e vale a decomposição na forma do teorema (1.3.08).

Para completarmos a demonstração usaremos o seguinte fato:

$n_p(M.N) = n_p(M) + n_p(N)$ para cada P.

Seja, agora, $M \subseteq N$.

Então $MN^{-1} \subseteq R$. Assim $n_p(MN^{-1}) \geq 0$ para cada ideal primo P. Mas $n_p(M.N^{-1}) = n_p(M) + n_p(N^{-1}) = n_p(M) - n_p(N)$. Logo $n_p(M) \geq n_p(N)$.

Para provarmos a) considere o ideal M + N.

Este ideal é, por definição, o menor ideal fracionário contendo M e N. Assim $M \subset M + N$ e $N \subset M + N$. Pelo que foi visto $n_p(M+N) \leq n_p(M)$ e $n_p(M+N) \leq n_p(N)$

Então $n_p(M+N) \leq \min \{n_p(M), n_p(N)\}$

Para a outra desigualdade, tomemos o ideal

$A = P_1^{\alpha_1} \ldots P_n^{\alpha_n}$, onde $\alpha_i = \min\{n_{p_i}(M), n_{p_i}(N)\}$

Pelo que já foi provado, $A \subset M$ e $A \subset N$. Assim $A \subset M + N$. Logo $n_p(M + N) \geq n_p(A) = \min\{n_p(M), n_p(N)\}$

Segue-se, das desigualdades acima que

$n_p(M + N) = \min\{n_p(M), n_p(N)\}$

Para b) tome o ideal $M \cap N$

Temos que $M \cap N \subset M$ e $M \cap N \subset N$. Assim

$n_p(M \cap N) \geq n_p(M)$ e $n_p(M \cap N) \geq n_p(N)$, o que nos dá:

$n_p(M \cap N) \geq \max\{n_p(M), n_p(N)\}$

Tomemos o ideal

$B = P_1^{\beta_1} \ldots P_r^{\beta_r}$ onde $\beta_i = \max\{n_p(M), n_{p_i}(N)\}$

Assim $B \subset M$ e $B \subset N$. Como $M \cap N$ é o maior ideal fracionário contido em M e N termos $B \subset M \cap N$. Logo $n_p(M \cap N) \leq \max\{n_p(M), n_p(N)\}$, seguindo-se que $n_p(M \cap N) = \max\{n_p(M), n_p(N)\}$

Finalmente, para a última afirmação do teorema (1.3.08) devemos notar que:

$$N.M^{-1} = N\,(R:M)$$

e como

$$[\,N.(R:M)\,]\,.\,M = N\,[(R:M).M] \subset N.R \subset N,$$

segue-se que

$$NM^{-1} \subseteq (N:M).$$

Por outro lado

$$(N:M) = (N:M).R = (N:M)\,MM^{-1} \subseteq N\,M^{-1}$$

Assim $(N:M) = NM^{-1}$, seguindo-se o resultado.

(1.4) - Aplicações

(1.4.01) - Definição - Seja K um corpo. Uma valorização discreta em K é uma aplicação v de $K' = K - \{0\}$ sobre $\mathbb{Z}$ tal que:

a. $v(xy) = v(x) + v(y)$

b. $v(x + y) \geq \min \{v(x) , v(y)\}$

Assim se R é um anel de Dedekind com corpo de frações K, pode-se definir, para cada ideal primo P de R, uma valorização

$$v_p : K' \longrightarrow \mathbb{Z}$$

$$x \longrightarrow n_p(x) \text{ , onde } n_p(x) = n_p(\ (x)\ )$$

É fácil ver que:

(1.4.02) - Para todo x em K', o número de $n_p(x)$, tais que $n_p(x) \neq 0$ é finito.

(1.4.03) - x está em R se, e somente se, $n_p(x) \geq 0$ para todo p.

(1.4.04) - Dados os ideais primos $P_1, P_2, \ldots, P_n$ com respectivas valorizações $v_1, \ldots, v_n$, e os inteiros $K_1, \ldots, K_n$ existe um x em K* tal que $v_i(x) = K_i$ e $v_p(x) \geq 0$ para todo ideal primo P , $P \neq P_i$.

(1.4.05) - Nota - A afirmação (1.4.03) caracteriza o anel R enquanto que a afirmação (1.4.04) é conhecida como CONDIÇÃO DE INDEPENDÊNCIA FRACA.

(1.4.02) e (1.4.03) são óbvios.

Para demonstrarmos (1.4.04) precisaremos do seguinte:

(1.4.06) - Lema - Dados os ideais A , $P_1, \ldots, P_m$ de R, com $A \neq 0$ e $P_1, \ldots, P_m$ ideais primos, existe x em $R' = R - \{0\}$ tal que x pertence a A e $(x) = A \cdot B$, onde B é um ideal de R tal que não está contido e é diferente de P_i, para todo $i = 1,2,\ldots,m$.

Prova - Dado o ideal A, de R, podemos escrever $A = P_1^{K_1} \ldots P_n^{K_n}$ onde $n \geq m$

Sejam os ideais:

$$A' = AP_1 \ldots P_m$$

e

$$A_i = A'P_i^{-1} = AP_1 \ldots \hat{P}_i \ldots P_m, \text{ para cada } i=1,\ldots,m.$$

É claro que $A_i \subsetneq A'$ $(A = P_i A_i \subset A_i)$.

Para cada i, seja $x_i \in A_i - A'$. Então $n_{p_i}(x_i) = K_i$, isto é, $x_i \in P_i^{K_i}$ mas $x_i \notin P_i^{K_i+1}$. (Basta ver que $(x_i) \subset A_i$, o que nos dá $n_{p_i}(x_i) \geq n_{p_i}(A_i) = K_i$. Se $n_{p_i}(x_i) \geq K_i + 1$ teríamos $x_i \in A'$. Logo $n_{p_i}(x_i) = K_i$). Agora se $i \neq j$ é fácil ver que $n_{p_i}(x_j) \geq K_j + 1$

Faça $x = x_1 + x_2 + \ldots + x_m$, e suponha que $n_{p_i}(x) = r_i$. Afirmo que $r_i = K_i$. De fato:

$$(x) = (x_1 + \ldots + x_m) \subset (x_1) + (x_2) + \ldots + (x_m).$$

Assim

$$n_{p_i}(x) \geq n_{p_i}((x_1) + (x_2) + \ldots + (x_m)) = \min\{n_{p_i}(x_j)\}$$

com $j = 1, 2, \ldots, m$.

Então $n_{p_i}(x) \geq K_i$.

Uma vez que $(x_1 + x_2 + \ldots + \hat{x}_r + \ldots + x_m) \in P_i^{K_i+1}$ e $x_i \notin P_i^{K_i+1}$, não podemos ter $n_{p_i}(x) \geq K_i + 1$, pois neste caso teríamos $(x) \subset P_i^{K_i+1}$, isto é, $x \in P_i$.

Logo $n_{p_i}(x) = K_i$, provando o lema.

Finalmente para mostrarmos a CONDIÇÃO DE INDEPENDÊNCIA FRACA, sejam

$l_i = \max\{-K_i, 0\} \geq 0$ para cada $i = 1, 2, \ldots, n$

Considere $A = P_1^{l_1} \ldots P_n^{l_n}$.

Pelo lema (1.4.06) existirá $y \in R^*$ tal que

$$(y) = P_1^{\ell_1+K_1} \ldots P_n^{\ell_n+K_n} . Q_1^{s_r} \ldots Q_r^{s_r} . Q_{r+1}^{s_{r+1}} - Q_m^{s_m}$$

com Q_i e P_i incomparáveis para todos i e j.

Tome $Z = \frac{y}{x}$ em K.

Assim:

$$(Z) = \left(\frac{y}{x}\right) = (y)\,(x)^{-1} = P_1^{\ell_1 + K_1} \ldots P_n^{\ell_n+K_n} . Q_1^{s_1} \ldots Q_r^{s_r} .$$

$$. Q_{r+1}^{s_{r+1}} \ldots Q_m^{s_m} \ldots P_1^{-\ell_1} \ldots P_n^{-\ell_n} Q_1^{-s_1} \ldots Q_r^{-s_r} =$$

$$= P_1^{K_1} \ldots P_n^{K_n} Q_{r+1}^{s_{r+1}} \ldots Q_m^{s_m}$$

Isto basta para concluir a afirmação(1.4.04)pois, como se observa, cada s_i, para $i = r + 1, \ldots m$ é maior do que ou igual a zero, uma vez que $y \in R^*$.

Como consequência das afirmações acima temos:

(1.4.07) - Proposição - Se R é um anel de Dedekind então $R = \bigcap R_p$ onde P percorre o conjunto dos ideais primos de R.

Prova - Seja $y \in \bigcap_{(p)} R_p$

Então, para cada P, existem x_p em R e s_p em R-P, tais que:

$$y = \frac{x_p}{s_p}$$

Assim, para cada P,

$$v_p(y) = v_p\left(\frac{x_p}{s_p}\right) = v_p(x_p) - v_p(s_p).$$

Como $s_p \notin P$, $v_p(s_p) = 0$. E assim

$$v_p(y) = v_p(x_p) \geq 0.$$

Pela observação (1.4.03) y pertence a R. Logo $\bigcap_{(p)} R_p \subset R$.

Por outro lado, se x pertence a R, então x pertence a R_p para todo P. Assim $R \subset \bigcap_{(p)} R_p$ para todo p. Valendo o resultado.

(1.4.08) - Proposição - Se R é um anel de Dedekind, R é integralmente fechado.

Prova - Mostraremos que R_p é integralmente fechado para cada ideal primo P de R.

Temos que $R_p = \{x \in K ; v_p(x) \geq 0\} \cup \{0\}$, portanto R_p é um anel de valorização. De fato, dado $x \in K^*$, se $v_p(x) < 0$, então $-v_p(x) > 0$. Mas $-v_p(x) = v_p(x^{-1})$. Assim x^{-1} pertence a R_p.

Para mostrarmos que R_p é integralmente fechado, seja $x \in K^*$ e suponha que x é inteiro sobre R_p. Assim existem $a_1, \ldots, a_n$ em R_p, tais que:

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \qquad (1.4.09)$$

para algum $n \in \mathbb{N}$.

Queremos mostrar que $x \in R_p$.

Como R_p é um anel de valorização, temos que $x^{-1} \notin R_p$ ou $x^{-1} \in R_p$.

i) Se $x^{-1} \notin R_p$, então $x \in R_p$ e vale o resultado.

ii) Se $x^{-1} \in R_p$, então multiplicando a igualdade (1.4.09), por x^{1-n}, teremos:

$$x + a_1 + \ldots + a_n x^{1-n} = 0$$

ou seja,

$$x = -(a_1 + \ldots + a_n x^{1-n})$$

Logo $x \in R_p$ e, portanto, R_p é integralmente fechado para cada P.

Finalmente, seja $x \in K$, inteiro sobre R.

Como $R \subset R_p$, x é inteiro sobre R_p para todo P. Desde que R_p é integralmente fechado, x pertence a R_p, para todo P.

Mas $R = \bigcap_{(P)} R_p$, portanto $x \in R$.

Logo R é integralmente fechado.

(1.5) - Uma caracterização mais convencional para anéis de Dedekind

Com a definição, para anéis de Dedekind, dada neste trabalho, pretendemos generalizar a teoria de divisores do conjunto dos inteiros, para um anel qualquer.

Agora pretendemos provar a equivalência entre a "nossa" definição e a definição convencional, encontrada por exemplo, em [4].

Provaremos também que, em anéis de Dedekind, a condição de independência fraca pode ser fortificada, o que nos dará uma outra caracretização para estes anéis.

Vejamos algumas caracterizações para anéis de Dedekind.

Mas primeiramente vejamos o:

(1.5.01) - Lema - Seja R um domínio no qual todo ideal primo não nulo é inversível. Então todo ideal A de R contém um produto de ideais primos cada um dos quais contendo A.

Prova - Seja Σ o conjunto dos ideais de R que não gozam desta propriedade.

Suponha $\Sigma \neq \emptyset$.

Seja $B_0 \subset B_1 \subset \cdots \subset B_n \subset \cdots$ uma cadeia de ideais de Σ e $B = \bigcup_{i=1}^{\infty} B_i$

B é um elemento de Σ, pois caso contrário, teríamos, $P_1 \ldots P_n \subset B$, onde os P_i são ideais primos de R e $B \subset P_i$ para todo $i = 1,2,\ldots, n$. Como os P_i são finitamente gerados, por serem inversíveis, o produto $P_1 \ldots P_n$ também o é.

Assim existiria n_o tal que B_{n_o} conteria todos os geradores de $P_1,\ldots,P_n$ e consequentemente conteria $P_1 . P_2 \ldots P_n$ o que por hipótese não ocorre. Logo B é um elemento de Σ.

Pelo lema de Zorn Σ possui elemento maximal.

Seja C um elemento maximal de Σ.

Como C não é ideal primo, pois $C \in \Sigma$, ele contém um produto D.G com $D \supset C$ e $G \supset C$ (faça $D=(x)+C$ e $G=(y)+C$ onde x e y são elementos de R tais que $x \notin C, y \notin C$ e $xy \in C$).

Pela maximalidade de C, D e G não estão em Σ. Assim $D \supset P_1 \ldots P_n$ e $G \supset Q_1 \ldots Q_m$; com $P_i \supset D$ e $Q_j \supset G$ para cada i e para cada j. O que é absurdo!

Logo $\Sigma = \emptyset$, seguindo-se o resultado.

(1.5.02) - Lema - Seja R um domínio no qual todo ideal primo não nulo é inversível. Então R é um domínio de Dedekind.

Prova - De acordo com a definição devemos provar que todo ideal A de R se escreve como um produto finito de ideais primos. Mas, pelo lema anterior, todo ideal A de R contém um produto de ideais primos cada um dos quais contendo A.

Demonstraremos este lema por indução sobre o número de fatores primos que aparecem no produto contido em A.

Se n = 1 teremos $P_1 \subset A \subset P_1$. Logo $P_1 = A$, valendo o resultado.

Suponha que o resultado é válido para n = k - 1, ou seja, suponha que, se $P_1 . P_2 \ldots P_{k-1} \subset A$, onde os P_i são i-

deais primos de R tais que $P_i \supset A$, para todo i, então $A = Q_1 \ldots Q_m$, onde os Q_j são ideais primos de R.

Para n = k, suponha que existe um ideal A' de R, contendo o produto $P_1 \ldots P_k$, de ideais primos de R, com cada P_i contendo A'.

Como cada P_i é inversível, teremos $P_2 \ldots P_K \subset P_1^{-1} A' \subset R$ e, por hipótese de indução, $P_1^{-1} A' = Q_1 \ldots Q_s$, onde os Q_i são ideais primos de R.

Logo $A' = P_1 Q_1 \ldots Q_s$ e, consequentemente, R é um anel de Dedekind.

Como consequência deste lema temos a seguinte caracterização:

(1.5.03) - Corolário - Seja R um domínio. Então R é um anel de Dedekind se, e somente se, o conjunto dos seus ideais fracionários é um grupo.

Prova - Se R é um anel de Dedekind, pelo teorema (1.3.08), todo ideal fracionário é inversível.

A recíproca é óbvia, pelo lema(1.5.02).

Provemos, finalmente, a equivalência entre as duas definições.

(1.5.04) - Teorema - (Noether-Krull) - Seja R um domínio,que

não é corpo. Então R é um anel de Dedekind se, somente se, R é noetheriano, integralmente fechado e Kdim R = 1.

Demonstração - Se R é um anel de Dedekind, pelo que foi visto anteriormente, R é noetheriano, integral - mente fechado e Kdim R = 1.

