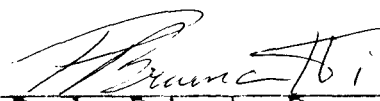


OS FATORES INVARIANTES DE MÓDULOS SOBRE ANÉIS DE DEDEKIND

Este exemplar corresponde a redação final da tese devidamente corrigida e defendida pela Srta. Cláudia Helena Dezotti e aprovada pela Comissão Julgadora.

Campinas, 19 de agosto de 1988

Prof. Dr.


Paulo Roberto Brumatti

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

"O matemático não estuda a matematica pura porque ela seja útil; ele a estuda porque deleita-se com ela, e deleita-se com ela porque ela é bela."

Poincaré

A meus pais

Agradecimentos

Gostaria de expressar meus sinceros agradecimentos a todos que de alguma forma colaboraram para a conclusão deste trabalho e, mesmo correndo o risco do esquecimento, gostaria de agradecer a algumas pessoas que me foram de particular importância.

Em primeiro lugar, ao Prof. Paulo Brumatti que muito mais que orientador me serve como exemplo de pessoa e de profissional.

Ao Prof. Antônio Paques pelo seu apoio e orientação no início de meu mestrado.

Ao Prof. Francisco Thayne pelo incentivo.

Aos amigos Jamil Ferreira, Maria Conceição Peres Young e Paulo César Bezerra pela força neste tempo.

Aos meus pais que souberam suportar e compreender minha ausência e muitas vezes meu desleixo em relação a eles.

A Carlos M. Diniz Jr., cuja presença foi imprescindível para a realização deste trabalho.

Aos professores do IMECC que de alguma maneira colaboraram na minha formação profissional.

Aos funcionários da secretaria de pós-graduação, Luis, Isabel e Aparecida e, da biblioteca do IMECC, em especial, a Marilda, pela assistência fornecida no decorrer desses anos.

Finalmente, a UNICAMP, pelo apoio financeiro, sem o qual seria impossível a realização deste trabalho.

Campinas, Agosto de 1988

Eláudia

ÍNDICE

INTRODUÇÃO		p. 01
CAPÍTULO I		p. 03
CAPÍTULO II		p. 25
CAPÍTULO III		p. 56
BIBLIOGRAFIA		p. 72

INTRODUÇÃO

À semelhança de módulos sobre domínios principais, temos por objetivo classificar os módulos livres de torção finitamente gerados sobre domínios de Dedekind. Assim provaremos que se R é domínio de Dedekind e M e N são R -módulos livres de torção finitamente gerados de mesmo rank, $N \subset KM$, temos que existem ideais fracionários $I_1 \supset I_2 \supset \dots \supset I_k$, $k = \text{rank de } M = \text{rank de } N$, tais que

$$M \simeq R \dot{+} \dots \dot{+} R \dot{+} I$$

$(k-1) R$ somandos e

$$N \simeq E_1 \dot{+} \dots \dot{+} E_{k-1} \dot{+} E_k I.$$

Mais que isso, se $N \subset M$ submódulo cujo rank é $1 \leq k$ então $N = E_1 \dot{+} \dots \dot{+} E_{k-1} \dot{+} N'$ onde cada $E_i \subset R$. Aos ideais E_i chamaremos de fatores invariantes de N em M , pois eles são unicamente determinados pelo par (M, N) .

Para tanto desenvolveremos no Capítulo I o conceito de domínio de Dedekind e suas propriedades. Isso será feito tendo como base o artigo clássico de Cohen [5]. Vários resultados acerca de ideais fracionários e anéis de valorização serão considerados de conhecimento do leitor (uma boa referência para isso são [13] e [4]).

No Capítulo II estudaremos o Teorema dos Fatores Invariantes propriamente dito e teremos por base bibliográfica Curtis e Reiner [6].

Finalmente no Capítulo III desenvolveremos algumas aplicações bem interessantes do citado teorema além de utilizá-lo para obter alguns resultados envolvendo objetos clássicos da álgebra

comutativa.

Um desses resultados é o que afirma que todo anel de Dedekind é um BCS-anel. A definição de BCS-anel é dada por Vasconcelos e Weibel [12] e foi motivada por sua aplicação à teoria de controle (para maiores referências vide [7], um pequeno histórico do problema pode ser mostrado em [11]).

CAPÍTULO I

ANÉIS DE DEDEKIND

Por anel entenderemos sempre um anel comutativo com identidade. Dado $I \subset R$ um ideal diremos ser *ideal próprio* se distinto de (0) e de R .

Denotaremos por $\text{Spec}(R)$ ao conjunto constituído de todos os ideais primos de R e por $\text{Max}(R)$ ao conjunto de todos os ideais maximais de R .

Neste capítulo temos por objetivo definir domínio de Dedekind e caracterizá-lo da forma mais completa possível.

Para tanto serão necessários alguns resultados fundamentais acerca de anéis Noetherianos e principalmente RM-anéis.

Estudaremos condições necessárias, e algumas vezes suficientes, para que um dado anel R seja um RM-anel e, também, verificaremos quando uma extensão integral de R herda tal propriedade.

Daremos condições suficientes para que um domínio seja de Dedekind e provaremos algumas equivalências acerca desta propriedade. Mais que isso, forneceremos condições para que uma dada extensão de um domínio de Dedekind verifique ser ela também um domínio de Dedekind.

Proposição (1.1): Dado um anel R , as seguintes afirmações são equivalentes:

- i) R satisfaz a *condição da cadeia ascendente* (cca)
- ii) R satisfaz a *condição máxima*

iii) todo ideal de R é finitamente gerado

Um anel satisfazendo a uma das afirmações anteriores (e consequentemente a todas) será dito anel Noetheriano.

Se R satisfaz a condição da cadeia descendente (ccd) (equivalentemente a condição mínima) diremos ser um anel de Artin ou Artiniano.

Se para todo $I \subset R$, $I \neq (0)$ e $I \neq R$, R/I satisfaz a condição mínima, diremos ser R um anel com a condição mínima restrita ou um RM-anel.

Facilmente se verifica que se para todo ideal $I \subset R$, $I \neq (0)$ e $I \neq R$, R/I é Noetheriano então R é Noetheriano.

Lema (1.2): Seja R um anel tal que $(0) = P_1 \dots P_n$ onde cada $P_i \in \text{Max}(R)$ e para todo i , $(P_1 \dots P_{i-1}) / (P_1 \dots P_{i-1} P_i)$ é um R/P_i -espaço vetorial de dimensão finita então R tem uma composição em série de ideais.

Demonstração:

Dado que $(P_1 \dots P_{i-1}) / (P_1 \dots P_{i-1} P_i)$ é um R/P_i -espaço vetorial de dimensão finita temos que existe uma composição em série entre $(P_1 \dots P_{i-1})$ e $(P_1 \dots P_i)$.

Como

$$R \supset P_1 \supset \dots \supset (P_1 \dots P_{i-1}) \supset (P_1 \dots P_{i-1} P_i) \supset \dots \supset (0) = P_1 \dots P_n$$

temos que R possui uma composição em série.

■

Teorema (1.3): Dado R um anel temos que R é Artiniano se e só se R Noetheriano e todo ideal primo é maximal.

Demonstração:

Suponhamos que R Noetheriano e que todo primo é maximal. Afirmamos ser (0) um produto de ideais maximais. De fato, seja Σ o conjunto de todos os ideais de R que não contém um produto finito de primos. Suponhamos que $\Sigma \neq \emptyset$, sendo R Noetheriano tomemos $I \in \Sigma$ maximal. Desde que I não é primo temos que existem ideais de R , A, B tais que $I \subset A, I \subset B, I \neq A, I \neq B$ e $AB \subset I$.

Da maximalidade de I temos que A e B contém ambos um produto finito de primos e assim também I o que é absurdo.

Logo $(0) = P_1 \dots P_n$ e sendo cada primo maximal a afirmação está verificada.

Além disso $(P_1 \dots P_{i-1}) / (P_1 \dots P_{i-1} P_i)$ é um R/P_i -espaço vetorial satisfazendo a condição da cadeia ascendente logo de dimensão finita e portanto, pelo lema (1.2), R é Artiniano.

Reciprocamente, suponhamos que R satisfaz a condição mínima e seja $P \in \text{Spec}(R)$ então R/P satisfaz a condição mínima e não tem divisores de zero. Seja $x \in R/P$ então existe $n \in \mathbb{N}$ tal que

$$(x^n) = (x^{n+1}) = \dots$$

então

$$x^n = b x^{n+1}, \quad b \in R/P$$

logo x inversível o que implica R/P corpo e consequentemente P maximal. De maneira analoga a anterior queremos provar que (0) é produto de

primos .

Primeiramente notemos que sendo R de Artin ele possui um número finito de ideais maximais . Logo se denotarmos por N o nilradical de R temos

$$N = M_1 \cap \dots \cap M_k \supset M_1 M_2 \dots M_k$$

onde os M_i são todos maximais .

Além disso , existe $h \in \mathbb{N}$ tal que

$$N^h = (0)$$

donde segue o desejado. Então do mesmo modo que anteriormente cada $(P_1 \dots P_{i-1}) / (P_1 \dots P_{i-1} P_i)$ é um R/P_i - espaço vetorial que satisfaz a condição mínima, logo de dimensão finita e pelo lema (1.2) temos R Noetheriano .

■

Corolário (1.4): Para que um anel R seja um RM-anel é necessário e suficiente que R seja Noetheriano e que todo primo próprio seja maximal .

Demonstração:

Suponhamos R um RM-anel então para qualquer $I \subset R$ ideal, $I \neq (0)$ e $I \neq R$ temos R/I Artiniano e pelo teorema (1.3) R/I Artiniano consequentemente R Noetheriano.

Seja $P \in \text{Spec}(R)$ e consideremos $0 \neq x \in P$. Seja

$$\phi : R \longrightarrow R/(x)$$

projeção canônica . Então $P/(x)$ ideal primo de $R/(x)$ e portanto $P/(x)$ é um ideal maximal de $R/(x)$ e consequentemente P é maximal.

Reciprocamente seja R Noetheriano e tal que todo ideal primo próprio é maximal então dado $I \subset R$ ideal, $I \neq (0)$, R/I é Noetheriano e todo seu primo é maximal logo pelo teorema (1.3) R/I é Artiniano .

■

Corolário (1.5): Um anel é Artiniano se e só se R é um RM-anel e R tem divisores de zero ou é um corpo.

Demonstração:

Se R satisfaz a condição mínima então é também um RM-anel e além disso todo primo é maximal . Suponhamos que R não tenha divisores de zero então (0) é primo e portanto maximal , consequentemente R é corpo . Para a suficiência basta observar que se R não é corpo então (0) não é primo e pelas condições do corolário (1.4) R é Noetheriano e todo primo é maximal . Basta agora aplicar (1.3) .

■

Teorema (1.6): Seja R um anel e suponhamos que todo ideal primo tem um número finito de geradores então R é Noetheriano .

Demonstração:

Seja

$$\mathcal{P} = \{ I \subset R \text{ ideal} ; I \text{ não possui número finito de geradores} \}$$

Suponhamos $\mathcal{S} \neq \emptyset$. então pelo Lema de Zorn $\mathcal{S}$ possui um elemento maximal , a saber $\mathcal{M}$. Como $\mathcal{M}$ não é primo , existem ideais de R , B e C , tais que $\mathcal{M} \subset B$, $\mathcal{M} \subset C$, $\mathcal{M} \neq B$, $\mathcal{M} \neq C$ e $BC \subset \mathcal{M}$. Da maximalidade de $\mathcal{M}$ temos que B e C possuem um número finito de geradores. Afirmamos ser R/C Noetheriano , de fato , a cada ideal de R/C corresponde um ideal de R que contém propriamente $\mathcal{M}$. logo é um R -módulo finitamente gerado. Desde que B/BC é um R/C - módulo finitamente gerado temos que $\mathcal{M}/BC$ como submódulo de B/BC também é um R/C - módulo finitamente gerado e consequentemente $\mathcal{M}/BC$ é um R -módulo finitamente gerado e desde que BC tem um numero finito de geradores também o tem $\mathcal{M}$, absurdo .

■

Diremos que um anel é um *RM-domínio* se além de ser um RM -anel ele é também um domínio .

Consideraremos agora o efeito da condição mínima restrita em uma extensão integral de R (ou seja , todo elemento do sobreanel é integral sobre R) ; os teoremas aqui abordados darão condições para que a condição mínima restrita de R implique na mesma para o sobreanel .

Adotaremos a convenção de que as expressões " fecho integral de R " e " R integralmente fechado " significam respectivamente " fecho integral de R em seu corpo de frações " e " R é integralmente fechado em seu corpo de frações " .

Teorema (1.7): Seja R um RM -domínio e T um domínio que é extensão integral de R . Consideremos U o corpo de frações de T e K o

corpo de frações de R . Se U é uma extensão finita de K então T é um RM-domínio. Na verdade, se I é um ideal próprio de T então T/I é um R -módulo com composição em série.

Demonstração:

Notemos primeiramente a seguinte equivalência: T é um RM-domínio se e só se T/I tem composição em série para todo $I \subset T$ um ideal próprio.

Logo é suficiente verificar somente a segunda conclusão. Para tanto basta mostrar que T/I é um R -módulo finitamente gerado. De fato, se tal acontecesse, considerando $A = I \cap R$, temos $T/I \cong R/A$ - módulo finitamente gerado. Como T integral sobre R temos $A \neq (0)$. Pelas hipóteses e pelo teorema (1.3) temos que R/A satisfaz a ambas as condições da cadeia e consequentemente também o faz T/I .

Como U é extensão finita K temos que existem $\alpha_1, \dots, \alpha_m \in T$ tal que

$$U = K(\alpha_1, \dots, \alpha_m).$$

Se $R' = R[\alpha_1, \dots, \alpha_m]$, desde que $\alpha_1, \dots, \alpha_m$ são integrais sobre R então R' é um R -módulo finitamente gerado. Consequentemente para provar que T/I é um R -módulo finitamente gerado basta mostrar que é um R' -módulo finitamente gerado.

