UNIVERSITÀ DEGLI STUDI DI FERRARA

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea Triennale in Matematica
Indirizzo Didattica della Matematica e Divulgazione Scientifica

MODULI PROIETTIVI E MODULI INIETTIVI SU ANELLI DI DEDEKIND

Relatore:
Chiar.mo Prof.
Josef Eschgfäller

Laureanda:
Giada Scarpone

Anno Accademico 2010-2011

Indice

Introduzione

In questa tesi sono trattati alcuni concetti base dell'algebra omologica (successioni esatte, moduli iniettivi, moduli proiettivi) con i quali vengono descritti e studiati enti più complessi come funtori, anelli noetheriani e anelli di Dedekind. Troviamo inoltre in questo lavoro nomi molto importanti per quanto riguarda l'algebra omologica, per esempio Eilenberg, Baer, Cartan, mostrando alcuni tra i loro principali risultati.

Sono presentate nel primo capitolo alcune nozioni dell'algebra (anelli integri, anelli con divisione, gruppi abeliani visti come $\mathbb{Z}$-moduli) utili per introdurre e comprendere i concetti sviluppati nei capitoli seguenti.

Nel secondo capitolo si illustrano alcuni concetti fondamentali per questa tesi. Si dimostra che, dato un anello R e definito il suo centro, l'insieme degli omomorfismi di R-moduli, $\mathrm{Hom}_R(M, N)$, è un $\mathrm{Centro}(R)$-modulo e quindi un R-modulo, qualora R sia commutativo; si introducono i funtori covarianti e controvarianti, si dimostrano alcune proprietà dei moduli come la legge modulare e si definiscono particolari moduli ad esempio i moduli fedeli. Definita inoltre la nozione di modulo semplice e anello semplice si deduce che ogni anello con divisione è anello semplice e che l'anello degli endomorfismi di un modulo semplice è un anello con divisione. Quest'ultimo risultato è noto come lemma di Schur. Ma anche altri risultati importanti sui moduli semplici sono dimostrati in questo capitolo; si verifica infatti che dato un anello R ogni R-modulo M è semplice se e solo se esiste un ideale massimale $\mathfrak{m}$ tale che M sia isomorfo ad $R/\mathfrak{m}$.

Il terzo capitolo tratta dei moduli liberi definiti come moduli dotati di una base. Si dimostra che i moduli su un anello con divisione sono liberi e ogni base di tali moduli è un sottoinsieme linearmente indipendente massimale. Si verifica inoltre che ogni base di un modulo libero è un sistema minimale di generatori; da ciò si ricava che se una base ha cardinalità infinita, qualsiasi altra base dello stesso modulo ha cardinalità infinita. Definendo modulo RDB (a rango ben definito) e anello ICB (invarianza di cardinalità delle basi), si dimostra che ogni anello con divisione è anello ICB. Da ciò si deduce che gli R-moduli R^n e R^m non sono isomorfi, per $n, m \in \mathbb{N}$ e n diverso di m, se R è un anello con divisione. Si deduce inoltre che anelli finiti e anelli commutativi sono anch'essi anelli ICB. Introducendo poi la traccia e la traccia senza torsione di un anello si dimostra che un anello dotato di traccia senza torsione è un anello ICB. Infine si verifica un risultato importante e spesso utilizzato nelle dimostrazioni dei capitoli seguenti, ovvero che ogni modulo è immagine omomorfa di un modulo libero.

Dopo aver definito anelli algebricamente finiti e stabilmente finiti, nel capitolo quarto si dimostra facilmente che ogni dominio è algebricamente finito e che se l'anello delle matrici $n \times n$ a coefficenti in R è algebricamente finito allora anche l'anello degli endomorfismi $\mathrm{End}_R R^n$ è algebricamente finito e ogni endomorfismo suriettivo di R-moduli da

R^n in R^n è un isomorfismo. Si dimostra inoltre che ogni anello stabilmente finito è anello ICB e ogni anello commutativo è stabilmente finito. Successivamente attraverso la definizione di modulo di Hopf, si deduce che ogni modulo noetheriano è di Hopf e quindi ogni anello noetheriano è stabilmente finito. Infine si verifica che un anello non algebricamente finito contiene un insieme infinito di idempotenti a due a due ortogonali.

Il capitolo quinto tratta le successioni esatte e le loro proprietà . Attraverso una serie di lemmi che studiano particolari diagrammi commutativi si arriva a dimostrare il primo, il secondo lemma dei Quattro e il lemma dei Cinque. Vediamo che $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, G) \cong G$ quando G è un gruppo abeliano e che $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, G) \cong G[m]$ dove $G[m] := \{g \in G \mid mg = 0\}$ e $m \in \mathbb{N}$; da ciò derivano risultati come $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}) = 0$ e $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/m) = \mathbb{Z}/m$. Si definisce quando una successione esatta si spezza, dimostrando alcuni risultati su tale proprietà legandola alla definizione di sommando diretto. In questo capitolo si studiano anche particolari successioni esatte tra le quali $0 \longrightarrow \mathbb{Z} \overset{\bigcirc\, mx}{\overset{x}{\longrightarrow}} \mathbb{Z} \overset{\pi}{\longrightarrow} \mathbb{Z}/m \longrightarrow 0$ che si dimostra essere non spezzabile.

Nel sesto capitolo vengono definiti i moduli proiettivi. Si dimostra che ogni modulo libero è proiettivo e che ogni modulo proiettivo è sommando diretto di un modulo libero. Si verifica che la somma diretta di moduli proiettivi è proiettiva e che se P è un modulo proiettivo, il funtore covariante $\mathrm{Hom}_R(P, -)$ è esatto. Infine teoremi noti sono contenuti in questo capitolo: il trucco di Eilenberg e il lemma di Schanuel.

In maniera analoga ai moduli proiettivi, nel settimo capitolo vengono affrontati i moduli iniettivi e le loro proprietà : un modulo iniettivo è sommando diretto di ogni modulo di cui è sottomodulo, il prodotto diretto di moduli iniettivi è iniettivo e la somma diretta di un numero finito di moduli iniettivi è iniettiva. Quest'ultimo risultato vale per un numero infinito di moduli iniettivi se questi sono definiti su un anello noetheriano. Anche qui vediamo che se Q è un modulo iniettivo il funtore controvariante $\mathrm{Hom}_R(-, Q)$ è esatto. Attraverso la definizione di estensione parziale di un omomorfismo si dimostra il noto criterio di Baer da cui si ricava che il campo dei quozienti di un anello integro e ogni spazio vettoriale su tale campo sono moduli iniettivi sull'anello integro. Si introducono i moduli divisibili dimostrando che ogni modulo iniettivo è divisibile e altri risultati che legano i due tipi di moduli. In questo capitolo sono contenuti anche risultati sui gruppi abeliani: un gruppo abeliano è iniettivo se e solo se è divisibile ed è sempre sottogruppo di un gruppo abeliano iniettivo. Si verifica inoltre la proposizione di Bass/Papp attraverso la dimostrazione che ogni modulo è sottomodulo di modulo iniettivo. Infine si definisce il concetto di estensione essenziale dimostrando poi che ogni modulo è iniettivo se e solo se non possiede un estensione essenziale propria.

Prendendo in considerazione solo anelli commutativi, nell'ottavo capitolo si definiscono moduli e anelli semisemplici. Si dimostra che un modulo è semisemplice se e solo se ogni suo sottomodulo è un sommando diretto, e che ogni sottomodulo e ogni immagine omomorfa di un modulo semisemplice è semisemplice. Si osserva che i sottomoduli semplici di un anello commutativo sono esattamente i suoi ideali generalizzati minimali, da cui deriva che ogni anello commutativo semisemplice è somma diretta di un numero finito di ideali generalizzati minimali. Infine si mostra che un anello commutativo è semisemplice se e solo se ogni modulo su tale anello è o iniettivo o proiettivo o semisemplice, e se e solo se ogni suo ideale è un modulo iniettivo.

Anche nel nono e ultimo capitolo si considerano solo anelli commutativi. Centro di questo capitolo sono gli anelli ereditari e quelli di Dedekind; si mostra subito facilmente che ogni anello ad ideali principali è di Dedekind. Illustrando i legami tra questi particolari anelli e i moduli descritti nei capitoli precedenti si dimostra che ogni sottomodulo di un modulo proiettivo su un anello ereditatio è proiettivo, che ogni sottomodulo di un modulo libero su un anello ad ideali principali è libero e che ogni modulo proiettivo su un anello ad ideali principali è libero. Vengono inoltre verificati alcuni risultati noti come il teorema di Kaplansky e il teorema di Cartan-Eilenberg. Infine la tesi si conclude mostrando che un anello integro è di Dedekind se e solo se ogni modulo divisibile su tale anello è iniettivo.

1. Notazioni

Osservazione 1.1. Usiamo il termine *anello* per denotare un anello (associativo) $\neq 0$, dotato di un elemento neutro della moltiplicazione. Quest'ultimo viene denotato con 1, oppure, quando bisogna indicare l'anello R stesso, con 1_R.

Similmente un omomorfismo di anelli $\varphi : R \to S$ deve soddisfare la condizione $\varphi(1_R) = 1_S$.

Se R è un anello, un R-*modulo* è un R-modulo sinistro M unitale, cioè tale che $1_R \cdot v = v$ per ogni $v \in M$.

Talvolta considereremo anche R-moduli destri, anch'essi unitali.

Definizione 1.2. Un *ideale* bilaterale, sinistro o destro di un anello R è per definizione $\neq R$. Se vogliamo includere anche R stesso, parliamo di *ideale* (bilaterale, sinistro o destro) *generalizzato*.

Il termine ideale senza specificazione della lateralità indica un ideale bilaterale.

Si noti che 0 è sempre un ideale perchè $R \neq 0$.

Osservazione 1.3. Siano R un anello e M un R-modulo. Allora R e M sono anche gruppi abeliani, quindi $\mathbb{Z}$-moduli, perciò per ogni $n \in N$ e per ogni $v \in M$ sono definiti gli elementi $n1_R \in R$ e $nv \in M$ e si ha

$$nv = \underbrace{v + v + \ldots + v}_{n} = \underbrace{(1_R + 1_R + \ldots + 1_R)}_{n} = (n1_R)v$$

Definizione 1.4. Per un insieme X ed $n, m \in \mathbb{N} + 1$ usiamo le seguenti notazioni:

X^n := insieme dei vettori colonna di lunghezza n formati da elementi di X;

X_m := insieme dei vettori riga di lunghezza m formati da elementi di X;

X_m^n := insieme delle matrici di m righe e n colonne formate da elementi di X.

Definizione 1.5. Sia R un gruppo abeliano (ad esempio un anello o un modulo su un anello) ed X un insieme. Allora denotiamo con $R^{\underline{X}}$ l'insieme delle applicazioni $u : X \longrightarrow R$ tale che sia finito l'insieme $\{x \in X \mid u(x) \neq 0\}$.

Definizione 1.6. Per un omomorfismo φ di gruppi (e quindi anche di anelli o moduli) denotiamo con $\operatorname{Ker} \varphi$ il nucleo, con $\operatorname{Im} \varphi$ l'immagine di φ.

Definizione 1.7. Sia R un anello.

(1) R si chiama un *dominio*, se per $a, b \in R \setminus 0$ si ha sempre $ab \neq 0$.

Un dominio commutativo è detto anche *dominio (o anello) integro*.

(2) Un elemento a di R si dice *invertibile*, se esiste un elemento $a^{-1} \in R$ tale che $a \cdot a^{-1} = a^{-1} \cdot a = 1_R$. Si vede facilmente che a^{-1}, quando esiste, è univocamente determinato.

Denotiamo con R^* l'insieme degli elementi invertibili di R.
Si dimostra facilmente che $(R^*, \cdot)$ è un gruppo.

(3) R si chiama un *anello con divisione* (in inglese *division ring* oppure *skew field*, in italiano talvolta anche *corpo*), se ogni elemento $\neq 0$ di R è invertibile, se cioè $R^* = R \setminus 0$.

È chiaro che ogni sottoanello di un anello con divisione è un dominio.

Definizione 1.8. Per un anello integro denotiamo con $\mathcal{K}(A)$ il suo campo dei quozienti.

2. Concetti fondamentali

Situazione 2.1. Sia R un anello.

Osservazione 2.2. Se negli assiomi per un R-modulo M rinunciamo alla condizione che il gruppo $(M,+)$ sia abeliano, ciò segue comunque automaticamente dagli altri assiomi.

<u>Dimostrazione.</u> Siano $x, y \in M$. Allora

$$x+y+x+y = 2(x+y) = 2x+2y = x+x+y+y$$

e dalla legge di cancellazione segue $y+x = x+y$.

Si noti che la dimostrazione funziona anche quando $2z = 0$ per ogni $z \in M$. Infatti in tal caso si ha ancora più facilmente

$$x+y+x+y = 0$$

e quindi $y+x = x+\underbrace{x+y+x+y}_{0}+y = x+y$

Definizione 2.3. Denotiamo con $\mathfrak{Mod}(R)$ la categoria degli R-moduli. Per $M, N \in \mathfrak{Mod}(R)$ sia $\mathrm{Hom}_R(M,N)$ l'insieme degli omomorfismi $\varphi : M \longrightarrow N$ in $\mathfrak{Mod}(R)$.

Poniamo $\mathrm{End}_R(M) := \mathrm{Hom}_R(M,M)$.

Similmente denotiamo con $\mathfrak{Mod}(R,\mathrm{destra})$ la categoria degli R-moduli destri e con $\mathrm{Hom}_R(M,N,\mathrm{destra})$ e $\mathrm{End}_R(M,\mathrm{destra})$ i corrispondenti insiemi di omomorfismi.

Definizione 2.4. Definiamo il *centro* di R ponendo

$$\mathrm{Centro}(R) := \{\ \lambda \in R \mid \lambda a = a\lambda \text{ per ogni } a \in R\ \}$$

E' chiaro che $\mathrm{Centro}(R)$ è un sottoanello commutativo di R.

Osservazione 2.5. Siano $M, N \in \mathfrak{Mod}(R)$. Allora:

(1) $\mathrm{Hom}_R(M,N)$ diventa un gruppo abeliano ponendo

$$\varphi + \psi := \bigcirc_v \varphi v + \psi v$$

(2) Per $\varphi \in \mathrm{Hom}_R(M,N)$ e $\lambda \in \mathrm{Centro}(R)$ anche $\lambda\varphi := \bigcirc_x \lambda\varphi x$ appartiene a $\mathrm{Hom}_R(M,N)$.

<u>Dimostrazione.</u> (1) Immediato.

(2) Siano $\varphi \in \mathrm{Hom}_R(M,N)$ e $\lambda \in \mathrm{Centro}(R)$. È chiaro che $\lambda\varphi \in \mathrm{Hom}_{\mathbb{Z}}(M,N)$. Bisogna ancora dimostrare che per $a \in R$ e $x \in M$ si ha
$(\lambda\varphi)(ax) = a\lambda\varphi x$. Sfruttando l'ipotesi che $\lambda \in \mathrm{Centro}(R)$ abbiamo però
$(\lambda\varphi)(ax) = \lambda(\varphi(ax)) = \lambda(a\varphi x) = (\lambda a)(\varphi x) = (a\lambda)\varphi x = a\lambda\varphi x$.

Corollario 2.6. *Siano* $M, N \in \mathfrak{Mod}(R)$. *Allora* $\mathrm{Hom}_R(M,N)$ *è in modo naturale un* $\mathrm{Centro}(R)$*-modulo.*

Se R è commutativo, $\mathrm{Hom}_R(M,N)$ *è quindi un R-modulo.*

Osservazione 2.7. Sia $M \in \mathfrak{Mod}(R)$. Allora $\mathrm{End}_R(M)$ è un anello con le operazioni naturali definite da

$$\varphi + \psi := \bigcirc_x \varphi x + \psi x$$
$$\varphi\psi := \bigcirc_x \varphi(\psi x)$$

Nota 2.8. (1) Sia $M \in \mathfrak{Mod}(R)$. Allora otteniamo un funtore covariante e additivo:

$$\mathrm{Hom}_R(M,-) : \mathfrak{Mod}(\mathrm{R}) \longrightarrow \mathfrak{Mod}(\mathrm{Centro}(R))$$

e quindi anche $\mathfrak{Mod}(R) \longrightarrow \mathfrak{Mod}(\mathbb{Z})$, se per $X, Y \in \mathfrak{Mod}(R)$ e $\varphi \in \mathrm{Hom}_R(X,Y)$ poniamo

$$\mathrm{Hom}_R(M,-)(X) := \mathrm{Hom}_R(M,X)$$
$$\mathrm{Hom}_R(M,-)(\varphi) := \bigcirc_\psi \varphi\psi \in \mathrm{Hom}_{Centro(R)}(\mathrm{Hom}_R(M,X), \mathrm{Hom}_R(M,Y))$$

Se R è commutativo otteniamo quindi un funtore covariante e additivo $\mathfrak{Mod}(R) \longrightarrow \mathfrak{Mod}(R)$.

(2) Sia $N \in \mathfrak{Mod}(R)$. Allora otteniamo un funtore controvariante e additivo:

$$\mathrm{Hom}_R(-,N) : \mathfrak{Mod}(R) \longrightarrow \mathfrak{Mod}(\mathrm{Centro}(R))$$

e quindi anche $\mathfrak{Mod}(R) \longrightarrow \mathfrak{Mod}(\mathbb{Z})$, se per $X, Y \in \mathfrak{Mod}(R)$ e $\varphi \in \mathrm{Hom}_R(X,Y)$ poniamo

$$\mathrm{Hom}_R(-,N)(X) := \mathrm{Hom}_R(X,N)$$
$$\mathrm{Hom}_R(-,N)(\varphi) := \bigcirc_\psi \psi\varphi \in \mathrm{Hom}_{Centro(R)}(\mathrm{Hom}_R(Y,N), \mathrm{Hom}_R(X,N))$$

<u>Dimostrazione.</u> Ciò segue facilmente dalle considerazioni precedenti; cfr. ad es. Rotman, pagg. 39-40.

Lemma 2.9. *M sia un R-modulo ed A, B, C sottomoduli di M. Allora* $(A+B) \cap (A+C) = A + ((A+B) \cap C)$

<u>Dimostrazione.</u> (1) Sia $x = a + b = a' + c$ con $a, a' \in A$, $b \in B$, $c \in C$. Allora $c = a - a' + b \in (A+B) \cap C$, per cui $x = a' + c \in A + ((A+B) \cap C)$.

(2) Sia $x = a + \tilde{a} + b$ con $a, \tilde{a} \in A$, $b \in B$ ed $\tilde{a} + b \in C$. Raccogliendo $x = a + (\tilde{a} + b)$ vediamo che $x \in A + C$, raccogliendo $x = (a + \tilde{a}) + b$ vediamo che $x \in A + B$.

Corollario 2.10 (legge modulare). *M sia un R-modulo ed A, B, C sottomoduli di M tali che $A \subset B$. Allora*

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

Definizione 2.11. (1) Sia M un R-modulo. Per un sottoinsieme $X \subset M$ poniamo

$X^\perp := \{a \in R \mid aX = 0\}$

(2) Sia N un R-modulo destro. Per un sottinsieme $Y \subset N$ poniamo

$Y_\perp := \{a \in R \mid Ya = 0\}$

Osservazione 2.12. (1) Siano M un R-modulo ed $X \subset M$. Allora $X^\perp$ è un ideale sinistro generalizzato di R. Se $X \neq 0$, allora $X^\perp \neq R$.
Se $M \neq 0$, allora $M^\perp$ è un ideale di R.