Suponha que R é noetheirano, integralmente fechado e que Kdim R = 1. Mostremos que R é um anel de Dedekind.

Pelo lema (1.5.02) basta mostrarmos que todo ideal primo de R é inversível.

Sejam P um ideal primo, não nulo, de R e $P^* = (R:P) = \{x \in K ; xP \subset R\}$, onde K é o corpo de frações de R.

Provaremos que $PP^* = R$.

Como $1 \in P^*$ então $P \subset PP^*$. Mas P é maximal, portanto $PP^* = P$ ou $PP^* = R$.

Provemos que existe $a \in P^* - R$ e que, neste caso, $PP^* = R$.

Seja $x \in P - \{0\}$

Como R é noetheriano, pelos lemas (0.2.57) e (0.2.58).

$$(1.5.05) \quad (x) = Q_1 \cap Q_2 \cap \ldots \cap Q_r$$

onde cada Q_i é um ideal primário com radical P_i.

Pelo lema (0.2.60), para cada i, existe $n_i \in \mathbb{N}$ tais que

$$Q_i \supset P_i^{n_i}.$$

Assim teremos

$$P \supset \bigcap P_i^{n_i}.$$

Como dados os ideais A e B temos $r(A \cap B) = r(A) \cap r(B)$, teremos:

$$P = r(P) \supset r(\bigcap P_i^{n_i}) = \bigcap r(P^{n_i}) = \bigcap P_i.$$

Portanto, pelo lema (0.2.05), $P \supset P_{io}$ para algum i_o. Pela maximalidade dos P_i, $P = P_{io}$.

Podemos, sem perda de generalidade, supor $P = P_1$ e que:

$$(x) \supset P_1^{n_1} \ldots P_r^{n_r}$$

mas

$$(x) \not\supset P_1^{\alpha_1} \ldots P_r^{\alpha_r}$$

com $\alpha_i < n_i$.

Então existe $y \in P_1^{n_1 - 1} \cdot P_2^{n_2} \ldots P_r^{n_r} - (x)$

Como $(x) \supset P_1^{n_1} \ldots P_r^{n_r}$, dado $p \neq 0$ em P existe $r \in R$ tal que

$$rx = py$$

Assim $y/x \in P^* - R$, uma vez que $y \notin (x)$.

Logo existe um elemento em $P^* - R$.

Provemos, agora, que $P.P^* = R$.

Suponhamos que fosse $PP^* = P$.

Tome então $p \in P$ e $a \in P^* - R$ e considere a cadeia de ideais de R:

$$(p) \subseteq (p,pa) \subseteq (p,pa,pa^2) \subseteq (p,pa,pa^2,pa^3) \subseteq \ldots$$

Como R é noetheriano esta cadeia é estacionária, isto é, existe n tal que:

$$(p,pa,pa^2,\ldots,pa^n) = (p,pa,pa^2,\ldots,pa^{n+1}) =$$

$$= (p,pa,pa^2,\ldots,pa^{n+1}) = \ldots$$

Assim existem $a_o, a_1, \ldots, a_n$ em R , tais que:

$$pa^{n+1} = \sum_{i=o}^{n} a_i pa^i$$

o que nos dá

$$a^{n+1} = \sum_{i=o}^{n} a_i a^i$$

Esta última igualdade nos dá uma relação de dependência inteira de a sobre R, o que não pode ocorrer pois R é integralmente fechado e a $\notin$ R.

Logo P.P* = R, concluindo a prova.

Uma outra caracterização para anéis de Dedekind é a que se segue:

(1.5.06) - Teorema - Seja R um anel noetheriano tal que Kdim(R) = 1. Então R é um anel de Dedekind se, e somente se, as suas localizações por ideais primos são anéis de valorização discreta.

Demonstração - Seja R um anel de Dedekind com cor-

po de frações K, e considere

$$v_p : K^* = K - \{0\} \longrightarrow \mathbb{Z}$$
$$x \longmapsto n_p(x)$$

onde $n_p(x)$ é o expoente da potência do ideal primo P que aparece na decomposição de (x).

Neste caso R_p é o anel da valorização v_p.

De fato, seja $x \in K^*$ e suponha que $v_p(x) \geq 0$. Isto é, $x = a/b$ onde depois de simplificadas as potências de ideais primos comuns na decomposição de (a) e (b) não aparecerá expoente negativo para P. Em outras palavras, $b \notin P$.

Logo $a/b \in R_p$

Por outro lado, se $a/b \in R_p$ então $v_p(a/b) \geq 0$

Portanto R_p é o anel de valorização de v_p.

Reciprocamente, suponha que as valorizações de R são anéis de valorização discreta e provemos que R é um anel de Dedekind. Para tanto basta provarmos que R é integralmente fechado. Mas isto foi provado no lema (0.2.29).

Uma outra caracterização para anéis de Dedekind é dada por:

(1.5.07) - Corolário - Seja R um domínio local. R é um anel de valorização discreta se, e somente se todo ideal fracionário de R é inversível. Ou equivalente, R é um domínio de Dedekind local se, e somente se, R é um anel de valorização discreta.

Prova - Seja R um anel de valorização discreta. Mostraremos que R é um anel de Dedekind, consequentemente, pelo corolário (1.5.03), todo ideal fracionário de R é inversível.

Mas todo anel de valorização discreta é um anel principal e, consequentemente, um anel de Dedekind.

Provemos esta nossa primeira afirmação

Como R é um anel de valorização discreta, existe uma valorização.

$$v : K^{*} \longrightarrow \mathbb{Z}$$

tal que:

$$R = \{x \in K^{*} \text{ tal que } v(x) \geq 0\}.$$

Sejam A um ideal de R e $\Omega = \{v(x);\ x \in A\}$.

Como $A \subset R$ e v é sobrejetiva, Ω tem um menor elemento. Sejam n_o esse elemento e $x_o \in A$ tal que $v(x_o) = n_o$.

Afirmo: $A = (x_o)$

De fato, seja $y \in A$. Então

$v(y) \geq v(x_o)$

Se $v(y) = v(x_o)$, então $v(x_o y^{-1}) = 0$. Logo $y \in (x_o)$.

Se $v(y) > v(x_o)$, então $v(y) = v(x_o) + k$ onde $k > 0$.

Como v é sobrejetiva existe y_1 em R tal que

$$v(y_1) = k,$$

logo teremos:

$$v(y) = v(x_o) + v(y_1) = v(x_o y_1),$$

o que nos dá

$$y \in (x_o)$$

E assim R é um anel principal.

Reciprocamente, suponha que R é um anel local e que todo ideal fracionário de R é inversível.

Nestas condições R é um anel de Dedekind com um único ideal primo diferente de zero.

Mas, como $R = \bigcap P_p$, onde P é ideal primo de R, teremos:

$$R = R_p.$$

Logo R é um anel de valorização discreta.

(1.5.08) - Proposição - Seja R um anel de Dedekind local. Então R é um domínio principal.

Prova - Como um anel de Dedekind todo ideal primo, não nulo, é maximal, R tem um único ideal primo não nulo.

Seja P este ideal e tome $x \in P - P^2$. Nestas condições $(x) = P$.

Logo todo ideal de R é gerado por uma potência de x.

(1.6) O Teorema do Resto Chinês e Algumas Aplicações a Anéis

de Dedekind.

Neste parágrafo pretendemos dar uma extensão da proposição (1.5.08), bem como usar o teorema do resto chinês para obtermos alguns resultados interessantes sobre anéis de Dedekind.

(1.6.01) - Teorema do Resto Chinês - (T.R.C.) - Um anel R satisfaz o teorema do Resto Chinês se, e somente se:

"Dados $A_1, A_2, \ldots, A_n$ ideais de R e $x_1, x_2, \ldots, x_n$ em R o sistema de congruência $x \equiv x_i$ mód(A_i) tem solução se, e somente se, estas congruências são duas a duas compatíveis. Isto é:

$$x_i \equiv x_j \text{ mód}(A_i + A_j) \ , \ i \neq j".$$

Provaremos que um anel de Dedekind R satisfaz o teorema do Resto Chinês e, como consequência, teremos que todo anel de Dedekind com um número finito de ideais primos é um domínio principal.

Faremos isto, provando as equivalências abaixo:

(1.6.02) - T.R.C $\leftrightarrow$ a). $A \ (B + C) = (A \ B) + (A \ C)$
b). $A + (B \ C) = (A + B) \ (A + C)$

(1.6.03) - T.R.C $\leftrightarrow$ Condição de Independência Forte, isto é

"Dados $P_1, P_2, \ldots, P_n$ ideais primos de R, $x_1, x_2, \ldots, x_n$ elementos de R e $k_1, k_2 \ldots k_n$, inteiros positivos, existe $x \in K' = K - \{0\}$ tal que $v_i(x - x_i) = k_i$ onde v_i é a valorização associada a P_i

(1.6.04) Condição de independência forte $\leftrightarrow$ condição de independência fraca

A equivalência (1.6.02) vale para anéis quaisquer enqunato que nas outras duas usaremos o fato de R ser um anel de Dedekind.

Para (1.6.02), como ter solução implica serem duas a duas compatíveis, faremos a seguinte demonstração:

(1.6.05) distributividade $\rightarrow$ (compatibilidade $\rightarrow$ ter solução)

(1.6.06) (compatibilidade $\rightarrow$ ter solução) $\rightarrow$ distributividade.

Para (1.6.05) usaremos indução sobre o número de congruências.

Para n = 2, se

$$x_1 \equiv x_2 \ \text{mód}(A_1 + A_2)$$

teremos

$$x_1 - x_2 = a_1 - a_2 \quad \text{onde } a_1 \in A_1 \text{ e } a_2 \in A_2$$

Assim $x_1 - a_1 = x_2 - a_2$

O elemento $x = x_1 - a_1$ é solução para o sistema $x \equiv x_i \ \text{mód}(A_i)$. De fato

$$x_1 - a_1 \equiv x_1 \ \text{mód}(A_1)$$

e

$$x_1 - a_1 = x_2 - a_2 \equiv x_2 \ \text{mód}(A_2).$$

Suponhamos que o resultado vale para n = k-1. Provemos, então, que também vale para n = k.

Temos que encontrar um $x \in R$ tal que $x \equiv x_i \mod(A_i)$ com $x_i \equiv x_j \mod(A_i + A_j)$ se $i \neq j$, para $i = 1,2,\ldots,,k$.

A idéia é reduzirmos o sistema para o caso de k - 1 congruências.

Nós conhecemos uma solução x' para o sistema

$$x \equiv x_i \mod(A) \quad i = 1,2,\ldots, k-1$$

Assim o sistema de k congruências é equivalente a encontrar um x tal que:

$$(1.6.07) \qquad x \equiv x' \mod(A_i) \text{ e } x \equiv x_k \mod(A_k)$$

ou equivalente,

$$(1.6.07)' \qquad x \equiv x' \mod\left(\bigcap_{i=1}^{k-1} A_i\right) \text{ e } x \equiv x_k \mod(A_k).$$

Se

$$(1.6.08) \qquad x' \equiv x_k \mod\left(\bigcap_{i=1}^{k-1} A_i + A_k\right)$$

o sistema (1.6.07)' tem solução, por hipótese de indução.

Como valem as leis distributivas, o sistema (1.6.08) é equivalente à:

$$(1.6.08)' \quad x' \equiv x_k \mod\left(\bigcap_{i=1}^{k-1} (A_i + A_k)\right)$$

e como

$$x' \equiv x_i \mod(A_i) \text{ e } x_k \equiv x_i (A_i + A_k)$$

o sistema (1.6.07) tem solução. Concluindo a demonstração.

Para (1.6.06) provaremos apenas o caso de três ideais, pois o caso geral pode ser obtido deste por indução sobre o número de ideais. Assim vamos provar que se A,B e B' são ideais de R, então:

$$A + (B \cap B') = (A + B) \cap (A + B')$$

e

$$A \cap (B + B') = (A \cap B) + (A \cap B').$$

É claro que $A + (B \cap B') \subset (A + B) \cap (A + B')$

e

$$(A \cap B) + (A \cap B') \subset A \cap (B + B').$$

Para as outras duas inclusões seja, primeiramente, $d \in (A + B) \cap (A + B')$. Então podemos escrever

$$d = a + b = a' + b'$$

onde $a , a' \in A$, $b \in B$ e $b' \in B'$

Queremos escrever $d = x + y$ onde $x \in A$ e $y \in B \cap B'$. Ou melhor, queremos encontrar um $x \in R$ tal que:

$$x \equiv 0 \quad \text{mód}(A)$$

$$x \equiv d \quad \text{mód}(B)$$

$$x \equiv d \quad \text{mód}(B')$$

Para que este sistema tenha solução basta mos-

trarmos que as congurências são compatíveis, isto é,

$$d \in A + B' \quad e \quad d \in A + B$$

Mas, por hipótese, $d \in A + (B \cap B')$ e portanto o sistema tem solução.

Logo $(A + B') \cap (A + B) \subset A + (B \cap B')$ e assim vale:

$$A + (B \cap B') = (A + B') \cap (A + B).$$

Seja $d \in A \cap (B + B')$. Queremos provar que $d \in (A \cap B) + (A \cap B')$, isto é, queremos escrever $d = x + y$ onde $x \in A \cap B$ e $y \in A \cap B'$. Ou, equivalentemente, encontrar uma solução para o sistema

$$(1.6.09) \quad \begin{cases} x \equiv 0 \pmod{(A)} \\ x \equiv 0 \pmod{(B)} \\ x \equiv d \pmod{(A)} \\ x \equiv d \pmod{(B')} \end{cases}$$

Para que (1.6.09) tenha solução basta verificarmos as quatro compatibilidades.

i) $d \equiv 0 \pmod{(A)}$

ii) $d \equiv 0 \pmod{(A + B')}$

iii) $d \equiv 0 \pmod{(A + B)}$

iv) $d \equiv 0 \pmod{(B + B')}$

Mas elas se verificam pela escolha de d. Portan-

to o sistema (1.6.09) tem solução e vale:

$$A \cap (B + B') \subset (A \cap B) + (A \cap B')$$

Logo $A \cap (B + B') = (A \cap B) + (A \cap B')$, Ficando provada a equivalência (1.6.02).

Para (1.6.03) procederemos da mesma maneira que para (1.6.02), ou seja, provaremos que:

(1.6.10) (compatibilidade → ter solução) → condição de independência forte.

(1.6.11) condição de independência forte (compatibilidade → ter solução)

Para a primeira implicação sejam $k_1,\ldots,k_n$ em $\mathbb{N}$, $x_1,\ldots,x_n$ em R e $v_1,\ldots,v_n$ valorizações de K associaidas aos ideais primos $P_1,\ldots,P_n$.

Escolha $a_i \in P_i^{k_i} - P_i^{k_i+1}$

Considere o sistema de congruências

$$(1.6.12) \quad \begin{cases} x \equiv x_i \mod (P_i^{k_i}) \\ x \equiv x_i + a_i \mod (P_i^{k_i+1}) \end{cases}$$

Pelo Teorema de Resto Chinês este sistema tem solução uma vez que as congruências são duas a duas compatíveis. De fato:

$$\text{i)}\quad P_i^{K_i} + P_j^{K_j} = (1) \text{ se } i \neq j$$

e

$$\text{ii)}\quad P_i^{K_i} + P_j^{K_j + 1} = (1) \text{ se } i \neq j$$

pois, para $i \neq j$, se denotarmos por $r(P)$ o radical do ideal P, teremos:

$$r(P_i^{K_i} + P_j^{K_j+1}) = r(r(P_i^{K_i}) + r(P_j^{K_i})) = r(P_i + P_j) = r(1)$$

O que nos dá $P_i^{K_i} + P_j^{K_j+1} = (1)$.