Como o corpo de frações de R' é igual ao corpo de frações T para provar o teorema basta considerar o caso especial em que R e T tem o mesmo corpo de frações.

□

Definição (1.8): Dado R anel e M e N R -módulos definiremos

$$(M : N) = \{ x \in R ; xN \subset M \}$$

Teorema (1.9): Sejam R um RM-domínio, T um anel contendo R e contido no corpo de frações de R , K . Então T é também um RM-domínio, mais que isso, se I é ideal próprio de T então T/I é R -módulo finitamente gerado.

Demonstração:

Por raciocínio análogo ao feito anteriormente é suficiente verificar a segunda asserção da conclusão, isto é, que dado I ideal próprio de T , T/I é um R -módulo finitamente gerado.

Seja $a/b \in I \subset T \subset K$ onde $a \in R$, $b \in R - \{0\}$ e $a \in I \cap R$. É suficiente mostrar que T/Ra é um R -módulo finitamente gerado (de fato, do teorema do isomorfismo para módulos temos que $(T/I) \cong (T/Ra)/(I/Ra)$).

Definamos

$$A_i = Ta^i \cap R, \quad i = 1, 2, \dots$$

Desde que $A_i \supset A_{i+1}$ e R/Ra é Artiniano temos que existe $n \in \mathbb{N}$ tal que

$$A_{n+1} + Ra = A_{n+2} + Ra = \dots$$

Agora $A_n(a^{-n})$ é um R -módulo finitamente gerado e o mesmo será verdade para T/Ra se pudermos mostrar que T/Ra é imagem de $A_n(a^{-n})$ pelo

homomorfismo canônico

$$\begin{aligned}\pi : T &\longrightarrow T/Ta \\ x &\longrightarrow x + Ta\end{aligned}$$

Seja β um elemento qualquer de T/Ta . Ele provém de um elemento $\alpha = b/c \in T$, $b \in R$, $c \in R - \langle 0 \rangle$, isto é, $\beta = \alpha + Ta$.

Sendo R Noetheriano, existe $0 < k \in \mathbb{Z}$ tal que

$$(Rc : Ra^k) = (Rc : Ra^{k+1}) = (Rc : Ra^k) : Ra$$

donde temos que Ra não está contido em nenhum primo de $(Rc : Ra^k)$ e desde que todo primo próprio de R é maximal

$$(Rc : Ra^k) + Ra = R.$$

Assim

$$1 = xa + y, \quad x \in R, \quad y \in (Rc : Ra^k)$$

Portanto

$$a^k = xa^{k+1} + ya^k \in Ra^{k+1} + Rc$$

donde

$$a^k = ra^{k+1} + tc, \quad r, t \in R$$

consequentemente

$$\alpha a^k = \alpha r a^{k+1} + tb$$

portanto

$$\alpha + Ta = tb/(a^k) + Ta$$

Então podemos assumir que $\alpha = e/(a^k)$, $e \in R$.

Mais que isso podemos assumir que $k = n$. De fato, se $k < n$ tome $\alpha = (ea^{n-k})/(a^n)$. Se $k > n$ então

$$e = \alpha a^k \in Ta^k \cap R = A_k \subset A_{k+1} + Ra$$

assim

$$e + Ta^{k+1} = fa + Ta^{k+1}, \quad f \in R$$

ou seja

$$e = fa + sa^{k+1}, \quad s \in T$$

portanto

$$\alpha = e/(a^k) = (f/(a^{k-1})) + sa$$

logo

$$\alpha + Ta = f/(a^{k-1}) + Ta$$

Se $k-1 = n$ acabou senão refaço o raciocínio. Consequentemente $\alpha = g/(a^n)$, $g \in R$, e assim $g \in A_n$ completando a prova.

■

Um RM-domínio integralmente fechado será dito um *domínio de Dedekind*.

Seja R um domínio e K o corpo de frações de R , dado $I \subset R$ ele será dito um *R-ideal fracionário em K* se é um R -módulo tal que existe $a \in R - \{0\}$ com $aI \subset R$. Se I é um ideal de R dizemos que I é um *R-ideal integral*.

Dado I R -ideal fracionário definiremos

$$I^{-1} = \{ x \in K ; xI \subset R \}$$

e diremos que I é inversível se $II^{-1} = R$. De modo mais explícito I R-ideal fracionário é inversível se e só se existem $a_1, \dots, a_n \in I$ e $b_1, \dots, b_n \in K$ tal que

$$i) b_i I \subset R, i = 1, \dots, n$$

$$ii) a_1 b_1 + \dots + a_n b_n = 1, i \in R.$$

Observemos que se $I \subset K$ é um R-módulo finitamente gerado então I é um ideal fracionário.

Lema (1.10): Seja R um domínio e K seu corpo de frações. Se todo ideal integral próprio de R é inversível então R é integralmente fechado.

Demonstração:

Seja $\alpha \in K$ integral sobre R (ou seja existe $0 < n \in \mathbb{Z}$ e $r_0, \dots, r_{n-1}$ elementos de R tal que $r_0 + r_1 \alpha + \dots + r_{n-1} \alpha^{n-1} + \alpha^n = 0$).

Consideremos $I = R[\alpha]$, sabemos que I é um R-módulo finitamente gerado contido em K , portanto é um R-ideal fracionário.

Logo existe $c \in R - \{0\}$ tal que $cI \subset R$.

Portanto por hipótese cI inversível, ou seja, existe J R-ideal fracionário com $(cI)J = R$. Como $I = c^{-1}(cI)$ temos que I é inversível e desde que $I^2 = I$ temos $I \subset R$ donde $\alpha \in R$.

■

Lema (1.11): Se R é um domínio de Dedekind local e $\mathcal{M}$ é seu ideal maximal então R é principal e todo ideal integral próprio I é da forma $I = \mathcal{M}^n$ (isto é, R é um anel de valorização discreta).

Demonstração:

Provemos que $\mathcal{M}$ é principal. Notemos primeiramente que $\text{Spec}(R) = \langle \mathcal{M} \rangle$.

Seja $a \in \mathcal{M} - \langle 0 \rangle$ então $\sqrt{Ra} = \mathcal{M}$. Sendo R Noetheriano temos que existe um número natural n tal que $\mathcal{M}^n \subset Ra$. Seja n escolhido de tal modo que $\mathcal{M}^n \subset Ra$ e $\mathcal{M}^{n+1} \not\subset Ra$.

Logo existe $b \in \mathcal{M}^{n+1}$ e $b \notin Ra$.

Considere $x = a/b \in K = \text{cfr}(R)$. Então $x^{-1} \notin R \rightarrow x^{-1}$ não é integral sobre $R \rightarrow x^{-1}\mathcal{M} \not\subset \mathcal{M}$ (se isso ocorresse como $\mathcal{M} = Ra_1 + \dots + \dots + Ra_k$, $a_i \in \mathcal{M}$, teríamos $x^{-1}a_i = r_{i1}a_1 + \dots + r_{ik}a_k$, $1 \leq i \leq k$

donde $\sum_{j=1}^n (r_{ij} - \delta_{ij}x^{-1})a_j = 0$. Se $C = (r_{ij} - \delta_{ij}x^{-1})$, matriz $k \times k$,

temos $\det(C)\mathcal{M} = 0 \rightarrow \det(C) = 0 \rightarrow x^{-1}$ integral sobre R).

Mas $(b/a)\mathcal{M} = (b\mathcal{M})/a \subset \mathcal{M}^n/a \subset R \rightarrow x^{-1}\mathcal{M} = R \rightarrow \mathcal{M} = Rx$.

Tome agora $I \subset \mathcal{M}$, $I \neq \langle 0 \rangle$, seja $n' \in \mathbb{N}$ tal que $I \subset \mathcal{M}^{n'}$ e $I \not\subset \mathcal{M}^{n'+1}$ (se isso não fosse possível teríamos $I \subset \bigcap \mathcal{M}^n = \langle 0 \rangle$, absurdo).

Seja $0 \neq y \in I$ então $y = ax^{n'}$ e $a \in \mathcal{M}$, como R local então $a \in U(R) \rightarrow x^{n'} \in I \rightarrow \mathcal{M}^{n'} \subset I$.

■

Proposição (1.12): Seja R domínio de Dedekind e $\langle 0 \rangle \neq I$ R -ideal fracionário. Então I é inversível.

Demonstração:

Provaremos primeiro que se I' é um R -ideal integral e R é Dedekind então I' é produto de primos. De fato, temos que

$$I' = \bigcap_{i=1}^m Q_i \text{ onde } Q_i \text{ é } P_i\text{-primário}$$

decomposição primária minimal. Como os P_i são dois a dois comaximais também o são os Q_i , consequentemente

$$I' = Q_1 \dots Q_n$$

Além disso, se A é integralmente fechado também o é cada A_{P_i} . Para cada i temos então A_{P_i} domínio local Noetheriano de dimensão 1 integralmente fechado, consequentemente, pelo lema (1.11) é anel de valorização discreta, assim

$$Q_i A_{P_i} = (P_i A_{P_i})^{n_i} = P_i^{n_i} A_{P_i}$$

e como Q_i e $P_i^{n_i}$ são P_i -primários temos $Q_i = P_i^{n_i}$. Assim

$$I' = P_1^{n_1} \dots P_m^{n_m}$$

Seja I um R -ideal fracionário então existe $a \in R - \{0\}$ tal que aI é um R -ideal integral e portanto

$$aI = P_1^{n_1} \dots P_k^{n_k}.$$

Portanto se mostrarmos que cada ideal integral maximal é inversível teremos que aI é inversível e portanto também I (pois $I = a^{-1}aI$).

Seja $P \in \text{Max}(R)$ e $0 \neq b \in P$ então

$$R_b = P_1^{a_1} \dots P_k^{a_k}, \quad P_i \in \text{Spec}(R), \quad a_i \in \mathbb{N} - \{0\}$$

Como $P \supset R_b$ temos $P = P_i$ para algum i e sendo R_b inversível obviamente também o é P .

■

Corolário (1.13): Seja R um domínio de Dedekind então todo anel entre R e seu corpo de frações é também um domínio de Dedekind.

Demonstração:

Seja $K = \text{cfr}(R)$ e S o anel com $R \subset S \subset K$. Pelo teorema (1.9) temos que S é RM-domínio, falta pois verificar que S é integralmente fechado. Mas pelo lema (1.10) é suficiente provar que todo S -ideal integral próprio é inversível. Seja I S -ideal integral. Como S é Noetheriano temos

$$I = Sa_1 + \dots + Sa_m, \quad a_i \in I, \quad i = 1, \dots, m$$

Consideremos $J = Ra_1 + \dots + Ra_m$ que é R -ideal fracionário, logo como $I = SJ$ e J inversível temos $I(J^{-1}S) = SJ(J^{-1}S) = SR = S$, ou seja, I inversível.

■

Teorema (1.14): Seja R um domínio onde todo ideal próprio é produto de ideais primos então R é domínio de Dedekind.

Demonstração:

Observemos que qualquer fatorização em ideais primos inversíveis é única. De fato, suponhamos

$$P_1 \dots P_r = P'_1 \dots P'_s$$

onde os P_i , P'_j são primos e inversíveis. Podemos supor que P_1 é minimal no conjunto $\{P_1, \dots, P_r, P'_1, \dots, P'_s\}$. Então P_1 é igual a um P'_j desde que necessariamente contém algum P'_j .

Sendo P_1 inversível podemos cancelar este fator de ambos os lados e então procedemos por indução.

Provaremos agora que todo ideal primo próprio P é inversível e maximal.

Seja $0 \neq x \in P$ e consideremos a fatorização em primos do ideal Rx

$$P \supset Rx = P_1 \dots P_m$$

Logo P contém algum fator de Rx , digamos P_1 . Desde que todo ideal principal é claramente inversível e P_1 é um fator de Rx temos P_1 inversível. Portanto é suficiente provar que P_1 é maximal.

Se P_1 não o fosse, existiria $c \in R - \langle 0 \rangle$, $c \notin P_1$ tal que

$$Rc + P_1 \subset R \quad \text{e} \quad Rc + P_1 \neq R$$

consequentemente

$$Rc + P_1 = P'_1 \dots P'_r$$

com $P_i^* \in \text{Spec}(R)$. Assim também

$$Rc^2 + P_1 = Q_1 \dots Q_t, \quad Q_j \in \text{Spec}(R).$$

Consideremos $R' = R/P_1$ e denotando por $\bar{x}$ a classe residual de x em R/P_1 , temos

$$\overline{Rc} = \overline{Rc^2} = \overline{Q_1} \dots \overline{Q_t}.$$

Logo

$$\overline{P_1}^2 \dots \overline{P_r}^2 = \overline{Q_1} \dots \overline{Q_t}.$$

Sendo os $\overline{P_i}$ e $\overline{Q_j}$ fatores de um ideal principal e portanto, inversíveis, esta fatorização é única e os ideais $\overline{Q_1}, \dots, \overline{Q_t}$ constituem-se nos ideais $\overline{P_1}, \dots, \overline{P_r}$, cada um contado duas vezes. Portanto

$$Rc^2 + P_1 = (Rc + P_1)^2$$

o que implica que

$$P_1 \subset Rc + P_1^2$$

Então, se $b \in P_1$ temos $b = dc \in P_1^2$, para algum $d \in R$, o que implica $dc \in P_1$ e como $c \notin P_1$ temos $d \in P_1$.

$$\text{Assim } b \in P_1c + P_1^2 \rightarrow P_1 = P_1(Rc + P_1).$$

Da inversibilidade de P_1 temos $Rc + P_1 = R$, absurdo.

Portanto P_1 é maximal.

Assim todo ideal próprio fatora-se em ideais maximais inversíveis,

consequentemente , todo ideal próprio de R é inversível e pelo lema (1.10) R é integralmente fechado.

Para que R seja Dedekind resta apenas verificar que R Noetheriano , mas isto é consequência imediata do fato que todo primo próprio inversível é finitamente gerado e portanto usando da hipótese podemos concluir que R é Noetheriano .

■

Teorema (1.15): Se R é um domínio tal que todo ideal primo é inversível então R é um domínio de Dedekind .