(2) Siano N un R-modulo ed $Y \subset N$. Allora $Y^\perp$ è un ideale destro generalizzato di R. Se $Y \neq 0$, allora $Y^\perp \neq R$.
Se $N \neq 0$, allora $N_\perp$ è un ideale di R.

Dimostrazione. (1) Siano $a, b \in X^\perp, c \in R$ ed $x \in X$. Allora
$(a+b)x = ax + bx = 0 + 0 = 0$ e $(ca)x = c(ax) = c0 = 0$.
Se $x \neq 0$, $1x = x \neq 0$, per cui $1 \notin X^\perp$.
Nel caso $X = M$ abbiamo inoltre anche $acx = 0$.

(2) Nello stesso modo.

Definizione 2.13. Un R-modulo M si dice *fedele*, se $M^\perp = 0$.

Osservazione 2.14. M sia un R-modulo ed I un ideale di R con $I \subset M^\perp$. Allora M è in modo naturale un R/I-modulo, se per $v \in M$ ed $a \in R$ poniamo

$(a + I)v := av$

Dimostrazione. Bisogna solo dimostrare che questa operazione è ben definita. Siano $a, b \in R$ con $b - a \in I$. Allora

$bv = (a + (b - a))v = av + (b - a)v = av$

perché per ipotesi $b - a \in M^\perp$.

Definizione 2.15. Un R-modulo M si chiama *semplice*, se sono soddisfatte le seguenti condizioni:
(1) $M \neq 0$.
(2) Se N è un sottomodulo di M, allora $N = 0$ oppure $N = M$.

Osservazione 2.16. Siano M un R-modulo e $v \in M \setminus 0$. Allora Rv è un sottomodulo $\neq 0$ di M.

Dimostrazione. È chiaro che Rv è un sottomodulo di M.

Inoltre $v = 1v \in Rv$ e per ipotesi $v \neq 0$.

Lemma 2.17. *Per un R-modulo $M \neq 0$ sono equivalenti:*

(1) M è semplice.

(2) $Rv = M$ per ogni $v \in M \setminus 0$.

Dimostrazione. (1) $\Longrightarrow$ (2) : Chiaro, tenendo conto dell'oss. 2.16.

(2) $\Longrightarrow$ (1): Sia N un sottomodulo $\neq 0$ di M. Allora esiste $v \in N \setminus 0$ e per ipotesi $Rv = M$. Ma $Rv \subset N$, per cui $N = M$.

Definizione 2.18. L'anello R si chiama *semplice*, se R non possiede ideali $\neq 0$.

Un anello semplice può comunque contenere ideali sinistri o destri non banali.

Osservazione 2.19. R è in modo naturale un R-modulo (e anche un R-modulo destro). Gli ideali sinistri generalizzati di R sono esattamente i sottomoduli di R.

Proposizione 2.20. *Sono equivalenti:*

(1) R è un anello con divisione.

(2) R è un R-modulo semplice.

(3) R è un R-modulo destro semplice.

Dimostrazione. (1) $\Longrightarrow$ (2): Sia $a \in R \setminus 0$. Per il lemma 2.17 è sufficente dimostrare che $Ra = R$.

Per ipotesi però esiste $b \in R$ con $ba = 1$. Sia $c \in R$. Allora $c = c1 = cba \in Ra$.

(2) $\Longrightarrow$ (1): Sia ancora $a \in R \setminus 0$. Per ipotesi $Ra = R$. Perciò esiste un elemento $b \in R$ tale che $ba = 1$. Ogni elemento di $R \setminus 0$ possiede quindi un inverso a sinistra. Per poter affermare che $(R \setminus 0, \cdot)$ è un gruppo, è quindi sufficente dimostrare che $(R \setminus 0, \cdot)$ è un semigruppo.

Siano $u, v \in R \setminus 0$. Per quanto abbiamo appena dimostrato, esistono $x, y \in R$ tali che $xu = yv = 1$. Sia adesso $uv = 0$. Allora $v = xuv = 0$, in contrasto all'ipotesi $v \neq 0$.

Corollario 2.21. *Ogni anello con divisione è un anello semplice.*

Definizione 2.22. M sia un R-modulo. Allora:
(1)
$$\begin{aligned}\text{Sottomoduli}(M) &:= \text{Sottomoduli}_R(M)\\ &:= \textit{insieme dei sottomoduli di } M.\end{aligned}$$

(2) Per un sottoinsieme $X \subset M$ sia

$$\begin{aligned}\text{Sottomoduli}(M:X) &:= \text{Sottomoduli}_R(M:X)\\ &:= \{N \in \text{sottomoduli}(M) \mid X \subset N\}.\end{aligned}$$

Lemma 2.23. *Siano M,N R-moduli e $\varphi : M \longrightarrow N$ un omomorfismo. Allora esiste una biezione naturale*

$$\begin{aligned}\text{Sottomoduli}(M : Ker\varphi) &\longleftrightarrow \text{Sottomoduli}(\operatorname{Im}\varphi)\\ P &\longmapsto \varphi(P)\\ \varphi^{-1}(Q) &\longleftarrow\!\shortmid\, Q\end{aligned}$$

Dimostrazione. Corsi di algebra oppure Dolcini, pagg. 45-46.

Lemma 2.24. *M sia un R-modulo semplice e $v \in M \setminus 0$. Sia $\varphi := \underset{a}{\bigcirc} av : R \longrightarrow M$. Allora:*

(1) φ è un omomorfismo di R-moduli.

(2) $\mathfrak{m} := \operatorname{Ker} \varphi$ è un ideale massimale di R.

(3) $M \cong R/\mathfrak{m}$ (come R-modulo).

Dimostrazione. (1) Siano $a, b, c \in R$. Allora

$$\varphi(ab + c) = (ab + c)v = abv + cv = a\varphi(b) + \varphi(c)$$

quindi φ è un omomorfismo di R-moduli.

(2) Per il lemma 2.23 gli ideali generalizzati di R che contengono $\mathfrak{m}$ sono esattamente le controimmagini $\varphi^{-1}(N)$, dove N è un sottomodulo di M. Per ipotesi M è semplice, perciò le uniche possibilità sono $\varphi^{-1}(0) = \mathfrak{m}$ e $\varphi^{-1}(M) = R$. Ciò mostra che $\mathfrak{m}$ è un ideale massimale.

(3) Siccome M è semplice e $v \neq 0$, del lemma 2.17 abbiamo $\operatorname{Im} \varphi = Rv = M$. Quindi φ è suriettiva, per cui $M \cong R/\mathfrak{m}$.

Proposizione 2.25. *Un R-modulo M è semplice se e solo se esiste un ideale massimale $\mathfrak{m}$ di R tale che $M \cong R/\mathfrak{m}$.*

Dimostrazione. (1) La condizione è necessaria per il lemma 2.24.

(2) $\mathfrak{m}$ sia un ideale massimale di R tale che $M \cong R/\mathfrak{m}$. È sufficiente dimostrare che $R/\mathfrak{m}$ è un R-modulo semplice. Ma ciò è chiaro per la biezione naturale $\operatorname{Sottomoduli}_{R/\mathfrak{m}} R/\mathfrak{m} \longleftrightarrow \operatorname{Sottomoduli}_R(R : \mathfrak{m})$.

Teorema 2.26 (lemma di Schur). *M sia un R-modulo semplice.*

Allora $\operatorname{End}_R(M)$ è un anello con divisione.

Dimostrazione. Sia $\varphi \in \operatorname{End}_R(M)$ e $\varphi \neq 0$. Allora $\operatorname{Ker} \varphi \neq M$ e $\operatorname{Im} \varphi \neq 0$. Siccome M è semplice, ciò implica $\operatorname{Ker} \varphi = 0$ e $\operatorname{Im} \varphi = M$. Dunque φ è biettiva e quindi un isomorfismo.

Osservazione 2.27. Per un R-modulo M l'applicazione

$$\theta_M := \underset{a}{\bigcirc} \underset{x}{\bigcirc} ax : R \longrightarrow \operatorname{End}_{\mathbb{Z}}(M)$$

è un omomorfismo di anelli.

Dimostrazione. È chiaro che θ_M è un omomorfismo di gruppi e che $\theta_M(1_R) = \operatorname{id}_M$. Ora siano $a, b \in R$. Allora per $x \in M$ abbiamo

$$\theta_M(ab)x = abx = (\theta_M a)(\theta_M b)x$$

Osservazione 2.28. Sia M un R-modulo. Allora $\operatorname{Ker} \theta_M = M^{\perp}$.

Perciò M è fedele se e solo se l'omormorfismo $\theta_M : R \longrightarrow \operatorname{End}_{\mathbb{Z}}$ è iniettivo.

Dimostrazione. Infatti

$$\begin{aligned}\operatorname{Ker}\theta_M &= \{a \in R \mid \bigcirc_x ax = 0\} \\ &= \{a \in R \mid ax = 0 \textit{ per ogni } x \in M\} = M^{\perp}\end{aligned}$$

3. Moduli liberi

Situazione 3.1. R sia un anello.

Definizione 3.2. Siano M un R-modulo ed $E \subset M$. Denotiamo con

$$RE := \{a_1e_1 + \ldots + a_me_m \mid m \in \mathbb{N}+1, e_1, \ldots, e_m \in E, a_1, \ldots, a_m \in R\}$$

il sottomodulo generato da E. Per definizione $R\emptyset = 0$.

(1) E si dice *sistema di generatori* di M, se $RE = M$.

(2) E si dice *linearmente indipendente*, se, dati elementi *distinti* $e_1, \ldots, e_m \in E$, una relazione $a_1e_1 + \ldots + a_me_m = 0$ con $a_1, \ldots, a_m \in R$ implica $a_1 = \ldots = a_m = 0$.

(3) E si chiama una *base* di M, se E è un sistema linearmente indipendente di generatori di M.

Definizione 3.3. Un R-modulo si dice *libero* se possiede una base.

Osservazione 3.4. Sia M un R-modulo. Allora ogni sottoinsieme linearmente indipendente di M è contenuto in un insieme linearmente indipendente massimale.

Dimostrazione. Sia $\mathcal{C}$ una catena non vuota di insiemi linearmente indipendenti in M e sia $E = \bigcup\limits_{F \in \mathcal{C}} F$. È chiaro che $F \subset E$ per ogni $F \in \mathcal{C}$. Verifichiamo che E è linearmente indipendente. Siano $e_1, \ldots, e_m \in E$ elementi distinti tali che $a_1e_1 + \ldots + a_me_m = 0$ con $a_1, \ldots, a_m \in R$. Per definizione di E esistono allora $F_1, \ldots, F_m \in \mathcal{C}$ con $e_1 \in F_1, \ldots, e_m \in F_m$. Siccome $\mathcal{C}$ è una catena, si ha ad esempio $F_k \subset F_m$ per ogni k, cosicché $e_1, \ldots, e_m$ appartengono tutti a F_m. Ma F_m è linearmente indipendente, perciò necessariamente $a_1 = \ldots = a_m = 0$.

L'enunciato segue dal lemma di Zorn.

Lemma 3.5. *Siano R un anello con divisione, M un R-modulo ed E un sottoinsieme linearmente indipendente di M. Sia $v \in M \setminus RE$.*

Allora $E \cup \{v\}$ è ancora linearmente indipendente.

Dimostrazione. Siano $f_1, \ldots, f_m \in E \cup \{v\}$ tutti distinti e $a_1, \ldots, a_m \in R$ tali che $a_1f_1 + \ldots + a_mf_m = 0$.

(1) Se tutti gli f_j appartengono ad E, necessariamente $a_1 = \ldots = a_m = 0$, perché E è un insieme linearmente indipendente.

(2) Altrimenti, siccome gli f_j sono tutti distinti ed elementi di $E \cup v$, si ha ad esempio $f_1 = v$ ed $f_2, \ldots, f_m \in E$. Abbiamo quindi $a_1v = -a_2f_2 \ldots - a_mf_m$ nel caso $m \geq 2$ e invece $a_1v = 0$ nel caso $m = 1$. Per la lineare indipendenza di E è chiaro che è sufficiente dimostrare che $a_1 = 0$. Assumiamo, per assurdo, che $a_1 \neq 0$. Utilizzando l'ipotesi che R sia un anello con divisione, nel caso $m = 1$ avremo $v = a_1^{-1}a_1v = 0 \in RE$, una contraddizione.

Se invece $m \geq 2$, allora $v = -a_1^{-1}a_2 - \ldots - a_1^{-1}a_mf_m \in RE$, ancora una contraddizione.

Osservazione 3.6. Siano M un R-modulo, E un sistema di generatori di M ed F un sottoinsieme linearmente indipendente di M con $E \subset F$. Allora $E = F$.

Dimostrazione. Assumiamo, per assurdo, che $E \neq F$. Allora esiste $f \in F \setminus E$. Siccome E è un sistema di generatori, esistono però (tranne nel caso non banale $E = \emptyset$ in cui $M = 0$) $e_1, \ldots, e_m \in E$ tutti distinti ed $a_1, \ldots, a_m \in R$ tali che $a_1e_1 + \ldots + a_me_m = f$, ovvero
$a_1e_1 + \ldots + a_me_m - f = 0$.

Siccome $f \notin E$, anche gli elementi $f, e_1, \ldots, e_m$ sono tutti distinti. Ciò non è possibile, perché F è linearmente indipendente e il coefficente di f è $1 \neq 0$.

Corollario 3.7. *Siano M un R-modulo ed E una base di M. Allora E è un sottoinsieme linearmente indipendente massimale di M.*

Proposizione 3.8. *Siano R un anello con divisione, M un R-modulo ed E un sottoinsieme di M. Allora sono equivalenti:*

(1) E è una base di M.

(2) E è un sottoinsieme linearmente indipendente massimale di M.

Dimostrazione. (1) $\Longrightarrow$ (2): Cor. 3.7.

(2) $\Longrightarrow$ (1): E sia un sottoinsieme linearmente indipendente massimale di M. Dobbiamo dimostrare che $RE = M$. Per assurdo assumiamo che esista $v \in M \setminus RE$. Per il lemma 3.5 $F = E \cup v$ è ancora linearmente indipendente. Ma $E \subsetneqq F$ perché sicuramente $v \notin E$, essendo $v \notin RE$. Ciò è una contraddizione alla massimalità di E.

Teorema 3.9. *R sia un anello con divisione. Allora ogni R-modulo possiede una base ed è quindi libero.*

Dimostrazione. Sia M un R-modulo. L'insieme $\emptyset$ è linearmente indipendente, perciò dall'oss 3.4 segue che M contiene un sottoinsieme linearmente indipendente massimale E. Per la prop. 3.8 E è una base di M.

Osservazione 3.10. G sia un gruppo abeliano finito. Allora $\emptyset$ è l'unico sottoinsieme linearmente indipendente di G.

Dimostrazione. Sia $n := |G|$. Allora $ng = 0$ per ogni $g \in G$ e ciò implica che un sottoinsieme non vuoto di G non può essere linearmente indipendente.

Definizione 3.11. Sia X un insieme. Per ogni $x \in X$ definiamo la funzione caratteristica $\delta_x : X \longrightarrow R$ ponendo

$$\delta_x(y) := \delta_x^y := \begin{cases} 1 & \text{se } y = x \\ 0 & \text{se } y \neq x \end{cases}$$

È chiaro che $\delta_x \in R^{\underline{X}}$. Si osservi che δ_x non dipende solo da x, ma anche da X ed R. Poniamo inoltre $\delta_X := \{\delta_x \mid x \in X\}$.

Proposizione 3.12. *Sia X un insieme. Allora $R^{\underline{X}}$ è un modulo libero con base δ_X.*

Dimostrazione. (1) Dimostriamo che δ_X è un sistema di generatori. Sia $f : X \longrightarrow R$ tale che l'insieme $\{x \in X \mid f(x) \neq 0\}$ sia finito, ad esempio uguale a $\{x_1, \ldots, x_m\}$ con gli x_j tutti distinti. Allora $f = f(x_1)\delta_{x_1} + \ldots + f(x_m)\delta_{x_m}$.

(2) Dimostriamo che δ_X è linearmente indipendente. Siano $\delta_{x_1}, \ldots, \delta_{x_m}$ elementi distinti di δ_X (ciò accade se e solo se i punti $x_1, \ldots, x_m$ sono distinti) e siano $a_1, \ldots a_m \in R$ e tali che $f := a_1\delta_{x_1} + \ldots + a_m\delta_{x_m} = 0$. Allora per ogni k si ha $a_k = f(x_k) = 0$.

Proposizione 3.13. *Siano M un R-modulo libero ed E una base di M. Allora l'applicazione $\psi : M \longrightarrow R^{\underline{E}}$ definita da*

$$\psi(a_1e_1 + \ldots + a_me_m) := a_1\delta_{e_1} + \ldots + a_m\delta_{e_m}$$

per elementi distinti $e_1, \ldots, e_m \in E$ ed $a_1, \ldots, a_m \in R$ è ben definita e un isomorfismo di R-moduli.

Dimostrazione. Verifica immediata. Il caso $M = 0$ è banale.

Lemma 3.14. *Siano M un R-modulo ed E un sistema di generatori minimale di M con $|E| = \infty$.*

Allora per ogni sistema di generatori F di M vale $|F| \geq |E|$.

Dimostrazione. Sia, per assurdo, F un sistema di generatori di M con $|F| < |E|$. Per ogni $f \in F$ esiste un insieme finito $E_f \subset E$ tale che $f \in RE_f$. Sia $E_F := \bigcup\limits_{f \in F} E_f \subset E$. Allora $F \subset RE_F$ e quindi $M = RF \subset RE_F$, per cui E_F risulta essere un sistema di generatori di M.

(1) Sia $|F| < \infty$. Allora anche $|E_F| < \infty$, per cui $E_F \subsetneqq E$, una contraddizione alla minimalità di E.

(2) Sia $|F| = \infty$. Allora $|E_F| = |F| < |E|$, per cui ancora $E_F \subsetneqq E$, in contrasto con la minimalità di E.

Osservazione 3.15. M sia un R-modulo libero ed E una base di M. Allora E è un sistema di generatori minimale di M.

Dimostrazione. Ciò segue dall'oss. 3.6.

Proposizione 3.16. *Siano M un R-modulo libero ed E una base di M. Se $|E| = \infty$, allora per ogni base F di M si ha $|F| = |E|$.*

Dimostrazione. Sia F un'altra base di M. Per l'oss. 3.15 E ed F sono entrambi sistemi di generatori minimali di M, cosicché l'enunciato segue dal lemma 3.14.

Definizione 3.17. (1) Diciamo che un R-modulo libero M è un modulo RDB (*a rango ben definito*), se tutte le basi di M possiedono la stessa cardinalità.

In tal caso questa cardinalità si chiama il *rango* di M.

(2) Diciamo che R è un anello ICB (*invarianza di cardinalità delle basi*), se ogni R-modulo libero è un modulo RDB.

In inglese si usa l'abbreviazione IBN (*invariant basis number*).

Osservazione 3.18. Per la prop. 3.16 affinché R sia un anello ICB è sufficiente dimostrare che per $n, m \in \mathbb{N} + 1$ l'isomorfismo $\mathbb{R}^n \cong \mathbb{R}^m$ in $\mathfrak{Mod}(R)$ implica $n = m$.

Lemma 3.19 (principio dello scambio di Steinitz). *R sia un anello con divisione ed M un R-modulo, $E \subset M$ ed $e, f \in M$ tali che $f \in RE$, $f \notin R(E \setminus e)$.*

Allora $e \in R((E \setminus e) \cup f)$.