Por outro lado, para $i = j$, $x_i = x_i + a_i \ \mod(P_i^{K_i} + P_1^{K_i+1})$

pois $x_i - x_i - a_i = a_i \in P_i^{K_i} \quad P_i^{K_i} + P_i^{K_i+1}$.

Seguindo-se o resultado.

Reciprocamente, sejam os ideais $A_1, A_2, \ldots, A_n$ de R e $x_1, \ldots, x_n$ em R. Queremos encontrar $x \in R$ tal que

$$(1.6.13) \qquad x \equiv x_i \ \mod(A_i)$$

supondo que $x_i - x_j \in A_i + A_j$, se $i \neq j$.

Como R é um anel de Dedekind, cada A_i pode ser escrito na forma

$$A_i = \prod_{j=1}^{n} P_j^{\alpha_{ij}} \quad i = 1,2,\ldots, n \ , \ m \geq n$$

Assim a congruência $x \equiv x_i \ \mathrm{m\bar{o}d}(A_i)$ pode ser escrita na forma

$$(1.6.14) \qquad x \equiv x_i \ \mathrm{m\bar{o}d}\left(\prod_{j=1}^{m} P_j^{\alpha_{ij}}\right)$$

Desde que os P_j são co-maximais, (1.6.14) é equivalente à:

$$(1.6.14)' \qquad x \equiv x_i \ \mathrm{m\bar{o}d}\left(\bigcap_{j=1}^{m} P_j^{\alpha_{ij}}\right)$$

Portanto o sistema (1.6.13) se reduz à:

$$x \equiv x_i \ \mathrm{m\bar{o}d}(P_j^{\alpha_{ij}}), \quad j = 1,2,\ldots,m, \quad i = 2,\ldots,n$$

supondo que

$$x_i - x_s \in A_i + A_s = \prod_{j=1}^{m} P_j^{\min\{\alpha_{ij},\, \alpha_{sj}\}}$$

Fixado j, seja $x^{(j)}$ em R satisfazendo a última congruência acima. Tal $x^{(j)}$ sempre existe. Basta tomarmos, por exemplo, $x^{(j)} = x_{io}$ onde

$$x_{io} \in \{x_1,\ldots,x_n\}$$

e

$$v_{pj}(x_{io}) = \alpha_j = \max\{\alpha_{ij},\ i = 1,2,\ldots,n\}$$

Assim nosso problema se reduz a

Dados:

$P_1,\ldots,P_m$, ideais

$v_1,\ldots, v_m$, valorizações associadas aos P_i

$\alpha_1, \ldots, \alpha_m \in \mathbb{N}$

$x^{(1)}, \ldots, x^{(m)}$

encontrar $x \equiv x_i$ mód (A_i).

Pela condição de independência forte existe $x \in R^*$ tal que

$$v_j(x - x^{(j)}) = \alpha_j \ , \ j = 1,2,\ldots, m$$

Mas

$$x - x_i = x - x^{(j)} + x^{(j)} - x_i$$

onde $x - x^{(j)}$ e $x^{(j)} - x_i$ estão em $P_j^{\alpha_{ij}}$ para todo i.

Assim $x - x_i \in P_j^{\alpha_{ij}}$ para todo i e para todo j, ou seja:

$$x - x_i \in \bigcap_{j=1}^{m} P_j^{\alpha_{ij}} = \prod_{j=1}^{m} P_j^{\alpha_{ij}} = A_i$$

Logo $x \equiv x_i$ mód(A_i)

Finalmente passemos à terceira equivalência.

Mostremos que a condição de independência forte implica na fraca, ou seja, mostremos que dadas as valorizações $v_1, v_2, \ldots, v_n$, de K e os inteiros $K_1, K_2, \ldots, K_n$, existe x em $K^* = K - \{0\}$ tal que: $v_i(x) = K_i$

e

$$v_p(x) \geq 0 \quad \text{se} \quad P \neq P_i$$

sabendo que dadas as valorizações $v_1, v_2, \ldots, v_n$ de K, os inteiros $K_1', K_2', \ldots, K_n'$ e os elementos $x_1, x_2, \ldots, x_n$, de R, existe x em $R^* = R - \{0\}$ tal que $v_i(x - x_i) = K_i'$ e $v_p(x) \geq 0$ para todo $P \neq P_i$.

Para tanto, sejam $\ell_i = |K_i| + 1$.

Pela condição de independência forte, existe $x \in R^*$ tal que:

$$v_i(x) = \ell_i \quad \text{e} \quad v_p(x) \geq 0 \quad \text{se } P \neq P_i$$

$$\text{Assim } (x) = P_1^{\ell_1} \cdot \ldots \cdot P_n^{\ell_1} \cdot P_{n+1}^{\ell_{n+1}} \cdot \ldots \cdot P_m^{\ell_m},$$

onde $\ell_i \geq 0$ para todo $i = 1, 2, \ldots, m$.

Sejam

$$m_i = \begin{cases} \ell_i + K_i & \text{se } i = 1, 2, \ldots, n \\ \ell_i & \text{se } i = n+1, \ldots, m. \end{cases}$$

Novamente existe y em R^* tal que

$$v_i(y) = m_i \text{ e } v_p(y) \geq 0 \text{ , se } P \neq P_i.$$

Considere o elemento y/x em K^*.

Observe que:

i) para $i = 1, 2, \ldots, n$

$$v_i(y/x) = v_i(y) - v_i(x) = n_i - \ell_i = K_i$$

ii) para $i = n+1, n+2, \ldots, m$

$$v_i(y/x) = v_i(y) - v_i(x) = 0$$

iii) para $P \neq P_i$

$v_p(y/x) = v_p(y) \geq 0$

Logo y/x tem a propriedade desejada.

Finalmente vejamos que a condição de independência fraca implica na forte.

Primeiramente veremos os seguintes lemas:

(1.6.15) - Lema - Sejam R um anel de Dedekind, K seu corpo de frações, P um ideal primo de R, v_p a valorização de K associada a P, n um inteiro positivo e b um elemento de R. Para cada elemento u em $R - PR_p$ existe um elemento a em R tal que $v_p(ua - b) \geq 1$.

Prova - Esta demonstração será feita por indução sobre n.

Para n = 1

Como a aplicação

$$\phi : R \longrightarrow R_p/PR_p$$

$$x \longmapsto \frac{x}{1} + PR_p$$

é sobrejetiva, $\phi(R)$ é um corpo. Portanto o elemento $\phi(u)$ tem um inverso em $\phi(R)$, isto é, existe a' em R tal que a'u - 1 está em PR_p. Assim ba'u - b, também está em PR_p. Assim $v_p(ba'u - b) \geq 1$

Tome $a = ba'$.

Suponha que o resultado seja válido para algum $K \geq 1$.

Pela condição de independência fraca, existem t e u_1 em R, tais que:

i) $v_p(t) = K$.

ii) $v_p(u_1) = 0$

iii) Se $v_q(t) \neq 0$ então $v_q(u_1) = v_q(t)$

Seja $b = u_1(ua - 1)\, t^{-1}$

Obviamente b está em R pois $v_p(b) \geq 0$ para todo ideal primo P de R. Como $u_1 u$ está em $R - PR_p$, existe c em R tal que $v_p(u_1uc - b) \geq 1$.

Faça $d = a - tc$.

É claro que d está em R e, como

$$u_1(ud-1) = u_1u(a-tc) - u_1 = v_1(ua-1) - u_1utc =$$
$$= t(b-u_1uc),$$

$v_p(ud-1) \geq K + 1$. Seguindo-se o resultado.

(1.6.16) - Lema - Sejam R um anel de Dedekind; K seu corpo de frações; $v_1, v_2, \ldots, v_m$ valorizações de K associadas aos ideais primos $P_1, P_2, \ldots, P_m$; $x_1, x_2, \ldots,$ xm elementos de K; e n um número natural. Existe x em K tal que $v_i(x-x_i) \geq K$ e $v_p(x) \geq 0$ para todo ideal P, diferente de P_i, $i=1,2,\ldots, m$.

Prova - Como $x_i \in K$ $(i = 1,2,\ldots,m)$, podemos es-

creyer $x_i = b_i c^{-1}$ onde b_i e c $b_i Rc$ estão em R.

Sejam P_{m+1} , $P_{m+2},\ldots,P_n$, ideais primos de R, distintos de $P_i (i = 1,2,\ldots, m)$, tais que $v_i(c) \neq 0$ $(i = m + 1 , m + 1,\ldots,n)$.

Faça $b_{m+1} = b_{m+2} = \ldots = b_n = 0$ e

$K' = \max \{K + v_i(c)\}$ $(i = m + 1, m + 2,\ldots, n)$.

Pela condição de independência fraca, para cada $i = 1,2,\ldots, n$, existe u_i em R tal que:

i) $v_i(u_i) = 0$

e

ii) $v_j(u_i) \geq K'$.

Pelo lema (1.6.15) existem $a_i (i = 1,2,\ldots, n)$ em R, tais que $v_i(a_i u_i - b_i) \geq K'$

Seja $b = a_1u_1 + a_2u_2\ldots+ a_nu_n$.

Obviamente b está em R e

$$v_i(b-b_i) = v_i(u_1a_1+\ldots+u_ia_i - b_i+\ldots+u_na_n) \geq$$

$$\geq \min \{v_i(u_ja_j - s_{ij}b_j)\} \geq K'$$

Logo $x = bc^{-1}$ tem a propriedade desejada.

Para a condição de independência forte sejam $v_1, v_2,\ldots, v_n$ valorizações de R, associadas aos ideais primos

$P_1, P_2, \ldots, P_n$; $k_1, k_2, \ldots, k_n$ números inteiros e

$x_1, x_2, \ldots, x_n$ elementos de K.

Como $v_i : K \longrightarrow \mathbb{Z}$ é sobrejetiva, existem elementos $y_1, y_2, \ldots, y_n$ em K, tais que $v_i(y_i) = k_i$.

Seja $K > \max \{0, k_1, k_2, \ldots, k_n\}$

Pelo lema (1.6.16) existem x e y em K, tais que

i) $v_i(x-x_i) \geq K$.

ii) $v_i(y-y_i) \geq K$

iii) $v_p(x) \geq 0$ e $v_p(y) \geq 0$ se $P \neq P_i$.

Assim nós temos

$$v_i(x-x_i+ y-y_i) \geq K > k_i = v_i(y_i)$$

E, portanto,

$$v_i(x+y-x_i) = k_i \text{ e } v_p(x+y) \geq 0 \text{ se } P \neq P_i$$

Logo x + y tem a propriedade desejada

Temos, agora, o seguinte teorema:

(1.6.17) - Teorema - Em um anel de Dedekind valem

i) $A \cap (B+C) = (A \cap B) + (A \cap C)$

ii) $A + (B \cap C) = (A + B) \cap (A + C)$

para todos ideais A, B e C de R.

Demonstração - Como R é um anel de Dedekind , vale a condição de independência fraca. Pelo que foi visto vale a condição de independência forte. Consequentemente valem o Teorema do Resto Chinês e as distributividades acima

(1.6.18) - Corolário - Um anel de Dedekind R, com um número finito de ideais primos é um domínio principal.

Prova - Uma vez que todo ideal de R se escreve como um produto de ideais primos, basta-nos provar que todo ideal primo é principal.

Sejam $P_1,\ldots, P_n$ os únicos ideais primos de R.

Se existir x_i em $P_i - P_i^2$, tal que $x_i \notin \bigcup_{j=1}^{n} P_j$, $j \neq i$, então $P_i = (x_i)$ e concluiremos a demonstração.

Encontrar um x_i nestas condições, é equivalente a encontrar um x_i satisfazendo:

$$(1.6.19)\quad \begin{cases} x_i \equiv y_o \mod (P_i^2) \;, & y_o \in P_i - P_i^2 \\ x_i \equiv 1 \mod (P_j) \;, & i \neq j \\ x_i \equiv x_o \mod (P_n) \;, & x_o \in P_i - P_n \end{cases}$$

tais x_o e y_o sempre existem pois cada P_j é maximal. Assim as congruências são compatíveis.

Logo o sistem (1.6.19) tem solução

(1.6.20) - Corolário - Em um anel de Dedekind R, todo ideal

fracionário é gerado por dois elementos, um dos quais podendo ser escolhido arbitrariamente.

Prova - Já vimos que todo ideal fracionário é o produto de um ideal fracionário principal por um ideal de R. Assim basta estudarmos os ideais de R.

Sejam A um ideal de R e x um elemento qualquer de A.

Assim teremos:

$$A = P_1^{r_1} \dots P_n^{r_n}$$

e

$$(x) = P_1^{\alpha_1} \dots P_n^{\alpha_n} P_{n+1}^{\alpha_{n+1}} \dots P_m^{\alpha_m}$$

onde $\alpha_i \geq r_i$ para $i = 1,2,\dots, n$ e $\alpha_i \geq 0$ para $i=n+1,\dots,m$

Pela condição de independência forte, fazendo $x_i = 0$, existe $y \in R^*$ tal que

i) $v_i(y) = r_i$, se $i = 1,2,\dots,n$

ii) $v_i(y) = 0$, se $i = n+1,\dots,m$

iii) $v_p(y) \geq 0$, se $P \neq P_i$, $i = 1,2,\dots,m$

Como $v_i((x) + (y)) = \min \{v_i(x), v_i(y)\}$, temos $v_p((x) + (y)) \leq v_p(A)$ para todo ideal primo P de R. Assim $A \subset (x) + (y) = (x,y)$.

Por outro lado

$$v_p(y) \geq v_p(A)$$

para cada ideal primo P, é assim

$$(y) \subset A$$

Como, por escolha, $(x) \subset A$, teremos $(x) + (y) \subset A$.

Logo $A = (x) + (y) = (x,y)$. E, portanto, A é gerado por dois elementos.

(1.6.21) - Corolário - Se R é um anel de Dedekind, e A é um ideal de R, então R/A é um domínio principal.

Prova - Seja B um ideal de R contendo A. Pelo corolário anterior, B é gerado por dois elementos um dos quais podendo ser escolhido em A.

Assim podemos escrever $B = (x) + (y)$ onde $x \in A$.

Logo $\overline{B} = B/A = (\overline{y})$

O corolário (1.6.18) nos dá uma condição suficiente para que um anel de Dedekind R, seja um anel principal. Note que esta condição não é necessária, pois o anel $\mathbb{Z}$ dos inteiros é um anel de Dedekind que é principal e, como sabemos, possui uma infinidade de ideais primos.

Sabemos que para que um anel R não seja principal basta que ele possua um ideal não principal. Mas em anéis de Dedekind vale o seguinte:

(1.6.22) - Proposição - Se R é um anel de Dedekind, que não é principal, então R possui um número infinito de ideais primos que não são principais.

Para provramos isto necessitaremos de alguns resultados que demonstraremos a seguir.

(1.6.23) - Lema - Sejam R um anel de Dedekind e S um sistema multiplicativamente fechado de R. A aplicação ϕ, do conjunto dos ideais fracionários de R no conjunto dos ideais fracionários de $S^{-1}R$, definida por $\phi(A) = A(S^{-1}R)$ é um homomorfismo sobrejetor.

Prova - A aplicação está bem definida pois, se A é um ideal fracionário de R então existe $d \in R$ tal que $dA \subset R$, e assim $dA(S^{-1}R) \subset S^{-1}R$. Logo $A(S^{-1}R)$ é um ideal fracionário de $S^{-1}R$.

Que ϕ é um homomorfismo é óbvio.

Resta-nos, portanto, provar que ϕ é sobrejetiva.

Seja D um ideal fracionário de $S^{-1}R$.