Demonstração:

Afirmamos inicialmente que todo ideal primo próprio é maximal . De fato , se dado $P \in \text{Spec}(R)$, $P \neq (0)$, ele não fosse maximal, existiria um ideal primo $Q \neq (0)$ com

$$(0) \subset P \subset Q \subset R$$

onde $P \neq (0)$ e $Q \neq R$.

Agora $PQ^{-1} \subset R$ e $(PQ^{-1})Q = P$ logo $PQ = P$ o que implica $R = Q$, absurdo .

Como todo primo próprio é inversível , cada um deles é um R -módulo finitamente gerado e pelo teorema (1.6) Temos R Noetheriano .

Consequentemente , dado I ideal próprio de R temos $P_1, \dots, P_r$ primos (não necessariamente distintos) tal que

$$P_1 \dots P_r \subset I \text{ e } I \subset P_i \text{ para cada } i$$

logo

$$P_1 \subset I(P_2)^{-1} \dots (P_r)^{-1} \subset R$$

Se $I(P_2)^{-1} \dots (P_r)^{-1} = R$ temos $I = P_2 \dots P_r$ e acabou, senão podemos supor que

$$P_1 = I(P_2)^{-1} \dots (P_r)^{-1}$$

e portanto pelo teorema (1.14) R domínio de Dedekind .

■

Teorema (1.16): Se R é um domínio Noetheriano, as seguintes condições são equivalentes :

I . R é um domínio de Dedekind

II . para todo $P \in \text{Max}(R)$, R_P é anel de valorização discreta

III . se $P \in \text{Max}(R)$, não existe ideal primário entre P e P^2 (e consequentemente nenhum ideal já que todo ideal entre P e P^2 é P -primário)

IV . um ideal primário pertencente a um ideal maximal é um produto de ideais primos

V . os ideais primários pertencentes a um ideal maximal são totalmente ordenados com respeito a inclusão

VI . para quaisquer três ideais de R temos

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

VII . para quaisquer três ideais de R temos

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

Demonstração:

Suponhamos (I) válida . Mostraremos que ela implica as restantes :

I $\rightarrow$ II

Utilizando diretamente os lemas (1.11) e (1.13).

I $\rightarrow$ III

Verifiquemos inicialmente a afirmação que todo ideal entre P e P^2 é P -primário .

Se $I \subset R$ é um ideal tal que $P^2 \subset I \subset P$ temos que $\sqrt{I} = P$ e $P \in \text{Max}(R)$ logo I é P -primário.

Seja Q P' -primário tal que $P^2 \subset Q \subset P$. Mas existe $0 < n \in \mathbb{Z}$ tal que $Q = (P')^n$ logo $P^2 \subset (P')^n \subset P \rightarrow P' = P \rightarrow Q = P$ ou $Q = P^2$.

I $\rightarrow$ IV

Sejam R domínio de Dedekind , $\mathcal{M} \in \text{Max}(R)$ e Q $\mathcal{M}$ - primário . Então existe $0 < n \in \mathbb{Z}$ tal que $Q = \mathcal{M}^n$.

I $\rightarrow$ V

Segue diretamente de IV

I $\rightarrow$ VI e VII

Se provarmos que dado A ideal próprio de R temos que

$$A = \bigcap \left\{ AR_P ; P \in \text{Max}(R) \right\}$$

e desde que a operação de localização preserva as operações básicas de ideais é suficiente verificar essas identidades em cada R_P , mais aí elas são triviais desde que os ideais formam um conjunto totalmente ordenado .

Provemos inicialmente que

$$R = \bigcap \left\{ R_P ; P \in \text{Max}(R) \right\}$$

Obviamente temos que $R \subset \bigcap \left\{ R_P ; P \in \text{Max}(R) \right\}$.

Suponhamos $x \in \bigcap \left\{ R_P ; P \in \text{Max}(R) \right\}$, logo $x = a/b$.

Para mostrar que $x \in R$ é suficiente mostrar que $a \in Rb$.

Seja $I = \{ y \in R ; ya \in Rb \}$. Se $I = R$ então acabou. Senão, seja

$\mathcal{M} \in \text{Max}(R)$ tal que $I \subset \mathcal{M} \subset R$, $\mathcal{M} \neq R$. Como $x \in \bigcap \left\{ R_P ; P \in \text{Max}(R) \right\}$ temos

$$a/b = x = a'/b', \quad b' \in \mathcal{M}$$

logo existe $s \notin \mathcal{M}$ tal que $sab' = sba' \in Rb \Rightarrow sb' \in I \subseteq \mathcal{M}$, absurdo já que $s \notin \mathcal{M}$ e $b' \in \mathcal{M}$.

Seja $A \subset R$ ideal. Queremos provar que $A = \bigcap \left\{ AR_P ; P \in \text{Max}(R) \right\}$.

Consideremos $I = \bigcap \left\{ AR_P ; P \in \text{Max}(R) \right\}$, portanto $I \subset R$ ideal.

Se provarmos que $AR_M = IR_M$ para todo $M \in \text{Max}(R)$ então $A = I$.

Obviamente $A \subset I$ e então $AR_M \subset IR_M$ para todo $M \in \text{Max}(R)$.

Seja $M \in \text{Max}(R)$ e suponhamos $x \in IR_M$, logo $x = a/s$ onde $a \in I$ e $s \notin M$.

Mas $I = \bigcap \left\{ AR_P ; P \in \text{Max}(R) \right\}$, em particular $a \in AR_M$ logo $a = b/s'$

com $b \in A$ e $s' \notin M$.

Então $x = a/s = (a/1)(1/s) = (b/s')(1/s) = b/(ss')$, ou seja, $x \in AR_M$,

conclui a demonstração.

Reciprocamente, mostraremos que II, III, IV, V, VI e VII implicam

em I .

II $\rightarrow$ I

Suponhamos que II válida então dado $P \in \text{Max}(R)$ além de ser o único maximal de R_P também é minimal aí , conseqüentemente é minimal em R .

Dai todo ideal primo próprio é maximal .

Além disso sendo cada R_P integralmente fechado também o é R , donde segue-se I .

III $\rightarrow$ I

Seja $P \in \text{Max}(R)$ e consideremos $R' = R_P$. Tomando $P' = PP_P$, não existe $J \subset R'$ ideal tal que $P'^2 \subset J \subset P'$. Conseqüentemente se $a \in P'$ e $a \notin P'^2$ temos $R'a + P'^2 = P'$ e pelo lema de Nakayama $P' = R'a$ então R' anel de valorização discreto seguindo-se então I .

IV $\rightarrow$ I

Seja Q P -primário onde $P \in \text{Max}(R)$. Logo temos

$$P_1^{h_1} \dots P_n^{h_n} = Q \subset P \quad , \quad P_i \in \text{Spec}(R) \text{ todos distintos}$$

Temos que existe i tal que $P_i \subset P$.

Sendo R Noetheriano temos que existe $0 < n \in \mathbb{Z}$ tal que

$$P^n \subset Q = (P_1)^{h_1} \dots (P_n)^{h_n} \subset P_j \quad , \text{ para cada } j \quad .$$

Logo $P = P_i$ e sendo que os P_j são todos distintos temos $P \subset P_j$ e

$P \not\subset P_j$, $i \neq j$.

Conseqüentemente $P_j = R$, $j \neq i$. E assim $Q = P^{h_1}$.

Seja Q' tal que $P^2 \subset Q' \subset P$, Q' P -primário . Então $\sqrt{Q'} = P' = P$ e portanto ou $Q' = P^2$ ou $Q' = P$ e como III $\rightarrow$ I segue-se o desejado .

V $\rightarrow$ I

Afirmamos que III se verifica. Seja $P \in \text{Max}(R)$, por hipótese temos todos os ideais primos pertencentes a P totalmente ordenados. Logo sabemos que P/P^2 é R/P - espaço vetorial no qual os subespaços são totalmente ordenados. Então necessariamente $\dim(P/P^2)=1$ o que implica III.

VI $\Rightarrow$ I

Assumamos VI verdadeira. Então P/P^2 é R/P - espaço vetorial cujos subespaços satisfazem a lei distributiva então necessariamente $\dim(P/P^2)=1$, pois se não o fosse, teríamos elementos e_1, e_2 distintos pertencentes a base de P/P^2 sobre R/P . Seja $K = R/P$

$$V = Ke_1 \oplus Ke_2$$

$$W = Ke_1$$

$$T = Ke_2$$

teríamos então $V \cap (W + T) = V \neq V \cap W = V \cap T = (0)$.

VII $\Rightarrow$ I

Afirmamos que V se verifica. De fato, se tal não ocorresse, existiria Q_1 e Q_2 P -primários, $P \in \text{Max}(R)$, nenhum contido no outro.

Seja $A = Q_1 \cap Q_2$ então

$$(A : Q_1), (A : Q_2) \subset P.$$

Logo $(A : Q_1) + (A : Q_2) \subset P \subset R$, $P \neq R$ e $A : (Q_1 : Q_2) = R$, absurdo.

■

CAPÍTULO II

MÓDULOS SOBRE DOMÍNIOS DE DEDEKIND (O TEOREMA DOS FATORES INVARIANTES)

Neste capítulo, a menos que explicitado, R será sempre um domínio de Dedekind (isto é, R é noetheriano, todo ideal primo não nulo é maximal e é integralmente fechado).

Os R - módulos M serão sempre unitários, isto é, $1m=m$ qualquer que seja $m \in M$.

Um R - módulo M é livre de torção se satisfaz: $\alpha m=0$, $\alpha \in R$ e $m \in M$, então $\alpha=0$ ou $m=0$. Daqui em diante, a menos que digamos o contrário, todo R - módulo será livre de torção.

Nosso objetivo será classificar todos os R - módulos finitamente gerados e desenvolver uma teoria de fatores invariantes semelhantes a que já conhecemos no caso de módulos sobre domínios principais (vide [2]). Os ideais fracionários serão de grande importância e os resultados básicos sobre eles consideraremos de conhecimento de todos.

Teorema (2.1): Seja M um R - módulo e K o corpo de frações de R . Então M pode ser mergulhado em um K - espaço vetorial KM .

Demonstração:

O espaço vetorial KM será definido através de uma construção semelhante a usada para se obter o corpo de frações de um domínio integral.

Consideremos

$$S = \left\{ (m, \alpha) ; m \in M, \alpha \in R, \alpha \neq 0 \right\}$$

e definamos a seguinte relação sobre S

$$(m_1, \alpha_1) \sim (m_2, \alpha_2) \iff \alpha_1 m_2 = \alpha_2 m_1.$$

Obviamente $\sim$ é reflexiva e simétrica. Verifiquemos a transitividade.

Suponhamos $(m_1, \alpha_1) \sim (m_2, \alpha_2)$ e $(m_2, \alpha_2) \sim (m_3, \alpha_3)$ então $\alpha_1 m_2 = \alpha_2 m_1$ e

$$\alpha_2 m_3 = \alpha_3 m_2.$$

Consequentemente

$$\alpha_1 (\alpha_3 m_2) = \alpha_3 (\alpha_1 m_2) = \alpha_1 (\alpha_2 m_3) = \alpha_2 (\alpha_1 m_3).$$

Logo

$$\alpha_2 (\alpha_3 m_1) = \alpha_1 m_3$$

e sendo M livre de torção e $\alpha_2 \neq 0$ temos $\alpha_3 m_1 = \alpha_1 m_3$.

Denotemos por M_S o conjunto das classes de equivalência de S por $\sim$

e, denotemos

$$m/\alpha = \text{a classe de equivalência de } (m, \alpha)$$

Definamos em M_S uma operação de adição por

$$m_1/\alpha_1 + m_2/\alpha_2 = \left(\alpha_2 m_1 + \alpha_1 m_2 \right) / \alpha_1 \alpha_2$$

facilmente se verifica a boa definição da operação e que ela satisfaz as condições para que $(M_S, +)$ seja grupo abeliano aditivo com elemento nulo $0/1$.

Definamos agora uma ação de $K = \text{cfr } (R)$ sobre o grupo $(M_S, +)$ dada

por

$$\begin{array}{ccc} K \times M_{\beta} & \longrightarrow & M_{\beta} \\ (\beta/\gamma, m/\alpha) & \longrightarrow & (\beta m)/(\gamma \alpha) \end{array}$$

com $\beta, \gamma, \alpha \in R, \gamma \neq 0, \alpha \neq 0$, e $m \in M$.

De modo quase imediato podemos verificar que essa definição independe da escolha de representantes e que satisfaz as condições para que M_{β} seja K - espaço vetorial. Daqui em diante denotaremos M_{β} por KM .

A aplicação

$$\begin{array}{ccc} M & \longrightarrow & KM \\ m & \longrightarrow & m/1 \end{array}$$

é obviamente um homomorfismo injetor de R - módulo. Desta maneira, podemos considerar M como R - submódulo de KM e denotaremos $m/1$ simplesmente por m .

■

Algumas observações:

1) Temos $m/\alpha = (1/\alpha)(m/1) = \alpha^{-1}m$ e deste modo os elementos de KM podem ser vistos como K - múltiplos de elementos de M , logo, para m_1 e $m_2 \in M$ temos

$$(\alpha/\beta)m_1 + (\gamma/\delta)m_2 = (\beta\delta)^{-1}(\alpha\delta m_1 + \beta\gamma m_2)$$

Consequentemente, se $M = \sum_{i=1}^k Rm_i, m_i \in M$, então $KM = \sum_{i=1}^k Km_i$, mais além,

se $M = \bigoplus_{i=1}^k R m_i$ então $KM = \bigoplus_{i=1}^k K m_i$. Portanto se M é R - módulo finitamente gerado então KM é um K - espaço vetorial de dimensão finita e mais ainda, se $\langle m_1, \dots, m_k \rangle$ é base de M (isto é, no caso em que M é livre) então $\{ m_1/1, \dots, m_k/1 \}$ é base de KM .

2) Uma maneira mais sofisticada de fabricar o K - espaço vetorial desejado seria considerar o produto tensorial $K \otimes_R M$ que é K - espaço vetorial e facilmente pode-se comprovar que

$$K \otimes_R M \longrightarrow KM$$

$$\sum \alpha_i \otimes m_i \longrightarrow \sum \alpha_i (m_i/1)$$

é um K - isomorfismo entre $K \otimes_R M$ e KM .