Dimostrazione. Evidentemente $e \in E$. Sia $f \in RE$. Per ipotesi esistono inoltre $e_2, \ldots, e_m \in E \setminus e$ e $a_1, \ldots, a_m \in R$ tali che
$f = a_1 e + a_2 e_2 \ldots + a_m e_m$ con $a_1 \neq 0$. Perciò
$e = a_1^{-1}(f - a_2 e_2 - \ldots - a_m e_m) \in R((E \setminus e) \cup f)$.

Lemma 3.20. *R sia un anello con divisione ed M un R-modulo. E ed F siano basi di M. Allora per ogni $e \in E$ esiste $f \in F$ tale che $(E \setminus e) \cup f$ sia ancora una base di M.*

Dimostrazione. Sia $e \in E$. Dall'oss. 3.15 segue che $E \setminus e$ non è più un sistema di generatori per M. Siccome F è un sistema di generatori, ciò implica che deve esistere $f \in F$ tale che $f \notin R(E \setminus e)$. Naturalmente invece $f \in RE$. Per il lemma 3.19 segue che $e \in R((E \setminus e) \cup f)$ e quindi è chiaro che $((E \setminus e) \cup f)$ è un sistema di generatori. Per il lemma 3.5 $(E \setminus e) \cup f$ è però linearmente indipendente e quindi una base.

Proposizione 3.21. *Un anello con divisione è un anello ICB.*

Dimostrazione. Siano M un R-modulo (automaticamente libero) ed E, F basi di M. Per la prop. 3.16 possiamo assumere che $|E|, |F| < \infty$. Sia $E = \{e_1, \ldots, e_n\}$ con gli e_i tutti distinti. Sia $|F| \leq n$. Per il lemma 3.20 esiste $f_1 \in F$ tale che $\{f_1, e_2, \ldots, e_n\}$ sia una base di M. Ciò implica $f_1 \neq e_2$. Riapplicando il lemma troviamo $f_2 \in F$ tale che $\{f_1, f_2, e_3, \ldots, e_n\}$ sia una base. Per l'oss. 3.15 f_2 deve essere distinto da f_1, perché $\{f_1, e_3, \ldots, e_n\}$ non è più una base e per la stessa ragione si ha anche $f_2 \neq e_3$. Proseguendo con la sostituzione troviamo elementi $f_1, \ldots, f_n \in F$, tutti distinti, tale che $\{f_1, f_2, \ldots, f_n\}$ è una base. Perciò $|F| \geq n$, cosicché necessariamente $|F| = n = |E|$.

Corollario 3.22. *R sia un anello con divisione ed $n, m \in \mathbb{N} + 1$ con $n \neq m$. Allora gli R-moduli R^n ed R^m non sono isomorfi.*

Dimostrazione. Ciò segue dalla prop. 3.21, tenendo conto della prop. 3.13. Cfr. oss. 3.18.

Osservazione 3.23. Siano $n, m \in \mathbb{N} + 1$ e $\varphi : R^n \longrightarrow R^m$ un omomorfismo di R-moduli. Allora φ determina univocamente una matrice $A \in R^m_n$ tale che $\varphi x = Ax$ per ogni $x \in R^n$ e viceversa.

Perciò gli R-moduli R^n ed R^m sono isomorfi se e solo se esistono matrici $A \in R_n^m$ e $B \in R_m^n$ tali che $AB = \delta_{(n)}$ e $BA = \delta_{(m)}$, dove con $\delta_{(k)}$ denotiamo la matrice identica in R_k^m.

Ciò mostra in particolare che R è un anello ICB se e solo se ogni R-modulo *destro* libero possiede un rango.

Osservazione 3.24. Siano X ed Y due insiemi della stessa cardinalità. Allora gli R-moduli $R^{\underline{X}}$ ed $R^{\underline{Y}}$ sono isomorfi.

Dimostrazione. Sia $\theta : X \longrightarrow Y$ una biezione. È immediato che l'applicazione $\bigcirc_v v \circ \theta : R^{\underline{Y}} \longrightarrow R^{\underline{X}}$ è un isomorfismo.

Nota 3.25. Siano T un anello e V un T-modulo libero di rango infinito ed $R := \mathrm{End}_T V$.

Allora $R^n \cong R^m$ (come R-moduli) per ogni $n, m \in \mathbb{N}$.

Dimostrazione. È sufficiente dimostrare che $R \cong R^2$.

Per l'oss. 3.24, applicata a T al posto di R, esiste un T-isomorfismo $\alpha : V \oplus V \longrightarrow V$. Allora abbiamo un isomorfismo di gruppi abeliani $R := \mathrm{Hom}_T(V,V) \xrightarrow{\varphi} R^2 \cong \mathrm{Hom}_T(V \oplus V, V)$ ponendo $\varphi := \mathrm{Hom}_T(V,-)(\alpha)$ come nella nota 2.8. Esplicitamente per $f \in R$ abbiamo $\varphi(f) = (f\alpha i_1, f\alpha i_2)$, dove i_1, i_2 sono le iniezioni canoniche $V \longrightarrow V \oplus V$.

Dobbiamo solo dimostrare che φ è un omomorfismo (e quindi isomorfismo) di R-moduli. Per $g \in R$ abbiamo però

$\varphi(gf)$=$(gf\alpha i_1, gf\alpha i_2)$=$g(f\alpha i_1, f\alpha i_2)$=$g\varphi(f)$

Lemma 3.26. *$\varphi : R \longrightarrow T$ sia un omomorfismo di anelli. Se T è un anello ICB, allora anche R è un anello ICB.*

Dimostrazione. Usiamo l'oss. 3.23.

Siano $A \in R_n^m$ e $B \in R_m^n$ con $n \neq m$ tale che $AB = \delta_{(m)}$ e $BA = \delta_{(n)}$. Sia $A' = T_n^m$ la matrice che si ottiene da A applicando l'omomorfismo φ ad ogni coefficiente di A e $B' \in T_m^n$ la matrice che si ottiene nello stesso modo da B; allora risulta $A'B' = \delta_{(m)}$ e $B'A' = \delta_{(n)}$, in contrasto con l'ipotesi che T sia un anello ICB.

Corollario 3.27. *Se esiste un omomorfismo di anelli $\varphi : R \longrightarrow K$, dove K è un anello con divisione, allora R è un anello ICB.*

Corollario 3.28. *Ogni anello commutativo è un anello ICB.*

Dimostrazione. Siano R un anello commutativo ed $\mathfrak{m}$ un ideale massimale di R. Allora $R/\mathfrak{m}$ è un campo. Considerando la proiezione canonica $R \longrightarrow R/\mathfrak{m}$, dal lemma 3.26, essendo $R/\mathfrak{m}$ un anello ICB, vediamo che anche R è un anello ICB.

Corollario 3.29. *Se esiste un omomorfismo di anelli $\varphi : R \longrightarrow A$, dove A è un anello commutativo, allora R è un anello ICB.*

Osservazione 3.30. Ogni anello finito è un anello ICB.

Dimostrazione. Sia R un anello con $|R| < \infty$ e $R^n \cong R^m$. Allora $|R|^n = |R|^m$ e quindi $n = m$.

Definizione 3.31. Una *traccia* su R è un omomorfismo di gruppi abeliani $\tau : R \longrightarrow G$ con un gruppo abeliano $(G, +)$ tale che $\tau(ab) = \tau(ba)$ per ogni $a, b \in R$.

τ si dice *senza torsione*, se $\tau(1_R)$ è senza torsione, cioè se $n\tau(1_R) \neq 0$ per ogni $n \in \mathbb{N} + 1$.

Teorema 3.32. *Se R possiede una traccia senza torsione, allora R è un anello ICB.*

Dimostrazione. Siano $A \in R_n^m$ e $B \in R_m^n$ tale che $AB = \delta_{(m)}$ e $BA = \delta_{(n)}$. Per l'oss. 3.23.è sufficiente dimostrare che necessariamente $n = m$.

Per ogni $i = 1, \ldots, m$ abbiamo $\sum\limits_{j=1}^{n} A_j^i B_i^j = (AB)_i^i = 1_R$ e quindi $\sum\limits_{i=1}^{m} \sum\limits_{j=1}^{n} A_j^i B_i^j = m1_R$ e similmente $\sum\limits_{j=1}^{n} \sum\limits_{i=1}^{m} B_i^j A_j^i = n1_R$. Sia τ una traccia senza torsione su R. Allora

$$m\tau(1_R) = \sum_{i=1}^{m} \sum_{j=1}^{n} \tau(A_j^i B_i^j) = \sum_{i=1}^{m} \sum_{j=1}^{n} \tau(B_i^j A_j^i) = \sum_{j=1}^{n} \sum_{i=1}^{m} \tau(B_i^j A_j^i) = n\tau(1_R).$$

Siccome $\tau(1_R)$ è senza torsione, ciò implica $n = m$.

Proposizione 3.33. *Siano X un insieme, M un R-modulo ed $f : X \longrightarrow M$ un'applicazione qualsiasi. Allora esiste un unico omomorfismo di R-moduli $\varphi : R^{\underline{X}} \longrightarrow M$ tale che $\varphi(\delta_x) = f(x)$ per ogni $x \in X$.*

Dimostrazione. Chiaro.

Proposizione 3.34. *Sia M un R-modulo. Allora esistono un R-modulo libero L e un omomorfismo suriettivo $L \longrightarrow M$.*

Se M è finitamente generato, anche L può essere scelto in modo che L sia finitamento generato.

Dimostrazione. Sia E un sistema di generatori di M. Consideriamo l'inclusione $i : E \longrightarrow M$. Allora per la prop. 3.33 esiste un omomorfismo di R-moduli $\varphi : R^{\underline{E}} \longrightarrow M$ tale che $\varphi(\delta_e) = i(e) = e$.

Se M è finitamente generato, possiamo scegliere E finito.

4. Anelli algebricamente finiti

Situazione 4.1. Sia R un anello.

Definizione 4.2. R si dice *algebricamente finito* (o finito nel senso di Dedekind oppure finito nel senso di von Neumann), se per $a, b \in R$ con $ab = 1$ si ha $ba = 1$.

Osservazione 4.3. Sono equivalenti:

(1) R è algebricamente finito

(2) Se $a, b \in R$ sono tali che $ab = 1$, allora $axb \neq 0$ per ogni $x \in R \setminus 0$.

Dimostrazione. (1) $\Longrightarrow$ (2) Siano $a, b \in R$ tali che $ab = 1$ ed R algebricamente finito. Per ipotesi $ba = 1$. Sia $x \in R$ con $axb = 0$. Allora $0 = baxba = 1x1 = x$.

(2) $\Longrightarrow$ (1) Siano $a, b \in R$ ed ab=1. Allora $a(1 - ab)b = ab - abab = 0$. Per ipotesi ciò implica $1 - ba = 0$.

Osservazione 4.4. Ogni dominio è algebricamente finito

Dimostrazione. Ciò segue dall'oss. 4.3 e può essere dimostrato anche direttamente così :

Siano $a, b \in R$ tali che $ab = 1$. Allora $a(1 - ba) = a - aba = a - 1a = 0$, e siccome necessariamente $a \neq 0$, dobbiamo avere $1 - ba = 0$.

Definizione 4.5. R si dice *stabilmente finito*, se per ogni $n \in \mathbb{N} + 1$ l'anello R_n^n è algebricamente finito.

Lemma 4.6. *Siano M_1 ed M R-moduli e $\varphi : M_1 \longrightarrow M$, $\psi : M \longrightarrow M_1$ omomorfismi tali che $\psi\varphi = \mathrm{id}$.*

Allora $M = \operatorname{Im}\varphi \oplus \operatorname{Ker}\psi$.

Dimostrazione. (1) Sia $x \in M$. Allora $x = \varphi(\psi(x)) + x - \varphi(\psi(x))$. Inoltre $\psi(x - \varphi(\psi(x))) = \psi(x) - \psi(\varphi(\psi(x))) = \psi(x) - \psi(x) = 0$, per cui $x \in \operatorname{Im}\varphi + \operatorname{Ker}\psi$.

(2) Sia $x \in \operatorname{Im}\varphi \cap \operatorname{Ker}\psi$. Allora esiste $y \in M_1$ tale che $x = \varphi(y)$. Ma allora $0 = \psi(x) = \psi(\varphi(y)) = y$, per cui anche $x = 0$.

Proposizione 4.7. *Sia $n \in \mathbb{N} + 1$. Allora sono equivalenti:*

(1) R_n^n è algebricamente finito.

(2) $\operatorname{End}_R R^n$ è algebricamente finito.

(3) Non esiste un R-modulo $N \neq 0$ tale che $R^n \cong R^n \oplus N$.

(4) Ogni endomorfismo suriettivo di R-moduli $R^n \longrightarrow R^n$ è un isomorfismo.

Dimostrazione. (1) $\Longleftrightarrow$ (2) Chiaro, perché possiamo identificare $\operatorname{End}_R R^n$ con R_n^n.

(2) $\Longrightarrow$ (3) Sia $R^n \cong R^n \oplus N$. Allora esistono un sottomodulo W di R^n con $W \cong N$ ed un endomorfismo $\varphi : R^n \longrightarrow R^n$ che induce un isomorfismo $\varphi_0 : R^n \longrightarrow \operatorname{Im}\varphi$ tale che $R^n = \operatorname{Im}\varphi \oplus W$.

Definiamo $\psi : R^n \longrightarrow R^n$ in modo tale che $(\psi = \varphi_0^{-1}, \text{in} \operatorname{Im}\varphi)$ e $(\psi = 0, \text{in} W)$. Allora $\psi\varphi = \text{id}$ e per ipotesi ciò implica $\varphi\psi = \text{id}$. Ma ciò è possibile solo se $W = 0$.

(3) $\Longrightarrow$ (2) Siano $\psi, \varphi \in \operatorname{End}_R R^n$ con $\psi\varphi = \text{id}$. Allora l'applicazione ψ è suriettiva, mentre l'applicazione φ è iniettiva e induce quindi un isomorfismo $\varphi_0 : R^n \longrightarrow \operatorname{Im}\varphi$. Per il lemma 4.6 abbiamo $R^n = \operatorname{Im}\varphi \oplus \operatorname{Ker}\psi$ e quindi $R^n \cong R^n \oplus \operatorname{Ker}\varphi$. Per ipotesi ciò implica $\operatorname{Ker}\psi = 0$, cosicché ψ è un isomorfismo. Ma allora $\varphi = \psi^{-1}$ e quindi $\varphi\psi = \text{id}$.

(2) $\Longrightarrow$ (4) Sia $\varphi : R^n \longrightarrow R^n$ un endomorfismo suriettivo rappresentato dalla matrice A nella base standard. Per l'ipotesi di suriettività di φ esiste $B \in R_n^n$ tale che $AB = \delta$. Quindi esiste un endomorfismo ψ rappresentato dalla matrice B per cui $\varphi\psi = \text{id}$. Ma $\operatorname{End}_R R^n$ è per ipotesi algebricamente finito, quindi anche $\varphi\psi = \text{id}$ e vediamo che φ è un isomorfismo.

(4) $\Longrightarrow$ (2) Siano $\psi, \varphi \in \operatorname{End}_R R^n$ con $\psi\varphi = \text{id}$. Allora ψ è un endomorfismo suriettivo, quindi per ipotesi un isomorfismo, per cui $\operatorname{Ker}\psi = 0$. Per il lemma 4.5 però $R^n = \operatorname{Im}\varphi \oplus \operatorname{Ker}\psi$ e quindi $R^n = \operatorname{Im}\varphi$ e quindi anche φ è un isomorfismo e ciò implica $\varphi\psi = \text{id}$.

Corollario 4.8. *Un anello stabilmente finito è un anello ICB.*

Definizione 4.9. Un *quasisottoanello* di R è un sottoinsieme $S \subset R$ tale che:

(1) $(S, +)$ è un sottogruppo di $(R, +)$.

(2) $(S, \cdot)$ è un sottosemigruppo di $(R, \cdot)$.

(3) $(S, \cdot)$ è un monoide.

Si noti che allora $(S, +, \cdot)$ è un anello. Non chiediamo però che 1_S coincida con 1_R.

Esempio 4.10. Sia Λ un insieme non vuoto. Per ogni $\lambda \in \Lambda$ sia dato un anello R_λ. Allora $R := \prod\limits_{\lambda \in \Lambda} R_\lambda$ è un anello, di cui ogni R_μ è un quasisottoanello tramite l'inclusione naturale $\underset{a}{\bigcirc} \underset{\lambda}{\bigcirc} \delta_\lambda^\mu a$, ma non un sottoanello tranne nel caso banale $|\Lambda| = 1$.

Lemma 4.11. *R sia un anello stabilmente finito ed S un quasisottoanello di R. Allora anche S è stabilmente finito.*

Dimostrazione. Siano $n \in \mathbb{N} + 1$ ed $A, B \in S_n^n$ tali che $AB = 1_S\delta$. Poniamo $f := 1_R - 1_S$. Allora f è idempotente e si ha $Sf = fS = 0$. Inoltre

$$(A + f\delta)(B + f\delta) = AB + f^2\delta = (1_S + f)\delta = \delta$$

Ma R è stabilmente finito, quindi

$$\delta = (B + f\delta)(A + f\delta) = BA + f\delta$$

per cui $BA = (1_R - f)\delta = 1_S\delta$.

Corollario 4.12. *Sia Λ un insieme non vuoto. Per ogni $\lambda \in \Lambda$ sia dato un anello R_λ. Poniamo $R := \prod\limits_{\lambda\in\Lambda} R_\lambda$. Allora sono equivalenti:*

(1) R è stabilmente finito.

(2) Ogni R_λ è stabilmente finito.

Dimostrazione. (1) $\Longrightarrow$ (2): Ciò segue dal lemma 4.11, perché ogni R_λ è quasisottoanello di R.

(2) $\Longrightarrow$ (1): Chiaro, ragionando sui singoli coefficenti delle matrici.

Proposizione 4.13. *Ogni anello commutativo è stabilmente finito.*

Dimostrazione. Siano $n \in \mathbb{N}+1$ ed $A, B \in R^n_n$ tale che $AB = \delta$. Siccome R è un anello commutativo, sono valide le formule del calcolo dei determinanti. In particolare abbiamo $\det A \det B = 1$ e $A_{\text{ad}}A = AA_{\text{ad}} = (\det A)\delta$. La matrice A è quindi invertibile. Ciò implica $B = A^{-1}$ e quindi $BA = \delta$.

Definizione 4.14. Un R-modulo M si dice di *Hopf*, se ogni endomorfismo suriettivo è $M \longrightarrow M$ è un isomorfismo.

Proposizione 4.15. *M sia un R-modulo noetheriano. Allora M è di $Hopf$.*

Dimostrazione. Sia $\varphi : M \longrightarrow M$ un endomorfismo suriettivo. Dobbiamo dimostrare che φ è iniettivo.

Sia $x \in \operatorname{Ker}\varphi$ con $x \neq 0$. Sia $n \in \mathbb{N}+1$. Siccome anche φ^n è suriettivo, esiste $y \in M$ tale che $\varphi^n(y) = x$. Allora $\varphi^{n+1}(y) = 0$, mentre per ipotesi $\varphi^n(y) = x \neq 0$. Siccome $\operatorname{Ker}\varphi^n \subset \operatorname{Ker}\varphi^{n+1}$, abbiamo quindi

$$\operatorname{Ker}\varphi \underset{\neq}{\subset} \operatorname{Ker}\varphi^2 \underset{\neq}{\subset} \ldots \underset{\neq}{\subset} \operatorname{Ker}\varphi^n \underset{\neq}{\subset} \ldots$$

in contrasto con l'ipotesi che M sia noetheriano.