Como $S^{-1}R$ é um anel de Dedekind, temos que $D = Q_1^{e_1} \ldots Q_r^{e_r}$, ponde cada Q_i é um ideal primo de $S^{-1}R$. Assim, para cada i, existe um ideal primo P_i de R, tal que

$Q_i = P_i(S^{-1}R)$.

Tome $E = P_1^{e_1} \ldots P_r^{e_r}$

Então $\phi(E) = \phi(P_1^{e_1}\ldots) = \phi(P_1)^{e_1} \ldots \phi(P_r)^{e_r} =$

$= (P_1(S^{-1}R))^{e_1} \ldots (P_r(S^{-1}R))^{e_r} = Q_1^{e_1} \ldots Q_r^{e_r} = D.$

Logo ϕ é um homomorfismo sobrejetivo.

(1.6.24) - Definição - Seja R um anel de Dedekind. O grupo multiplicativo dos ideais fracionários de R é chamado grupo de ideais de R e será denotado por I

Seja K* o grupo multiplicativo do corpo de frações de R. A aplicação:

$$\phi : K^* \longrightarrow I$$
$$u \longmapsto uR$$

é um homomorfismo de grupos. A imagem P, de ϕ, é chamada grupo dos ideais fracionários principais e o grupo quociente I/P é chamado de grupo de classes de R.

(1.6.25) - Lema - Sejam R um anel de Dedekind e S um sistema multiplicativamente fechado de R. Para cada ideal fracionário A, de R, seja $\bar{A}$ a classe do grupo de classes de R à qual A pertence. Então a aplicação σ, que leva $\bar{A}$ em $\overline{A(S^{-1}R)}$ é um homomorfismo sobrejetor do grupo de classes de R sobre o grupo de classes de $S^{-1}R$.

Prova - Sejam P(resp. P_s) o grupo dos ideais fracionários principais de R (resp. $S^{-1}R$) e I(resp.I_s) o grupo de ideais de R (resp.$S^{-1}R$).

Queremos mostrar que:

$$\sigma : I/P \longrightarrow I_\delta/P_\delta$$
$$\overline{A} \longmapsto \overline{A(S^{-1}R)}$$

é um homomorfismo sobrejetor.

Sabemos que existem os homomorfismos

$$\phi_1 : I \longrightarrow I/P$$
$$A \longmapsto \overline{A}$$

e

$$\phi_2 : I_s \longrightarrow I_s/P_s$$
$$B \longmapsto \overline{B}$$

Sejam C e D dois ideais fracionários de R. Então teremos:

$$\sigma(\overline{C}\ \overline{D}) = \sigma(\overline{CD}) = \overline{CD(S^{-1}R)} = \overline{C(S^{-1}R).(D(S^{-1}R)} =$$
$$= \overline{C(S^{-1}R)}.\overline{D(S^{-1}R)} = \sigma(\overline{C}).\sigma(\overline{D})$$

Logo σ é um homomorfismo

Nota: Na primeira e na quarta igualdade usamos ϕ_1 e ϕ_2, respectivamente, enquanto que na terceira usamos o lema(1.6.23)

Para provarmos que σ é sobrejetiva, seja $\overline{B}$ em

I_s/P_s e seja B um representante da classe $\bar{B}$. Pelo lema (1.6.23) existe um ideal fracionário A em $\bar{I}$ tal que $B = A(S^{-1}R)$. Seja $\bar{A}$ a classe à qual A pertence. Assim teremos:

$$\sigma(A) = \overline{A(S^{-1}R)} = \bar{B}$$

Logo σ é um homomorfismo sobrejetor .

(1.6.26) - Lema - O núcleo de σ é gerado por todos os $\bar{P}_i$, onde P_i percorre o conjunto dos ideais primos de R tais que $P_i \cap S \neq \emptyset$

Prova - Se $P_i \cap S \neq \emptyset$ então $P_i(S^{-1}R) = S^{-1}R$. Suponha que C é um ideal fracionário de R tal que $\bar{C} = \bar{P}_{io}$, isto é, $C = dP_{io}$ para algum d no corpo de frações de R.

Então $C(S^{-1}R) = dP_{io}(S^{-1}R)) = d(P_{io}S^{-1}) = d(S^{-1}R)$. Assim $C(S^{-1}R)$ está no grupo de ideais fracionários principais de R.

Por outro lado, suponha que C é um ideal fracionário de R tal que $C(S^{-1}R) = x(S^{-1}R)$. Nós podemos escolher x em C, pois, desde que $C(S^{-1}R) = x(S^{-1}R)$, temos que $x \in C(S^{-1}R)$, isto é, $x = c(r/s)$ onde $c \in C$, $r \in R$ e $s \in S$. E assim $x(S^{-1}R) = c(S^{-1}R)$.

Logo podemos tomar x em C.

O ideal $C^{-1}(xR)$ é um ideal próprio de R(pois $xR \subset C$ e, portanto, $C^{-1}(xR) \subset C^{-1}C = R$) , e mais:

$$(C^{-1}xR)\ (S^{-1}R) = C^{-1}(xR(S^{-1}R)) = C^{-1}(x(S^{-1}R))$$
$$= C^{-1}(C(S^{-1}R) = S^{-1}R.$$

Em outras palavras, $C^{-1}(xR) = P_1^{e_1}\ldots P_r^{e_r}$ onde $P_i \cap S \neq \emptyset$, para cada $i = 1,2,\ldots,r$. Então

$$\overline{C^{-1}\ xR} = \bar{P}_1^{e_1}\ldots\ \bar{P}_r^{e_r}.$$

O que nos dá:

$$\overline{C^{-1}} = \bar{P}_1^{e_1}\ldots\ \bar{P}_r^{e_r}$$

Logo $\bar{C} = \bar{P}_1^{-e_1}\ldots\ \bar{P}_r^{-e_r}$, completando a prova.

Agora podemos provar a proposição (1.6.22).

Sejam R um anel de Dedekind que não é principal (deixaremos para o capítulo 2 um exemplo de um tal anel) e S o sistema multiplicativamente fechado gerado por todos os elementos primos de R. Como $S^{-1}R$ não é principal, pois R não o é, pelo corolário (1.6.18), $S^{-1}R$ tem um número infinito de ideais primos próprios. Seja Q um desses ideais. Então $Q = P(S^{-1}R)$ onde P é um ideal primo próprio de R. Se Q fosse principal, P também o seria, isto é, $P = pR$ com $p \in P$. Neste caso p seria um elemento primo de R e, consequentemente, estaria em S. E assim $P(S^{-1}R)$ seria igual a $S^{-1}R$. Logo Q não é principal. Provando a proposição(1.6.22).

Nota - Esta proposição se torna ainda mais relevante porque

ela nos fornece casos de anéis de Dedekind nos quais todos os ideais primos são gerados por exatamente dois elementos.

Para finalizar este capítulo, veremos um outro fato interessante que ocorre em anéis de Dedekind.

(1.6.27) - Proposição - Seja R um anel de Dedekind com pelo menos um ideal primo em cada classe do grupo de classes de ideal. Então para todo sistema multiplicativamente fechado S, $S^{-1}R$ terá um ideal primo em cada classe, exceto , possivelmente, na classe principal.

Prova - Pelo lema (1.6.25), cada classe de $S^{-1}R$ é a imagem de uma classe de R.

Seja $\bar{D}$ uma classe não principal de $S^{-1}R$. Então $\bar{D} = \overline{C(S^{-1}R)}$, onde C é um ideal fracionário de R. Por hipótese, existe um ideal primo P de R, tal que $\bar{C} = \bar{P}$.

Se $P(S^{-1}R) = S^{-1}R$ então, como $C = dP$, teremos

$$C(S^{-1}R) = dP(S^{-1}R) = d(S^{-1}R)$$

isto é, $C(S^{-1}R)$ é um ideal principal. E assim $\bar{D}$ é a classe principal de $S^{-1}R$. Como este não é o caso, $P(S^{-1}R)$ é diferente de $S^{-1}R$. Logo $P(S^{-1}R)$ é um ideal primo de $S^{-1}R$ e, como

$$C(S^{-1}R) = dP(S^{-1}R),$$

teremos

$$\overline{P(S^{-1}R)} = \overline{C(S^{-1}R)} = \bar{D}$$

Logo $P(S^{-1}R)$ é um ideal primo na classe $\bar{D}$. Seguindo-se o resultado.

2 - EXTENSÕES DE ANÉIS DE DEDEKIND

(2.1) - Introdução

Neste capítulo estamos interessados em resolver os dois problemas seguintes:

(2.1.01) - Problema - Se R é um anel de Dedekind, com corpo de frações K e L é uma extensão de K, em que condições $R' = I_L(R)$ = fecho integral de R em L é um anel de Dedekind?

(2.1.02) - Problema - Se R é um anel de Dedekind com corpo de frações K e L é um subcorpo de K, em que condições $R'' = L \cap R$ é um anel de Dedekind?

Para o primeiro, mostraremos que basta que L seja uma extensão finita de K. Já para o segundo veremos que se K for uma extensão finita de L e R for inteiro sobre R", então R" é um anel de Dedekind.

(2.2) Provaremos, inicialmente, que se L for uma extensão finita e separável de K então $R' = I_L(R)$ é um anel de Dedekind. Veremos depois, que o resultado também vele quando L for uma extensão finita e puramente inseparável. Assim concluiremos

que o resultado é válido para toda extensão finita de K, usando o fato que se L é uma extensão finita de K, então L é uma extensão puramente inseparável de uma extensão separável de K.

Temos então o seguinte:

(2.2.01) - Lema - Sejam R um anel de Dedekind e K seu corpo de frações. Se L é uma extensão finita e separável de K, então $R' = I_L(R)$ é um anel de Dedekind.

Prova - Pelo teorema (1.5.04), basta provarmos que R' é noetheriano, integralmente fechado e que a dimensão de Krull de R' é 1.

R' é integralmente fechado pois é o fecho integral de R em L e, pelo "LYING OVER", todo ideal primo, não nulo, de R' é maximal.

Então resta-nos provar que R' é noetheriano.

Como L é uma extensão separável de K existe uma base $x_1, x_2, \ldots, x_n$, de L sobre K tal que:

$$(2.2.02)\quad R' \subseteq \sum_{i=1}^{n} Rx_i$$

Como $\sum_{i=1}^{n} Rx_i$ é um R-módulo finitamente gerado, R' também o é. Logo se R for um anel noetheriano então R' também o será.

Portanto, $R' = I_L(R)$ é um anel de Dedekind.

(2.2.03) - Lema - Sejam R um anel de Dedekind com corpo de frações K e L uma extensão puramente inseparável e de grau finito de K. Então $R' = I_L(R)$ é um anel de Dedekind.

Prova - Como L é uma extensão puramente inseparável, temos que a característica de K é um número primo, digamos, p. E como L/K é finita existe um inteiro r tal que $x^{p^r} \in K$ para cada x em L.

Para cada $f \in \mathbb{N}$, seja $K_f = \{a \in L ; a^{p^f} \in K\}$.

É claro que K_f é um subcorpo de L, contendo K, e vale:

$$K = K_0 \subset K_1 \subset \ldots\ldots \subset K_r = L.$$

Vale também

(2.2.04) se $a \in K_f$ então $a^p \in K_{f-1}$.

De fato, se $a \in K_f$ então $a^{p^f} \in K$. Mas $a^{p^f} = (a^p)^{p^{f-1}}$. Logo

$$a^p \in K_{f-1}$$

Por (2.2.04), para provarmos que R' é um anel de Dedekind basta estudarmos o caso em que a^p está em K, para cada a em L, ou seja:

(2.2.05) - Lema - Se R é um anel de Dedekind com corpo de frações K, e se L é uma extensão puramente inseparável e de grau finito de K tal que $L^p \subset K$, onde p é a caracterísca de K,

então $R' = I_L(R)$ é um anel de Dedekind.

Prova - R' pode ser caracterizado como:

$$R' = \{a \in L;\ a^p \in R\}.$$

De fato, se $a \in L$ e $a^p \in R$, então a é raiz de $x^p - a^p$ que pertence a $R[x]$. Logo $a^p \in R'$. Reciprocamente, se $a \in R'$ então $a \in L$. Como $a^p \in K$, por hipótese, e $R = R' \cap K$, temos que $a^p \in R$.

Seja Ω o fecho algébrico de K.

É claro que $L \leq \Omega$.

Sejam $K'' := \{x \in \Omega,\ x^p \in K\}$ e $R'' = I_{K''}(R)$.

Assim como R', R'' é o conjunto dos elementos x de K tais que x^p está em R, isto é:

$$R'' = \{x \in K'';\ x^p \in R\}.$$

A aplicação de Frobenius

$$\phi : K'' \longrightarrow K$$

$$x \longmapsto x^p$$

é, obviamente, um homomorfismo sobrejetor, e sua restrição a R'' é sobre R.

Como ϕ é injetiva, R'' é isomorfo a R e, conseqüentemente, é um anel de Dedekind.

Seja agora A um ideal de R'. Considere a exten-

são de A a R" , $A^e = R"A$. Como R" é um anel de Dedekind, A^e é inversível , existindo portanto:

i) $a_1, a_2, \ldots, a_n$ em A^c.

e

ii) $b_1, b_2, \ldots, b_n$ em $(A^c)^{-1} = (R" : R"A)$.

tais que:

$$(2.2.06) \qquad \sum_{i=1}^{n} a_i b_i = 1.$$

Na realidade os a_i podem ser tomados em A pois, R" sendo um anel de Dedekind A^e é finitamente gerado,ou seja, $A^e = (x_1, x_2, \ldots, x_s)$ onde $x_i \in R"A$, para cada $i = 1,2,\ldots,s$.

Assim podemos escrever:

$$x_1 = r_{11}c_1 + r_{12}c_2 + \ldots + r_{sm}c_m$$

$$x_2 = r_{21}c_1 + r_{21}c_2 + \ldots + r_{sm}c_m$$

. . . .

. . . .

. . . .

$$x_s = r_{s1}c_1 + r_{s2} + \ldots + r_{sm}c_m$$

onde $r_{ij} \in R"$ para cada i e para cada j, sendo nulos quando necessário, e $c_j \in A$ para cada j.

Assim teremos

$$A^e = (c_1, \ldots, c_m).$$

e, assim, podemos tomar os a_i em A.

Segue-se de (2.2.06) que:

$$(2.2.07) \qquad \sum_{i=1}^{n} a_i^p b_i^p = 1 .$$

Queremos mostrar que A é inversível.

Sabemos que $A.(R':A) \quad R'$. Assim devemos provar apenas que $R' \quad A.(R':A)$.

Seja $x \in R'$.

Então, por (2.2.07),

$$x = \sum_{i=1}^{n} x a_i^p b_i^p = \sum_{i=1}^{n} (x a_i) \, (a_i^{p-1}) \, b_i^p$$

Como $xa_i \in A$, se provarmos que $a_i^{p-1} b_i^p \in (R' : A)$ teremos o resultado.

Sabemos que:

$$(2.2.08) \qquad a_i^{p-1} b_i \in L, \text{ pois } a_i \in R' \text{ e } b_i^p \in \dot{K}$$

e

$$(2.2.09) \qquad (a_i^p \, b_i^p).\, A \subseteq R'' \text{ , pois } (b_i^p \, a_i^{p-1}).\, A \subset b_i^p . A^p \subseteq$$

$$\subseteq (b_i A)^p \quad R''$$

Por (2.2.09) , $(a_i^{p-1} \, b_i) \, A \leq R'' \bigcap L = R'$

Logo $a_i^{p-1} b_i^p \in (R':A)$ e, consequentemente, A é

inversível.

Mostramos com isso que todo ideal de R' é inversível, em particular, os ideais primos. Então, pelo lema (1.5.02) , R' é um anel de Dedekind.