Definição (2.2): Seja M um R - módulo, por R - rank de M entenderemos a dimensão de KM como K - espaço vetorial e denotaremos por $\text{rank}(M) = (KM:K)$, onde $(KM:K)$ = dimensão de KM como K -espaço vetorial. Algumas vezes nos referiremos a $\text{rank}(M)$ por $(M:R)$.

Como já vimos, se M R - módulo finitamente gerado então $\text{rank}(M) < \infty$. Contudo a recíproca não é válida, bastando para tanto considerar $M = K$ onde K é o corpo de frações de R .

Proposição (2.3): Seja M um R - módulo finitamente gerado então $\text{rank}(M)$ é igual ao número máximo de elementos R - livres de M .

Demonstrações:

Um conjunto $\{m_i\}_{i \in A}$ é dito R -livre se sempre que

$$r_{1i}m_{1i} + \dots + r_{ti}m_{ti} = 0$$

com $r_{ik} \in R$, então $r_{ik} = 0$, $1 \leq k \leq t$.

Seja n o número máximo de elementos de M R -livres. Consideremos $\langle m_1, \dots, m_n \rangle$ um conjunto de elementos R -livres de M . Então se

$$(r_1/s_1)(m_1/1) + \dots + (r_n/s_n)(m_n/1) = 0$$

com $s_i \neq 0$, $r_i \in R$, temos

$$r_1 s_2 \dots s_{n-1} m_1 + \dots + r_i s_1 \dots \hat{s}_i \dots s_{n-1} m_i + \dots + r_n s_1 \dots s_{n-1} m_n = 0$$

como $s_1 \dots \hat{s}_i \dots s_n \neq 0$ para cada i e desde que $\langle m_1, \dots, m_n \rangle$ é R -livre temos $r_i = 0$ para cada i e consequentemente $\langle m_1, \dots, m_n \rangle$ é conjunto linearmente independente sobre K . Portanto $\text{rank}(M) \geq n$.

Provaremos que se $\{p_1/\alpha_1, \dots, p_t/\alpha_t\} \subset KM$ é tal que $t > n$ então conjunto é linearmente dependente sobre K .

Seja

$$(\beta_1/\gamma_1)(p_1/\alpha_1) + \dots + (\beta_t/\gamma_t)(p_t/\alpha_t) = 0$$

então

$$\beta_1(\gamma_1 \dots \gamma_t)(\alpha_2 \dots \alpha_t)p_1 + \dots + \beta_i(\gamma_1 \dots \hat{\gamma}_i \dots \gamma_t)(\alpha_1 \dots \hat{\alpha}_i \dots \alpha_t)p_i + \dots +$$

$$+ \dots + \beta_t(\gamma_1 \dots \gamma_{t-1})(\alpha_1 \dots \alpha_{t-1})p_t = 0.$$

Da maximalidade de n , segue que existe $1 \leq j \leq t$ tal que

$$\beta_j(\gamma_1 \dots \hat{\gamma}_j \dots \gamma_t)(\alpha_1 \dots \hat{\alpha}_j \dots \alpha_t) \neq 0$$

logo $\beta_j \neq 0$ e portanto $\left\{ p_1/\alpha_1, \dots, p_t/\alpha_t \right\}$ é linearmente dependente,

que implica $\text{rank}(MD) \leq n$.

■

Sejam M e N dois R - módulos e $\theta : M \longrightarrow N$ um R - isomorfismo entre eles. Então θ pode ser extendido a um K - isomorfismo $\theta* : KM \longrightarrow KN$ dado por $\theta*(m/s) = \theta(m)/s$, onde $m \in M$ e $s \in R - \{0\}$. Observe que se $m \in M$ e $\xi \in K$ então $\theta*(\xi m) = \xi \theta*(m) = \xi \theta(m)$. Consequentemente se $m \in M$ e $\xi \in K$ são tais que $\xi m \in M$ então

$$\theta(\xi m) = \xi \theta(m) \quad (A)$$

Definição (2.4): Sejam dados A e B ideais fracionários. Diremos que eles são R - ideais equivalentes, e denotaremos $A \equiv B$, se existe $\gamma \in K$, $\gamma \neq 0$, tal que $A = \gamma B$.

Facilmente vemos ser esta uma relação de equivalência. Assim se denotarmos

F = conjunto de todos os R - ideais fracionários de K

podemos considerar $\mathbb{F}/\equiv$ e por classe de ideal de A entenderemos a classe de equivalência de A , denotada por $\bar{A}$. Ou seja

$$\bar{A} = \left\{ B \in \mathbb{F}; B = \gamma A \text{ para algum } \gamma \in K, \gamma \neq 0 \right\}$$

Note que se $A_i \equiv B_i$, $i = 1, 2$, então $A_1 A_2 \equiv B_1 B_2$.

Podemos assim definir uma multiplicação sobre $\mathbb{F}$ dada por

$$\bar{A} \bar{B} = \overline{AB}$$

Tal multiplicação satisfaz :

i) comutatividade

ii) $\bar{R}$ (classe dos ideais principais) é o elemento identidade

iii) $\bar{A} \bar{A}^{-1} = \bar{R}$, isto é $\overline{A^{-1}} = \overline{(A)}^{-1}$

Portanto $\mathbb{F}/\equiv$ é um grupo multiplicativo abeliano. Tal grupo é chamado o classe grupo de R e denotado por $\mathcal{C}(R)$.

Lema (2.5): Os R -ideais fracionários A, B são R -isomorfos se e só se pertencem a mesma classe de ideal.

Demonstração:

Obviamente se $A \equiv B$, ou seja, existe $\gamma \in K$, $\gamma \neq 0$ tal que $A = \gamma B$ basta considerar

$$\begin{array}{ccc} \phi : A & \longrightarrow & B \\ x & \longrightarrow & \gamma x \end{array}$$

Reciprocamente, suponhamos $\theta : A \longrightarrow B$ R -isomorfismo e

estenda-mo-lo a $\theta' : KA \longrightarrow KB$ K - isomorfismo . Temos então

$$\theta'(\xi m) = \xi \theta'(m) \quad , \quad m \in KA \quad , \quad \xi \in K$$

Em particular, se $m=1$ e $\xi \in A$ temos

$$\theta(\xi) = \theta'(\xi) = \xi \theta'(1)$$

logo dado $n \in B$, existe $\xi \in A$ tal que

$$n = \theta(\xi) = \xi \theta'(1)$$

ou seja $B = \theta'(1)A$.

■

Daremos agora um primeiro passo na classificação dos R -
modulos finitamente gerados considerando o caso em que seu rank é 1 .

Lema (2.6): Seja M um R - módulo finitamente gerado cujo
rank é 1 . Então M é R - isomorfo a um R - ideal fracionário em K .

Demonstração:

Seja $K = \text{cfr}(R)$. Por hipótese, existe $m/s \in KM$ tal que $KM = K(m/s)$,
 $m \in M$, $m \neq 0$.

Consideremos

$$I = \left\{ \alpha \in K; \alpha m \in M \right\}$$

que é um R - submódulo de K .

Definamos $\phi : I \longrightarrow M$ um R -homomorfismo onde $\phi(\alpha) = \alpha m$. Podemos

facilmente verificar que ϕ é injetora e sobrejetora. Agora, desde que ϕ é R - isomorfismo e M é R - módulo finitamente gerado, também $\phi^{-1}(M)$ é R - módulo finitamente gerado. Assim I é um ideal fracionário.

■

Lema (2.7): Seja M um R - módulo finitamente gerado. Se $\alpha \in K$ é tal que $\alpha M \subset M$ então $\alpha \in R$.

Demonstração:

Seja $m \in M$, $m \neq 0$ e consideremos $I = \left\{ \beta \in K; \beta m \in M \right\}$. Já vimos ser I um R -ideal fracionário e obviamente $I \supset R$.

Suponhamos que $\alpha \in K$ é tal que $\alpha M \subset M$. Assim $\alpha \in I$, o que implica $R[\alpha] \subset I$.

Desde que I é R - módulo finitamente gerado e R domínio de Dedekind segue que $R[\alpha]$ é R - módulo finitamente gerado e consequentemente α é integral sobre R . Sendo R integralmente fechado, temos $\alpha \in R$.

■

Definição (2.8): Sejam R um anel comutativo com identidade, M um R - módulo (não necessariamente livre de torção) e N um R - submódulo de M . Diremos que N é submódulo puro de M , se dado $\alpha \in R$, $\alpha \neq 0$, $\alpha N = N \cap \alpha M$.

Desde que a inclusão $\alpha N \subset \left[N \cap \alpha M \right]$ é óbvia temos: N é

puro se e só se dado $m \in M$ e $\alpha \in R$ tal que $\alpha m \in N$ então existe $n \in N$ tal que $\alpha m = \alpha n$.

Algumas consequências imediatas desta observação:

1) Se N é um somando direto de M então N é puro.

2) Se M é um R -módulo livre de torção, N é puro se e só se para todo $m \in M$ e $\alpha \in R$ com $\alpha m \in N$ tivermos que $m \in N$.

3) Se M/N é livre de torção então N é puro. Se M é livre de torção e N é puro então M/N é livre de torção.

4) Seja $K = \text{cfr}(R)$ e $\langle v_1, \dots, v_n \rangle$ uma K -base de um K -espaço vetorial V_0 . Consideremos $M = Rv_1 \oplus \dots \oplus Rv_n$ e W_0 um K -subespaço vetorial de V_0 . Então $W_0 \cap M$ é submódulo puro de M . Mas que isso, se tomarmos S um subconjunto arbitrário de M e considerarmos KS o K -espaço de V_0 gerado por S , $KS \cap M$ é o único submódulo puro minimal de M contendo S .

Dados $M_1, \dots, M_k$ R -módulos definimos como soma direta externa, e denotamos por

$$M* = M_1 \dot{+} M_2 \dot{+} \dots \dot{+} M_k$$

o conjunto de todas as k -uplas $(m_1, \dots, m_k)$, $m_i \in M_i$, $1 \leq i \leq k$, com a adição dada por

$$(m_1, \dots, m_k) + (n_1, \dots, n_k) = (m_1 + n_1, \dots, m_k + n_k)$$

e produto por um elemento de R dado por

$$r(m_1, \dots, m_k) = (rm_1, \dots, rm_k).$$

Deste modo $M*$ é um R -módulo.



Sejam $I_1, \dots, I_n$ R-ideais fracionários em K , então $I_1 + \dots + I_n$ é um R-módulo, livre de torção, finitamente gerado e de rank igual a n .

Queremos saber se a recíproca é verdadeira, isto é, se dado M um R - módulo livre de torção finitamente gerado cujo rank é n , então este é isomorfo a uma soma direta externa de n R - ideais fracionários. A resposta é afirmativa e o resultado segue como um teorema:

Teorema (2.9): Todo M R - módulo finitamente gerado de rank igual a n é isomorfo a uma soma direta externa de n R - ideais fracionários.

Demonstração:

Faremos por indução sobre o rank de M . Para o caso $\text{rank}(M) = 1$ é exatamente o lema (2.6). Consideremos $n \geq 2$ e suponhamos válido o resultado para rank igual a $n-1$.

Consideremos M mergulhado em KM e escolhamos $m \in M$, $m \neq 0$.

Seja $N = Km \cap M$ o submódulo puro gerado por m . Então M/N é livre de torção, finitamente gerado e $\text{rank}(M/N) = n-1$ (para tanto facilmente se verifica que $K(M/N) \cong KM/KN$ como K - espaço vetorial).

Segue então da hipótese de indução que existem $n-1$ R - ideais fracionários tais que

$$M/N \cong I_1 + \dots + I_{n-1} \quad (B)$$

deste modo para se concluir a demonstração é suficiente verificar que N é um somando direto de M .

Realmente se mostrarmos que $M = N \oplus T$ para algum R - submódulo T teremos

$$T \cong M/N \cong I_1 \dot{+} \dots \dot{+} I_{n-1}$$

Por outro lado, N R - módulo finitamente gerado de rank 1 e portanto, novamente do lema (2.6) temos $N \cong I$, I R - ideal fracionário, seguindo-se daí o desejado.

Segue de (B) que existe

$$\varphi : M \longrightarrow I_1 \dot{+} \dots \dot{+} I_{n-1} \quad R\text{-homomorfismo sobrejetor}$$

tal que $\ker \varphi = N$. Para cada j , seja $M_j = \varphi^{-1}(I_j)$ e $\varphi_j = \varphi|_{M_j}$.

Então $\varphi_j : M_j \longrightarrow I_j$ é um R - homomorfismo sobrejetor cujo kernel é N . Afirmamos ser N um somando direto para cada M_j .

Desde que $I_j I_j^{-1} = R$, existem $\alpha_1, \dots, \alpha_t \in I_j^{-1}$ e $\beta_1, \dots, \beta_t$ elementos de I_j tal que

$$\alpha_1 \beta_1 + \dots + \alpha_t \beta_t = 1$$

Escolhamos $x_1, \dots, x_t \in M_j$ tal que $\varphi_j(x_i) = \beta_i$, $1 \leq i \leq t$.

Além disso para $\gamma \in I_j$, $\gamma \neq 0$, $\gamma \alpha_i \in R$.

Consideremos

$$z = (\gamma \alpha_1)x_1 + \dots + (\gamma \alpha_t)x_t \in M_j$$

então

$$\varphi(z) = \varphi \left(\sum_{i=1}^t (\gamma \alpha_i)x_i \right) = \gamma$$

Seja $T_j = Kz \cap M_j$ submódulo puro de M_j gerado por z . Afirmamos que

$M_j = T_j \oplus N$. De fato:

$$i) T_j \cap N = (0)$$

Se $x \in T_j \cap N$ temos $x = \xi z$ onde $\xi \in K$, mas

$$0 = \varphi(x) = \varphi(\xi z) = \xi \varphi(z) = \xi \gamma$$

e desde que $\gamma \neq 0$ temos $\xi = 0$, ou seja, $x = 0$

$$ii) M_j = T_j + N$$

Seja $x \in M_j$. Seja $\rho = \varphi_j(x) \in I_j$ então desde que $\rho \alpha_i \in R$,

$1 \leq i \leq t$, consideremos o seguinte elemento de M_j

$$\omega = \rho \alpha_1 x_1 + \dots + \rho \alpha_t x_t$$

então

$$\omega = \gamma \gamma^{-1} \rho \alpha_1 x_1 + \dots + \gamma \gamma^{-1} \rho \alpha_t x_t = \gamma^{-1} \rho z$$

Ou seja $\omega \in M_j \cap Kz = T_j$.