Lemma 4.16. *L'anello R sia noetheriano a sinistra. Allora ogni R-modulo finitamente generato è noetheriano.*

Dimostrazione. Goodearl/Warfield, pagina 3.

Corollario 4.17. *L'anello R sia noetheriano a sinistra. Allora ogni R-modulo finitamente generato è $Hopf$.*

Proposizione 4.18. *Ogni anello noetheriano a sinistra è stabilmente finito.*

Dimostrazione. Ciò segue dal cor 4.17 e dal punto (4) della prop. 4.7.

Corollario 4.19. *Ogni anello noetheriano a sinistra è un anello ICB.*

Osservazione 4.20. Un esempio di un anello algebricamente finito, ma non stabilmente finito, è dato in Lam[LMR], pag. 19.

Proposizione 4.21. *Siano $a, b \in R$ tali che $ab = 1$ e $ba \neq 1$.*

Per $i, j \in \mathbb{N} + 1$ poniamo $e_{ij} := b^i(1 - ba)a^j$. Siano $i, j, k, l \in \mathbb{N} + 1$. Allora:

(1) $a^i b^i = 1$.

(2) $(1 - ba)^2 = 1 - ba$.

(3) $e_{ij} \neq 0$.

(4) $e_{ij}e_{kl} = 0$ per $j \neq k$.

$e_{ij}e_{jk} = e_{ik}$.

(5) $e_{ii}^2 = e_{ii}$.

Dimostrazione. (1) Per ipotesi abbiamo $ab = 1$. Perciò

$a^i b^i = \underbrace{a \ldots aa}_{i}\underbrace{bb \ldots b}_{i} = \underbrace{a \ldots a}_{i-1} 1 \underbrace{b \ldots b}_{i-1} = \ldots = 1$

(2) $(1 - ba)^2 = (1 - ba)(1 - ba) = 1 - ba - ba + baba = 1 - ba$.

(3) Per assurdo sia $e_{ij} = b^i(1 - ba)a^j = 0$. Allora

$0 = a^i b^i (1 - ba)a^j b^j = 1 - ba$, cioè $ba = 1$ in contrasto con le ipotesi.

(4) Osserviamo che $a(1 - ba) = 0 = (1 - ba)b$. Sia $j < k$. Dal punto (1) otteniamo allora

$e_{ij}e_{kl} = b^i(1 - ba)a^j b^k(1 - ba)a^l = b^i(1 - ba)b^{k-j}(1 - ba)a^l = 0$

Similmente si vede che $e_{ij}e_{kl} = 0$ per $j > k$. Invece

$e_{ij}e_{jk} = b^i(1 - ba)a^j b^j(1 - ba)a^k = b^i(1 - ba)^2 a^k = b^i(1 - ba)a^k = e_{ik}$

(5) Ciò segue da (4).

Corollario 4.22. *R non sia algebricamente finito. Allora R contiene un insieme infinito di idempotenti a due a due ortogonali.*

Dimostrazione. Nella prop. 4.21 poniamo $e_i := e_{ii}$ per $i \in \mathbb{N}+1$. Allora ogni e_i è idempotente e per $i \neq j$ si ha $e_i e_j = e_{ii}e_{jj} = 0$. Questi elementi sono quindi a due a due ortogonali e devono perciò essere tutti distinti.

5. Successioni esatte

Situazione 5.1. Sia R un anello. Quando non indicato diversamente, M, N, $\ldots$ siano R-moduli e per un sottomodulo N di M con $N \xrightarrow{i} M$ denotiamo l'inclusione canonica, con $M \xrightarrow{\pi} M/N$ la proiezione canonica.

Definizione 5.2. Una successione finita o infinita

$$\ldots \longrightarrow M_{k-1} \xrightarrow{\varphi_{k-1}} M_k \xrightarrow{\varphi_k} M_{k+1} \longrightarrow \ldots$$

di R-moduli si dice *esatta*, se $\operatorname{Ker} \varphi_k = \operatorname{Im} \varphi_{k-1}$ per ogni k.

Proposizione 5.3. *(1) Una successione* $0 \longrightarrow M \xrightarrow{\varphi} N$ *è esatta se e solo se* φ *è iniettiva.*

(2) Una successione $M \xrightarrow{\varphi} N \longrightarrow 0$ *è esatta se e solo se* φ *è suriettiva.*

(3) Una successione $0 \longrightarrow M \xrightarrow{\varphi} N \longrightarrow 0$ *è esatta se e solo se* φ *è biiettiva.*

Definizione 5.4. Una *successione esatta breve* è una successione esatta della forma

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

Esempio 5.5. N sia un sottomodulo di M. Allora la successione

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\pi} M/N \longrightarrow 0$$

è esatta.

Definizione 5.6. Siano X, Y insiemi ed $f : X \longrightarrow Y$ un'applicazione. Se Y_0 è un sottoinsieme di Y tale che $\operatorname{Im} f \subset Y_0$, allora l'applicazione $\underset{x}{\bigcirc} f(x) : X \longrightarrow Y_0$ si chiama la *corestrizione* di f ad Y_0.

Proposizione 5.7. *La successione* $0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ *sia esatta. Allora il diagramma*

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & M \arrow[r, "\psi"] \arrow[d, "\mathrm{id}"'] & M'' \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & \operatorname{Im} \varphi \arrow[r, "i"] & M \arrow[r, "\pi"] & M/\operatorname{Im} \varphi \arrow[r] & 0
\end{tikzcd}$$

è commutativo, in cui α *è la corestrizione di* φ *ad* $\operatorname{Im} \varphi$ *e* $\gamma := \underset{\psi x}{\bigcirc} \pi x$.

α *e* γ *sono isomorfismi.*

Dimostrazione. (1) È chiaro che il diagramma è commutativo e che α è un isomorfismo.

(2) Dobbiamo solo dimostrare che γ è ben definito ed è un isomorfismo. Siano $x, y \in M$ tali che $\psi x = \psi y$. Ciò significa $x - y \in \operatorname{Ker} \psi = \operatorname{Im} \varphi$, per cui $\pi x = \pi y$. Perciò γ è ben definito. Dimostriamo che γ è iniettivo: Sia $x \in M$ tale che $\pi x = 0$. Allora $x \in \operatorname{Im} \varphi = \operatorname{Ker} \psi$, per cui $\psi x = 0$. Dimostriamo che γ è suriettivo: Sia $x \in M$. Allora $\pi x = \gamma \psi x \in \operatorname{Im} \psi$.

In verità γ è semplicemente l'isomorfismo canonico $M'' \cong M/\operatorname{Ker}\psi$ ben noto dall'algebra.

Osservazione 5.8. (1) La successione $0 \longrightarrow M' \xrightarrow{\varphi} M$ sia esatta. Allora è esatta la successione

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\pi} M/\operatorname{Im}\varphi \longrightarrow 0$$

(2) La successione $M \xrightarrow{\varphi} M'' \longrightarrow 0$ sia esatta. Allora è esatta la successione

$$0 \longrightarrow \operatorname{Ker}\varphi \xrightarrow{i} M \xrightarrow{\varphi} M'' \longrightarrow 0$$

Definizione 5.9. Siano date due successioni finite o infinite

$$\ldots \longrightarrow M_{k-1} \xrightarrow{\varphi_{k-1}} M_k \xrightarrow{\varphi_k} M_{k+1} \longrightarrow \ldots$$

$$\ldots \longrightarrow N_{k-1} \xrightarrow{\psi_{k-1}} N_k \xrightarrow{\psi_k} N_{k+1} \longrightarrow \ldots$$

di R-moduli definite per gli stessi insiemi di indici.

Un *omomorfismo* $\underset{k}{\bigcirc}(M_k, \varphi_k) \longrightarrow \underset{k}{\bigcirc}(N_k, \psi_k)$ è una famiglia $\underset{k}{\bigcirc} f_k$ di omomorfismi $f_k : M_k \longrightarrow N_k$ tale che il diagramma

$$\begin{tikzcd}
\ldots \arrow[r] & M_k \arrow[r, "\varphi_k"] \arrow[d, "f_k"] & M_{k+1} \arrow[r] \arrow[d, "f_{k+1}"] & \ldots \\
\ldots \arrow[r] & N_k \arrow[r, "k"] & N_{k+1} \arrow[r] & \ldots
\end{tikzcd}$$

sia commutativo per ogni k.

L'omomorfismo $\underset{k}{\bigcirc} f_k$ si chiama un *isomorfismo*, se ogni f_k è un isomorfismo.

Osservazione 5.10. Nella prop. 5.7 abbiamo dimostrato che ogni successione esatta $0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ è in modo naturale isomorfa alla successione esatta $0 \longrightarrow \operatorname{Im}\varphi \xrightarrow{i} M \xrightarrow{\pi} M/\operatorname{Im}\varphi \longrightarrow 0$.

Osservazione 5.11. Siano N un sottomodulo di M e P un sottomodulo di N. Allora è esatta la successione

$$0 \longrightarrow N/P \xrightarrow{i} M/P \xrightarrow{\varphi} M/N \longrightarrow 0$$

in cui $\varphi(x+P) := x + N$.

Dalla prop. 5.7 otteniamo il noto isomorfismo naturale $M/N \cong (M/P)/(N/P)$.

Lemma 5.12. *Il diagramma*

$$\begin{tikzcd}
M \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & M' \arrow[d, "\beta"] \\
N \arrow[r, "\psi"] & N'
\end{tikzcd}$$

sia commutativo. α e β siano isomorfismi. Allora è commutativo anche il diagramma

$$\begin{tikzcd} N \arrow[r, "\psi"] \arrow[d, "\alpha^{-1}"'] & N' \arrow[d, "\beta^{-1}"] \\ M \arrow[r, "\varphi"] & M' \end{tikzcd}$$

<u>Dimostrazione.</u> Per ipotesi $\beta\varphi = \psi\alpha$ e quindi $\psi = \beta\varphi\alpha^{-1}$ e poi $\beta^{-1}\psi = \varphi\alpha^{-1}$.

Lemma 5.13. *Sia dato un diagramma commutativo*

$$\begin{tikzcd} M_2 \arrow[r, "\varphi_2"] & M_3 \arrow[r, "\varphi_3"] \arrow[d, "f_3"] & M_4 \arrow[d, "f_4"] \\ & N_3 \arrow[r, "\psi_3"] & N_4 \end{tikzcd}$$

in cui la riga è esatta ed f_4 è iniettivo.

Allora $\operatorname{Ker} f_3 \subset \operatorname{Im} \varphi_2$.

<u>Dimostrazione.</u> L'iniettività di f_4 implica $\operatorname{Ker} f_4\varphi_3 = \operatorname{Ker} \varphi_3$. Perciò $\operatorname{Ker} f_3 \subset \operatorname{Ker} \psi_3 f_3 = \operatorname{Ker} f_4\varphi_3 = \operatorname{Ker} \varphi_3 = \operatorname{Im} \varphi_2$.

Lemma 5.14. *Sia dato un diagramma commutativo*

$$\begin{tikzcd} M_1 \arrow[r, "\varphi_1"] \arrow[d, "f_1"'] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[d, "f_3"] \\ N_1 \arrow[r, "\psi_1"] & N_2 \arrow[r, "\psi_2"] & N_3 \end{tikzcd}$$

in cui la seconda riga è esatta, f_1 è suriettivo ed f_2 è iniettivo.

Allora $\operatorname{Ker} f_3 \cap \operatorname{Im} \varphi_2 \subset \operatorname{Im} \varphi_2\varphi_1$.

<u>Dimostrazione.</u> La suriettività di f_1 implica $\operatorname{Im} \psi_1 = \operatorname{Im} \psi_1 f_1 = \operatorname{Im} f_2\varphi_1$. Sia $x \in \operatorname{Ker} f_3 \cap \operatorname{Im} \varphi_2$. Allora $f_3 x = 0$ ed esiste $y \in M_2$ tale che $\varphi_2 y = x$. Dunque $0 = f_3\varphi_2 y = \psi_2 f_2 y$, quindi $f_2 y \in \operatorname{Ker} \psi_2 = \operatorname{Im} \psi_1 = \operatorname{Im} f_2\varphi_1$. Esiste allora $z \in M_1$ tale che $f_2 y = f_2\varphi_1 z$. Dall'iniettività di f_2 segue $y = \varphi_1 z$, per cui $x = \varphi_2 y = \varphi_2\varphi_1 z$.

Teorema 5.15 (primo lemma dei Quattro). *Sia dato un diagramma commutativo*

$$\begin{tikzcd} M_1 \arrow[r, "\varphi_1"] \arrow[d, "f_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[r, "\varphi_3"] \arrow[d, "f_3"] & M_4 \arrow[d, "f_4"] \\ N_1 \arrow[r, "\psi_1"] & N_2 \arrow[r, "\psi_2"] & N_3 \arrow[r, "\psi_3"] & N_4 \end{tikzcd}$$

nel quale siano soddisfatte le seguenti condizioni:

(1) La prima riga è esatta in M_3.

(2) La seconda riga è esatta in N_2.

(3) f_1 è suriettivo.

(4) f_2 e f_4 sono iniettivi.

Allora $\operatorname{Ker} f_3 \subset \operatorname{Im} \varphi_2\varphi_1$.

Se quindi $\varphi_2\varphi_1 = 0$, allora f_3 è iniettivo.

Dimostrazione. Per il lemma 5.13 $\operatorname{Ker} f_3 \subset \operatorname{Im} \varphi_2$. Usando il lemma 5.14 abbiamo $\operatorname{Ker} f_3 = \operatorname{Ker} f_3 \cap \operatorname{Im} \varphi_2 \subset \operatorname{Im} \varphi_2\varphi_1$.

Osservazione 5.16. Sia dato un diagramma commutativo

$$\begin{tikzcd} M_1 \arrow[r, "\varphi_1"] \arrow[d, "f_1"] & M_2 \arrow[d, "f_2"] \\ N_1 \arrow[r, "\psi_1"] & N_2 \end{tikzcd}$$

in cui f_1 sia suriettivo. Allora $\operatorname{Im} \psi_1 \subset \operatorname{Im} f_2$.

Dimostrazione. Per la suriettività di f_1 abbiamo

$$\operatorname{Im} \psi_1 = \operatorname{Im} \psi_1 f_1 = \operatorname{Im} f_2\varphi_1 \subset \operatorname{Im} f_2$$

Lemma 5.17. *Sia dato un diagramma commutativo*

$$\begin{tikzcd} M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[r, "\varphi_3"] \arrow[d, "f_3"] & M_4 \arrow[d, "f_4"] \\ N_2 \arrow[r, "\psi_2"] & N_3 \arrow[r, "\psi_3"] & N_4 \end{tikzcd}$$

in cui la prima riga è esatta, f_3 è suriettivo ed f_4 e iniettivo.

Allora $\operatorname{Ker} \psi_3\psi_2 \subset \operatorname{Ker} \psi_2 + \operatorname{Im} f_2$.

Dimostrazione. Sia $x \in \operatorname{Ker} \psi_3\psi_2$. Per la suriettività di f_3 esiste un y tale che $\psi_2 x = f_3 y$. Da ciò segue che $0 = \psi_3\psi_2 x = \psi_3 f_2 y = f_4\varphi_3 y$. L'iniettività di f_4 implica $y \in \operatorname{Ker} \varphi_3 = \operatorname{Im} \varphi_2$, quindi esiste z tale che $y = \varphi_2 z$. Da ciò segue $\psi_2 x = f_3 y = f_3\varphi_2 z = \psi_2 f_2 z$, per cui $x - f_2 z \in \operatorname{Ker} \psi_2$, cosicché $x = x - f_2 z + f_2 z \in \operatorname{Ker} \psi_2 + \operatorname{Im} f_2$.

Teorema 5.18 (secondo lemma dei Quattro). *Sia dato un diagramma commutativo*

$$\begin{tikzcd} M_1 \arrow[r, "\varphi_1"] \arrow[d, "f_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[r, "\varphi_3"] \arrow[d, "f_3"] & M_4 \arrow[d, "f_4"] \\ N_1 \arrow[r, "\psi_1"] & N_2 \arrow[r, "\psi_2"] & N_3 \arrow[r, "\psi_3"] & N_4 \end{tikzcd}$$

nel quale sono soddisfatte le seguenti condizioni:

(1) La prima riga è esatta in M_3.

(2) La seconda riga è esatta in N_2.

(3) f_4 è iniettivo.

(4) f_1 ed f_3 sono suriettivi.

Allora $\operatorname{Ker} \psi_3\psi_2 \subset \operatorname{Im} f_2$.

Se quindi $\psi_3\psi_2 = 0$, allora f_2 è suriettivo.

Dimostrazione. Per il lemma 5.17 e l'oss. 5.16 abbiamo

$$\operatorname{Ker} \psi_3\psi_2 \subset \operatorname{Ker} \psi_2 + \operatorname{Im} f_2 = \operatorname{Im} \psi_1 + \operatorname{Im} f_2 \subset \operatorname{Im} f_2$$

Corollario 5.19. *Sia dato un diagramma commutativo*

$$\begin{tikzcd} & M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[r, "\varphi_3"] \arrow[d, "f_3"] & M_4 \arrow[d, "f_4"] \\ 0 \arrow[r, "\psi_1"] & N_2 \arrow[r, "\psi_2"] & N_3 \arrow[r, "\psi_3"] & N_4 \end{tikzcd}$$

nel quale sono soddisfatte le seguenti condizioni:

(1) La prima riga è esatta.

(2) La seconda riga è esatta in N_2.

(3) f_2 *ed* f_4 *sono iniettivi.*

Allora f_3 *è iniettivo.*

Dimostrazione. Consideriamo il diagramma completato

$$\begin{tikzcd} 0 \arrow[r, "\varphi_1"] \arrow[d, "f_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[r, "\varphi_3"] \arrow[d, "f_3"] & M_4 \arrow[d, "f_4"] \\ 0 \arrow[r] & N_2 \arrow[r, "\psi_2"] & N_3 \arrow[r, "\psi_3"] & N_4 \end{tikzcd}$$

f_1 è banalmente suriettivo e $\varphi_2\varphi_1 = 0$. Dal teorema 5.15 segue che f_3 è iniettivo.

Corollario 5.20. *Sia dato un diagramma commutativo*

$$\begin{tikzcd} & M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[r, "\varphi_3"] \arrow[d, "f_3"] & M_4 \arrow[d, "f_4"] \\ 0 \arrow[r, "\psi_1"] & N_2 \arrow[r, "\psi_2"] & N_3 \arrow[r, "\psi_3"] & N_4 \end{tikzcd}$$

nel quale sono soddisfatte le seguenti condizioni:

(1) La prima riga è esatta.

(2) La seconda riga è esatta in N_2.

(3) $\psi_3\psi_2 = 0$.

(4) f_3 *è suriettivo ed* f_4 *è iniettivo.*

Allora f_2 *è suriettivo.*

Dimostrazione. Consideriamo il diagramma completato

$$\begin{tikzcd} 0 \arrow[r, "\varphi_1"] \arrow[d, "f_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[r, "\varphi_3"] \arrow[d, "f_3"] & M_4 \arrow[d, "f_4"] \\ 0 \arrow[r] & N_2 \arrow[r, "\psi_2"] & N_3 \arrow[r, "\psi_3"] & N_4 \end{tikzcd}$$

f_1 è banalmente suriettivo, cosicchè f_2 è suriettivo per il teorema 5.18.

Osservazione 5.21. Sia dato un diagramma commutativo

$$\begin{tikzcd} 0 \arrow[r] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[d, "f_3"] \\ & N_2 \arrow[r, "\psi_2"] & N_3 \end{tikzcd}$$

in cui la prima riga sia esatta.