Finalmente passemos ao

(2.2.10) - Teorema - Sejam R um anel de Dedekind com corpo de frações K e L uma extensão finita de K. O fecho integral de R em L é um anel de Dedekind.

Demonstração - Como L é uma extensão finita de K, temos que L é uma extensão puramente inseparável de uma extensão separável de K, a saber, K_s o fecho separável de K em L.

Sejam $R' = I_{K_s}(R)$ e $R'' = I_L(R)$.

Então R" é inteiro sobre R e, consequentemente, $R'' = I_L(R)$.

Pelos lemas (2.2.01) e (2.2.03), $R'' = I_L(R)$ é um anel de Dedekind.

No lema (2.2.05) mostramos que se L é uma extensão puramente inseparável de K e se existe um inteiro q,que é uma potência do expoente característico de K, tal que $L^q \subseteq K$, então todo anel de Dedekind de L se contrai a um anel de Dedekind de K.

Este resultado pode ser generalizado de tal maneira que nos dará como consequência imediata uma resposta ao segundo problema do início deste capítulo.

A generalização é assim enunciada.

(2.2.11) - Teorema - Sejam K um corpo e L uma extensão finita, normal e separável de uma extensão puramente inseparável L', de K. Suponha que existe uma potência q da característica de K tal que $L'^{q} \subseteq K$. Se T é um anel de Dedekind de L, que é inteiro sobre $R' = K \cap T$, então R' é um anel de Dedekind.

Demonstração - Suponha inicialmente L' = L.

Assim L é uma extensão finita e puramente separável de K.

Provaremos que todo ideal A de $R' = T \cap K$ é inversível e, consequentemente, R' é um anel de Dedekind.

Considere o ideal $A^e = AT$, onde A é um ideal de R.

Como T é um anel de Dedekind, AT é inversível. Assim existem $a_1, a_2, \ldots, a_n$ em A^e e $b_1, b_2, \ldots, b_n$ em $(A^e)^{-1}$ tais que:

$$(2.2.12) \qquad \sum_{i=1}^{n} a_i b_i = 1$$

Como no lema (2.2.05), os a_i podem ser tomados em A.

Para provarmos que A é inversível devemos provar

apenas que $R' \subset (R' : A)A$, pois a outra inclusão é sempre verdadeira.

Seja $x \in R'$.

De (2.2.12) teremos

$$(2.2.13) \quad \sum_{i=1}^{n} a_i^q b_i^q = 1$$

e, consequentemente,

$$x = \sum_{i=1}^{n} x a_i (a_i^{q-1} b_i^q)$$

Mas, como xa_i está em A para cada i, teremos que provar apenas, que para cada i, $a_i^{q-1} b_i^q$ está em $(R' : A)$.

Sabemos que:

$$(2.2.14) \quad a_i^{q-1} b_i^q \in K,$$

pis $a_i \in A$ e para cada x de T, $x^p \in K$, e

$$(2.2.15) \quad a_i^q \, , \, b_i^q . A \subset b_i^q . A^q \subset (b_i A)^q \subset K \cap T = R'$$

Assim $a_i^{q-1} b_i^q$ está em $(R' : A)$, seguindo-se o resultado.

Para o caso geral, é suficiente provarmos que $L' \cap T$ é um anel de Dedekind, ou seja, podemos supor $L' = K$.

Assim L é uma extensão de Galois e de grau finito de K.

Seja A um ideal próprio de R'.

Desde que T é um anel de Dedekind, $A^e = TA$ é inversível, existindo elementos $a_1, a_2, \ldots, a_s$ de A e $x_1, x_2, \ldots, x_s$ de L tais que:

$$\sum_{i=1}^{s} a_i x_i = 1 \quad \text{e} \quad x_i A \subset T$$

Denotando por $x^{(j)}$ os conjugados distintos ou não de x_i sobre K, teremos a relação:

$$\prod_{j=1}^{n} \left(\sum_{i=1}^{s} a_i x_i^{(j)} \right) = 1 \tag{2.2.16}$$

onde n é o grau da extensão de L sobre K.

A relação (2.2.16) pode ser escrita na forma

$$\sum_{n} m(a) \, P_m(x_i^{(j)}) = 1$$

onde os m(a) são monômios de grau n em a_i

Da teoria de Galois, $P_m(x_i^{(j)}) \in K$, pois é deixado fixo por todo automorfismo de L, uma vez que em $P_m(x_i^{(j)})$ os automorfismos de L se comportam como permutações.

Se de cada monômio m(a) tirarmos um fator, digamos a_i, a relação (2.2.16) nos fornece

$$\sum_{i=1}^{s} a_i b_i = 1$$

onde b_i é uma soma de produtos de monômios em a_j de grau n-1 pelos polinômios simétricos elementares $P_m(x_i^{(j)})$. Consequentemente $b_i \in K$.

Por outro lado, como

(2.2.17) $x_i A \subset T$,

(2.2.18) T é inteiro sobre R' , e.

(2.2.19) T é um anel de Dedekind, o que acarreta

$$I_L(R') = I_L(T) = T$$

temos que

$$x_i^{(j)}{}_A \; T.$$

Portanto

$$b_i A \subset \sum_m P_m(x_i^{(j)}) A^{n-1} A \subset T$$

e

$$b_i A \subset \sum_m P_m(x_i^{(j)}) A^{n-1} A \subset K.$$

O que nos dá

$$b_i A \subset K \cap T = R'$$

Logo A é inversível e, portanto, R' é um anel de Dedekind.

Finalmente temos o

(2.2.20) - Teorema - Sejam R um anel de Dedekind com corpo de frações K, e L um subcorpo de K tal que K/L é finita, e $T = R \cap L$. Se R é inteiro sobre T então T é um anel de Dedekind.

Demonstração - Se K é uma extensão normal de L, desde que K é uma extensão normal e separável de uma extensão finita e puramente inseparável de L, a saber, o fecho inseparável de L em K, o resultado é imediato do teorema (2.2.11).

o caso geral pode ser reduzido a este se substituirmos K pela menor extensão normal de L contendo K, digamos K',e R por $R' = I_{K'}(R)$

É claro que $T = R' \cap L$ e R' é um anel de Dedekind, já que K' é uma extensão finita de K.

(2.2.21) - Observação - Como prometemos no capítulo 1, daremos aqui um exemplo de anel de Dedekind que não é um anel principal.

Sabemos, do teorema (2.2.10), que o fecho integral de um anel de Dedekind em uma extensão finita do seu corpo de frações é um anel de Dedekind. Logo se tomarmos o anel $\mathbb{Z}$ dos inteiros, o fecho integral de $\mathbb{Z}$ em $Q(\sqrt{-5})$ será $\mathbb{Z}[\sqrt{-5}]$. Como $Q(\sqrt{-5})$ é uma extensão finita de Q, $\mathbb{Z}[\sqrt{-5}]$ é um anel de Dedekind. Basta mostrarmos de $\mathbb{Z}[\sqrt{-5}]$ não é

principal. Mas para isto, basta observarmos que em $\mathbb{Z}[\sqrt{-5}]$, o elemento 6 admite duas decomposições, à saber:

$$6 = (1-\sqrt{-5})\ (1+\sqrt{-5})$$

e

$$6 = 2.3.$$

Simples cálculos provam que 2,3, $1+\sqrt{-5}$ e $1-\sqrt{-5}$ são elementos primos de $\mathbb{Z}[\sqrt{-5}]$. Assim $\mathbb{Z}[\sqrt{-5}]$ não é um anel de fatorização única. Logo não pode ser um anel principal.

(2.2.22) - Observação - Todo anel de Dedekind que aparece em teoria dos números ou em geometria algébrica é obtido como o fecho integral de um anel principal conveniente. Mas existe um anel de Dedekind que não é obtido desta forma.

De fato, seja $R = \mathbb{Z}[\sqrt{-5}]$. Como já vimos, R é um anel de Dedekind que não é principal. Sabe-se, da álgebra elementar, que $p_1 = 3 + 2\sqrt{-5}$ e $p_2 = 3 - 2\sqrt{-5}$ geram dois ideais primos de R que são distintos. Seja S o sistema multiplicativamente fechado gerado por p_1, ou seja, $S = \{p_1^k\}, k \geq 0$. Pelo lema (1.6.26), $S^{-1}R$ é um anel de Dedekind que não é principal.

Sejam F o corpo de frações de R e Q o corpo dos números racionais. $S^{-1}R$ não pode ser o fecho integral de um anel principal com corpo de frações F, uma vez que anéis principais são integralmente fechados. Se $S^{-1}R$ fosse o fecho integral de um anel principal C, com corpo de frações Q, como p_1 é uma unidade de $S^{-1}R$, p_2 também deveria ser. De fato, se p_1 é

uma unidade (em $S^{-1}R$) existe $a \in S^{-1}R$ tal que:

$$p_1 . a = 1$$

Como F/Q é normal de grau 2, existe σ pertencente ao grupo de Galois de F sobre Q tal que $\sigma(p_1) = p_2$ e assim:

$$\sigma(p_1 . a) = \sigma(p_1)\sigma(a) = \sigma(1) = 1$$

o que nos dá:

$$p_2 \, \sigma(a) = 1.$$

Como estamos supondo $S^{-1}R$ o fecho integral de C em F, e como $a \in S^{-1}R$ teremos:

$a^n + c_1 a^{n-1} + \ldots + c_n = 0$, onde $c_i \in C$ cada i. E portanto,

$$\sigma(a^n + c_1 a^{n-1} + \ldots + c_n) = 0 \, .$$

Assim

$$\sigma(a)^n + c_1 \, (a)^{n-1} + \ldots + c_n = 0$$

Logo $\sigma(a) \in S^{-1}R$ e, consequentemente, p_2 seria unidade em $S^{-1}R$.

Como p_2 não é unidade, não existe um anel principal C, com corpo de frações Q, tal que $S^{-1}R$ seja o fecho integral de C em F. Desde que estas duas possibilidades são as únicas possíveis (pois $[F:Q] = 2$) fica provado que $S^{-1}R$ é um anel de Dedekind que não é o fecho integral de um anel principal.

3 - DECOMPOSIÇÃO DE IDEAIS PRIMOS EM EXTENSÕES DE ANÉIS DE DEDEKIND.

(3.1) Introdução

Nós já sabemos, do capítulo anterior, que se R é um anel de Dedekind, com corpo de frações K e L é uma extensão finita de K, então R', o fecho integral de R em L, é também um anel de Dedekind.

Sabemos também que se P é um ideal primo de R, distinto de zero, então $P^e = PR'$ é um ideal de R'. Sendo R' um anel de Dedekind P^e se escreve como um produto de ideais primos, digamos:

$$P^e = \beta_1^{e_1} . \beta_2^{e_2} \ldots \beta_r^{e_r}$$

onde cada β_i é um ideal primo de R'.

O que nós queremos estudar, neste capítulo, é o número r de β_i e a multiplicidade de cada um deles.

(3.2) Notação

Nas condições acima, cada e_i é chamado de índice de ramificação de β_i sobre R' e, chamamos $f_i = [R'/\beta_i : R/p]$

de grau de inércia ou grau de restos.

(3.3) Para tal estudo temos inicialmente o

(3.3.01) - Lema - Sejam R um anel de Dedekind, K seu corpo de frações, L uma extensão finita de K, P um ideal primo de R e R' um sobre-anel de R em L, isto é, R' é um anel contido em L que contém R. Se A é um ideal de R' acima de P então, como um R/P - espaço vetorial,

$$\dim_{R/P} R'/A \leq [L:K]$$

Prova Note primeiramente que, como R é um anel de Dedekind, teremos:

$$R/P \simeq R_p/PR_p \quad \text{e} \quad R'/A \simeq R'_p/AR'_p$$

De fato, defina, para o primeiro isomorfismo,

$$\sigma : R_p \longrightarrow R/P$$

$$x = f/g \longmapsto \bar{f}.\bar{g}^{-1}$$

Observe que σ está bem definida pois se $f/g = f'/g'$, então $fg' = gf'$, o que nos dá: $\bar{f}\bar{g}' = \bar{g}\,\bar{f}'$. Como R/P é um corpo, pois P é um ideal maximal, e desde que g e g' não estão em P, existem os elementos $\bar{g}$ e $\bar{g}'^{-1}$. Logo $\bar{f}\bar{g}^{-1} = \bar{f}'\bar{g}'^{-1}$

Provemos que σ é um homomorfismo sobrejetor com

núcleo PR_p.

Sejam f/g e f'/g' elementos de R_p. Temos que

i) $\sigma(f/g + f'/g') = \sigma(\frac{fg'+gf'}{gg'}) = \overline{(fg'+gf')}.\overline{(gg')}^{-1}$

$= \bar{f}\,\bar{g}^{-1} + \bar{f}'\bar{g}'^{-1} = \sigma(f/g) + \sigma(f'/g')$

ii) $\sigma(f/g \,.\, f'/g') = \sigma(ff'/gg') = \overline{(ff')}\,\overline{(gg')}^{-1} =$

$= (\bar{f}\,\bar{g}^{-1})(\bar{f}'.\bar{g}'^{-1}) = \sigma(f/g) \,..\, (f'/g')$

Assim σ é um homomorfismo

Seja, agora, $\bar{f} \in R/P$.

Tome $x = f/1 \in R_p$.

Temos que $\sigma(x) = \sigma.(f/1) = \bar{f}$.

Portanto σ é um homomorfismo sobrejetor.

Calculemos, finalmente, o núcleo de σ.

Seja $x \in R_p$, tal que $\sigma(x) = \bar{0}$.

Assim $x = f/g$ onde $f \in R$ e $g \in R-P$, e $\bar{f}\,\bar{g}^{-1} = \bar{0}$. Multiplicando esta última igualdade por $\bar{g}$ teremos $\bar{f} = \bar{0}$, ou seja $f \in P$. Portanto $\mathrm{Ker}\sigma \subset PR_p$.

Por outro lado, se $x \in PR_p$ então $x = f/g$, com $f \in P$ e $g \in R-P$. Então $\sigma(x) = \sigma(f/g) = \bar{f}.\bar{g}^{-1} = \bar{0}$.

Assim $\mathrm{Ker}\ \sigma = PR_p$.

Logo σ é um homomorfismo sobrejetor com núcleo PR_p.

Pelo teorema fundamental dos homomorfismos

$$R_p/PR_p \cong R/P,$$

seguindo-se o resultado.

Para o segundo isomorfismo, basta definirmos o homomorfismo:

$$\sigma_1 : R'_p \longrightarrow R'/A.$$

$$x = f/g \longmapsto \bar{f}\,\bar{g}^{-1}.$$

Observe que, também neste caso, tem sentido falar em $\bar{g}^{-1}$, pois $g \in (R - P)$ e, portanto $\bar{g}$ tem um inverso em R/P. Como $R/P \subset R'/A$, $\bar{g}$ tem inverso em R'/A.

Assim, no lema, podemos substituir P, R , A e R' por PR_p, R_p, AR_p e R'_p respectivamente.

A vantagem desta substituição é que R_p, além de anel de Dedekind, é um anel de valorização discreta. Assim PR_p é um ideal principal, digamos $PR_p = pR_p$

Sejam $\bar{x}_1$, $\bar{x}_2$, $\bar{x}_3, \ldots, \bar{x}_k$ elementos de R'_p/AR'_p , linearmente independentes sobre R_p/pR_p, e $x_1, x_2, \ldots, x_k$ seus representantes em R'_p.

Considere uma possível relação não trivial

$$\Sigma\, a_i x_i = 0$$

onde cada a_i está em R_p. Podemos ainda supor, sem perda de generalidade, que nem todos os a_i são divisíveis por p.