Além disso

$$\varphi(\omega) = \varphi(\gamma^{-1} \rho z) = \gamma^{-1} \rho \varphi(z) = \rho = \varphi(x)$$

consequentemente $(\omega - x) \in N$. Assim $x = \omega + (x - \omega)$.

Para cada M_j encontramos T_j submódulo puro de M_j tal que $M_j = T_j \oplus N$

e $\varphi(T_j) = \varphi(M_j) = I_j$. Afirmamos que $M = (T_1 + \dots + T_{n-1}) \oplus N$.

Desde que

$$\varphi(T_1 + \dots + T_{n-1}) = I_1 + \dots + I_{n-1}$$

temos $M = T_1 + \dots + T_{n-1} + N$.

Se $t_1 + \dots + t_{n-1} \in N$ onde cada $t_i \in T_i$ então temos que $\varphi(t_1) + \dots + \varphi(t_{n-1}) = 0$, mas cada $\varphi(t_i) \in I_i$ donde $\varphi(t_i) = 0$.

Consequentemente cada $t_i = 0$, o que completa a prova.

■

Uma outra prova muito interessante do mesmo teorema é dada por Rotman em [10] utilizando-se de módulos projetivos.

Outra observação referente a esta demonstração é que em nenhum momento o fato de $N = Km \cap M$ influiu na prova de ser N um somando direto de M . A informação relevante foi a de ser N um submódulo puro de M . Portanto, seguindo a mesma demonstração podemos enunciar o seguinte resultado :

Proposição (2.10): Sejam M R - módulo finitamente gerado e $N \subset M$ R - submódulo, então

$$N \text{ puro} \iff N \text{ somando direto de } M$$

Suponhamos agora

$$M \cong I_1 + \dots + I_n \quad (C)$$

onde os I_j são R - ideais fracionários não nulos em K . Podemos encontrar elementos não nulos $\alpha_1, \dots, \alpha_n$ em K tal que $\alpha_j I_j \subset R$.

Além disso, desde que $I_j \cong \alpha I_j$, temos

$$M \cong \alpha I_1 + \dots + \alpha I_n$$

Consequentemente, multiplicando $\langle I_j \rangle$ por elementos não nulos convenientes de K podemos considerar em $(\mathbb{C})$ que cada $I_j \supset R$.

Seja

$$\psi : M \longrightarrow I_1 + \dots + I_n$$

o isomorfismo assumido em $(\mathbb{C})$.

Tomemos agora $m_j \in M$ tal que

$$\psi(m_j) = (0, \dots, 1, \dots, 0)$$

onde 1 aparece na j -ésima posição, então

$$\psi(m) = (a_1, \dots, a_n) = a_1(1, 0, \dots, 0) + \dots + a_n(0, \dots, 0, 1)$$

com $a_j \in I_j$, donde

$$m = \psi^{-1}(a_1(1, 0, \dots, 0)) + \dots + \psi^{-1}(a_n(0, \dots, 0, 1))$$

por (A) temos

$$m = a_1 m_1 + \dots + a_n m_n$$

Desde que ψ injetora, segue a unicidade de representação, ou seja,

$$M = I_1 m_1 \oplus \dots \oplus I_n m_n \quad (\mathbb{D})$$

De certa maneira temos que $\langle m_1, \dots, m_n \rangle$ constituem-se uma "base" de M .

O próximo teorema dá uma condição, em termos dos I_j , necessária e suficiente para que dois módulos sejam isomorfos.

Teorema (2.11): Sejam $M \cong I_1 \dot{+} \dots \dot{+} I_m$ e $N \cong J_1 \dot{+} \dots \dot{+} J_n$ onde os I_i e J_j são R -ideais fracionários. Então $M \cong N$ se e só se $m = n$ e os produtos $I_1 \dots I_m, J_1 \dots J_m$ são da mesma classe de ideal.

Antes de demonstrarmos tal teorema vamos apresentar alguns resultados auxiliares que usaremos na sua prova.

Lema (2.12): Sejam R domínio de Dedekind e A e B R -ideais integrais. Então existe C um R -ideal integral tal que AC é principal e C e B são co-primos.

Demonstração:

Desde que R domínio de Dedekind, podemos expressar

$$A = P_1^{a_1} \dots P_n^{a_n}$$

e

$$B = Q_1^{b_1} \dots Q_m^{b_m}$$

com $P_i, Q_j \in \text{Spec}(R), a_i, b_j \in \mathbb{N} \cup \{0\}$.

Seja $\alpha_i \in P_i^{a_i} - P_i^{a_i+1}$ e $\alpha_i \notin Q_i$. Pelo teorema do Resto Chinês existe α em R tal que $\alpha \equiv \alpha_i \pmod{(P_i^{a_i+1})}$.

Então $\alpha \in P_i^{a_i} - P_i^{a_i+1}$ e $\alpha \notin Q_i$. Consequentemente

$$\alpha \in \cap P_i^{a_i} = P_1^{a_1} \dots P_n^{a_n} = A$$

Consideremos o R -módulo $R\alpha + AB \subset A$. Temos então que $R\alpha + AB = A$.

Como $R\alpha \subset A$, existe C R -ideal tal que $\alpha R = AC$ (R Dedekind), logo,

$$AC + AB = A$$

e sendo A inversível temos

$$C + B = R$$

■

Corolário (2.13): Sejam I e J R -ideais fracionários próprios. Então existem $\alpha, \beta \in K$ tais que αI e βJ são R -ideais integrais e co-primos.

Demonstração:

Consideremos os R -ideais fracionários J e I^{-1} . Então existem β e γ em K tais que βJ e γI^{-1} são integrais. Pelo lema (2.12) existe F integral tal que $F\gamma I^{-1} = R\alpha$ e $F + \beta J = R$, o que conclui a prova.

■

Corolário (2.14): Sejam I_1, I_2 R -ideais fracionários e E_1, E_2 ideais integrais tais que $E_2 \subset E_1, E_2 \neq (0)$. Então existe

$$\phi : I_1 + I_2 \longrightarrow R + I_1 I_2$$

um R -isomorfismo tal que $\phi(E_1 I_1 + E_2 I_2) = E_1 + E_2 I_1 I_2$.

Demonstração:

Pelo corolário (2.13) podemos assumir I_1, I_2 integrais e $I_1 + E_2 I_2 = R$. Sejam $\alpha_1 \in I_1$ e $\alpha_2 \in E_2 I_2$ tais que $\alpha_1 - \alpha_2 = 1$.

Definamos

$$\phi : I_1 + I_2 \longrightarrow R + I_1 I_2$$

onde $\phi(\beta_1, \beta_2) = (\beta_1 + \beta_2, \alpha_1 \beta_2 + \alpha_2 \beta_1)$.

Facilmente vemos ser ϕ injetora. Verifiquemos pois a sobrejeção. Seja $(r, x) \in R + I_1 I_2$ então ele é imagem de $(r\alpha_1 - x, x - \alpha_2 r)$ por ϕ .

Agora, se $(r, x) \in E_1 + E_2 I_1 I_2$ então

$$r\alpha_1 - x \in I_1 E_1 + E_2 I_1 I_2 \subset E_1 I_1$$

$$x - \alpha_2 r \in E_2 I_1 I_2 + E_2 I_1 I_2 \subset E_2 I_2$$

Por outro lado, se $(\beta_1, \beta_2) \in E_1 I_1 + E_2 I_2$ temos que

$$\beta_1 + \beta_2 \in E_1 I_1 + E_2 I_1 \subset E_1$$

$$\beta_1 \alpha_2 + \beta_2 \alpha_1 \in E_1 E_2 I_1 I_2 + E_2 I_1 I_2 \subset E_2 I_1 I_2$$

ou seja

$$\phi (E_1 I_1 + E_2 I_2) \subset E_1 + E_2 I_1 I_2.$$

■

Corolário (2.15): Dados $I_1, \dots, I_n$ R - ideais fracionários temos então que

$$I_1 + \dots + I_n \cong R + \dots + R + (I_1 \dots I_n)$$

onde existem $(n - 1)$ somandos para R .

Demonstração do teorema (2.11):

Assumamos inicialmente que $M \cong N$ então $m = (M : R) = (N : R) = n$.

Podemos supor que cada I_k, J_k contém R , desde que é sempre possível considerar ao invés deles alguém de sua classe de ideal.

Seja $\theta : M \longrightarrow N$ o R - isomorfismo considerado e suponhamos que para $1 \in I_k$,

$$\theta (0, \dots, 1, \dots, 0) = (\alpha_{k1}, \dots, \alpha_{km})$$

onde temos 1 na k -ésima posição e zeros nas restantes e cada $\alpha_{kl} \in J_l$.

Então

$$M = I_1 (1, 0, \dots, 0) + \dots + I_m (0, 0, \dots, 1)$$

donde

$$\theta (M) \subset I_1 (\alpha_{11}, \dots, \alpha_{1m}) + \dots + I_m (\alpha_{m1}, \dots, \alpha_{mn})$$

assim

$$\theta(CM) = \left(\sum_k \alpha_{k1} I_k, \dots, \sum_k \alpha_{km} I_k \right)$$

consequentemente

$$J_l = \alpha_{1l} I_1 + \dots + \alpha_{ml} I_m, \quad l = 1, \dots, m.$$

Assim $J_1 \dots J_m \supset (\alpha_{1v_1} \dots \alpha_{mv_m}) (I_1 \dots I_m)$ onde $(v_1, \dots, v_m)$ é qualquer permutação de $(1, \dots, m)$.

Se $\delta = \det \left(\alpha_{ij} \right)_{1 \leq i, j \leq m}$ vemos que $J_1 \dots J_m \supset \delta (I_1 \dots I_m)$.

De maneira análoga, podemos encontrar $\beta_{lk} \in I_k$ tal que

$$\theta(\beta_{1i}, \dots, \beta_{mi}) = (0, \dots, 1, \dots, 0)$$

onde 1 aparece na i-ésima posição e zero nas restantes.

Então $(\beta_{ij})(\alpha_{ij}) = \text{Id}$ e consequentemente $\det(\beta_{ij}) = \delta^{-1}$.

Do mesmo modo podemos ver que $I_1 \dots I_m \supset \delta^{-1} (J_1 \dots J_m)$.

Ou seja

$$\delta (I_1 \dots I_m) = J_1 \dots J_m$$

Provemos a recíproca. Para tanto é suficiente que dados I_1, I_2 ideais fracionários tenhamos $I_1 + I_2 \cong R + I_1 I_2$ o que segue imediatamente do corolário (2.14) tomando $E_1 = E_2 = R$.

■

Para a demonstração do teorema do fator invariante

desenvolveremos alguns resultados preliminares que serão de muita utilidade na prova do teorema, outros, como no caso do teorema de Krull-Schmidt, serão apenas mencionados já que suas demonstrações fogem do objetivo deste capítulo.

Seja R um anel comutativo e M um R -módulo, então M é um módulo indecomponível se $M \neq (0)$ e se não é possível expressar M como soma direta de dois submódulos não triviais, ou seja, se $M = N \oplus N'$ com N e N' submódulos de M então ou $N = (0)$ ou $N' = (0)$.

Teorema (2.16) (Teorema de Krull-Schmidt): Seja R um anel comutativo com identidade. Seja M um R -módulo satisfazendo a ambas as condições da cadeia. Suponhamos que

$$M = M_1 \oplus \dots \oplus M_k = N_1 \oplus \dots \oplus N_h$$

sejam duas decomposições de M em somas diretas de submódulos não nulos indecomponíveis. Então $h = k$ e $M_i \cong N_i$, $i = 1, \dots, h$.

Proposição (2.17): Sejam $\{P_1, \dots, P_n\} \subset \text{Spec}(R)$ um conjunto de primos distintos e $\langle a_1, \dots, a_n \rangle$ um conjunto de inteiros não negativos. Então existem $\alpha \in R$ e B um R -ideal integral relativamente primo a cada P_i tais que

$$\alpha R = \left[P_1^{a_1} \dots P_n^{a_n} \right] B$$

Demonstração:

Para cada i , existe C_i integral tal que C_i é co-primo a $P_1 \dots P_n$ e

$C_i P_i^{a_i} = R \alpha_i$ com $\alpha_i \in R$. Então seja $B = \prod C_i$ e $\alpha = \alpha_1 \dots \alpha_n$.

■

Corolário (2.18): Sejam $\{P_1, \dots, P_n\} \subset \text{Spec}(R)$ onde os P_i são todos distintos e $\langle a_1, \dots, a_n \rangle$ números inteiros (não necessariamente positivos). Então existem $\alpha \in K$ e $B \subset R$ - ideal integral relativamente primo a cada P_i tais que

$$R\alpha = \left[P_1^{a_1} \dots P_n^{a_n} \right] B$$

Demonstração:

Suponhamos que $a_1, \dots, a_m$ com $m \leq n$ sejam negativos e $a_{m+1}, \dots, a_n$ sejam não negativos. Então $-a_1, \dots, -a_m$ são positivos e pela proposição (2.17) existem $\alpha' \in R$ e B' integral tais que

$$B' \left[P_1^{-a_1} \dots P_m^{-a_m} \right] = R\alpha'$$

e

$$P_1^{a_1} \dots P_m^{a_m} = (\alpha')^{-1} B'$$

Mas sendo R Dedekind temos $B' = Q_1^{b_1} \dots Q_h^{b_h}$, como B' relativamente primo a cada P_i temos que $P_1, \dots, P_m, Q_1, \dots, Q_h$ são todos distintos. Novamente utilizando da proposição (2.17) temos que existem $\gamma \in R$ e C integral tais que $CB' = R\gamma$ e C co-primo com os P_j e Q_i , $i = 1, \dots, h$, $j = 1, \dots, m$.