Se f_3 è iniettivo, allora anche f_2 è iniettivo.

<u>Dimostrazione.</u> Per l'iniettività di f_3 abbiamo

$\operatorname{Ker} f_2 \subset \operatorname{Ker} \psi_2 f_2 = \operatorname{Ker} f_3\varphi_2 = \operatorname{Ker} \varphi_2 = 0$

Osservazione 5.22. Sia dato un diagramma commutativo

$$\begin{tikzcd}
M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[d, "f_3"] & \\
N_2 \arrow[r, "\psi_2"] & N_3 \arrow[r] & 0
\end{tikzcd}$$

in cui la seconda riga sia esatta.

Se f_2 è suriettivo, allora anche f_3 è suriettivo.

<u>Dimostrazione.</u> Si tratta di un caso speciale dell'oss. 5.16.

Proposizione 5.23. *Sia dato un diagramma commutativo*

$$\begin{tikzcd}
0 \arrow[r] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[r, "\varphi_3"] \arrow[d, "f_3"] & M_4 \arrow[d, "f_4"] \\
0 \arrow[r] & N_2 \arrow[r, "\psi_2"] & N_3 \arrow[r, "\psi_3"] & N_4
\end{tikzcd}$$

nel quale sono soddisfatte le seguenti condizioni:

(1) La prima riga è esatta.

(2) La seconda riga è esatta in N_2.

(3) $\psi_3\psi_2 = 0$.

(4) f_3 è un isomorfismo ed f_4 è iniettivo.

Allora f_2 è un isomorfismo.

<u>Dimostrazione.</u> Per l'oss 5.21 f_2 è iniettivo e per il cor. 5.20 f_2 è anche suriettivo.

Corollario 5.24. *Sia dato un diagramma commutativo*

$$\begin{tikzcd}
M_1 \arrow[r, "\varphi_1"] \arrow[d, "f_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[r] \arrow[d, "f_3"] & 0 \\
N_1 \arrow[r, "\psi_1"] & N_2 \arrow[r, "\psi_2"] & N_3 &
\end{tikzcd}$$

nel quale sono soddisfatte le seguenti condizioni:

(1) La prima riga è esatta in M_3.

(2) La seconda riga è esatta in N_2.

(3) $\varphi_2\varphi_1 = 0$.

(4) f_1 è suriettivo ed f_2 è iniettivo.

Allora f_3 è iniettivo.

<u>Dimostrazione.</u> Si tratta di un caso speciale del teorema 5.15.

Corollario 5.25. *Sia dato un diagramma commutativo*

$$\begin{tikzcd}
M_1 \arrow[r, "\varphi_1"] \arrow[d, "f_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[r] \arrow[d, "f_3"] & 0 \\
N_1 \arrow[r] & N_2 \arrow[r, "\psi_2"] & N_3 &
\end{tikzcd}$$

nel quale sono soddisfatte le seguenti condizioni:

(1) La prima riga è esatta in M_3.

(2) La seconda riga è esatta in N_2.

(3) f_1 e f_3 sono suriettivi.

Allora f_2 è suriettivo.

Dimostrazione. Si tratta di un caso speciale del teorema 5.18.

Proposizione 5.26. *Sia dato un diagramma commutativo*

$$\begin{tikzcd}
M_1 \arrow[r, "\varphi_1"] \arrow[d, "f_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[r] \arrow[d, "f_3"] & 0 \\
N_1 \arrow[r, "\psi_1"] & N_2 \arrow[r, "\psi_2"] & N_3 \arrow[r, "\psi_3"] & 0
\end{tikzcd}$$

nel quale sono soddisfatte le seguenti condizioni:

(1) La prima riga è esatta in M_3.

(2) La seconda riga è esatta.

(3) $\varphi_2\varphi_1 = 0$.

(4) f_1 è suriettivo e f_2 è un ismorfismo.

Allora f_3 è un isomorfismo.

Dimostrazione. Per il l'oss. 5.22 f_3 è suriettivo e per il cor. 5.24 f_3 è iniettivo.

Teorema 5.27 (lemma dei Cinque). *Sia dato un diagramma commutativo*

$$\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r, "\varphi_1"] \arrow[d, "f_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "f_2"] & M_3 \arrow[r] \arrow[d, "f_3"] & 0 \\
0 \arrow[r] & N_1 \arrow[r, "\psi_1"] & N_2 \arrow[r, "\psi_2"] & N_3 \arrow[r] & 0
\end{tikzcd}$$

nel quale entrambe le righe siano esatte.

Se due delle tre frecce verticali f_1, f_2, f_3 sono isomorfismi, allora anche la terza è un isomorfismo.

Dimostrazione. (1) Siano f_1 ed f_2 isomorfismi. Allora per la prop. 5.26 f_3 è un isomorfismo.

(2) Siano f_1 e f_3 isomorfismi. Allora f_2 è iniettivo per il cor. 5.19 e suriettivo per il cor. 5.25.

(3) Siano f_2 ed f_3 isomorfismi. Allora f_1 è un isomorfismo per la prop. 5.23.

Lemma 5.28. *Sia dato un diagramma commutativo*

$$\begin{array}{ccccccc} & & M_1 & \xrightarrow{\varphi_1} & M_2 & \xrightarrow{\varphi_2} & M_3 \\ & & & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} \\ 0 & \longrightarrow & N_1 & \xrightarrow{\psi_1} & N_2 & \xrightarrow{\psi_2} & N_3 \end{array}$$

nel quale siano soddisfatte le seguenti condizioni:

(1) $\varphi_2\varphi_1 = 0$*.*

(2) La seconda riga è esatta.

Allora esiste, univocamente determinato, un omomorfismo $f_1 : M_1 \longrightarrow N_1$ *che rende commutativo il diagramma*

$$\begin{array}{ccccc} M_1 & \xrightarrow{\varphi_1} & M_2 & \xrightarrow{\varphi_2} & M_3 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} \\ N_1 & \xrightarrow{\psi_1} & N_2 & \xrightarrow{\psi_2} & N_3 \end{array}$$

<u>Dimostrazione.</u> Da $\psi_2 f_2 \varphi_1 = f_3\varphi_2\varphi_1 = 0$ vediamo che $\operatorname{Im} f_2\varphi_1 \subset \operatorname{Ker}\psi_2 = \operatorname{Im}\psi_1$. È quindi definita la corestrizione $g : \operatorname{Im}\varphi_1 \longrightarrow \operatorname{Im}\psi_1$ di $(f_2, \text{in} \operatorname{Im}\varphi_1)$ a $\operatorname{Im}\psi_1$. Siccome ψ_1 è iniettiva, la corestrizione $\widetilde{\psi}$, di N_1 a $\operatorname{Im}\psi_1$ è biettiva, cosicché otteniamo un diagramma commutativo

$$\begin{array}{ccccc} M_1 & \xrightarrow{\widetilde{\varphi_1}} & \operatorname{Im}\varphi_1 & \xrightarrow{i} & M_2 \\ & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle f_2} \\ N_1 & \xrightarrow{\widetilde{\psi_1}} & \operatorname{Im}\psi_1 & \xrightarrow{i} & N_2 \end{array}$$

(in cui $\widetilde{\varphi_1}$ è la corestrizione di φ_1 a $\operatorname{Im}\varphi_1$) che ci permette di definire $f_1 : M_1 \longrightarrow N_1$ ponendo $f_1 = \widetilde{\psi_1}^{-1} g\widetilde{\varphi_1}$.

Più esplicitamente, per $x \in M_1$ ed $y \in N_1$ abbiamo $f_1x = y$ se e solo se $\psi_1 y = f_2\varphi_1 x$. È immediato che il secondo diagramma nell'esempio è commutativo. Dalla relazione $\psi_1 f_1 = f_2\varphi_1$ vediamo che f_1 non può essere definita in altro modo, perchè ψ_1 è iniettivo.

Lemma 5.29. *Sia dato un diagramma commutativo*

$$\begin{array}{ccccccc} M_1 & \xrightarrow{\varphi_1} & M_2 & \xrightarrow{\varphi_2} & M_3 & \longrightarrow & 0 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & & & \\ N_1 & \xrightarrow{\psi_1} & N_2 & \xrightarrow{\psi_2} & N_3 & & \end{array}$$

nel quale sono soddisfatte le seguenti condizioni:

(1) La prima riga è esatta.

(2) $\psi_2\psi_1 = 0$*.*

Allora esiste, univocamente determinato, un omomorfismo $f_3 : M_3 \longrightarrow N_3$ *che rende commutativo il diagramma*

$$\begin{array}{ccccc} M_1 & \xrightarrow{\varphi_1} & M_2 & \xrightarrow{\varphi_2} & M_3 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} \\ N_1 & \xrightarrow{\psi_1} & N_2 & \xrightarrow{\psi_2} & N_3 \end{array}$$

Dimostrazione. (1) Si deve in ogni caso avere $f_3\varphi_2 = \psi_2 f_2$ e ciò per la suriettività di φ_2 implica che $f_3 = \bigcirc_{\varphi_2 x} \psi_2 f_2 x$.

(2) Dobbiamo dimostrare che f_3 in questo modo risulta ben definita. Siano $x, y \in M_2$ tali che $\varphi_2 x = \varphi_2 y$. Allora $x - y \in \operatorname{Ker}\varphi_2 = \operatorname{Im}\varphi_1$, perciò esiste $z \in M_1$ tale che $\varphi_1 z = x - y$. Perciò $f_2 x - f_2 y = f_2\varphi_1 z = \psi_1 f_1 z$, per cui $\psi_2 f_2 x - \psi_2 f_2 y = \psi_2\psi_1 f_1 z = 0$.

(3) È chiaro che f_3 è un omomorfismo di moduli.

Osservazione 5.30. Fissati $M, N \in \mathfrak{Mod}(R)$, nel seguito consideriamo i funtori $\operatorname{Hom}_R(M, -)$ e $\operatorname{Hom}_R(-, N)$ come funtori (contravarianti nel seconda caso) $\mathfrak{Mod}(R) \longrightarrow \mathfrak{Mod}(\mathbb{Z})$. Cfr. nota 2.8.

Riferendoci a quella nota useremo talvolta le abbreviazioni $\varphi_* := \bigcirc_{\psi} \varphi\psi$ e $\varphi^* := \bigcirc_{\psi} \psi\varphi$.

Teorema 5.31. *Sia data una successione esatta*
$0 \longrightarrow M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3$.

Allora per ogni R-modulo X la successione di gruppi abeliani

$$0 \longrightarrow \operatorname{Hom}(X, M_1) \xrightarrow{\varphi_{1*}} \operatorname{Hom}(X, M_2) \xrightarrow{\varphi_{2*}} \operatorname{Hom}(X, M_3)$$

è esatta.

Dimostrazione. (1) Dobbiamo dimostrare che φ_{1*} è iniettivo.
Sia $\psi \in \operatorname{Hom}(X, M_1)$ tale che $\varphi_{1*}\psi = 0$. Ciò significa $\varphi_1\psi x = 0$ per ogni $x \in X$, pertanto $\psi x = 0$ per ogni $x \in X$ perchè φ_1 è iniettivo.

(2) Dobbiamo dimostrare che $\operatorname{Im}\varphi_{1*} = \operatorname{Ker}\varphi_{2*}$. In primo luogo abbiamo $\varphi_{2*}\varphi_{1*} = (\varphi_2\varphi_1)_* = 0_* = 0$.

Sia ora $\alpha \in \operatorname{Ker}\varphi_{2*}$. Allora $\varphi_{2*}\alpha = \varphi_2\alpha = 0$ e quindi $\operatorname{Im}\alpha \subset \operatorname{Ker}\varphi_2 = \operatorname{Im}\varphi_1$. Per ogni $x \in X$ esiste perciò un $u_x \in M_1$ tale che $\alpha x = \varphi_1 u_x$. u_x è univocamente determinato perchè φ_1 è iniettivo. Si verifica facilmente che $\beta := \bigcirc_{x} u_x : X \longrightarrow M_1$ è un omomorfismo ed è chiaro che $\varphi_1\beta = \alpha$.

Teorema 5.32. *Sia data una successione esatta*
$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \longrightarrow 0$.

Allora per ogni R-modulo Y la successione di gruppi abeliani

$$0 \longrightarrow \operatorname{Hom}(M_3, Y) \xrightarrow{\varphi_2^*} \operatorname{Hom}(M_2, Y) \xrightarrow{\varphi_1^*} \operatorname{Hom}(M_1, Y)$$

è esatta.

Dimostrazione. (1) Dobbiamo dimostrare che φ_2^* è iniettivo. Sia $\psi \in \operatorname{Hom}(N_3, Y)$ tale che $\varphi_2^*\psi = 0$. Allora $\psi\varphi_2 x = 0$ per ogni $x \in N_2$, ma φ_2 è suriettivo, quindi ciò equivale a $\psi y = 0$ per ogni $y \in N_3$, per cui $\psi = 0$.

(2) Dobbiamo dimostrare che $\operatorname{Im}\varphi_2^* = \operatorname{Ker}\varphi_1^*$. In primo luogo abbiamo $\varphi_1^*\varphi_2^* = (\varphi_2\varphi_1)^* = 0^* = 0$. Sia ora $\alpha \in \operatorname{Ker}\varphi_1^*$, cioè tale che $\alpha\varphi_1 = 0$. Allora $(\alpha, \operatorname{in}\operatorname{Im}\varphi_1) = (\alpha, \operatorname{in}\operatorname{Ker}\varphi_2) = 0$. Definiamo $\beta : M_3 \longrightarrow Y$ con $\beta := \bigcirc_{\varphi_2 x} \alpha x$. Dalla relazione appena vista segue che β è un omomorfismo ben definito ed è chiaro che $\alpha = \beta\varphi_2 = \varphi_2^*\beta$.

Osservazione 5.33. Sia G un gruppo abeliano.
Allora $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, G) \cong G$.

Più precisamente abbiamo $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, G) = \{\alpha_g \mid g \in G\}$ con $\alpha_g := \underset{n}{\bigcirc} ng$.

<u>Dimostrazione.</u> Sia $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, G)$. Allora φ è univocamente determinato da $\varphi(1)$, perché per $n \in \mathbb{Z}$ abbiamo $\varphi(n) = n\varphi(1)$.

D'altra parte per $\varphi(1)$ possiamo scegliere qualunque elemento di G, come segue ad esempio dalla prop. 3.33.

Definizione 5.34. Per un gruppo abeliano G ed $m \in N$ poniamo $G[m] := \{g \in G \mid mg = 0\}$.

Proposizione 5.35. *Siano G un gruppo abeliano ed $m \in \mathbb{N} + 2$. Allora*

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, G) \cong G[m]$$

<u>Dimostrazione.</u> Consideriamo la successione esatta

$$m\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/m \longrightarrow 0$$

Per il teorema 5.32 è esatta anche la successione

$$0 \longrightarrow \mathrm{Hom}(\mathbb{Z}/m, G) \xrightarrow{\pi^*} \mathrm{Hom}(\mathbb{Z}, G) \xrightarrow{i^*} \mathrm{Hom}(m\mathbb{Z}, G).$$

Perciò $\mathrm{Hom}(\mathbb{Z}/m, G) \cong \mathrm{Im}\, \pi^* = \mathrm{Ker}\, i^*$.

Per l'oss. 5.33 $\mathrm{Hom}(\mathbb{Z}, G) = \{\alpha_g \mid g \in G\}$ con $\alpha_g := \underset{n}{\bigcirc} ng$. È anche chiaro che $\alpha_g \neq \alpha_h$ per $g \neq h$. Sia $i^*\alpha_g = 0$. Ciò significa proprio $0 = (\alpha_g i)(1) = \alpha_g(m) = mg$. Dunque $\mathrm{Ker}\, i^* \cong G[m]$.

Corollario 5.36. *Sia $m \in \mathbb{N} + 2$. Allora $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}) = 0$.*

<u>Dimostrazione.</u> Infatti $\mathbb{Z}[m] = 0$.

Corollario 5.37. *Sia $m \in \mathbb{N} + 2$. Allora $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/m) = \mathbb{Z}/m$.*

<u>Dimostrazione.</u> Infatti $\mathbb{Z}/m[m] = \mathbb{Z}/m$.

Osservazione 5.38. Siano $m \in \mathbb{N} + 2$ e $\varphi := \underset{x}{\bigcirc} mx : \mathbb{Z} \longrightarrow \mathbb{Z}$.

Allora $\varphi^* := \mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z}/m)(\varphi) = 0$.

<u>Dimostrazione.</u> Per definizione $\varphi^* = \underset{\alpha}{\bigcirc} \alpha\varphi \colon \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/m) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/m)$.
Per $\alpha \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/m)$ abbiamo un diagramma commutativo

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\alpha"] & \mathbb{Z}/m \\
\mathbb{Z} \arrow[u, "\varphi"] \arrow[ur, "\varphi^*\alpha"'] &
\end{tikzcd}$$

Però per ogni $x \in \mathbb{Z}$ naturalmente $\alpha\varphi x = \alpha(mx) = m\alpha x = 0$.

Nota 5.39. Per $m \in \mathbb{N} + 2$ consideriamo la successione esatta di gruppi abeliani

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\varphi=\bigcirc_x mx} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/m \longrightarrow 0$$

(1) La successione indotta

$$\mathrm{Hom}(\mathbb{Z}/m,\mathbb{Z}) \xrightarrow{\pi_*} \mathrm{Hom}(\mathbb{Z}/m,\mathbb{Z}/m) \longrightarrow 0$$

non è esatta.

(2) La successione indotta

$$\mathrm{Hom}(\mathbb{Z},\mathbb{Z}/m) \xrightarrow{\varphi^*} \mathrm{Hom}(\mathbb{Z},\mathbb{Z}/m) \longrightarrow 0$$

non è esatta.

Dimostrazione. (1) Per il cor. 5.36 $\mathrm{Hom}(\mathbb{Z}/m,\mathbb{Z}) = 0$. Ma la successione $0 \longrightarrow \mathrm{Hom}(\mathbb{Z}/m,\mathbb{Z}/m) \longrightarrow 0$ non è esatta, perché $\mathrm{Hom}(\mathbb{Z}/m,\mathbb{Z}/m) \cong \mathbb{Z}/m$ per il cor. 5.37.

(2) Dimostriamo che $\varphi^* = 0$. Infatti per $\alpha \in \mathrm{Hom}(\mathbb{Z},\mathbb{Z}/m)$ ed $x \in \mathbb{Z}$ abbiamo $(\varphi^*\alpha)x = (\alpha\varphi)x = \alpha(mx) = m\alpha(1) = 0$. Siccome $\mathrm{Hom}(\mathbb{Z},\mathbb{Z}/m) \cong \mathbb{Z}/m \neq 0$, la successione indotta non può essere esatta.

Definizione 5.40. Dati M_1 ed M_2, denotiamo con $i_1 := \bigcirc_x (x,0) : M_1 \longrightarrow M_1 \oplus M_2$ e $i_2 := \bigcirc_y (0,y) : M_2 \longrightarrow M_1 \oplus M_2$ le iniezioni canoniche, con $\pi_1 := \bigcirc_{(x,y)} x : M_1 \oplus M_2 \longrightarrow M_1$ e $\pi_2 := \bigcirc_{(x,y)} y : M_1 \oplus M_2 \longrightarrow M_2$ le proiezioni canoniche.

Osservazione 5.41. La successione $0 \longrightarrow M_1 \xrightarrow{i_1} M_1 \oplus M_2 \xrightarrow{\pi_2} M_2 \longrightarrow 0$ è esatta.