Então modulando por AR'_p, teremos:

$$\Sigma\ \bar{a}_i\ \bar{x}_i = 0$$

onde $a_i \in R_p/pR_p$ e $x_i \in R'_p/AR'_p$, com os $\bar{a}_i$ nem todos nulos. Isto não pode acontecer pois os $\bar{x}_i$ são linearmente independentes sobre R_p/pR_p. Assim

$$\dim_{R_p/PR_p} R'_p/AR'_p \leq [L:K] .$$

Logo

$$\dim_{R/p} R'/A \leq [L:K] .$$

Provemos agora o seguinte teorema, conhecido como TEOREMA DA DESIGUALDADE FUNDAMENTAL:

(3.3.02) Teorema - Sejam R um anel de Dedekind com corpo de frações K, L uma extensão finita, de grau n, de K, R' o fecho integral de R em L, P um ideal primo de R e M = R-P e P^e a extensão de P a R'. Se tivermos $P^e = \beta_1^{e_1}\beta_2^{e_2}\ldots\beta_r^{e_r}$ e denotarmos por R_M o anel local R_p, por R'_M o anel de frações $M^{-1}R'$ e por f_i o grau de inércia $[R'/\beta_i : R/P]$ então:

$$\Sigma\ e_i f_i = \dim_{R/P} R'/P^e .$$

Consequentemente

$$\sum_{i=1}^{n} e_i f_i \leq [L:K]$$

$$R'/p^e \simeq S,$$

e portanto

$$\dim_{R/P} R/P^e = \sum_{i=1}^{r} \dim_{R/P} R'/\beta_i^{e_i}.$$

Como R' - módulo, $R'/\beta_i^{e_i}$ admite uma cadeia de composição, de comprimento e_i, a saber:

$$(3.3.03) \qquad R'/\beta_i^{e_i} \quad \beta_i/\beta_i^{e_i} \quad \beta_i^2/\beta_i^{e_i} \ldots \quad \beta_i^{e_i}/\beta_i^{e_i} = (0)$$

Para provarmos que tal cadeia é de composição, basta vermos que β_i^j/β_i^{j+1} é simples, isto é, não existe R'-módulo N tal que:

$$\beta_i^j/\beta_i^{j+1} \supset N \supset (0).$$

Mas isto é equivalente a β_i^j/β_i^{j+1} ser cíclico e existir um ideal maximal M de R' tal que $M(\beta_i/\beta_i^{j+1}) = (0)$.

Como β_i é um ideal maximal de R' e $\beta_i.\beta_i/\beta_i^{j+1} = (0)$, basta verificarmos que β_i^j/β_i^{j+1} é cíclico. Mas isto é verdade pois todo ideal em um anel de Dedekind é gerado por dois elementos.

Assim a cadeia (3.3.03) é uma cadeia de composição de comprimento e_i.

Para calcularmos $\dim_{R/p} R'/\beta_i^{e_i}$, utilizaremos o seguinte fato

$$\dim_{R/P} R'/\beta_i^{e_i} = \dim_{R/P} \beta_i/\beta_i^{e_i} + \dim_{R/P} (R'/\beta_i^{e_i}) \,/\, (\beta_i/\beta_i^{e_i})$$

Como

$$(R'/\beta_i^{e_i}) \;/\; (\beta_i/\beta_i^{e_i}) \simeq R'/\beta_i .$$

podemos escrever:

$$(3.3.04) \qquad \dim_{R/P} R'/\beta_i^{e_i} = \dim_{R/P} R'/\beta_i + \dim_{R/P} \beta_i/\beta_i^{e_i} .$$

Do mesmo modo

$$\dim_{R/P} \beta_i/\beta_i^{e_i} = \dim_{R/P} \beta_i^2/\beta_i^{e_i} + \dim_{R/P} \beta_i/\beta_i^2$$

Substituindo este resultado em (3.3.04) teremos:

$$\dim_{R/P} R'/\beta_i = \dim_{R/P} R'/\beta_i + \dim_{R/P} \beta_i/\beta_i^2 + \dim_{R/P} \beta_i^2/\beta_i^{e_i}$$

Procedendo de maneira análoga, teremos:

$$(3.3.05) \qquad \dim_{R/P} R'/\beta_i^{e_i} = \dim_{R/P} R'/\beta_i + \dim_{R/P} \beta_i/\beta_i^2 + \dim_{R/P} \beta_i/\beta_i^2$$

$$+ \dim_{R/P} \beta_i^2/\beta_i^3 \ldots + \dim_{R/P} \beta_i^{e_i+1} / \beta_i^{e_i}$$

Provaremos agora que $\dim_{R/P} \beta_i/\beta_i^{j+1}$, para cada $j = 0, 1, 2, \ldots, e_i-1$, é f_i (aqui $\beta_i^0 = R'$). Assim, como em (3.3.05) existem exatamente e_i parcelas, teremos

$$\dim_{R/P} R'/\beta_i^{e_i} = e_i f_i$$

Para $j = 0$ temos exatamente a definição de f_i.

Para $j \geq 1$ teremos

$$\dim_{R/P} \beta_i/\beta_i^{j+1} = \dim_{R'/\beta_i^j} \beta_i^j/\beta_i^{j+1} \cdot \dim_{R/P} R'/\beta_i$$

Assim, como $\dim_{R/p} R'/\beta_i = f_i$, se provarmos que

$\dim_{R'/\beta_i} \beta_i^j/\beta_i^{j+1} = 1$, teremos o resultado.

Para isto, lembremos que, sendo R' um anel de Dedekind, R'/β_i^{j+1} é um anel principal.

Logo existe $\bar{x} \in \beta_i^j/\beta_i^{j+1}$ tal que $\beta_i^j/\beta_i^{j+1} = (\bar{x})$

Defina

$$\sigma : R' \longrightarrow \beta_i^j/\beta_i^{j+1}.$$

$$a \longmapsto \overline{ax}$$

É fácil ver que σ é um homomorfismo sobrejetor , tal que $\beta_i \subset \text{Ker}\sigma$. Como β_i é um ideal maximal de R' e $\text{Ker}\sigma \neq R'$, teremos $\beta_i = \text{Ker}\sigma$. Assim $R'/\beta_i \simeq \beta_i^j/\beta_i^{j+1}$.

Logo

$$\dim_{R'/\beta_i} \beta_i^j/\beta_i^{j+1} = 1 \quad ,$$

e, consequentemente, $\dim_{R/p} R'/\beta_i^{e_i} = e_i f_i$.

Como $\dim_{R/p} R'/P^e = \sum_{i=1}^{r} \dim_{R/p} R'/\beta_i^{e_i}$

teremos

$$\dim_{R/p} R'/P^e = \sum_{i=1}^{r} e_i f_i$$

Valendo, portanto,

$$\sum_{i=1}^{r} e_i f_i \leq [L:K]$$

Para a última afirmação, suponha que

$\sum_{i=1}^{r} e_i f_i = [L:K]$. Devemos provar que R'_M é um R_M-módulo finito.

Como $\beta_i \cap M = \emptyset$, pois $M = R - P$ e $\beta_i \cap R = P$, os inteiros e_i, f_i e $[L:K]$ não se alteram se nós substituirmos R, R' e P por respectivamente R_M, R'_M e PR_M, (ver lema(3.3.01)).

Assim podemos supor que R é um anel principal e $P = pR$ para algum $p \in P$.

Mostramos, no lema(3.3.01) que se $\{\bar{x}_j\}$ é uma base de R'/P^e sobre R/P, podemos escolher alguns de seus representantes $\{x_j\}$ em R', linearmente independentes sobre R. Como $[L:K] = \dim_{R/P} R'/p^e$, $\{x_j\}$ é uma base de L sobre K.

Provaremos que $R' = \sum_{j=1}^{n} Rx_j$

É claro que $R' \supset \sum_{j=1}^{n} Rx_j$, pois $x_j \in R'$ e $R \subset R'$.

Tome $x \in R'$.

Como $\{x_j\}$ é uma base de L/K e $x \in L$, temos

$$x = \sum_{j=1}^{n} a_j x_j \quad \text{onde} \quad a_j \in K.$$

Sem perda de generalidade, podemos supor que nem todos os a_j estão em P, pois se isto acontecesse teríamos

$$x = \sum_{j=1}^{n} a_j x_j \quad \varepsilon \quad \sum_{j=1}^{n} Rx_j$$

Seja $v_p(a_j) = n_j$.

Para cada n_j existe m_j tal que $n_j + m_j \geq 0$.

Como $m_j = v_p(p^{mj})$, teremos $v_p(p^{mj}aj) \geq 0$, ou seja $p^{mj}aj \varepsilon R$.

Tome para m_j, o menor inteiro tal que $m_j+n_j \geq 0$ e seja $m = \max\{mj\}$

Suponha $m \neq 0$.

Assim teremos $p^m a_{j_0} \varepsilon R$ e $p^m a_{j_0} \varepsilon P$, para algum j. Portanto

$$p^m x = \sum_{i=1}^{n} p^m a_j x_j$$

Passando o quociente módulo $P^e = PR'$, obtemos

$$\bar{0} = \sum_{i=1}^{n} \bar{b}_j \bar{x}_j$$

onde $\bar{b}_j = \overline{p^m a_j} \varepsilon R/P$ e são nem todos nulos.

Isto é uma contradição com o fato de $\{x_j\}$ ser uma base de R'/P^e sobre R/P.

Logo $m = 0$ e $R' \subseteq \sum_{j=1}^{n} Rx_j$.

Assim, como provamos acima que $R' = \sum_{j=1}^{n} Rx_j$, temos que $R'_M = \sum_{j=1}^{n} R_M x_j$. Seguindo-se o resultado.

Reciprocamente, vamos supor que R'_M é um R_M-módulo finito.

Como R_M é um anel principal e L é o corpo de frações de R'_M, existe uma base $x_1, x_2, \ldots, x_n$ de L sobre K tal que

$$(3.3.06) \qquad R'_M = \sum_{i=1}^{n} R_M x_i$$

Então, se P é um ideal de R_M, $P = pR_M$ para algum $p \in P$ e, portanto, o ideal PR'_M também será principal, e nós podemos sem perda de generalidade, denotar PR'_M por pR'_M. Assim

$$(3.3.07) \qquad pR'_M = \sum_{i=1}^{n} pR_n x_i .$$

Como, por (3.3.06), cada elemento x de R'_M se escreve de maneira única na forma

$$x = a_1x_1 + a_2x_2 + \ldots + a_nx_n \ , \ a_i \in R_M$$

podemos definir um homomorfismo σ, sobrejetor e com núcleo pR'_M, de R'_M no produto cartesiano.

$$S = R_M/pR_M \times R_M/pR_M \times \ldots \times R_M/pR_M$$

da seguinte maneira:

$$\sigma : R'_M \longrightarrow S$$

$$x = a_1x_1 + \ldots + a_nx_n \longmapsto (\bar{a}_1 , \bar{a}_2, \ldots, \bar{a}_n).$$

Assim teremos

$$R'_M/pR'_M \simeq \prod_{i=1}^{n} (R_M/pR_M) \simeq \prod_{i=1}^{n} (R_M/pR_M)\, x_i .$$

Portanto

$$\dim_{R_M/pR_M} R'_M/pR'_M = n \text{ (nº de } x_i) = \left[L:K\right]$$

Pela demonstração do lema (3.3.01) e desde que os elementos de M, módulo P, são inversíveis teremos:

$$R'_M/pR'_M \simeq (R'/pR')_{\frac{M + pR}{pR'}} = R'/pR' = R'/p^e$$

e

$$R_M/pR_M \simeq (R/P)_{\frac{M + P}{P}} \simeq R/P$$

e, portanto,

$$\dim_{R/P} R'/P^e = \dim_{R_M/pR_M} R'_M/pR' = N = \left[L:K\right]$$

Mas

$$\dim_{R/P} R'/P^e = \Sigma\, e_i f_i .$$

Logo $\Sigma\, e_i f_i = n$, seguindo-se o resultado.

(3.3.08) - Corolário - Se L, como no teorema (3.3.03), é uma extensão separável de K tem-se $\Sigma\, e_i f_i = \left[L:K\right]$

Prova - Como L é uma extensão separável de K,

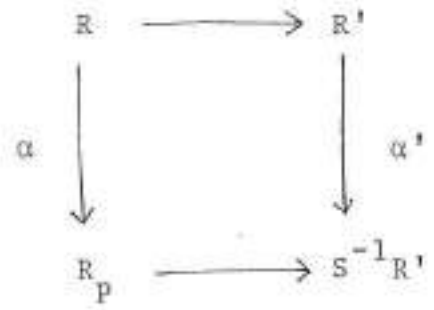
existe uma base $\{v_1, v_2, \ldots, v_n\}$ de L sobre K, tal que $R' \subset \sum_{i=1}^{n} Rv_i$, ou seja, R' é um R-módulo finito. Consequentemente R'_M é um R_M-módulo finito e pelo teorema (3.3.02), vale a igualdade.

O teorema (3.3.02) admite uma recíproca. É quando L/K é normal. Ela é dada como se segue:

(3.3.09) - Teorema - Sejam R um domínio integralmente fechado, K seu corpo de frações, L uma extensão finita e normal de K e R' o fecho integral de R em L. Se P é um ideal primo de R, então os β_i, ideais primos de R' acima de P, são todos conjugados uns dos outros. Se, além disso, R é um anel de Dedekind, os β_i são os fatores da decomposição de PR', os inteiros e_i (resp f_i) são todos iguais, digamos a e (resp.f). Se g é o número de ideais primos de R', acima de P, temos $e.f.g \leq [L:K]$. Se a extensão é separável, então $e.f.g = [L:K]$.

Prova - Como R' é inteiro sobre R, dado o ideal primo P, de R, existe um ideal primo Q de R' acima de P. De fato, sendo R' inteiro sobre R, o anel $S^{-1}R^1$, onde $S = R-P$, é inteiro sobre R_p.

Considere os homomorfismos:



Seja N um ideal maximal de $S^{-1}R$. Então $M = N \cap R_p$ é o ideal maximal de R_p. Se $Q = (\alpha')^{-1}(N)$, então Q é um ideal primo de R' e, como o diagrama acima é comutativo, nós temos $Q \cap R = \alpha^{-1}(M) = P$.

Sejam β, um ideal primo de R', acima de P e $\beta^{(j)}$ os seus conjugados, isto é, $\beta^{(j)} = s(\beta)$ para algum $s \in G$(= grupo de Galois de L sobre K.).

Desde que $R' = I_L(R)$, $s(R') = R'$ para cada $s \in G$. De fato, se $x \in R'$, $x = s(s^{-1}(x))$. Como $s^{-1} \in G$ e para cada $\sigma \in G$, $\sigma(x) \in R'$, teremos $s^{-1}(x) \in R'$. Assim $x = s(s^{-1}(x)) \in s(R')$. Portanto $R' \subset s(R')$ para cada $s \in G$. A outra inclusão é óbvia.

Consequentemente os $\beta^{(j)}$ são ideais primos de R' acima de P.

Suponha agora que os $\beta^{(j)}$ não são os únicos ideais primos de R' acima de P. Isto é, suponha que exista um ideal primo D, de R', acima de P e distinto dos $\beta^{(j)}$, para todo j..

Como R' é inteiro sobre R e P é maximal, dois ideais de R' acima de P são iguais ou incomparáveis.

Desde que $D \neq \beta^{(j)}$ para cada j, tome $x \in D - \bigcup \beta^{(j)}$. Este x existe pois se $D = \bigcup \beta^{(j)}$ então $D = \beta_j$

para algum j.

Assim nem x, nem os conjugados de x, nem o produto de x por seus conjugados, nem potência alguma deste produto, estão em $\beta^{(j)}$. Em particular em β. Mas alguma potência deste produto é a norma de x, que está em R, pois $x \in R'$.