Então $C \begin{pmatrix} P_1^{a_1} & \dots & P_m^{a_m} \end{pmatrix} = \alpha^{-1} B' C = R(\alpha^{-1} \gamma).$

■

Proposição (2.19): Sejam A R - ideal integral e B R - ideal fracionário então $R/A \cong B/(AB)$ como grupo aditivo.

Demonstração:

Pelo corolário (2.18) existe C R - ideal integral tal que $C + A = R$ e $CB = R\rho$, $\rho \in K$.

Consideremos o R - homomorfismo definido por

$$\begin{aligned} \theta : R &\longrightarrow B/(AB) \\ x &\longrightarrow \rho x + AB \end{aligned}$$

onde $\rho x + AB$ denota a classe residual de ρx em AB .

Então desde que $A + C = R$ temos $AB + R\rho = AB + BC = B$.

Dado $b \in B$ temos que existe $x \in AB$ e $y \in R$ tal que $b = x + \rho y$ e consequentemente $b + AB = \rho y + AB$.

Calculemos o $\ker(\theta)$. Obviamente $A \subset \ker(\theta)$, basta ver que desde que $R\rho = BC \subset B$ temos $\rho \in B$.

Suponhamos $x \in R$ com $\rho x + AB = 0 + AB$ então $\rho x \in AB$ o que implica $\rho x C \subset ABC = \rho A$ e consequentemente $x C \subset A$.

Como existem $a \in A$ e $c \in C$ tais que $a + c = 1$, temos

$$x = xa + xc \in A$$

donde $\ker(\theta) = A$.

■

Teorema (2.20) (Teorema dos fatores invariantes): Sejam M e N R - módulos finitamente gerados de mesmo rank e tal que $N \subset KM$. Então existem elementos $m_1, \dots, m_k \in M$ e R - ideais fracionários $I_1, \dots, I_k, E_1, \dots, E_k$ tais que $E_j \supset E_{j+1}$, $j = 1, \dots, k-1$ e

$$M = I_1 m_1 \oplus \dots \oplus I_k m_k$$

$$N = E_1 I_1 m_1 \oplus \dots \oplus E_k I_k m_k$$

Os ideais $E_1, \dots, E_k$ são unicamente determinados pelo par M, N e serão ditos *fatores invariantes de N em M* .

Demonstração:

Desde que $N \subset KM$ e $\text{rank } N = \text{rank } M$ podemos considerar M e N mergulhados no mesmo K - espaço vetorial KM .

Suponhamos $k = 1$, temos pelo lema (2.6) que existem I e J ideais fracionários tais que $M \cong I$ e $N \cong J$.

Portanto existem $m \in M$ e $n \in N$ tais que

$$M = Im \quad \text{e} \quad N = Jn$$

Como $M \subset KM = KN$ temos $m/1 = n/\alpha$, com $\alpha \in R$, o que implica $n = m\alpha$.

Logo $N = Jm$.

Como podemos considerar que $R \subset J$ temos $N = Jm = (JI^{-1}) Im$.

Suponhamos válido o resultado para módulos de rank $\leq (k-1)$.

Sendo M R - módulo finitamente gerado temos

$$M = Rm_1 + \dots + Rm_r$$

Para cada m_i , $i = 1, \dots, r$, existem $\alpha_i \in R$ e $n_i \in N$ tais que

$$m_i/1 = n_i/\alpha_i.$$

Seja $\gamma = \alpha_1 \dots \alpha_r$ então $\gamma M \subset N$.

Consideremos

$$E' = \left\{ \alpha \in R; \alpha N \subset M \right\}$$

que já sabemos não nulo (faça raciocínio idêntico ao utilizado para encontrar γ tal que $\gamma M \subset N$). Afirmamos ser E' um R -ideal fracionário. De fato, seja $\alpha \in E'$ então $\alpha N \subset M$ logo $\gamma \alpha N \subset N$ e pelo lema (2.7) temos que $\gamma \alpha \in R$. Consequentemente $\gamma E' \subset R$.

Da própria definição de E' temos ser ele o maior ideal tal que $E'N \subset M$.

Seja $E = (E')^{-1}$ então ele é o único ideal minimal tal que $N \subset EM$.

Desde que $E'N \subset M$ então $EE'N = N \subset EM$. Suponhamos F R -ideal fracionário com $N \subset FM$ então $F^{-1}N \subset F^{-1}(FM) = M$ logo $F^{-1} \subset E' = E^{-1}$.

Assim $E = ER = EFF^{-1} \subset EE^{-1}F \subset F$ donde segue a afirmação.

Sejam $P_1, \dots, P_s \in \text{Spec}(R)$ distintos tais que ou $P_i \supset \gamma R$ ou P_i

aparece com expoente negativo na fatorização de E em potências de ideais primos.

Para cada i , $1 \leq i \leq s$, seja $n_i \in N$ tal que $n_i \notin P_i EM$ (como E é o único ideal minimal fracionário tal que $N \subset EM$, qualquer que seja P ideal integral temos $N \not\subset PEM$).

Escolhamos agora $\mu_i \in R$, $1 \leq i \leq s$, tal que

$$\mu_i \equiv 0 \pmod{\prod_{j \neq i} P_j} \quad \text{e} \quad \mu_i \not\equiv 0 \pmod{P_i}$$

(observe que se $\prod_{j \neq i} P_j \subset P_i$ existiria $j \neq i$ tal que $P_j \subset P_i$, logo $P_j = P_i$, absurdo).

Consideremos então

$$n = \sum_{i=1}^s \mu_i n_i \in N$$

então $n \notin P_i EM$, $1 \leq i \leq s$. De fato, suponhamos que tal não ocorresse

ou seja, existisse um i , suponhamos $i = 1$, tal que $n \in P_1 EM$.

Como para qualquer $i \neq 1$, $\mu_i n_i \in P_1 N \subset P_1 EM$, temos $\mu_i n_i \in P_1 EM$.

Sendo P_1 maximal temos

$$R\mu_1 + P_1 = R$$

consequentemente $1 = \mu\mu_1 + p$, $p \in P_1$ e $\mu \in R$.

Dai $n_1 = \mu\mu_1 n_1 + pn_1 \in P_1 EM$, absurdo.

Consideremos $Kn \cap N$ e $Kn \cap M$ submódulos puros de N e M respectivamente, ambos de rank 1.

Assim, pelo lema (2.6) existem R -ideais fracionários A e B , que podemos supor contendo R , tais que $Kn \cap N \cong A$ e $Kn \cap M \cong B$.

Portanto temos

$$Kn \cap N = An \quad \text{e} \quad Kn \cap M = Bn$$

Então $E'An \subset E'N \subset M \rightarrow E'An \subset Kn \cap M = Bn \rightarrow E'A \subset B$.

Sabemos que existem $\alpha, \beta \in R - \langle 0 \rangle$ tais que $\alpha E'A \subset R$ e $\beta B \subset R$.

Então $\alpha\beta E'A \subset \alpha\beta B \subset R \rightarrow$ existe C um R -ideal integral tal que $\alpha\beta E'A = \alpha\beta BC$. Assim $E'A = BC$.

Além disso $\gamma Bn \subset \gamma N \subset N \rightarrow \gamma Bn \subset Kn \cap N = An \rightarrow \gamma B \subset A \rightarrow R\gamma \subset EC$.

Portanto todo ideal primo pertencente a C ou contém Ry ou ocorre no "denominador" de E . Consequentemente os ideais primos pertencentes a C se encontram entre os $P_1, \dots, P_s$.

Por outro lado, se $C \subset P_i$ temos $n \in An = ECBn \subset CEM \subset P_i EM$, absurdo.

Consequentemente $C = R$ e $B = E'A$.

Sejam $N_1 = An$ e $M_1 = Bn (= E'An)$ que são submódulos puros de rank 1 de N e M respectivamente.

Pela proposição (2.10) existe M_1' submódulo de M tal que $M = M_1 \oplus M_1'$.

Afirmamos que

$$N = N_1 \oplus N_1' \quad \text{onde} \quad N_1' = KM_1' \cap N \quad (E)$$

Como $KN_1 = KM_1$ e $KN_1' = KM_1'$ temos $N_1 \cap N_1' \subset KM_1 \cap KM_1'$.

Seja $m/s \in KM_1 \cap KM_1'$ então existem $m_1 \in M_1$, $m_1' \in M_1'$, $s', s'' \in R$, $s, s' \neq 0$, tais que $m/s = m_1/s' = m_1'/s''$.

Mas $M = M_1 \oplus M_1'$ então $m = m_2 + m_2'$, $m_2 \in M$, $m_2' \in M_1'$.

Então $m_2/s + m_2'/s = m_1/s'$ donde $m_2s + m_2's = m_1s$ o que implica $m_2's = 0$ e então $m_2' = 0$.

De maneira analoga temos $m_2 = 0$ e então $KM_1 \cap KM_1' = (0)$, consequentemente $N_1 \cap N_1' = (0)$.

Como $N \subset EM = E(M_1 \oplus M_1') \subset EM_1 + EM_1'$. Se $x \in N$, então $x = \alpha n + y$ onde $\alpha \in K$ e $y \in KM_1'$.

Logo

$$E'x = E'\alpha n + E'y$$

mas $E'x \in M$, $E'\alpha n \in KM_1'$, $E'y \in KM_1'$, $KM = KM_1' \oplus KM_1''$ e sendo M livre de torção a inclusão de M em KM é injetora.

Logo $E'\alpha n \in M_1' \Rightarrow \alpha n \in EM_1' = N_1' \Rightarrow y \in N \cap KM_1'$, o que conclui a prova de (E).

Temos então

$$M = Bn \oplus M_1' \quad \text{e} \quad N = EBn \oplus N_1'$$

Além disso $KM_1' = KN_1'$ e $\text{rank } M_1' = \text{rank } N_1' = k-1$ consequentemente utilizando-nos da hipótese de indução, temos a existência de

$m_1, \dots, m_{k-1} \in M_1'$ e ideais fracionários $A_1, \dots, A_{k-1}$, $E_1, \dots, E_{k-1}$

em K com $E_j \supset E_{j+1}$, $j = 1, \dots, k-2$, tal que

$$M_1' = A_1 m_1 \oplus \dots \oplus A_{k-1} m_{k-1}$$

$$N_1' = E_1 A_1 m_1 \oplus \dots \oplus E_{k-1} A_{k-1} m_{k-1}$$

Portanto, para se concluir a demonstração de existência é suficiente provar que $E \supset E_1$.

É imediato que $EM_1' \supset N_1'$. Mas E_1 é o único R -ideal fracionário minimal tal que $E_1 M_1' \supset N_1'$ logo $E \supset E_1$.

Provaremos agora que $E_1, \dots, E_k$ estão unicamente determinados por M e N . Se considerarmos $E_1 M$ temos

$$E_1 M = E_1 I_1 m_1 \oplus E_1 I_2 m_2 \oplus \dots \oplus E_1 I_k m_k$$

$$N = E_1 I_1 m_1 \oplus (E_1^{-1} E_2) (E_1 I_2) m_2 \oplus \dots \oplus (E_1^{-1} E_k) (E_1 I_k) m_k$$

onde $E_1^{-1}E_j \in R$, podemos então assumir que os $\{E_i\}$ são ideais integrais.

Então

$$M/N \cong \left(I_{1m_1} \oplus \dots \oplus I_{km_k} \right) / \left(E_1 I_{1m_1} \oplus \dots \oplus E_k I_{km_k} \right) \cong \left(I_1 / (E_1 I_1) \right) \dot{+} \dots \dot{+} \\ \dot{+} \dots \dot{+} \left(I_k / (E_k I_k) \right)$$

mas pela proposição (2.19)

$$M/N \cong R/E_1 \dot{+} \dots \dot{+} R/E_k$$

onde cada R/E_i é um R - módulo cíclico com $\text{Ann}(R/E_i) = E_i$, $1 \leq i \leq k$.

Mais que isso, cada R/E_i satisfaz a ambas as condições da cadeia (já que existe um número finito de ideais entre R e E_i) portanto também M/N satisfaz a ambas as condições da cadeia. Agora como $E_1 \supset \dots \supset E_k$ para cada i

$$E_i = \prod_{j=1}^h P_j^{\alpha_{ij}}$$

e mais ainda, se $i < l$, $\alpha_{ij} \leq \alpha_{lj}$, $P_j \in \text{Spec}(R)$ todos distintos.

Pelo teorema do Resto Chinês temos

$$R/E_i \cong R/(P_1^{\alpha_{i1}}) + \dots + R/(P_h^{\alpha_{ih}})$$

Afirmamos ser cada $R/(P_j^{\alpha_{ij}})$ indecomponível, de fato, sejam $\bar{I}$ e $\bar{J}$ em $R/(P_j^{\alpha_{ij}})$ onde I e J são ideais de R tais que $I, J \supset P_j^{\alpha_{ij}}$.

Então $I = P_j^r$, $J = P_j^s$ com $0 < r, s < \alpha_{ij}$, e obviamente $\bar{I} \cap \bar{J} \neq (0)$.

Temos então

$$M/N \cong R/(P_1^{\alpha_{11}}) + \dots + R/(P_h^{\alpha_{1h}}) + \dots + R/(P_1^{\alpha_{k1}}) + \dots + R/(P_h^{\alpha_{kh}})$$

E pelo teorema (2.16) (de Krull-Schmidt) o conjunto $\{P_j^{\alpha_{ij}}\}$ está univocamente determinado pelo par M e N . Seja $S_j = (\alpha_{1j}, \dots, \alpha_{kj})$ o conjunto das potências do primo P_j , então $E_1 = \prod_{j=1}^h P_j^{\min \langle S_j \rangle}$. Se $\delta_j = \min \langle S_j \rangle$, $E_2 = \prod_{j=1}^h P_j^{\min \langle S_j - \langle \delta_j \rangle \rangle}$, e assim por diante. Consequentemente os E_i estão univocamente determinados pelo par M e N .