Definizione 5.42. Diciamo che una successione esatta

$$0 \longrightarrow M_1 \xrightarrow{\varphi} M \xrightarrow{\psi} M_2 \longrightarrow 0$$

si spezza, quando è isomorfa ad una successione esatta della forma

$$0 \longrightarrow N_1 \xrightarrow{i_1} N_1 \oplus N_2 \xrightarrow{\pi_2} N_2 \longrightarrow 0$$

Definizione 5.43. M_1 sia un sottomodulo di M. Allora diciamo che M_1 è un *sommando diretto* di M se esiste un sottomodulo M_2 di M tale che $M = M_1 \oplus M_2$.

Proposizione 5.44. *La successione* $0 \longrightarrow M_1 \xrightarrow{\varphi} M$ *sia esatta. Allora sono equivalenti:*

(1) $\mathrm{Im}\,\varphi$ *è sommando diretto di* M.

(2) Esiste un omomorfismo $\sigma : M \longrightarrow M_1$ *tale che* $\sigma\varphi = \mathrm{id}$.

Dimostrazione. (1) $\Longrightarrow$ (2): Sia N un sottomodulo di M tale che $M = N \oplus \mathrm{Im}\,\varphi$. Sia $x \in M$. Allora x possiede una rappresentazione $x = y + \varphi u$ con $y \in N$ e $u \in M_1$ univocamente determinati, perché φ è iniettivo. Possiamo quindi definire $\sigma x := u$. È chiaro che in questo modo si ottiene un omomorfismo e per definizione si ha $\sigma\varphi u = u$ per ogni $u \in M_1$.

(2) $\Longrightarrow$ (1): Per il lemma 4.6 abbiamo $M = \mathrm{Im}\,\varphi \oplus \mathrm{Ker}\,\sigma$.

Proposizione 5.45. *La successione* $M \xrightarrow{\psi} M_2 \longrightarrow 0$ *sia esatta. Allora sono equivalenti:*

(1) $\operatorname{Ker}\psi$ *è sommando diretto di* M*.*

(2) Esiste un omomorfismo $\tau : M_2 \longrightarrow M$ *tale che* $\psi\tau = \mathrm{id}$.

Dimostrazione. (1) $\Longrightarrow$ (2) Sia N un sottomodulo di M tale che $M = \operatorname{Ker}\psi \oplus N$. Sia $y \in M_2$. Siccome ψ è suriettivo esiste $x \in M$ tale che $\psi x = y$. Per ipotesi $x = u + v$ con $u \in \operatorname{Ker}\psi$ e $v \in N$ univocamente determinati. Allora poniamo $\tau y := v$.

Bisogna dimostrare che l'applicazione τ è ben definita. Sia quindi $y = \psi x'$ con $x' = u' + v'$, $u' \in \operatorname{Ker}\psi$ e $v' \in N$. Allora $y = \psi u + \psi v = \psi v$ e similmente $y = \psi v'$, cosicché $v - v' \in N \cap \operatorname{Ker}\psi = 0$, ovvero $v = v'$.

È chiaro che τ è un omomorfismo. Inoltre

$$\psi\tau y = \psi v = \psi(u + v) = \psi x = y$$

(2) $\Longrightarrow$ (1): Per il lemma 4.6 abbiamo $M = \operatorname{Im}\tau \oplus \operatorname{Ker}\psi$.

Definizione 5.46. (1) Diciamo che una successione esatta $0 \longrightarrow M_1 \xrightarrow{\varphi} M$ *si spezza*, se $\operatorname{Im}\varphi$ è sommando diretto di M.

(2) Diciamo che una successione esatta $M \xrightarrow{\psi} M_2 \longrightarrow 0$ *si spezza*, se $\operatorname{Ker}\psi$ è sommando diretto di M.

Proposizione 5.47. *La successione*

$$0 \longrightarrow M_1 \xrightarrow{\varphi} M \xrightarrow{\psi} M_2 \longrightarrow 0 \qquad (*)$$

sia esatta. Allora sono equivalenti:

(1) La successione (*) si spezza.

(2) $\operatorname{Ker}\psi = \operatorname{Im}\varphi$ *è sommando diretto di* M*.*

(3) Esiste un omomorfismo $\sigma : M \longrightarrow M_1$ *tale che* $\sigma\varphi = \mathrm{id}$.

(4) Esiste un omomorfismo $\tau : M_2 \longrightarrow M$ *tale che* $\psi\tau = \mathrm{id}$.

Dimostrazione. (1) $\Longrightarrow$ (2): La successione (*) si spezzi. Allora esiste un isomorfismo

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & M_1 \arrow[r, "\varphi"] \arrow[d, "f_1"] & M \arrow[r, "\psi"] \arrow[d, "f_2"] & M_2 \arrow[r] \arrow[d, "f_3"] & 0 \arrow[d] \\
0 \arrow[r] & N_1 \arrow[r, "\iota_1"] & N_1 \oplus N_2 \arrow[r, "\pi_2"] & N_2 \arrow[r] & 0
\end{tikzcd}$$

Ponendo $\sigma := f_1^{-1}\pi_1 f_2$ allora $\sigma\varphi = \mathrm{id}$. Per la prop. 5.44 $\operatorname{Ker}\psi = \operatorname{Im}\varphi$ è sommando diretto di M.

(3) $\Longleftrightarrow$ (2) Per la prop. 5.44.

(4) $\Longleftrightarrow$ (2) Per la prop. 5.45.

(3) $\Longrightarrow$ (1): $\operatorname{Ker}\psi$ sia sommando diretto di M. Allora la successione (*) è già nella forma

$$0 \longrightarrow M_1 \cong \operatorname{Im}\varphi \longrightarrow M = \operatorname{Ker}\sigma \oplus \operatorname{Im}\varphi \longrightarrow M_2 \longrightarrow 0$$

Teorema 5.48. *La successione*

$$0 \longrightarrow M_1 \xrightarrow{\varphi} M \xrightarrow{\psi} M_2 \longrightarrow 0 \qquad (*)$$

sia esatta. Allora sono equivalenti:

(1) La successione (*) si spezza.

(2) Per ogni R-modulo X la successione

$$0 \longrightarrow \mathrm{Hom}(X, M_1) \xrightarrow{\varphi_*} \mathrm{Hom}(X, M) \xrightarrow{\psi_*} \mathrm{Hom}(X, M_2) \longrightarrow 0$$

è esatta.

(3) Per ogni R-modulo Y la successione

$$0 \longrightarrow \mathrm{Hom}(M_2, Y) \xrightarrow{\psi^*} \mathrm{Hom}(M, Y) \xrightarrow{\varphi^*} \mathrm{Hom}(M_1, Y) \longrightarrow 0$$

è esatta.

Dimostrazione. (1) $\Longrightarrow$ (2): Per il teorema 5.31 dobbiamo solo dimostrare che ψ_* è suriettivo. Sia $\beta \in \mathrm{Hom}(X, M_2)$. Allora dobbiamo dimostrare che esiste $\alpha \in \mathrm{Hom}(X, M)$ tale che $\beta = \psi\alpha$. Per la prop. 5.47 esiste però τ tale che $\psi\tau = \mathrm{id}_{M_2}$, quindi $\beta = \mathrm{id}_{M_2}\beta = \psi\tau\beta$, cosicché possiamo scegliere $\alpha = \tau\beta$.

(2) $\Longrightarrow$ (1): Consideriamo $X = M_2$. Sia $\mathrm{id} \in \mathrm{Hom}(M_2, M_2)$ allora esiste $\tau \in \mathrm{Hom}(M_2, M)$ tale che $\mathrm{id} = \psi_*\tau = \psi\tau$. Quindi per la prop.5.47 la successione si spezza.

(1) $\Longrightarrow$ (3): Per il teorema 5.32 dobbiamo solo dimostrare che φ^* è suriettivo. Dunque dobbiamo dimostrare che per ogni $\beta \in \mathrm{Hom}(M_1, Y)$ esiste $\alpha \in \mathrm{Hom}(M, Y)$ tale che $\beta = \alpha\varphi$. Per la prop. 5.47 esiste σ tale che $\sigma\varphi = \mathrm{id}_{M_1}$, quindi $\beta = \beta\,\mathrm{id} = \beta\sigma\varphi$, cosicché possiamo supporre $\alpha = \beta\sigma$.

(3) $\Longrightarrow$ (1): Poniamo $Y = M_1$. Sia $\mathrm{id} \in \mathrm{Hom}(M_1, M_1)$. Allora esiste $\sigma \in \mathrm{Hom}(M, M_1)$ tale che $\mathrm{id} = \varphi^*\sigma = \sigma\varphi$. Pertanto per la prop. 5.47 la successione si spezza.

Esempio 5.49. La successione esatta

$$0 \longrightarrow \mathbb{Z} \xrightarrow[x]{\bigcirc\, mx} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/m \longrightarrow 0$$

dalla nota 5.39 non si spezza, perché $\mathrm{Hom}(\mathbb{Z}/m, \mathbb{Z}) = 0$, come sappiamo dal cor. 5.36.

Nota 5.50. La successione esatta

$$0 \longrightarrow M_1 \xrightarrow{\varphi} M \xrightarrow{\psi} M_2 \longrightarrow 0$$

si spezzi. Allora $M \cong M_1 \oplus M_2$.

Dimostrazione. Per la prop. 5.47 esiste un omomorfismo $\tau : M_2 \longrightarrow M$ tale che $\psi\tau = \mathrm{id}$. Siccome φ e τ sono iniettivi, dal lemma 4.6 abbiamo

$$M = \mathrm{Ker}\,\psi \oplus \mathrm{Im}\,\tau = \mathrm{Im}\,\varphi \oplus \mathrm{Im}\,\tau \cong M_1 \oplus M_2$$

6. Moduli proiettivi

Situazione 6.1. Sia R un anello. M, N, P, siano R-moduli.

Definizione 6.2. P si chiama *proiettivo*, se ogni successione esatta $M \longrightarrow P \longrightarrow 0$ si spezza.

Proposizione 6.3. *Siano dati un modulo libero L e un diagramma*

$$\begin{tikzcd} & L \arrow[d, "\alpha"] & \\ M \arrow[r, "\varphi"] & M_2 \arrow[r] & 0 \end{tikzcd}$$

in cui la riga è esatta. Allora esiste un omomorfismo $\beta : L \longrightarrow M$ che rende commutativo il diagramma

$$\begin{tikzcd} & L \arrow[dl, "\beta"'] \arrow[d, "\alpha"] \\ M \arrow[r, "\varphi"] & M_2 \end{tikzcd}$$

<u>Dimostrazione.</u> Sia E una base di L. Per la suriettività di φ per ogni $e \in E$ esiste $x_e \in M$ tale che $\varphi x_e = \alpha e$. Usando l'assioma della scelta possiamo definire un'applicazione $\beta_0 := \bigcirc_e x_e : E \longrightarrow M$. Per la prop. 3.33 esiste un (unico) omomorfismo $\beta : L \longrightarrow M$ tale che $\beta_{|E} = \beta_0$. Pertanto $\varphi\beta e = \varphi x_e = \alpha e$ per ogni $e \in E$ e quindi $\varphi\beta = \alpha$.

Teorema 6.4. *P è proiettivo se e solo se per ogni diagramma di R-moduli*

$$\begin{tikzcd} & P \arrow[d, "\alpha"] & \\ M \arrow[r, "\varphi"] & M_2 \arrow[r] & 0 \end{tikzcd}$$

in cui la riga è esatta, esiste un omomorfismo $\beta : P \longrightarrow M$ che rende commutativo il diagramma

$$\begin{tikzcd} & P \arrow[dl, "\beta"'] \arrow[d, "\alpha"] \\ M \arrow[r, "\varphi"] & M_2 \end{tikzcd}$$

<u>Dimostrazione.</u> (1) P sia proiettivo. Per la prop 3.34 esistono un modulo libero L e una successione esatta $L \xrightarrow{\theta} P \longrightarrow 0$. Quest'ultima si spezza, perché P è proiettivo. Esiste quindi un omomorfismo $\tau : P \longrightarrow L$ tale che $\sigma\tau = \mathrm{id}$. Considerando il diagramma

$$\begin{tikzcd} L \arrow[r, "\theta"] & P \arrow[d, "\alpha"'] & \\ M \arrow[r, "\varphi"] & M_2 \arrow[r] & 0 \end{tikzcd}$$

vediamo dalla prop. 6.3 che esiste un omomorfismo $\gamma : L \longrightarrow M$ tale che $\varphi\gamma = \alpha\theta$. In tutto abbiamo allora un diagramma commutativo

$$\begin{tikzcd}
 & P \arrow[dl, "\tau"'] \arrow[d, "\mathrm{id}"] \\
L \arrow[r, "\theta"] \arrow[d, "\gamma"'] & P \arrow[d, "\alpha"] \\
M \arrow[r, "\varphi"] & M_2
\end{tikzcd}$$

da cui otteniamo un omomorfismo $\beta = \gamma\tau$.

Infine $\varphi\beta = \varphi\gamma\tau = \alpha\theta\tau = \alpha\,\mathrm{id} = \alpha$.

(2) P abbia la proprietà richiesta. Sia $M \xrightarrow{\varphi} P \longrightarrow 0$ una successione esatta. Per ipotesi possiamo completare il diagramma

$$\begin{tikzcd}
 & P \arrow[d, "\mathrm{id}"] & \\
M \arrow[r, "\varphi"] & P \arrow[r] & 0
\end{tikzcd}$$

con un omomorfismo $\tau : P \longrightarrow M$ tale che $\varphi\tau = \mathrm{id}$. Ciò significa proprio che la successione esatta $M \xrightarrow{\varphi} P \longrightarrow 0$ si spezza.

Corollario 6.5. *Ogni modulo libero è proiettivo.*

Teorema 6.6. *Sono equivalenti:*

(1) P è proiettivo.

(2) P è isomorfo a un sommando diretto di ogni R-modulo di cui è immagine omomorfa.

(3) P è sommando diretto di un modulo libero.

Dimostrazione. (1) $\Longrightarrow$ (2): Siano P proiettivo e $M \xrightarrow{\psi} P \longrightarrow 0$ una successione esatta di R-moduli. Per ipotesi esiste un omomorfismo $\tau : P \longrightarrow M$ tale che $\varphi\tau = \mathrm{id}$. τ è perciò iniettivo quindi $P \cong \mathrm{Im}\,\tau$ e per il lemma 4.6 $M = \mathrm{Im}\,\tau \oplus \mathrm{Ker}\,\varphi$. Pertanto P è isomorfo a un sommando diretto di M.

(2) $\Longrightarrow$ (3): Per la prop 3.34 P è immagina omomorfa di un modulo libero L e per ipotesi è isomorfo a un sommando diretto di L.

(3) $\Longrightarrow$ (1): Sia N un R-modulo tale che $L := P \oplus N$ sia libero. Allora il diagramma

$$\begin{tikzcd}
L \arrow[r, "\pi_1"] & P \\
P \arrow[u, "i_1"] \arrow[ur, "\mathrm{id}"'] &
\end{tikzcd}$$

è commutativo. Infatti per $x \in P$ si ha $\pi_1 i_1 x = \pi_1(x, 0) = x$. Sia ora $M \xrightarrow{\varphi} P \longrightarrow 0$ una successione esatta di R-moduli. Per la prop. 6.3 esiste un omomorfismo $\gamma : L \longrightarrow M$ con $\varphi\gamma = \pi_1$, cosicché otteniamo un diagramma commutativo

$$
\begin{tikzcd}
 & M \arrow[d, "\varphi"] \\
L \arrow[ur, "\gamma"] \arrow[r, "\pi_1"] & P \\
P \arrow[u, "i_1"] \arrow[ur, "\mathrm{id}"'] &
\end{tikzcd}
$$

Sia $\tau := \gamma i_1$. Allora $\varphi\tau = \varphi\gamma i_1 = \pi_1 i_1 = \mathrm{id}$.

Corollario 6.7. *Ogni sommando diretto di un R-modulo proiettivo è proiettivo.*

Corollario 6.8. *Sia I un insieme e per ogni $i \in I$ sia dato un R-modulo M_i. Allora $\bigoplus\limits_{i\in I} M_i$ è proiettivo se e solo se ogni sommando M_i è proiettivo.*

Esempio 6.9. $\mathbb{Z}/2$ non è proiettivo come $\mathbb{Z}$-modulo.

Dimostrazione. Consideriamo l' omomorfismo di proiezione $\varphi = \bigcirc\limits_{x} x\%2 : \mathbb{Z}/4 \longrightarrow \mathbb{Z}/2$. L'omomorfismo φ è suriettivo, ma $\mathbb{Z}/2$ non è sommando diretto di $\mathbb{Z}/4$. Quindi per il teorema 6.6 $\mathbb{Z}/2$ non è proiettivo.

Corollario 6.10. *Sia e un idempotente di R. Allora Re è un R-modulo proiettivo.*

Dimostrazione. Infatti $R = Re \oplus R(1-e)$, cosicché Re è sommando diretto del modulo libero R.

Osservazione 6.11. R sia algebricamente finito ed e un idempotente di R con $e \neq 0, 1$.

Allora l'R-modulo Re (proiettivo per la prop 6.10) non è libero.

Dimostrazione. Re sia libero. Siccome è finitamente generato, per la prop.3.34 deve esistere $n \in \mathbb{N}+1$ tale che $Re \cong R^n$. Ciò implica

$$R = Re \oplus R(1-e) \cong R^n \oplus R(1-e) \cong R \oplus (R^{n-1} \oplus (1-e)R)$$

Siccome $R^n \oplus R(e-1) \neq 0$ (anche per $n = 1$), ciò contraddice l'ipotesi che R sia algebricamente finito, come si vede dalla prop. 4.7.

Proposizione 6.12 (trucco di Eilenberg). *Sia P proiettivo. Allora esiste un R-modulo libero L tale che $P \oplus L \cong L$.*

Dimostrazione. Per il teorema 6.6 esiste un R-modulo Q tale che $E := P \oplus Q$ è libero. Per ogni $n \in \mathbb{N}$ sia $F_n := E$. Poniamo $L := \bigoplus_{n\in\mathbb{N}} F_n$. Ma allora per l'associatività della somma diretta

$$
\begin{aligned}
P \oplus L &= P \oplus (N \oplus P) \oplus (N \oplus P) \oplus \ldots \\
&\cong (P \oplus N) \oplus (P \oplus N) \oplus \ldots \cong E \oplus E \oplus E \ldots = L.
\end{aligned}
$$

Definizione 6.13. Una famiglia $\bigcirc\limits_{i\in I} \alpha_i$ con $\alpha_i \in \mathrm{Hom}_R(M, N)$ per ogni i si dice *puntualmente finita*, se per ogni $x \in M$ l'insieme $\{i \in I \mid \alpha_i(x) \neq 0\}$ è finito.

Proposizione 6.14. *Sono equivalenti:*

(1) P proiettivo.

(2) Esistono un insieme I e per ogni $i \in I$ un elemento $e_i \in P$ e un elemento $\alpha_i \in \mathrm{Hom}_R(P,R)$ tali che la famiglia $\bigcirc_{i\in I} \alpha_i$ sia puntualmente finita e per ogni $x \in P$ si abbia $x = \sum_{i\in I} \alpha_i(x)e_i$.

<u>Dimostrazione.</u> (1) $\Longrightarrow$ (2): Siano F un R-modulo libero e $g : F \longrightarrow P$ un omomorfismo tale che $g := \bigcirc_{a_i} e_i$ per ogni $i \in I$ e $F := \bigoplus a_i R$. Essendo P proiettivo esiste un omomorfismo $h : P \longrightarrow F$ tale che $h(x) = \sum_{i\in I} \alpha_i(x)a_i$ per ogni $x \in P$. Applicando g abbiamo $a = gh(a) = \sum_{i\in I} \alpha_i(x)e_i$ dove $a_i := g(e_i) \in P$.