Então como a norma de x está em R e em D, estará também em $P = R \cap D$. O que não pode acontecer pois $P \subset \beta$.

Logo os únicos ideais primos de R', acima de P, são os conjugados de β.

Suponhamos agora que R é um anel de Dedekind.

Se P é um ideal primo de R, os ideais primos de R', acima de P, são aqueles que aparecem na decomposição de PR'.

Para a igualdade dos e_i e dos f_i basta estudarmos o seguinte:

(3.3.10) - Igualdade dos f_i - Seja $\sigma \in G$.

Considere os homomorfismos.

$$R' \xrightarrow{\sigma} R' \xrightarrow{\phi} R'/\beta,$$

onde β é um dos ideais primos que aparecem na decomposição de PR'.

Como $\phi \circ \sigma$ é sobrejetiva, pelo teorema fundamental dos homomorfismos:

$$R'/Ker(\phi \circ \sigma) \simeq R'/\beta.$$

Mas

$$Ker(\phi o \sigma) = \{x \in R' \; ; \; \sigma(x) \in \beta\} =$$

$$= \{x \in R' \; ; \; x \in \sigma^{-1}(\beta)\} = \sigma^{-1}(\beta)$$

E como $\sigma^{-1}(\beta) = \beta^{(j_0)}$ para algum $\beta^{(j_0)}$, conjugado de β, teremos:

$$R'/\beta^{(j_0)} \simeq R'/\beta \; ,$$

valendo, assim, a igualdade dos f_i.

(3.3.11) - Igualdade dos e_i - Seja $PR' = \beta_1^{e_i} \beta_2^{e_r} \ldots \beta_r^{e_r}$.

Sabemos que os β_j, para $j = 2,3,\ldots, r$ são os conjugados de β_1, isto é, para cada $j = 2,3,\ldots,r$, existe $\sigma_j \in G$; tal que $\sigma_j(\beta_j) = \beta_1$

Como $\sigma_j(PR') = PR'$, teremos

$$\sigma_j(PR') = \sigma_j(\beta_1)^{e_1} \sigma_j(\beta_2)^{e_2} \ldots \sigma_j(\beta_j)^{e_j} \ldots \sigma_j(\beta_r)^{e_r}$$

Mas $\sigma_j(\beta_j) = \beta_1$, portanto

$$\sigma_j(PR') = \sigma_j(\beta_1)^{e_1} \sigma_j(\beta_2)^{e_2} \ldots \beta_1^{e_2} \ldots \sigma_j(\beta_r)^{e_r}.$$

Pela unicidade da decomposição de PR' teremos $e_1 = e_j$ para cada j.

Logo os e_i são todos iguais.

Finalmente, as duas últimas afirmações são consequência dos Teoremas anteriores pois, como sabemos,

(3.3.12) $\quad \sum e_i f_i \leq [L:K]$,

e desde que os e_i e os f_i são todos iguais, digamos a e e a f, respectivamente, teremos

$$\sum_{i=1}^{g} ef \leq [L:K] \text{ , onde g é o número de } \beta_i$$

O que nos dá: $gef \leq [L-K]$

Se L é uma extensão normal de K, então vale a igualdade em (3.3.12). Logo $gef = [L:K]$

Ficando provado o Teorema.

Sabemos, da teoria dos anéis, que todo domínio principal (D.P) é um anel de fatorização única (D.F.U), mas nem todo D.F.U é um D.P. (por exemplo $K[x,y]$ onde K é um corpo e x e y são indeterminadas). Assim sempre nos vem a seguinte pergunta:

"O que falta a um D.F.U. para ser um D.P?"

A resposta que podemos dar é a seguinte:

(3.3.13) - Lema - Seja R um domínio de integridade. Então R é um domínio principal se, e somente se, R é um anel de Dedekind e um domínio fatorial.

Prova - Se R é um D.P., R é um D.F.U. e um anel

de Dedekind.

A recíproca é uma consequência do seguinte

(3.3.14) - Lema - Um domínio R é um domínio principal se, e somente se, R é um domínio fatorial e todo ideal primo próprio é maximal.

Prova - Se R é um domínio principal, o resultado é óbvio.

Reciprocamente, suponha que R é um domínio fatorial no qual todo ideal primo próprio é maximal.

Sabemos que em um domínio fatorial todo ideal primo minimal (no conjunto dos ideais primos) é principal . De fato, sejam P um ideal primo minimal de R e $a \in P$, $a \neq 0$. Se a é irredutível, como R é um domínio fatorial, o ideal aR é um ideal primo. Pela minimalidade de P, aR = P. Se a é redutível, $a = p_1 \ldots p_r$ onde os p_i são elementos irredutíveis de R. Assim, como P é um ideal primo, $p_{i_o} \in P$ para algum i_o. E, novamente, pela minimalidade de P, $P = p_{i_o}R$. Logo todo ideal primo minimal é um ideal principal.

Seja A um ideal próprio de R.

O conjunto Σ dos ideais principais de R contendo A é não vazio, pois R é um ideal principal. Além disso , pelo Lema de Zorn, Σ tem um elemento minimal. De fato, seja

(3.3.15) $\quad A_1 \supset A_2 \supset A_3 \supset \ldots \supset A_n \supset \ldots \supset A$

uma cadeia de ideais de Σ. Queremos provar que esta cadeia é estacionária para podermos aplicar o Lema de Zorn.

Seja $a \in A - \{0\}$

Sendo R um domínio fatorial podemos escrever $a = p_1 \cdot p_2 \cdots p_r$, onde cada p_i é um elemento primo de R. E como $A \subset A_i$ para todo i , e $A_i = a_i R$, teremos que

$$a_i / p_1 \cdot p_2 \cdots p_r$$

Então os elementos irredutíveis que aparecem na decomposição dos a_i são, no máximo, os p_i. Isto é, cada a_i é uma combinação dos p_i. Como os p_i são em número finito, os a_i distintos, também o serão.

Logo a cadeia (3.3.15) é estacionária e, pelo Lema de Zorn, Σ tem um elemento minimal.

Seja yR um elemento minimal de Σ

Como $A \subset yR$, segue-se que $A = yA_1$ onde A_1 é um ideal de R.

Observe que y pode ser tomado como não unidade de R pois, como sabemos, todo ideal primo próprio de R está contido em um ideal maximal. Como cada ideal primo é maximal, este ideal primo é também minimal (entre os ideais primos). Como vimos anteriormente, este ideal minimal é principal. Logo y pode ser tomado como não unidade de R.

Se $A_1 = R$, o problema está resolvido.

Caso contrário, existe $z \in R$ tal que $A_1 \subset zR$ com z não unidade de R.

Note que, agora, devemos ter, necessariamente, $A_1 = zR$ pois

$$A = yA_1 \subset zR.\ yR = yzR \subset yR$$

e assim, pela minimalidade de yR, teríamos yR = yzR, o que é um absurdo pois z não é unidade em R.

Portanto $A_1 = zR$ e, assim, A = yzR.

Logo R é um domínio principal.

4 - UM EXEMPLO NÃO ELEMENTAR DE ANEL DE DEDEKIND.

(4.1) - Introdução

Para finalizar este trabalho, daremos um exemplo, não elementar, de anel de Dedekind, bem como algumas de suas características.

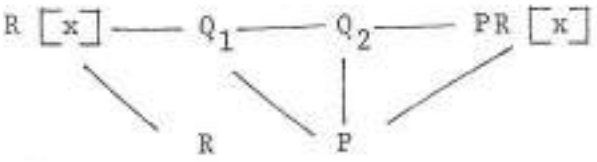
Para tanto necessitaremos de alguns resultados que veremos agora.

(4.2.01) - Lema - Seja R um domínio de integridade com corpo de frações K e seja x uma indeterminada. Existe uma correspondência biunívoca entre os ideais primos de $R[x]$ que se contraem para 0 em R e os ideais primos de $K[x]$.

Prova - Considere o sistema multiplicativamente fechado de R, $S = R - \{0\}$. Então $S^{-1}R = K$ e, naturalmente, $S^{-1}(R[x]) = K[x]$. Assim, pelo teorema da correspondência entre os ideais primos de $S^{-1}R([x])$ e os ideais de $R[x]$ que não interceptam S, existe uma correspondência biunívoca entre os ideais primos de $K[x]$ e os ideais primos P, de $R[x]$, tais que $P \cap S = \emptyset$. Mas se $P \cap S = \emptyset$ então $P \cap R = \{0\}$. Provando o lema.

(4.2.02) - Lema - Seja R um anel. Não pode existir em $R[x]$ uma cadeia de três ideais primos distintos com a mesma contração em R.

Prova - Suponha que tenhamos uma cadeia de três ideais primos distintos, em $R[x]$, com a mesma contração em R, a saber:



Passando ao anel quociente $R[x] / PR[x]$ teremos:

$$\frac{R}{P}[x] = \frac{P[x]}{PR[x]} \supset \frac{Q_1}{PR[x]} \supset \frac{Q_1}{PR[x]} \supset (\overline{0})$$

Pelo lmea (4.2.01), existe uma correspondência biunívoca, preservando ordem, entre os ideias primos de $R[x] / PR[x]$ que se contraem para $(\overline{0})$ e os ideais primos de $K[x]$, onde $K = c.f(R/P)$. Assim em $K[x]$ teremos uma cadeia com três ideais primos e distintos. Mas isto é absurdo, pois $K[x]$ é um domínio principal. Logo, em $R[x]$, não podemos ter uma cadeia com três ideais (distintos)se contraindo para o mesmo ideal de R.

(4.2.03) - Definição - Dizemos que uma cadeia descendente de ideais primos a partir de P tem comprimento n se, e somente se, existem n + 1 ideais primos distintos tais que:

$$P = P_o \supset P_1 \supset \ldots \supset P_n$$

(4.2.04) - Definição - Dizemos que um ideal primo P tem altura n, e escrevemos alt(P) = n, se existir uma cadeia descendente, a partir de P, de comprimento n e se não pudermos ter nenhuma cadeia descendente, a partir de P, de comprimento maior do que n.

(4.2.05) - Lema - Seja P um ideal primo de R, com altura n. No anel de polinômios $R[x]$, denote $P^* = PR[x]$. Seja Q um ideal primo de $R[x]$, contendo propriamente P^* e que se contraia para P, em R. Então:

$$n \leq alt(P^*) \leq 2n$$

$$n + 1 \leq alt\ (Q) \leq 2n+1$$

Prova - Seja $P = P_0 \supset P_1 \supset \ldots \supset P_n$ uma cadeia descendente a partir de P.

Usando * para a extensão de um ideal de R a um ideal de $R[x]$ teremos:

(4.2.06) $\quad Q \supset P_0^* \supset P_1^* \supset \ldots \supset P_n^*$.

Observe, primeiramente, que se P é um ideal primo de R então $PR[x]$ é um ideal primo de $R[x]$. De fato, considere o homomorfismo sobrejetivo:

$$\sigma : R[x] \longrightarrow (R/P)[x]$$

$$a_1+\ldots+a_n x^n \longmapsto \bar{a}_1+\ldots+\bar{a}_n x^n .$$

Temos que $\operatorname{Ker}\sigma = PR[x]$

Logo $\dfrac{R[x]}{PR[x]} \qquad R/P[x]$

Como P é um ideal primo de R, R/P é um domínio de integridade e assim $\dfrac{R[x]}{PR[x]}$ é um domínio de integridade. Consequentemente $PR[x]$ é um ideal primo de $R[x]$.

Assim a cadeia (4.2.06) é uma cadeia de ideais primos. Isto mostra que:

$$n \leq \operatorname{alt}(P^*) \leq \operatorname{alt}(Q).$$

Seja, agora,

$$(4.2.07) \qquad P^* \supset P_1 \supset \ldots \supset P_m^*$$

uma cadeia descendente a partir de P*

Tome a contração em R de cada ideal em (4.2.07).

Somente P* pode se contrair para P, pois se $(P_1^*)^c = P$ teríamos:

$$PR[x] = (P_1^*)^{ce} \subset P_1^* \subset P^* = PR[x] ,$$

e assim o comprimento de (4.2.07) não seria n.

Pelo lema (4.2.02), no máximo dois P_i^* distintos podem se contrair para o mesmo P_i em R. Então, como alt(P)=n existem no máximo 2n P_i^* distintos. Logo.

$$n \leq alt(P^*) \leq 2n$$

De maneira análoga, prova-se que $alt(Q) \leq 2n+1$, valendo portanto as desigualdades

$$n + 1 \leq alt(Q) \leq 2n + 1.$$

(4.2.08) - Lema - Sejam P um ideal primo de R, com altura n, PR[x] a extensão de P a R[x] e Q um ideal de R[x] contendo PR[x] tal que sua contração em R é P. Se R é um anel de Dedekind, então:

$$alt(PR[x]) = n \text{ e } alt(Q) = n + 1$$

Prova - Em virtude do lema (4.2.05), precisamos provar, apenas, que $alt(PR[x]) \leq n$ e $alt(Q) \leq n + 1$.

Observe, primeiramente, que como P é um ideal maximal R/P é um corpo e, portanto, (R/P)[x] é um anel principal. Assim a extensão a R/P[x] de qualquer ideal primo de R contendo P terá altura 1.

Provemos então que alt(PR[x]) é n.

Suponha que tivéssemos alt(PR[x]) > n. Então PR[x] conteria um ideal primo P_0, com altura n.

Seja P_1 a contração de P_0 em R.

É claro que P_1 está propriamente contido em P pois, se fosse $P_1 = P$ teríamos:

$$PR[x] \supset P_0 \supset P_1 R[x] = PR[x]$$

E, neste caso, a altura de P* seria n. Como isto não ocorre, P_1 está contido propriamente em P e, consequentemente, tem altura menor do que n.

(4.2.09) - Afirmo: A única maneira possível de termos a altura de P_0 igual a n é termos P_1 com altura n-1 e P_0 contendo $P_1 R[x]$

Prova - Provaremos o resultado por indução sobre o comprimento n da cadeia.

Para n = 1 teremos

$$PR[x] \supset \ldots \supset P_0 \supset Q_1$$

$$P \supset P_1$$

Neste caso teremos $Q_1 = P_1 R[x]$, pois caso contrário, teríamos P_0 com altura 2. Assim vale o resultado.

Suponha o resultado válido para uma cadeia de comprimento n - 1.

Provaremos o resultado para uma cadeia de comprimento n.

Considere as cadeias:

$$(4.2.10) \qquad PR[x] \supset \ldots \supset P_0 \supset Q_1 \supset \ldots \supset Q_n$$

$$(4.2.11) \qquad P \supset \ldots \supset P_1 \supseteq \ldots \supseteq P_n$$

onde $P_i = Q_i^c$, para cada i.

Como a altura de P_1 é menor do que n, por hipótese de indução, $P_1R[x]$ tem altura menor que n e valem:

i) $P_1R[x] \subset P_0$

ii) $alt(P_1R[x]) = alt(P_1) < n$

Se a altura de P_1 não fosse n - 1, deveríamos necessariamente ter na cadeia (4.2.10) dois pares $\{Q_j, Q_{j_1}\}$ e $\{Q_s, Q_{s_1}\}$ tais que $Q_j^c = Q_{j_1}^c = P_j$ e $Q_s^c = Q_{s_1}^c = P_s$.

Suponha, sem perda de generalidade, que $j < j_1 < s < s_1$.

Nós devemos ter $Q_{j_1} = P_j^* = P_jR[x]$, pois, caso contrário, teríamos três ideais de $R[x]$ (Q_j, Q_{j_1}, P_j^*) se contraindo para um mesmo ideal de R, o que não pode acontecer.