■

Algumas observações imediatas :

- 1) No teorema se assumirmos que $N \subset M$ então $R \subset E'$ e assim $E \subset R$.
- 2) Desde que $m_1, \dots, m_k \in M$ temos $1 \in I_j$ para cada j , ou seja, temos $R \subset I_j$.

Corolário (2.21): Sejam M e N R - módulos finitamente gerados tais que $N \subset KM$ e $\text{rank } M = k$. Então existem $m_1, \dots, m_k \in M$ e ideais fracionários $I_1, \dots, I_k, E_1, \dots, E_l$ tais que $E_i \supset E_{i+1}$ para $i = 1, \dots, l-1$ e $l = \text{rank } N$ e

$$M = I_1 m_1 \oplus \dots \oplus I_k m_k$$

$$N = E_1 I_1 m_1 \oplus \dots \oplus E_l I_l m_l$$

onde se $N \subset M$ cada E_i é integral.

Demonstração:

Como $N \subset KM$ temos que $KN \subset KM$. Se provarmos que $M = M' \oplus M''$ onde

$\text{rank } M' = \text{rank } N$ e $N \subset KM'$ o resultado segue diretamente de (2.20).

Consideremos $M' = KN \cap M$, então dado $\alpha \in R - \langle 0 \rangle$

$$\alpha M' = \alpha(KN \cap M) = \alpha(KN) \cap \alpha M = \alpha(KN) \cap \alpha M \cap M$$

e desde que $\alpha(KN) = KN$ temos

$$\alpha M' = (KN \cap M) \cap \alpha M = M' \cap \alpha M$$

e assim M' é submódulo puro de M e por (2.10) temos M' somando direto de M .

■

Corolário (2.22): Todo R - módulo finitamente gerado é isomorfo a uma soma direta externa de R - ideais fracionários e R - módulos da forma R/I , onde I ideal integral .

Demonstração:

Temos $M = Rm_1' + \dots + Rm_n'$. Consideremos o R - módulo livre com base $\langle f_1, \dots, f_n \rangle$ e a aplicação

$$\begin{array}{ccc} \theta : F & \longrightarrow & M \\ f_i & \longrightarrow & m_i' \end{array}$$

então

$$M \cong F/\ker \theta \cong \left(I_1 m_1 \oplus \dots \oplus I_n m_n \right) / \left(E_1 I_1 m_1 \oplus \dots \oplus E_l I_l m_l \right) \cong R/E_1 \dot{+} \dots \dot{+} \\ \dot{+} \dots \dot{+} R/E_l \dot{+} I_{l+1} \dot{+} \dots \dot{+} I_m$$

■

CAPÍTULO III

APLICAÇÕES DO TEOREMA DOS FATORES INVARIANTES

Neste capítulo, a menos que explicitado, R será sempre um domínio de Dedekind.

Alguns resultados interessantes da álgebra comutativa são aqui apresentados utilizando-se como ferramenta básica, nas demonstrações, os dados acerca dos fatores invariantes obtidos no capítulo anterior.

Os fatos aqui relatados não são inéditos, e diferentes demonstrações podem ser encontradas na literatura clássica em álgebra comutativa. Os motivos que nos levaram a selecioná-los em alguns casos foram de fundo puramente estético (a elegância da demonstração do teorema do um e meio gerador), em outros casos, a atualidade da questão enfocada (BCS anéis, vide [12]).

Teorema (3.1) (Teorema do um e meio gerador): Sejam R um domínio de Dedekind e $I \subset R$, $I \neq (0)$, $I \neq R$ um ideal integral. Dado $a \in I - (0)$ então existe $b \in I$ tal que $I = Ra + Rb$.

Demonstração:

Seja $a \in I - (0)$ um elemento arbitrário. Como $\text{rank } I = \text{rank } Ra = 1$ temos pelo corolário (2.22) que

$$I/Ra \cong R/E$$

onde $E \subset R$ é um ideal integral.

Como obviamente R/E é um R - módulo principal ($R/E = R \bar{1}$) temos que $I/Ra = R \bar{b}$ para algum $b \in I$. Onde $I = Ra + Rb$.

■

Antes de enunciarmos o resultado acerca de BCS anéis, definiremos alguns objetos e desenvolveremos alguns fatos preliminares.

O primeiro deles versa acerca de um exercício sugerido por Curtis e Reiner em [6]. Colocaremos a redação original, demonstraremos ser tal versão impossível e apresentaremos uma redação alternativa.

Versão original :

"Seja M um R - módulo livre de torção finitamente gerado de rank n . N um submódulo de M de rank 1, e $E_1, \dots, E_l$ os fatores invariantes de N em M . Mostre que existe um ideal fracionário I e um isomorfismo

$$\theta : M \longrightarrow R \dot{+} \dots \dot{+} R \dot{+} I \quad (k \text{ somandos})$$

tal que

$$\theta(N) = \begin{cases} E_1 \dot{+} \dots \dot{+} E_{k-1} \dot{+} E_k I & , l = k \\ E_1 \dot{+} \dots \dot{+} E_l & , l < k \end{cases}.$$

Tal versão só é verdadeira quando $\text{rank } M = \text{rank } N$.

Tome por exemplo um domínio de Dedekind, D , e $I \subset D$ um ideal tal I^{s-1} não é principal. Tomando $M = I \dot{+} \dots \dot{+} I$ (s somandos)

e $N = I \dot{+} \dots \dot{+} I$ ($s-1$ somandos) temos pela versão dada no livro que $N \cong R^{s-1}$, mas já vimos por (2.15) que $N \cong R^{s-2} \oplus I^{s-1}$ e, por (2.11) teríamos então I^{s-1} principal, absurdo.

Aqui damos uma versão correta do exercício :

Teorema (3.2): Seja M um R -módulo livre de torção finitamente gerado cujo rank é k . Seja $N \subset M$ um R -submódulo com $\text{rank } N = 1$ e sejam $E_1, \dots, E_l$ os fatores invariantes de N em M . Então existe I um R -ideal fracionário e $\theta : M \longrightarrow R \dot{+} \dots \dot{+} R \dot{+} I$ (k somandos) R -isomorfismo tal que

$$\theta(N) = E_1 \dot{+} \dots \dot{+} E_{l-1} \dot{+} N' \quad , \quad E_1 \supset E_2 \supset \dots \supset E_{l-1}.$$

Além disso, se $k = 1$ então $N' = E_l I$.

Demonstração:

Pelo corolário (2.21) temos que

$$M \cong I_1 \dot{+} \dots \dot{+} I_k \quad e$$

$$N \cong E_1 I_1 \dot{+} \dots \dot{+} E_l I_l \quad , \quad E_l \supset E_{l+1} \quad , \quad E_l \text{ integral}$$

passo 1 :

Como já vimos, pelo lema (2.14), existe

$$\phi_1 : I_1 \dot{+} I_2 \longrightarrow R \dot{+} I_1 I_2$$

R - isomorfismo com $\phi_1 (E_1 I_1 + E_2 I_2) = E_1 + E_2 I_1 I_2$.

Seja $\theta_1 = (\phi_1, \text{id}|_{I_3 + \dots + I_k}) : I_1 + \dots + I_k \longrightarrow R + I_1 I_2 + I_3 + \dots + I_k$ onde $\theta_1 (E_1 I_1 + \dots + E_l I_l) = E_1 + E_2 I_1 I_2 + E_3 I_3 + \dots + E_l I_l$.

passo 2 :

Novamente utilizando (2.14) consideremos

Seja $\phi_2 : I_1 I_2 + I_3 \longrightarrow R + I_1 I_2 I_3$ tal que $\phi_2 (E_2 I_1 I_2 + E_3 I_3) = E_2 + E_3 I_1 I_2 I_3$.

Considere $\theta_2 = (\text{id}|_R, \phi_2, \text{id}|_{I_4 + \dots + I_k}) : R + I_1 I_2 + I_3 + \dots + I_k \longrightarrow R + R + I_1 I_2 I_3 + I_4 + \dots + I_k$ onde $\theta_2 (E_1 + E_2 I_1 I_2 + E_3 I_3 + \dots + E_l I_l) = E_1 + E_2 + E_3 I_1 I_2 I_3 + E_4 I_4 + \dots + E_l I_l$.

passo 1-1 :

Seja $\phi_{l-1} : I_1 I_2 \dots I_{l-1} + I_l \longrightarrow R + I_1 I_2 \dots I_{l-1} I_l$ onde

$\phi_{l-1} (E_{l-1} I_1 \dots I_{l-1} + E_l I_l) = E_{l-1} + E_l I_1 \dots I_l$.

Considere $\theta_{l-1} = (\text{id}|_{R + \dots + R}, \phi_{l-1}, \text{id}|_{I_{l+1} + \dots + I_k}) : R + \dots + R + I_1 \dots I_{l-1} + I_l + I_{l+1} + \dots + I_k \longrightarrow R + \dots + R + I_1 \dots I_l$

$$+ I_{l+1} + \dots + I_k \text{ onde } \theta_l \in (E_1 + \dots + E_{l-2} + E_{l-1}I_1 \dots I_{l-1} + E_l I_l) = \\ E_1 + \dots + E_{l-1} + E_l I_1 \dots I_l.$$

passo 1 :

$$\text{Seja } \phi : I_1 \dots I_l + I_{l+1} \longrightarrow R + I_1 \dots I_l \text{ onde}$$

$$\phi(E_l I_1 \dots I_l) = N_l.$$

$$\text{Considere } \theta_l = (\text{id}|_{R + \dots + R}, \phi_l \cdot \text{id}|_{I_{l+2} + \dots + I_k}) : R + \dots +$$

$$R + I_1 \dots I_l + I_{l+1} + \dots + I_k \longrightarrow R + \dots + R + I_1 \dots I_{l+1} + I_{l+2}$$

$$+ \dots + I_k \text{ onde } \theta_l \in (E_1 + \dots + E_{l-1} + E_l I_1 \dots I_l) = E_1 + \dots + E_{l-1} +$$

$$N_l.$$

passo k-1 :

$$\text{Seja } \phi_{k-1} : I_1 \dots I_{k-1} + I_k \longrightarrow R + I_1 \dots I_k. \text{ consideremos}$$

$$\theta_{k-1} = (\text{id}|_{R + \dots + R}, \phi_{k-1}) : R + \dots + R + I_1 \dots I_{k-1} + I_k \longrightarrow$$

$$+ R + \dots + R + I_1 \dots I_k \text{ e } \theta_{k-1} \in (E_1 + \dots + E_{l-1} + N_{k-2}) =$$

$$E_1 + \dots + E_{l-1} + N'.$$

$$\text{Então seja } I = I_1 \dots I_k \text{ e } \theta = \theta_{k-1} \circ \theta_{k-2} \circ \dots \circ \theta_2 \circ \theta_1 \text{ onde temos}$$

$$\theta \in (E_1 I_1 + \dots + E_l I_l) = E_1 + \dots + E_{l-1} + N', \text{ com } N' = E_l I \text{ se } l = k.$$

■

Definição (3.3): Sejam R anel comutativo, M um R -módulo e $N \subset M$ submódulo. Diremos que N é básico em M se qualquer que seja $P \in \text{Spec}(R)$, $N \not\subset PM$.

Definição (3.4): Dado R anel comutativo e

$$A = \left(a_{ij} \right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

matriz $m \times n$, com entradas em R , definiremos o conteúdo de A , e denotaremos por $c(A)$, como o ideal de R gerado pelos a_{ij} .

Algumas observações :

- 1) Suponhamos M um somando direto de L e $N \subset M$ um submódulo, então N é básico em M se e só se N é básico em L .
- 2) Seja R um domínio de Dedekind, M um R -módulo livre de torção finitamente gerado e $N \subset M$ submódulo com $\text{rank } M = n$ e $\text{rank } N = k$. Suponhamos ser N básico em M . Pelo teorema dos fatores invariantes temos que

$$M = I_1 m_1 \oplus \dots \oplus I_n m_n$$

$$N = E_1 I_1 m_1 \oplus \dots \oplus E_k I_k m_k$$

com I_i R -ideais fracionários, $E_i \supset E_{i+1}$ e E_i integrais.

Se $E_1 \subset R$, $E_1 \neq R$, existiria um $P \in \text{Spec}(R)$ tal que $E_1 \subset P$ donde $N \subset PM$ o que é absurdo. Logo temos $E_1 = R$ e

$$M = I_1 m_1 \oplus \dots \oplus I_n m_n$$

$$N = I_1 m_1 \oplus E_2 I_2 m_2 \oplus \dots \oplus E_k I_k m_k$$

Mais que isso, se $\text{rank } N = 1$ então $M = N \oplus N'$.

3) Sejam $M = R^n$ e $A = (a_{ij})$, matriz $n \times m$ com entradas em R .

Considere G o R -módulo gerado pelas colunas de A , então G básico em R^n se e só se $c(A) = R$.

Definição (3.5): Seja R um anel comutativo e $v = (v_1, \dots, v_n)$ em R^n , então diremos que v é unimodular se existirem $r_1, \dots, r_n$ em R tal que

$$\sum_{i=1}^n r_i v_i = 1.$$

Caracterizaremos agora os elementos unimodulares de R^n quando R é um domínio de Dedekind.

Proposição (3.6): Sejam R um domínio de Dedekind e $v = (v_1, \dots, v_n) \in R^n$. Então v é unimodular se e só se

$$R^n = Rv \oplus M$$

Demonstração:

Suponhamos v unimodular e consideremos $N = Rv$, então existem $I_1, \dots, I_n$ R -ideais fracionários, E ideal integral e $\langle m_1, \dots, m_n \rangle$

subconjunto de M tal que

$$R^n = I_{1,1} \oplus \dots \oplus I_{n,n}$$

$$Rv = N = EI_{1,1}$$

Se $E \subset R$, $E \neq R$ então existiria $P \in \text{Spec}(R)$ com $E \subset P$ e consequente-

mente $N \subset PM$. Então $v = \sum_{i=1}^k p_i m_i$, $p_i \in P$ e $m_i = (m_{i1}, \dots, m_{in}) \in M$.