(2) $\Longrightarrow$ (1): Siano F un R-modulo libero e $g : F \longrightarrow P$ un omomorfismo tali che $g := \bigcirc_{a_i} e_i$ per ogni $i \in I$ e $F := \bigoplus a_i R$. Allora esiste un omomorfismo $h : P \longrightarrow F$ tale che $h(x) = \sum_{i\in I} \alpha(x)a_i$. Ciò implica che P è isomorfo a un sommando diretto di F quindi P è proiettivo.

Nota 6.15. Siano $R := C([0,1],\mathbb{R})$ e $P := \{f \in R \mid \text{ esiste } \varepsilon > 0 \text{ tale che } [0,\varepsilon] \subset (f = 0)\}$. Allora P è un ideale dell'anello commutativo R e come R-modulo possiede le seguenti proprietà :

(1) P non è finitamente generato.

(2) P non è libero.

(3) P è proiettivo.

<u>Dimostrazione.</u> (1) P non è finitamente generato perché altrimenti esisterebbe $\varepsilon > 0$ tale che $[0,\varepsilon] \subset (f = 0)$ per ogni $f \in P$ e ciò evidentemente non è vero.

(2) P non è libero, perché se $f \in R$ è tale che $[0,\varepsilon] \subset (f = 0)$, allora possiamo trovare una funzione continua $g \in R$ con $g \neq 0$ tale che $(g = 0, \mathrm{in}[0, \varepsilon/2])$ e quindi $fg = 0$.

(3) La dimostrazione della proiettività di P si trova in Lam, pag. 26.

Teorema 6.16. *Sono equivalenti:*

(1) P è proiettivo.

(2) Il funtore $\mathrm{Hom}_R(P,-)$ è esatto, cioè per ogni successione esatta

$$0 \longrightarrow M_1 \xrightarrow{\varphi} M \xrightarrow{\psi} M_2 \longrightarrow 0$$

la successione di gruppi abeliani

$$0 \longrightarrow \mathrm{Hom}(P,M_1) \xrightarrow{\varphi_*} \mathrm{Hom}(P,M) \xrightarrow{\psi_*} \mathrm{Hom}(P,M_2) \longrightarrow 0$$

è esatta.

<u>Dimostrazione.</u> (1) $\Longrightarrow$ (2): Per il teorema 5.31 non resta che dimostrare la suriettività di ψ^*. Sia $\alpha \in \mathrm{Hom}(P,M_2)$. Per il teorema 6.4

esiste $\beta \in \mathrm{Hom}(P, M)$ tale che il diagramma

$$\begin{tikzcd} & P \arrow[dl, "\beta"'] \arrow[d, "\alpha"] \\ M \arrow[r, "\psi"] & M_2 \end{tikzcd}$$

sia commutativo e ciò significa proprio che $\alpha = \psi_* \beta$.

(2) $\Longrightarrow$ (1): Si può usare lo stesso ragionamento.

Osservazione 6.17. La successione $0 \longrightarrow M_1 \longrightarrow M \longrightarrow P \longrightarrow 0$ sia esatta e P proiettivo. Allora $M \cong M_1 \oplus P$.

Dimostrazione. Essendo P proiettivo, per la prop. 5.47 la successione si spezza e quindi per la nota 5.50 $M \cong M_1 \oplus P$.

Lemma 6.18 (lemma di Schanuel). *Sia dato un diagramma*

$$\begin{tikzcd} 0 \arrow[r] & E \arrow[r, "\alpha"] & P \arrow[r, "\beta"] & N \arrow[r] \arrow[d, "\mathrm{id}"'] & 0 \\ 0 \arrow[r] & F \arrow[r] & Q \arrow[r] & N \arrow[r] & 0 \end{tikzcd}$$

con le righe esatte in cui P è proiettivo. Allora:

(1) Esistono omomorfismi $\mu : P \longrightarrow Q$ e $\lambda : E \longrightarrow F$ tali che il diagramma

$$\begin{tikzcd} 0 \arrow[r] & E \arrow[r, "\alpha"] \arrow[d, "\lambda"'] & P \arrow[r, "\beta"] \arrow[d, "\mu"'] & N \arrow[r] \arrow[d, "\mathrm{id}"'] & 0 \\ 0 \arrow[r] & F \arrow[r, "\gamma"] & Q \arrow[r, "\delta"] & N \arrow[r] & 0 \end{tikzcd}$$

sia commutativo.

(2) La successione

$$0 \longrightarrow E \xrightarrow{\varphi} P \oplus F \xrightarrow{\psi} Q \longrightarrow 0$$

in cui

$$\varphi e := (\alpha e, \lambda e)$$
$$\psi(p, f) := \mu p - \gamma f$$

è esatta.

(3) Se anche Q è proiettivo, allora $P \oplus F \cong Q \oplus E$.

Dimostrazione. (1) L'omomorfismo μ esiste perché P è proiettivo, λ esiste per il lemma 5.28.

(2) È chiaro che φ e ψ sono omomorfismi.

(2a) Sia $\varphi e = 0$. Allora $\alpha e = 0$ e quindi $e = 0$ perché α è iniettivo .

(2b) $\psi\varphi e = \psi(\alpha e, \lambda e) = \mu\alpha e - \gamma\lambda e = 0$.

(2c) Sia $\psi(p, f) = 0$, cioè $\mu p = \gamma f$. Allora $\beta p = \delta\mu p = \delta\gamma f = 0$. Perciò esiste $e \in E$ tale che $\alpha e = p$. Pertanto $\gamma f = \mu p = \mu\alpha e = \gamma\lambda e$ e quindi $f = \lambda e$ perché γ è iniettivo. Perciò $(p, f) = (\alpha e, \lambda e) = \varphi e$.

(2d) Sia $q \in Q$. Allora esiste $p \in P$ tale che $\delta q = \beta p = \delta\mu p$. Quindi $q - \mu p \in \operatorname{Ker}\delta = \operatorname{Im}\gamma$, per cui esiste $f \in F$ tale che $q - \mu p = \gamma f$. Pertanto $q = \mu p + \gamma f = \psi(p, -f)$.

(3) Ciò segue dall'oss. 6.17.

7. Moduli iniettivi

Situazione 7.1. Sia R un anello. M, N, Q, $\ldots$ siano R-moduli.

Definizione 7.2. Q si chiama *iniettivo*, se ogni successione esatta $0 \longrightarrow Q \longrightarrow M$ si spezza.

Definizione 7.3. Un diagramma commutativo di R-moduli

$$\begin{tikzcd} M_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"] & M \arrow[d, "\gamma"] \\ N_1 \arrow[r, "\psi"] & N \end{tikzcd}$$

si chiama un *pushout*, se per ogni R-modulo T ed ogni coppia di omomorfismi f, g per i quali il diagramma

$$\begin{tikzcd} M_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"] & M \arrow[d, "g"] \\ N_1 \arrow[r, "f"] & T \end{tikzcd}$$

è commutativo, esiste un unico omomorfismo $h : N \longrightarrow T$ che rende commutativo il diagramma

$$\begin{tikzcd} M_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"] & M \arrow[d, "\gamma"] \arrow[ddr, "g"] & \\ N_1 \arrow[r, "\psi"] \arrow[drr, "f"'] & N \arrow[dr, "h"] & \\ & & T \end{tikzcd}$$

Proposizione 7.4. *Dati due omomorfismi di R-moduli*

$$\begin{tikzcd} M_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"] & M \\ N_1 & \end{tikzcd}$$

definiamo

$$U := \{(\alpha x, -\varphi x) \mid x \in M_1\}$$
$$N := (N_1 \oplus M)/U$$
$$\psi := \bigcirc_v (v, 0) + U : N_1 \longrightarrow N$$
$$\gamma := \bigcirc_w (0, w) + U : M \longrightarrow N$$

Allora il diagramma

$$\begin{tikzcd} M_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"] & M \arrow[d, "\gamma"] \\ N_1 \arrow[r, "\psi"] & N \end{tikzcd}$$

è un pushout.

<u>Dimostrazione.</u> (1) È chiaro che U è un sottomodulo di $N_1 \oplus M$, quindi N è ben definito.

(2) Dimostriamo che il diagramma è commutativo. Sia $x \in M_1$. Allora

$\gamma\varphi x = (0, \varphi x) + U$
$\psi\alpha x = (\alpha x, 0) + U$

per cui $\psi\alpha x - \gamma\varphi x = (\alpha x, -\varphi x) + U = 0$.

Sia dato un diagramma commutativo

$$\begin{tikzcd} M_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"] & M \arrow[d, "g"] \\ N_1 \arrow[r, "f"] & T \end{tikzcd}$$

Allora definiamo $h : N \longrightarrow T$ ponendo $h((v, w) + U) := fv + gw$.

(3) Dimostriamo che h è ben definita:

Sia $(v', w') + U = (v, w) + U$. Allora esiste $x \in M_1$ tale che $v' = v + \alpha x$, $w' = w - \varphi x$. Perciò $fv' + gw' = fv + f\alpha x + gw - g\varphi x = fv + gw$.

(4) È chiaro che h è un omomorfismo. Inoltre

$h\psi v = h((v, 0) + U) = fv$

$h\gamma w = h((0, w) + U) = gw$

(5) Dobbiamo ancora dimostrare che l'omomorfismo h costruito nel punto (2) è univocamente determinato. Ma se $k : N \longrightarrow T$ e un omomorfismo tale che $k\psi = f$, $k\gamma = g$, allora necessariamente

$$\begin{aligned} k((v, w) + U) &= k(((v, 0) + U) + ((0, w) + U)) \\ &= k(\psi v + \gamma w) \\ &= k\psi v + k\gamma w = fv + gw \end{aligned}$$

Lemma 7.5. *Il diagramma*

$$\begin{tikzcd} M_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"] & M \arrow[d, "\gamma"] \\ N_1 \arrow[r, "\psi"] & N \end{tikzcd}$$

sia un pushout.

Se φ è iniettivo, allora anche ψ è iniettivo.

<u>Dimostrazione.</u> Siccome due pushout per φ e α sono isomorfi (come si verifica facilmente), è sufficente dimostrare l'enunciato per il pushout standard costruito nella prop. 7.4. Usiamo le notazioni di quella prop.

Sia $\psi v = 0$. Ciò significa $(v, 0) + U = 0$, ovvero $(v, 0) = (\alpha x, -\alpha x)$ per un $x \in M_1$. Ma allora $\varphi x = 0$ e quindi $x = 0$ perché φ è iniettivo. Ciò implica $v = \alpha x = 0$.

Teorema 7.6. *Q è iniettivo se e solo se per ogni R-modulo*

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & M \\ & Q & \end{tikzcd}$$

in cui la riga è esatta, esiste un omomorfismo $\beta : M \longrightarrow Q$ che rende commutativo il diagramma

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & M \arrow[dl, "\beta"] \\ & Q & \end{tikzcd}$$

Dimostrazione. (1) Q sia iniettivo. Per ogni diagramma

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & M \\ & Q & \end{tikzcd}$$

in cui la prima riga è esatta, esistono per la prop. 7.4 ψ e γ tali che il seguente diagramma è commutativo ed è un pushout:

$$\begin{tikzcd} M_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"] & M \arrow[d, "\gamma"] \\ Q \arrow[r, "\psi"] & N \end{tikzcd}$$

Inoltre φ è iniettivo, quindi per il lemma 7.5 anche ψ è iniettivo, pertanto essendo Q iniettivo esiste un omomorfismo $\sigma : N \longrightarrow Q$ tale che $\sigma\psi = \mathrm{id}$. Definiamo ora $\beta = \sigma\gamma$ e vediamo che $\beta\varphi = \sigma\gamma\varphi = \sigma\psi\alpha = \alpha$.

(2) Q abbia la proprietà richiesta. Sia $0 \longrightarrow Q \xrightarrow{\varphi} M$ una successione esatta. Allora nel diagramma

$$\begin{tikzcd} 0 \arrow[r] & Q \arrow[r, "\varphi"] \arrow[d, "\mathrm{id}"'] & M \\ & Q & \end{tikzcd}$$

per ipotesi esiste un omomorfismo $\sigma : M \longrightarrow Q$ tale che $\sigma\varphi = \mathrm{id}$.

Osservazione 7.7. La successione $0 \longrightarrow Q \longrightarrow M \longrightarrow M_2 \longrightarrow 0$ sia esatta e Q sia iniettivo. Allora $M \cong Q \oplus M_2$.

Dimostrazione. Essendo Q iniettivo la successione si spezza e l'enunciato segue dalla nota 5.50.

Proposizione 7.8. *Sono equivalenti:*

(1) Q è iniettivo.

(2) Q è sommando diretto di ogni R-modulo di cui è sottomodulo.

Dimostrazione. (1) $\Longrightarrow$ (2): Q sia iniettivo e sottomodulo di un R-modulo M. Sia $Q \xrightarrow{i} M$ l'inclusione. Siccome Q è iniettivo esiste un omomorfismo $\sigma : M \longrightarrow Q$ tale che $\sigma i = \mathrm{id}$. Per il lemma 4.6 allora $N = \mathrm{Im}\, i \oplus \mathrm{Ker}\, \sigma = Q \oplus \mathrm{Ker}\, \sigma$.

(2) $\Longrightarrow$ (1): La successione $0 \longrightarrow Q \xrightarrow{\varphi} M$ sia esatta.
Sia $N := Q \cup (M \setminus \mathrm{Im}\, \varphi)$ il modulo che si ottiene sostituendo ogni elemento φx con x e ridefinendo in modo ovvio le operazioni algebriche. Sia
$\bar{\varphi} := \bigcirc_x \varphi x : Q \longrightarrow N$. Per ipotesi Q è sommando diretto di N, per cui esiste un omomorfismo $\sigma : N \longrightarrow Q$ tale che $\sigma\bar{\varphi} = \mathrm{id}$. Ma ciò significa semplicemente $\sigma\varphi = \mathrm{id}$.

Teorema 7.9. *Sono equivalenti:*

(1) Q è iniettivo.

(2) Il funtore controvariante $\mathrm{Hom}_R(-, Q)$ è esatto, cioè per ogni successione esatta

$$0 \longrightarrow M_1 \xrightarrow{\varphi} M \xrightarrow{\psi} M_2 \longrightarrow 0$$

la successione di gruppi abeliani

$$0 \longrightarrow \mathrm{Hom}(M_2, Q) \xrightarrow{\psi^*} \mathrm{Hom}(M, Q) \xrightarrow{\varphi^*} \mathrm{Hom}(M_1, Q) \longrightarrow 0$$

è esatta.

Dimostrazione. (1) $\Longrightarrow$ (2): Per il teorema 5.32 dobbiamo solo dimostrare che φ^* è suriettivo. Sia $\alpha \in \mathrm{Hom}(M_1, Q)$. Per il teorema 7.6 esiste allora $\beta \in \mathrm{Hom}(M, Q)$ tale che $\beta\varphi = \alpha$, ovvero $\alpha = \varphi^*\beta$.

(2) $\Longrightarrow$ (1): Si può usare lo stesso ragionamento.

Esempio 7.10. $\mathbb{Z}$ non è iniettivo (come $\mathbb{Z}$-modulo). Ciò mostra che un modulo libero non è necessariamente iniettivo.

Dimostrazione. Consideriamo l'applicazione $\varphi := \bigcirc_a ma : \mathbb{Z} \longrightarrow m\mathbb{Z}$, un omomorfismo iniettivo di gruppi abeliani. Non esiste però nessun omomorfismo $\sigma : m\mathbb{Z} \longrightarrow \mathbb{Z}$ tale che $\sigma\varphi = \mathrm{id}$. Infatti in tal caso si avrebbe $a = \sigma(ma) = m\sigma a$ per ogni $a \in \mathbb{Z}$. Ma ciò implicherebbe $m \mid a$ per ogni $a \in \mathbb{Z}$, una contraddizione.

Osservazione 7.11. Q è iniettivo se e solo se per ogni R-modulo M, ogni sottomodulo M_1 di M ed ogni omomorfismo $\alpha : M_1 \longrightarrow Q$ esiste un omomorfismo $\beta : M \longrightarrow Q$ tale che $\beta_{|M_1} = \alpha$.

Definizione 7.12. Siano M_1 un sottomodulo di M ed $\alpha : M_1 \longrightarrow Q$ un omomorfismo. *Un' estensione parziale* di α ad M è una coppia (H, β) tale che H è un sottomodulo di M con $M_1 \subset H$ e $\beta : H \longrightarrow Q$ è un omomorfismo tale che $\beta_{|M_1} = \alpha$.

Denotiamo con $\mathrm{Estp}(\alpha, M)$ l'insieme di tutte le estensioni parziali di α ad M.

Osservazione 7.13. Nella situazione della def. 7.12 l'insieme $\mathrm{Estp}(\alpha, M)$ diventa un insieme quasi ordinato se definiamo

$(H, \beta) \leq (K, \gamma)$: $\Longleftrightarrow$ $H \subset K$ e $\gamma_{|H} = \beta$

L'insieme $\mathrm{Estp}(\alpha, M)$ non è vuoto perché contiene (M_1, α).

Si verifica facilmente che sono soddisfatte le ipotesi del lemma di Zorn, perciò per ogni $(H, \beta) \in \mathrm{Estp}(\alpha, M)$ esiste un elemento massimale (K, γ) di $\mathrm{Estp}(\alpha, M)$ con $(H, \beta) \leq (K, \gamma)$.

Teorema 7.14 (criterio di Baer). *Sono equivalenti:*

(1) Q è iniettivo.

(2) Per ogni ideale sinistro I di R ed ogni omomorfismo di R-moduli $\alpha : I \longrightarrow Q$ esiste un omomorfismo di R-moduli $\beta : R \longrightarrow Q$ tale che $\beta_{|I} = \alpha$.

Dimostrazione. Seguiamo Rotman, pag. 118-119.

(1) $\Longrightarrow$ (2): Chiaro.

(2) $\Longrightarrow$ (1): Ci poniamo nella situazione della definizione 7.12. Sia (K, γ) un elemento massimale di $\mathrm{Estp}(\alpha, M)$ tale che $(H, \beta) \leq (K, \gamma)$. È sufficiente dimostrare che $K = M$. Assumiamo per assurdo che $K \neq M$.

Sia $x \in M \setminus K$ e $I := \{r \in R \mid rx \in K\}$. I è chiaramente un ideale sinistro di R. Sia $f : I \longrightarrow Q$ dato da $f(r) := \gamma(rx)$. Per ipotesi esiste $f^* : R \longrightarrow Q$ tale che $f^* i = f$.

Infine definiamo $K' = K + Rx$ e $\gamma' : K' \longrightarrow Q$ tale che $\gamma'(y + rx) = \gamma y + r f^*(1)$ con $y \in K$. Mostriamo che γ' è ben definita. Siano $y + rx = y' + r'x$; allora $(r - r')x = y' - y \in K$ e $r - r' \in I$ e quindi abbiamo $\gamma(y' - y) = \gamma((r - r')x) = f(r - r') = f^*(r - r') = (r - r')f^*(1)$, cioè $\gamma(y') - \gamma(y) = r f^*(1) - r' f^*(1)$ e quindi $\gamma(y') + r' f^*(1) = \gamma(y) + r f^*(1)$.

Chiaramente però $\gamma'(y) = \gamma(y)$ e quindi $(K, \gamma) \leq (K', \gamma')$ ma ciò è assurdo perchè (K, γ) è elemento massimale, mentre $K' \neq K$ perché $x \notin K$. Perciò $K = M$.