Como $alt(P_j) < n$, usando ainda a hipótese de indução, teríamos:

$$alt(P_j) = alt(P_j^*) = alt(Q_{j_1}) = (n - 1) - j.$$

Mas depois de P_j só existem (n - 1)- j ideais

primos na cadeia (4.2.11) e assim não poderíamos ter os ideais Q_s e Q_{s_1} se contraindo para o mesmo P_s. Logo a altura de P_1 deve ser n - 1, provando a afirmação.

Para mostrarmos que a altura de $PR[x]$ é n, passemos ao anel quociente R/P_1.

Como P/P_1 tem altura 1, (pela observação feita no início da prova deste lema), a altura de $(P/P_1).(R/P)[x]$ é 1.

Desde que:

$$(P/P_1).(R/P)[x] = \frac{PR[x]}{P_1R[x]}$$

não podemos ter ideais primos entre $PR[x]$ e $P_1R[x]$. Então devemos ter $PR[x] = P_0$. Seguindo-se o resultado.

Agora é fácil provar que a altura de Q é n + 1.

De fato, suponha que a altura de Q fosse maior do que n + 1.

Seja:

$$Q \supset Q_1 \supset \ldots \supset Q_s.$$

uma cadeia de ideais primos a partir de Q, com $s > n + 1$.

Considere a cadeia

$$P \supseteq P_1 \supseteq \ldots \supseteq P_s.$$

onde cada P_i é a contração de Q_i, em R.

Como a altura de P é n, deve existir pelo menos

dois conjuntos de dois ideais distintos $\{Q_j, Q_{j+1}\}$ e $\{Q_r, Q_{r+1}\}$ tais que

$$(Q_j^c = Q_{j+1}^c = P_j \quad e \quad Q_r^c = Q_{r+1}^c = P_r)$$

e mais

$$P_j^* = P_j R[x] = Q_{j+1} \quad e \quad P_r^* = P_r R[x] = Q_{r+1}.$$

Pelo que foi provado anteriormente(usando a mesma indução) a altura de P_j^* deve ser a mesma de P_j. Logo só podemos ter um conjunto de dois ideais primos se contraindo para o mesmo ideal primo em R. Portanto a altura de Q não pode ser maior do que n + 1. Como já sabemos que $alt(Q) \geq n+1$, devemos ter $alt(Q) = n + 1$. Seguindo-se o resultado.

(4.2.12) - Lema - Seja R um domínio de Dedekind com corpo quociente K. Para cada polinômio $f(x) = a_n x^n + \ldots + a_0$ de $K[x]$ seja o ideal fracionário $c(f) = (a_n, \ldots, a_0)$. Então $c(fg) = c(f).\ c(g)$.

Prova - Para cada ideal primo P de R, denote por v_p a valorização P-ádica de R. É imediato que:

$$v_p(c(f)) = \min \{v_p(a_i)\}$$

pois $c(f) = (a_0) + (a_1) + \ldots + (a_n)$.

Pela fatorização única de ideais fracionários em

anéis de Dedekind é suficiente provar que:

$$v_p(c(fg)) = v_p(c(f)) + v_p(c(g))$$

para cada ideal primo P de R.

Note que isto será verdade se for verdade em cada $R_p[x]$. De fato, suponha que para cada ideal primo P, de R, tenhamos, em $R_p[x]$,

$$v_p(c(fg)) = v_p(c(f)) + v_p(c(g)).$$

Sejam f e g polinômio de $R[x]$ e suponha que:

$$c(fg) = P_1^{\alpha_1} \ldots P_r^{\alpha_r}$$

Em $R_{p_i}[x]$ teremos

$$c(fg)\, R_{p_i}[x] = P_i^{\alpha_i} R_{p_i}[x]$$

Por hipótese

$$v_{p_i}(c(fg)R_{p_i}[x]) = v_{p_i}[c(f)R_{p_i}[x]] +$$

$$+ v_{p_i}[\, c(g)\, R_{p_i}[x]\,], \text{ isto é, se:}$$

$$c(f)\, R_{p_i}[x] = P_i^{m_i} R_{p_i}[x]$$

e

$$c(g)\, R_{p_i}[x] = P_i^{n_i} R_{p_i}[x]$$

então

$$\alpha_i = m_i + n_i$$

Logo

$$c(f) = P_1^{m_1} \ldots P_r^{m_r}$$

e

$$c(g) = P_1^{n_1} \ldots P_r^{n_r}$$

E assim $c(fg) = c(f) \cdot c(g)$.

Mas, sendo R_{p_i} um domínio principal, em R_{p_i} esta igualdade é verdadeira. Consequentemente o lema é verdadeiro.

(4.2.13) - Nota - Este último lema é importante porque mostra que, se R é um anel de Dedekind, o conjunto de todos os polinômios primitivos de $R[x]$ é um sistema multiplicativamente fechado de $R[x]$.

(4.3) Passemos finalmente ao nosso objetivo.

(4.3.01) - Exemplo - Sejam R um anel de Dedekind, S o sistema multiplicativamente fechado de $R[x]$ consistindo de todos os polinômios mônicos e T o sistema multiplicativamente fechado consistindo de todos os polinômios primitivos, isto

é, todos os polinômios f de $R[x]$ tais que $c(f) = R$. Os anéis $S^{-1}(R[x])$ e $T^{-1}(R[x])$ são, ambos, anéis de Dedekind.

De fato, como mostramos no capítulo zero, $R[x]$ é noetheriano e integralmente fechado. Assim $S^{-1}(R[x])$ e $T^{-1}(R[x])$ são, ambos, noetheriano e integralmente fechado. Portanto resta-nos mostrar que a dimensão de Krull de $S^{-1}(R[x])$ e de $T^{-1}(R[x])$ é 1.

Calculando primeiramente a dimensão de Krull de $S^{-1}(R[x])$.

Seja P um ideal primo de $R[x]$

Se $P \cap S \neq (0)$ então, $Q = P \cap S$ é um ideal primo de R, que é maximal, pois R é um anel de Dedekind.

Observe que se $P \neq QR[x]$ então, passando ao anel quociente $R[x] / QR[x]$, que é isomorfo a $(R/Q)[x]$, é fácil ver que:

$$P = QR[x] + f(x)\, R[x]$$

onde f(x) é um polinômio mônico, convenientemente escolhido.

Neste caso $P \cap S \neq \emptyset$, pois $f(x) \in P \cap S$, e portanto, $P(S^{-1}R[x]) = S^{-1}R[x]$.

Assim se $P \cap S \neq (0)$ e $P(S^{-1}R[x])$ é um ideal próprio de $S^{-1}(R[x])$ teremos $P = QR[x]$ onde $Q = P \cap R$. Pelo lema (4.2.08) a altura de P é 1 e, consequentemente a altura de $P(S^{-1}R[x])$ é 1.

Se $P \cap R = (0)$, então $PK[x]$ é um ideal primo de $K[x]$ on de K é o corpo de frações de R. Ainda neste caso, a latura de P é a mesma de $PK[x]$ que é 1. Assim a altura de $PS^{-1}(R[x])$ é 1

Logo $S^{-1}(R[x])$ é um anel de Dedekind.

Para mostrarmos que $T^{-1}(R[x])$ é um anel de Dedekind, basta observarmos que:

$$T^{-1}(R[x]) = T^{-1}(S^{-1}(R[x]))$$

Como $S^{-1}(R[x])$ é um anel de Dedekind, $T^{-1}(R[x])$ também o é.

(4.3.02) - Observação - $T^{-1}(R[x])$ é costumeiramente denotado por R(x).

(4.3.03) - Observação - Por todo este trabalho $S^{-1}(R[x])$ será denotado por R^1.

Vejamos agora algumas das características de R^1 e R(x).

(4.3.04) - Proposição - R^1 tem o mesmo grupo de classes de

ideal que R.

Prova - Considere a aplicação ϕ que leva $\bar{C}$ em $\overline{CR^1}$. ϕ é uma aplicação injetiva do grupo das classes de ideal de R sobre o de R^1.

Nós podemos provar que ϕ é injetiva mostrando que se dois ideais próprios D e E de R não estão na mesma classe então DR^1 e ER^1 também não estão na mesma classe.

Suponha que $\overline{DR^1} = \overline{ER^1}$

Assim

$$ER^1 = \left(\frac{f(x)}{g(x)}\right) DR^1$$

onde f(x) e g(x) pertencem a $R[x]$.

Sejam a o coeficiente líder de f(x), b o de g(x) e d um elemento qualquer de D. Então vale

$$d \cdot \frac{f(x)}{g(x)} = \frac{e(x)}{h(x)}$$

onde e(x) é um polinômio de $R[x]$, com coeficientes em E e h(x) é um polinômio mônico de $R[x]$. Portanto, temos:

$$d.f(x).h(x) = e(x).g(x).$$

O coeficiente líder de e(x) g(x) está em bE. Logo aD está contido em bE.

Tomando agora e pertencente a E temos que:

$$e = \frac{f(x)}{g(x)} \cdot \frac{d(x)}{h_1(x)}$$

onde d(x) é um polinômio de $R[x]$ com coeficientes em D e $h_1(x)$ é um polinômio mônico de $R[x]$. Assim temos:

$$e.g(x).h_1(x) = f(x).d(x).$$

O coeficiente líder de f(x).d(x) está em aD. Logo bE está contido em aD.

Temos, portanto, aD = bE e assim $\overline{D} = \overline{E}$.

Logo se $\overline{E} \neq \overline{D}$ então $\overline{DR^1} \neq \overline{ER^1}$ e, consequentemente, ϕ é injetiva.

Para provarmos a sobrejetividade de ϕ, seja P um ideal primo de R^1.

Como vimos anteriormente se $P \cap R \neq (0)$ então $P = QR^1$ onde Q é um ideal primo de R.

Assim $\overline{P} = \overline{QR^1}$ é imagem de uma classe de R.

Suponha agora que P é um ideal primo de R^1 tal que $P \cap R = (0)$

Seja $P_1 = P \cap R[x]$

Então $P_1 \cap R = (0)$ e $P^1 K[x]$ é um ideal primo de $K[x]$ onde K é o corpo de frações de R.

Como $K[x]$ é um domínio principal podemos escrever $P_1 K[x] = f(x).K[x]$, onde f(x) pode ser escolhido em $R[x]$.

Seja C = c(f)

Suponha que $g(x).f(x) \in R[x]$

Assim $c(fg) \subset R$ e como c(fg) = c(f).c(g), temos

que $c(f) \subset C^{-1}$. Portanto $g(x) \in C^{-1}R[x]$.

Reciprocamente se $g(x) \in C^{-1}R[x]$, Então $g(x).f(x) \in R[x]$.

Assim

$$P^1 = f(x).K[x] \cap R[x] = C^{-1}R[x].f(x)R[x]$$

e

$$P = P^1R^1 = C^{-1}R^1 f(x).R^1.$$

Portanto $\bar{P} = \overline{P^1R^1} = \overline{C^{-1}R^1}$.

Como o grupo das classes de ideal de R^1 é gerado por todos os ideais $\bar{P}$, onde P é um ideal primo de R^1, fica provada a proposição.

(4.3.05) - Corolário - R^1 tem um ideal primo em cada classe do grupo de classes.

Prova - Seja w uma não unidade de R.

Então o ideal

$$P^1 = (wx + 1) K[x] \cap R[x]$$

é um ideal primo de $R[x]$ que não intercepta S. Pela demonstração da proposição (4.3.04), temos

$$P^1 = C^{-1}R[x] . (wx + 1) R[x]$$

onde C é o ideal fracionário gerado por w e 1.

Como $P^1 \cap S = \emptyset$, P^1R^1 é um ideal primo de R^1.

Assim teremos

$$P = P^1R^1 = C^{-1}R[x] \cdot R^1.(wx+1)\,R[x].R^1 =$$
$$= (wx+1)R^1.$$

Portanto P é um ideal primo na classe principal.

Seja, agora, C um ideal próprio qualquer, numa classe não principal $\overline{D^{-1}}$.

Como já foi visto, C é gerado por dois elemen - tos, digamos c_0 e c_1.

Considere o ideal

$$Q^1 = (c_0 + c_1x).K[x] \cap R[x] .$$

Q^1 é um ideal primo de $R[x]$ que não intercepta S. Consequentemente $Q = Q^1R^1$ é um ideal primo de R^1.

Como sabemos (ver demonstração proposição (4.3.04))

$$Q = Q^1\,R^1 = C^{-1}R^1\,(c_0 + c_1x)R^1.$$

Então $\overline{Q} = \overline{C^{-1}R^1} = \overline{D}$.

Assim Q é um ideal primo na classe $\overline{D}$.

Logo R^1 tem um ideal primo em cada classe.

Agora, para finalizar, sobre o anel R(x) nós po

demos dizer o seguinte:

(4.3.06) - Proposição - Se R é um anel de Dedekind então R(x) é um domínio principal.

Prova - Desde que $R(x) = T^{-1}R^1$, o lema(1.6.25)e a prova do corolário (4.3.05) mostram que cada classe não principal de R(x) contém um ideal primo QR(x), onde Q é um ideal de R^1, do tipo

$$(c_0 + c_1x).\ K[x] \cap R^1$$

onde K é o corpo de frações de R e c_0 e c_1 estão em R.

Claramente

$$Q \cap R[x] = (c_0+c_1x)\ K[x] \quad R[x] =$$

$$= C^{-1}R[x]\ (c_0+c_1x)\ R[x]$$

Como

$$(Q \cap R[x]) \cap R = (0)$$

não podemos ter

$$Q \cap R[x] = PR[x]$$

para todo ideal primo P de R. E, desde que R é um anel de Dedekind e $Q \cap R[x]$ é um ideal primo de $R[x]$, pelo lema (4.2.08), não podemos ter:

$$Q \cap R[x] \subset PR[x]$$

para cada ideal primo P, de R.

Então existe em $Q \cap R[x]$ um polinômio primitivo de $R[x]$. Portanto

$$(Q \cap R[x])\ R(x) = QR(x) = R(x)$$

Logo, pelo lema (1.6.26), toda classe de R é levada na classe principal de R(x), isto é, R(x) é um domínio principal.

A importância maior da proposição (4.3.06) é mostrar que os ideais primos de R(x) são exatamente aqueles da forma PR(x) onde P é um ideal primo de R.

APÊNDICE

No capítulo 2, mostramos que se R é um anel de Dedekind com corpo de frações K e L é uma extensão de K, então R', o fecho integral de R em L é um anel de Dedekind. Aqui nós daremos um exemplo mostrando que se a extensão não é finita então não se tem, necessariamente, R' um anel de Dedekind.

Sejam $\mathbb{Z}$ o anel dos inteiros Q o corpo dos racionais e $\bar{Q}$, o fecho algébrico de Q. Nestas condições. $\mathbb{Z}'$, o fecho integral de $\mathbb{Z}$ em $\bar{Q}$ não é noetheriano, pois:

$$(\sqrt{2}) \subset (\sqrt[4]{2}) \subset (\sqrt[8]{2}) \subset \ldots \quad .$$

é uma cadeia ascendente de ideais de $\mathbb{Z}'$ que não é estacionaria.

Logo $\mathbb{Z}'$ não é um anel de Dedekind.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] NETO, Hermínio Borges. Notas sobre Anéis de Dedekind

[2] CLABORN, Luther. Dedekind Domains and Rings of Quotients.

[3] ZARISKI, Oscar & SAMUEL, Pierre. Comutative Álgebra. Princeton. D. Van Nostrand Company, 1959

[4] ATIYAH. H.F. & MACDONALD, I.G. Introducción Al Álgebra Commutativa. Espanha, Editorial Reverté,S.A.,1978.

[5] McCARTHY, P. J. Algebraic Extensions of Fields. Waltham, Blaisdell, 1966.

[6] ENDLER, Otto. Valuation Theory. Springer-Verlag,Berlin Heidelberg New York, 1972.