Assim $v_j = \sum_{i=1}^k p_i m_{ij}$, $j = 1, \dots, n$. Agora, existem $r_1, \dots, r_n$ com

com $\sum_{j=1}^n r_j v_j = 1$ donde $1 = \sum_{j=1}^n \left(\sum_{i=1}^k r_j p_i m_{ij} \right)$, ou seja, $1 \in P$, absurdo.

Consequentemente $E = R$ e $R^n = Rv \oplus M$.

Suponhamos $R^n = Rv \oplus M$ e tomemos $\{e_i\}_{i=1}^n$ base canônica de R^n . te-

mos então $e_i = r_i v + m_i$ e $v = v_1 e_1 + \dots + v_n e_n$ donde

$$v = \left(v_1 r_1 + \dots + r_n v_n \right) v + \left(v_1 m_1 + \dots + v_n m_n \right)$$

assim, $v_1 r_1 + \dots + v_n r_n = 1$, ou seja, v unimodular.

■

Corolário (3.7): $v \in R^n$ unimodular $\Leftrightarrow v$ é coluna de uma matriz, $n \times n$, inversível.

Demonstração:

Suponhamos que v é coluna de uma matriz $A = \left(a_{ij} \right)$, $1 \leq i, j \leq n$.

inversível.

Então $AA^{-1} = \text{Id} \Rightarrow \det(A) \det(A^{-1}) = \det(\text{Id}) = 1$.

Desenvolvendo o determinante de A pela coluna que é v , temos que v é unimodular.

Reciprocamente, se $v \in R^n$ é unimodular então $R^n = Rv \oplus M$. Pelo teorema (2.11) temos $M \cong R^{n-1}$. Assim v faz parte de uma base de R e considerando a matriz mudança de base em relação a base canônica temos v coluna de uma matriz inversível.

■

O próximo resultado dará condições suficientes para que um submódulo M de R^n , onde R é Dedekind, contenha um elemento unimodular.

Proposição (3.8): Seja $M \subset R^n$ R -submódulo básico de R^n onde R é um domínio de Dedekind, então:

- i) se $\text{rank } M = 1$, M contém um elemento unimodular se e só se M é um R -módulo principal
- ii) se $\text{rank } M > 1$ então M contém um elemento unimodular.

Demonstração:

i) Se $\text{rank } M = 1$.

Suponhamos que exista $m \in M$ unimodular então $N = Rm$ é básico em M . de fato, se existisse $P \in \text{Spec}(R)$ tal que $Rm \subset PM$ então $1 \in P$ o que é absurdo.

Além disso, dado que $\text{rank } M = \text{rank } N = 1$, existem E um ideal integral I um R-ideal fracionário tais que $M = Im_1$ e $N = EIm_1$, para algum m_1 de M, e pela observação (2) temos $E = R$, donde $M = Rm_1$.

Suponhamos que M é principal, temos que $M = Rm$ para algum $m \in M$.

Além disso, existem $I_1, \dots, I_n$ R-ideais fracionários tal que

$$R^n = I_1 m_1 \oplus \dots \oplus I_n m_n$$

e

$$M = I_1 m_1$$

pois M básico em R^n , donde $R^n = M \oplus M'$, assim, por (3.6), m é unimodular.

ii) Se $\text{rank } M > 1$.

Sendo M básico em R^n temos

$$R^n = I_1 m_1 \oplus \dots \oplus I_n m_n \in M = I_1 m_1 \oplus E_2 I_2 m_2 \oplus \dots \oplus E_k I_k m_k$$

com $k > 1$.

Por (3.2) existe $\phi : R^n \longrightarrow R^n$ isomorfismo tal que $\phi(M) = R \oplus M''$.

Assim existe $v = (v_1, \dots, v_n)$ tal que $\phi(v) = (1, 0, \dots, 0)$.

Logo

$$(1, 0, \dots, 0) = \phi(v_1 e_1 + \dots + v_n e_n) = \sum_{i=1}^n v_i \phi(e_i)$$

onde $\{e_i\}_{i=1}^n$ base canônica de R^n , e sendo $\phi(e_i) = (f_{i1}, \dots, f_{in})$

temos $(1, \dots, 0) = \left(\sum_{j=1}^n v_j f_{j1}, \dots, \sum_{j=1}^n v_j f_{jn} \right)$ donde $1 = \sum_{j=1}^n v_j f_{j1}$, assim v unimodular.

■

Definição (3.9): Sejam R um anel comutativo e $A = (a_{ij})$,

$1 \leq i \leq m$, $1 \leq j \leq n$, matriz $m \times n$, com entradas em R . Diremos que A representa 1 se existem $u = (u_1, \dots, u_m) \in R^m$ e $v = (v_1, \dots, v_n) \in R^n$ tais que $uAv^t = 1$.

Mais algumas observações :

4) A representa 1 se e só se o submódulo de R^n (respectivamente R^m) gerado pelas linhas (respectivamente pelas colunas) possui um elemento unimodular .

5) A representa 1 se e só se através de operações elementares nas linhas e colunas de A obtemos uma nova matriz com uma das entradas igual a 1 .

O resultado a seguir oferece uma condição necessária e suficiente para que um anel de Dedekind seja principal.

Teorema (3.10): Seja R um domínio de Dedekind. R é principal se e só se para toda matriz A com $c(A) = R$ temos que A representa 1 .

Demonstração:

Provemos a necessidade . Seja A matriz $m \times n$ tal que $c(A) = R$. Então o R -módulo gerado pelas colunas de A , a saber G , é básico em R^n .

Se $\text{rank } G > 1$, pela proposição (3.8) (ii) temos que G possui elemento unimodular. Se $\text{rank } G = 1$, dado que R principal temos que $G = Ra$, $a \in R^m$, e pela proposição (3.8) (i) temos que G possui elemento unimodular .

Por outro lado, suponhamos que $c(A) = R$ implique que A representa 1. Seja $I \subset R$ ideal, então por (3.1) temos que $I = Ra + Rb$, $a, b \in I$. Além disso, por (2.13), existe $\xi \in K$ com $\xi I \subset R$ e $I + \xi I = R$. Consideremos a matriz

$$A = \begin{pmatrix} a & b \\ \xi a & \xi b \end{pmatrix}$$

Então $c(A) = R$ e daí o R -módulo gerado pelas colunas de A , a saber G , possui elemento unimodular. Pela observação (3) temos que tal módulo é básico em R^2 .

Como $\text{rank } G = 1$, segue da proposição (3.8) (i) que G é principal. Mas

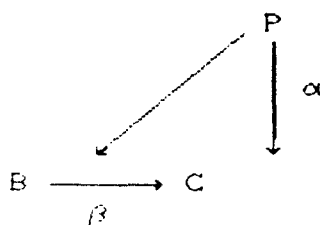
$$G = R(a, \xi a) + R(b, \xi b) = (Ra + Rb)(1, \xi) = I(1, \xi)$$

ou seja, $I \cong G$, portanto I principal.

■

Desenvolveremos agora de modo propriamente dito o resultado referente a BCS anéis. Antes disso porém daremos algumas definições.

Definição (3.11): Seja R um anel comutativo. Um R -módulo P é dito *projetivo* se dados C e B R -módulos, $\alpha : P \longrightarrow C$ um R -homomorfismo e $\beta : B \longrightarrow C$ R -homomorfismo sobrejetor, então existe um R -homomorfismo $\gamma : P \longrightarrow B$ tal que $\beta \circ \gamma = \alpha$ (o que é equivalente a dizer que o diagrama da página seguinte comuta) (vide [10]).

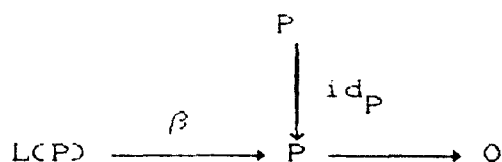


Daremos agora um teorema que caracteriza um módulo projetivo como um somando direto de um módulo livre .

Teorema (3.12): Um R -módulo P é projetivo se e só se é um somando direto de um módulo livre. Mais que isso, todo somando direto de um módulo projetivo é projetivo .

Demonstração:

Consideremos o R -módulo livre gerado por P , a saber $L(P)$. Temos então o seguinte diagrama



Sendo $L(P)$ um R -módulo livre, existe $\gamma : P \longrightarrow L(P)$ tal que $\gamma \circ \beta = \text{id}_P$ logo $L(P) = \ker \beta \oplus \gamma(P)$, onde $\gamma(P) \cong P$.

Reciprocamente, sendo F um R -módulo livre temos F projetivo . Suponhamos então P um somando direto de um módulo projetivo F , isto é , $F = P \oplus P'$.

Consideremos $i : P \longrightarrow F$ a inclusão e $p : F \longrightarrow P$ a projeção , donde $p \circ i = \text{id}_P$.

Temos então o seguinte diagrama

$$\begin{array}{ccccc} & & \rho & & \\ & & \longrightarrow & & \\ F & \xleftarrow{i} & P & & \\ & & \downarrow & & \\ B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

Logo, existe $\gamma : F \longrightarrow B$ tal que $\beta \cdot \gamma = \alpha \cdot \rho$. Seja $g = \gamma \cdot i$ então $\beta \cdot g = \beta \cdot \gamma \cdot i = \alpha \cdot \rho \cdot i = \alpha$. Donde P projetivo.

■

Corolário (3.13): A soma direta de módulos projetivos é um módulo projetivo.

O resultado a seguir será apenas enunciado e desde que sua demonstração foge ao nosso objetivo, aos interessados, remetemos a [9]. O que nos interessa realmente é uma consequência imediata que nos garante que todo módulo livre de torção finitamente gerado sobre um domínio de Dedekind é projetivo.

Proposição (3.14): Seja R domínio e $I \subset A$ ideal fracionário $I \neq (0)$. Então

$$I \text{ projetivo (como } R\text{-módulo)} \Leftrightarrow I \text{ inversível.}$$

Teorema (3.15): Seja R um domínio de Dedekind e M um R -módulo livre de torção finitamente gerado, então M é projetivo.

Demonstração:

Por (2.9) temos que $M \cong I_1 \oplus \dots \oplus I_n$, $n = \text{rank } M$, onde I_j são R -ideais fracionários. Sendo R Dedekind temos que cada I_j é inversível e por (3.14), projetivo. Por (3.13) segue o desejado.

■

Proposição (3.16): Seja R um anel comutativo. As seguintes asserções são equivalentes:

- i) todo submódulo básico finitamente gerado de um R -módulo projetivo P finitamente gerado contém um somando de rank 1 de P
- ii) para todo n , todo submódulo básico finitamente gerado de R^n contém um somando de rank 1 de R^n .

Demonstração:

Que (i) $\Rightarrow$ (ii) é imediato, basta tomar $P = R^n$.

Suponhamos que (ii) seja verdadeira. Por (3.12) temos que P é um somando direto de algum R^n e pela observação (1) segue que se um submódulo é básico em P também o é em R^n . Segue da hipótese que tal submódulo contém R e como por (3.12) podemos considerar

$$P = R \dot{+} \dots \dot{+} R \dot{+} I, \quad I \text{ } R\text{-ideal fracionário}$$

segue a conclusão desejada.

■

Definição (3.17): Um anel comutativo satisfazendo uma das asserções da proposição (3.16) é dito um *BCS anel*.

Teorema (3.18): Se R é um domínio de Dedekind então R é um *BCS anel*.

Demonstração:

Seja M um R -módulo projetivo finitamente gerado e G um seu submódulo básico. Sem perda de generalidade por (3.16) podemos assumir $M = R^n$, $n = \text{rank } M$. Suponhamos $\text{rank } G \geq 2$, por (3.2) e mais pela observação (2) temos

$$M = R \dot{+} \dots \dot{+} R$$

o

$$G = R \dot{+} E_2 \dot{+} \dots \dot{+} E_{k-1} \dot{+} N'$$

com $k = \text{rank } G$, donde segue o desejado.

Se $\text{rank } G = 1$, sendo ele básico em M temos pela observação (2) ser ele próprio um somando direto de M .

■

Referências Bibliográficas

- [1] - Atiyah, M. F., MacDonald, I. G., Introduction to Algebra Comutativa, Barcelona, Editorial Reverté S. A., 1980.
- [2] - Azevedo, A., Modulos sobre dominios principais, (VIII Colóquio Brasileiro de matemática), Rio de Janeiro, IMPA, 1971.
- [3] - Bass, H., Projective modules and simetric algebras, Rio de Janeiro, IMPA, 1980, (Monografias de Matemática 30).
- [4] - Cassels, J. W. S., Frölich, A., Algebraic Number Theory; Proceedings of an instructional conference organized by the London Mathematical Society (a NATO advanced study institute) with the support of the International Mathematical Union, London, Academic Press, 1967.
- [5] - Cohen, I. S., "Comutative rings with restricted minimum condition", Duke Math Journal, Vol. 7, pp. 27-42, 1960.
- [6] - Curtis, C. W., Reiner, I., Representation theory of finite groups and associative algebras, New York, John Wiley & Sons, 1962, (Pure and Applied Math., a series of texts and monographs XI).
- [7] - Hautus, M. L. J., Sontag, E. D., "New results on pole-shifting for parametrized families of systems", Journal of Pure and Applied Algebra, Vol. 40, No. 3, pp 229-244, 1986.
- [8] - Kunz, E., Introduction to comutative algebra and algebraic geometry, Boston, Birkhauser, 1985.
- [9] - Lafon, J. P., Les formalismes fondamentaux de l'algebre comutative, Paris, Hermann, 1974, (Collection enseignement des sciences 20).
- [10] - Rotman, J. J., An introduction to homological algebra, New York, Academic Press, 1979.
- [11] - Sontag, E. D., "Linear systems over comutative rings : a survey", Recherche de Automatic, Vol. 7, No. 1, pp 1-7, 1976.
- [12] - Vasconcelos, W. V., Weibel, C. A., BCS rings, New Brunswick, Rutgers University, 1988, (to appeal).

[13] - Zariski, O., Samuel, P., Comutative algebra (Vol.1), New York, Springer-Verlag, 1979, (Graduate Texts im Math. 28).