Lemma 7.15. *Un prodotto diretto di R-moduli iniettivi (di una famiglia arbitraria di fattori) è iniettivo.*

Dimostrazione. Siano $0 \longrightarrow M_1 \xrightarrow{\varphi} M$ una successione esatta e $\prod_{k \in K} Q_k$ una prodotto diretto di R-moduli iniettivi tali che si abbia il seguente diagramma

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & M \\ & \prod_{k \in K} Q_k & \end{tikzcd}$$

Consideriamo ora la proiezione $\pi_k : \prod_{k \in K} Q_k \longrightarrow Q_k$. Q_k è iniettivo, quindi esiste un omomorfismo $\beta_k : M \longrightarrow Q_k$ tale che $\beta_k \varphi = \pi_k \alpha$. Pertanto (per la definizione del prodotto diretto) esiste, univocamente determinato, un omomorfismo $\beta : M \longrightarrow \prod_{k \in K} Q_k$ come nel diagramma

$$\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r, "\varphi"] \arrow[d, "\alpha"] & M \arrow[dl, "\beta"'] \arrow[d, "\beta_k"] \\
 & \prod\limits_{k\in K} Q_k \arrow[r, "\pi_k"] & Q_k
\end{tikzcd}$$

Corollario 7.16. *La somma diretta di un numero finito di R-moduli iniettivi è iniettiva.*

<u>Dimostrazione.</u> Ciò segue dal lemma 7.15, perché la somma diretta di un numero finito di moduli coincide con il prodotto diretto.

Proposizione 7.17. *Siano R un anello noetheriano a sinistra e $\bigcirc\limits_{\lambda\in\Lambda} M_\lambda$ una famiglia di R-moduli, tutti iniettivi. Allora $\bigoplus\limits_{\lambda\in\Lambda} M_\lambda$ è iniettivo.*

<u>Dimostrazione.</u> Per il teorema 7.11 è sufficiente dimostrare che, dato il diagramma

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r, "i"'] \arrow[d, "\alpha"] & R \\
 & \bigoplus\limits_{\lambda\in\Lambda} M_\lambda &
\end{tikzcd}$$

dove I è un ideale sinistro di R, esiste un omomorfismo $g : R \longrightarrow \bigoplus\limits_{\lambda\in\Lambda} M_\lambda$ che rende commutativo il diagramma.

Per $x = \bigcirc\limits_{\lambda} x_\lambda \in \bigoplus\limits_{\lambda\in\Lambda} M_\lambda$ definiamo il supporto

$$\mathrm{Supp}(x) := \{\lambda \in \Lambda \mid x_\lambda \neq 0\}$$

un insieme finito. Essendo R noetheriano, I è finitamente generato, ad esempio $I = \{a_1, \ldots, a_n\}$. Anche l'insieme $S = \bigcup\limits_{j=1}^{n} \mathrm{Supp}(\alpha a_j)$ è finito e quindi $\mathrm{Im}\,\alpha \subset \bigoplus\limits_{s\in S} M_s$ è iniettivo per il cor. 7.16. Esiste quindi un R-omomorfismo $\gamma : R \longrightarrow \bigoplus\limits_{s\in S} M_s$ che composto con l'inclusione $\bigoplus\limits_{s\in S} M_s \longrightarrow \bigoplus\limits_{\lambda\in\Lambda} M_\lambda$ dà l'omomorfismo richiesto.

Proposizione 7.18. *R sia un anello integro. Allora:*

(1) $\mathcal{K}(R)$ è un R-modulo iniettivo.

(2) Ogni spazio vettoriale su $\mathcal{K}(R)$ è un R-modulo iniettivo.

<u>Dimostrazione.</u> È sufficiente dimostrare il punto (2).

(2) Siano E una spazio vettoriale su $\mathcal{K}(R)$ ed I un ideale di R. Sia $\alpha : I \longrightarrow E$ un omomorfismo di R-moduli tale che per ogni $a \in I$, $a \neq 0$, esiste $e_a \in E$ con $\alpha a = ae_a$. Dimostriamo ora che $e_a = e_b$ per ogni $a, b \in I \setminus 0$.

Abbiamo $\alpha ab = a\alpha b = abe_b$ e similmente $\alpha ba = bae_a$. Ma R è commutativo, quindi $\alpha ab = \alpha ba$ e pertanto $abe_b = abe_a$, cioè $ab(e_a - e_b) = 0$. Ma

R è integro, perciò , essendo $ab \neq, 0$ allora $e_a - e_b = 0$ e quindi $e_a = e_b$.

Sia ora $\beta : R \longrightarrow E$ tale che $\beta r = r\beta 1 = re_a$ per un qualche $a \in I$, $a \neq 0$. Allora β è un' estensione di α e quindi per il teorema 7.14 E è iniettivo.

Definizione 7.19. M si dice *divisibile*, se per ogni $a \in R$ ed ogni omomorfismo di R-moduli $Ra \xrightarrow{\alpha} M$ esiste un omomorfismo di R-moduli $\beta : R \longrightarrow M$ tale che $\beta_{|Ra} = \alpha$.

Osservazione 7.20. Ogni modulo iniettivo è divisibile.

Proposizione 7.21. *R sia un dominio. Allora sono equivalenti:*

(1) M è divisibile.

(2) Per ogni $x \in M$ per ogni $a \in R \setminus 0$ esiste $y \in M$ tale che $x = ay$.

(3) Per ogni $a \in R \setminus 0$ si ha $M = aM$.

Dimostrazione. (1) $\Longrightarrow$ (2): Siano $x \in M$ e $a \in R \setminus 0$. Consideriamo l'applicazione $\alpha : Ra \longrightarrow M$ tale che $\alpha(ra) = rx$. Siccome R è un dominio, l'applicazione α è ben definita. È chiaro che α è un omomorfismo di R-moduli. Essendo M divisibile esiste un omomorfismo $\beta : R \longrightarrow M$ tale che $\beta_{|aR} = \alpha$. Sia $y := \beta 1$. Allora $ay = a\beta 1 = \beta a = x$.

(2) $\Longrightarrow$ (1): La condizione nel punto (2) sia soddisfatta ed $\alpha : Ra \longrightarrow M$ un omomorfismo. Possiamo assumere $a \neq 0$, perché altrimenti $Ra = 0$ e possiamo scegliere $\beta = 0$. Per ipotesi esiste $y \in M$ tale che $\alpha a = ay$. Definiamo $\beta : R \longrightarrow M$ ponendo $\beta b := by$. È chiaro che β è un omomorfismo. Rimane da dimostrare che $\beta_{|Ra} = \alpha$. Però $\beta ba = bay = b\alpha a = \alpha ba$ per ogni $b \in R$.

(2) $\Longleftrightarrow$ (3): Chiaro.

Osservazione 7.22. R sia un dominio. Allora:

(1) Ogni somma diretta di R-moduli divisibile è divisibile.

(2) Ogni prodotto diretto di R-moduli divisibile è divisibile.

Proposizione 7.23. *R sia un dominio. Siano Q divisibile e $\varphi : Q \longrightarrow M$ un omomorfismo suriettivo. Allora anche M è divisibile.*

Dimostrazione. Siano $x \in M$ e $a \in R \setminus 0$. Per ipotesi esistono $v \in Q$ con $x = \varphi v$ e $w \in Q$ tale che $v = aw$. Allora $x = \varphi v = \varphi aw = a\varphi w$.

Proposizione 7.24. *Un modulo su un dominio ad ideali principali e' iniettivo se e solo se e' divisibile.*

Dimostrazione. Siano R un dominio ad ideali principali e M un modulo su R.

(1) Se M è iniettivo, allora M è divisibile per l'oss. 7.20.

(2) Sia M divisibile. Siano I un ideale di R ed $\alpha : I \longrightarrow M$ un omomorfismo. Per ipotesi $I = Ra$ per un qualche $a \in R$. Possiamo assumere $a \neq 0$. Siccome M è divisibile, esiste $x \in M$ tale che $\alpha a = ax$. L'applicazione $\beta := \bigcirc_{r} rx : R \longrightarrow M$ è un omomorfismo. Per un elemento

$s = ra \in I$ abbiamo infine $\beta s = \beta ra = r\beta a = rax = sx = \alpha s$. Quindi β è un'estensione di α e per il teorema 7.14 M è iniettivo.

Proposizione 7.25. *R sia un dominio ad ideali principali. Siano Q un R-modulo iniettivo ed N un sottomodulo di Q. Allora Q/N è iniettivo.*

Dimostrazione. Per l'oss. 7.19 Q è divisibile, pertanto anche Q/N è divisibile per la prop. 7.23. Dalla prop. 7.24 segue che Q/N è iniettivo.

Corollario 7.26. *Un gruppo abeliano è iniettivo se e solo se è divisibile.*

Corollario 7.27. *Siano D un gruppo abeliano divisibile ed N un sottogruppo di D. Allora D/N è divisibile.*

Proposizione 7.28. *Ogni gruppo abeliano è sottogruppo di un gruppo abeliano iniettivo.*

Dimostrazione. Sia G un gruppo abeliano. Per la prop. 3.34 esistono un gruppo abeliano libero F e un sottogruppo K di F tale che $G = F/K$. F può essere scritto nella forma $F = \mathbb{Z}^{\underline{X}}$ per qualche insieme X. Allora $G = F/K = \mathbb{Z}^{\underline{X}}/K \subset \mathbb{Q}^{\underline{X}}/K$. Per la prop. 7.18 $\mathbb{Q}$ è divisibile, quindi $\mathbb{Q}^{\underline{X}}$ è divisibile per la prop. 7.22. Dai cor. 7.26 e 7.27 segue che $\mathbb{Q}^{\underline{X}}/K$ è iniettivo.

Lemma 7.29. *Sia G un gruppo abeliano.*

(1) $\mathrm{Hom}_{\mathbb{Z}}(R,G)$ è un R-modulo, se per $\theta \in \mathrm{Hom}_{\mathbb{Z}}(R,G)$ ed $a, r \in R$ poniamo $(a\theta)r := \theta(ra)$.

(2) Sia M un R-modulo. Allora esiste una biezione naturale

$$\mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(R,G)) \longleftrightarrow \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(R,G))$$

che ad ogni $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(M,G)$ associa l'omomorfismo

$$\hat{\varphi} := \bigcirc_x \bigcirc_a \varphi(ax)$$

Dimostrazione. (1) Per $a, b, r \in R$ abbiamo

$(a(b\theta))r = (b\theta)(ra) = \theta(rab) = (ab)\theta r$

(2) Per $r, a \in R$ ed $x \in M$ abbiamo

$(\hat{\varphi}(rx))a = \varphi(arx) = (\hat{\varphi}x)(ar) = (r\hat{\varphi}x)a.$

Le altre verifiche sono banali.

Proposizione 7.30. *Sia D un gruppo abeliano divisibile.*

Allora $\mathrm{Hom}_{\mathbb{Z}}(R,D)$ è un R-modulo iniettivo.

Dimostrazione. Per il teorema 7.9 è sufficiente dimostrare che il funtore controvariante $\mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbb{Z}}(R,D))$ è esatto.

Ma per il lemma 7.29 abbiamo un'uguaglianza (funtoriale) $\mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(R,G)) = \mathrm{Hom}_{\mathbb{Z}}(M,D)$. Siccome D è divisibile e quindi iniettivo (per la prop. 7.24), il funtore controvariante $\mathrm{Hom}_{\mathbb{Z}}(-,D)$ è esatto. Si cfr. Rotman, pag. 123, oppure Menini, cap. 3.

Teorema 7.31. *Ogni R-modulo è sottomodulo di un R-modulo iniettivo.*

Dimostrazione. Sia M un R-modulo. Consideriamo prima M come gruppo abeliano. Definiamo $\varphi := \bigcirc_m \bigcirc_r mr : M \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(R,M)$. È chiaro che φ è un omomorfismo di gruppi; dimostriamo che φ è iniettivo. Siano $\varphi m = \varphi m'$. Allora $rm = rm'$ per ogni $r \in R$ ed in particolare per $r = 1$ quindi $m = m'$.

Per la prop. 7.28 esiste un gruppo abeliano iniettivo D di cui M è sottogruppo. Consideriamo l'iniezione $i : M \longrightarrow D$. Per l'esattezza di $\mathrm{Hom}_{\mathbb{Z}}(R,-)$ è iniettiva anche l'applicazione $i_* : \mathrm{Hom}_{\mathbb{Z}}(R,M) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(R,D)$ e quindi anche la composizione $i_*\varphi$.

Dobbiamo ora dimostrare che $i_*\varphi$ è un omomorfismo di R-moduli. Sia $a \in R$ e $m \in M$. Allora $(i_*\varphi)(am) = a[(i_*\varphi)(m)]$ dove $i_*\varphi = i\varphi = \varphi$ e $\varphi(am) : r \longrightarrow r(am)$. D'altra parte $a[(i_*\varphi)(m)] = a(\varphi m)$ dove $a(\varphi m)(r) = (\varphi m)(ra)$. Pertanto $(i_*\varphi m)(ra) = (ra)m$.

Proposizione 7.32 (Bass/Papp). *Se ogni somma diretta di R-moduli iniettivi è ancora un R-modulo iniettivo, allora R è notheriano a sinistra.*

Dimostrazione. Dimostriamo che per un anello non noetheriano R esistono un ideale I di R, una somma diretta $E := \bigoplus_{n\in N} E_n$di R-moduli iniettivi e un omomorfismo $\alpha : I \longrightarrow E$ per il quale non esiste un'estensione di α da R in E e quindi che E non è iniettivo.

Siccome R non è noetheriano, esiste una catena strettamente crescente di ideali $I_1 \subset I_2 \subset \ldots$ per la quale poniamo $I := \bigcup_{n\in\mathbb{N}} I_n$. Chiaramente $I/I_n \neq 0$ per ogni $n \in \mathbb{N}$. Per il teorema 7.31 I/I_n è sottomodulo di un modulo iniettivo E_n per ogni $n \in \mathbb{N}$. Dimostriamo che $E := \bigoplus_{n\in\mathbb{N}} E_n$ non è iniettivo.

Sia $\pi_n : I \longrightarrow I/I_n$ la proiezione canonica. Chiaramente, dato $a \in I$, $\pi_n(a) = 0$ per $n >> 0$ e quindi l'applicazione $f : \bigcirc_a \bigcirc_n \pi_n a : I \longrightarrow \prod_{n\in\mathbb{N}} (I/I_n)$ è tale che $\mathrm{Im}\, f \subset \bigoplus_{n\in\mathbb{N}} (I/I_n)$. Data l'inclusione $i : \bigoplus_{n\in\mathbb{N}} (I/I_n) \longrightarrow \bigoplus_{n\in\mathbb{N}} E_n$ definiamo $\alpha = i \circ f$.

Se esistesse un R-omomorfismo $\beta : R \longrightarrow E$ estensione di α, allora $\beta(1)$ sarebbe definito. Poniamo $\beta(1) = \bigcirc_n e_n$. Dato un indice $m \in \mathbb{N}$ sia ora $a_m \notin I_m$ allora $\pi_m(a_m) \neq 0$ e quindi $\beta(a_m) = \alpha(a_m)$ ha la m-esima coordinata diversa da zero. Ma $\beta(a_m) = a_m\beta(1) = a_m \bigcirc_n e_n = \bigcirc_n a_m e_n$ con $\pi_m(a_m) = a_m e_m \neq 0$. Pertanto $e_m \neq 0$ per ogni $m \in \mathbb{N}$ e ciò è assurdo. Non esiste dunque un'estensione di α e quindi E non è iniettivo.

Definizione 7.33. Un'*estensione essenziale* di M è un omomorfismo iniettivo di R-moduli $\alpha : M \longrightarrow E$ tale che per ogni sottomodulo $L \neq 0$ di E si abbia $L \cap \mathrm{Im}\,\alpha \neq 0$.

L'estensione essenziale $\alpha : M \longrightarrow E$ si dice *propria*, se α non è suriettivo.

Lemma 7.34. *$\alpha : M \longrightarrow E$ sia un'estensione essenzale e $\varphi : E \longrightarrow N$ un omomorfismo tale che $\varphi \circ \alpha$ è iniettivo. Allora φ è iniettivo.*

Dimostrazione. Dobbiamo dimostrare che $\operatorname{Ker} \varphi = 0$. Per assurdo poniamo $\operatorname{Ker} \varphi \neq 0$. Allora, essendo E un'estensione essenziale di M, si ha $\operatorname{Im} \alpha \cap \operatorname{Ker} \varphi \neq 0$. Sia $x \in \operatorname{Ker} \alpha \cap \operatorname{Im} \varphi$ ed $x \neq 0$. Sia $y \in M$ con $x = \alpha y$. Allora $0 = \varphi x = \varphi \alpha y$. Però $\operatorname{Ker} \varphi \alpha = 0$, per cui $y = 0$ e quindi anche $x = 0$.

Proposizione 7.35. *M è iniettivo se e solo se M non possiede un'estensione essenziale propria.*

Dimostrazione. (1) Sia M un modulo iniettivo. Dimostriamo la prima implicazione per assurdo. Sia $\alpha : M \longrightarrow E$ un'estensione propria di M, quindi $\alpha(M) \neq E$ e $S \cap \alpha(M) \neq \{0\}$ per ogni S sottomodulo di E diverso da zero. Essendo M iniettivo, quindi anche $\alpha(M)$, per la prop. 7.8 $\alpha(M)$ è sommando diretto di E, pertanto esiste un sottomodulo S di E tale che $E = S \oplus \alpha(M)$. Dunque $S \cap \alpha(M) = 0$ e $S \neq 0$ perché $\alpha(M) \neq E$ essendo l'estensione propria. Ciò però è in contraddizione con l'ipotesi che $S \cap \alpha(M) \neq \{0\}$ quindi M non possiede un'estensione essenziale propria.

(2) Sia M un R-modulo che non possiede un'estensione essenziale propria. Per il teorema 7.31 M è sottomodulo di un modulo iniettivo E dunque possiamo definire l'inclusione $i : M \longrightarrow E$.

Se E è un'estensione essenziale di M, non potendo essere propria, si ha $i(M) = E$ quindi $i(M) = M$ è iniettivo.

Se i non è un'estensione essenziale di M esiste un sottomodulo $S \neq 0$ di E tale che $S \cap i(M) = 0$. Per il lemma di Zorn esiste un sottomodulo massimale $N \subset E$ tale che $S \subset N$ e $N \cap i(M) = 0$. Consideriamo ora la proiezione canonica $\pi : E \longrightarrow E/N$. Dato che $N \cap i(M) = \operatorname{Ker} \pi \cap i(M) = 0$, l'applicazione $\pi_{|i(M)} = \pi \circ i$ è iniettiva. Inoltre essendo i un'estensione essenziale di M, per il lemma 7.34 anche π è iniettivo e quindi $N = 0$. Ma ciò è in contraddizione con l'ipotesi che $S \subset N$ ed $S \neq 0$ quindi i deve essere un'estensione essenziale di M, ed M pertanto iniettivo.

Nota 7.36. Sono equivalenti:

(1) R è noetheriano a sinistra e iniettivo come R-modulo.

(2) R è noetheriano a destra e iniettivo come R-modulo destro.

(3) Un R-modulo è iniettivo se e solo se è proiettivo.

(4) Un R-modulo destro è iniettivo se e solo se è proiettivo.

Dimostrazione. La dimostrazione non è immediata e si trova in Lam, pag. 413. Anelli che soddisfano le 4 condizioni equivalenti dell'enunciato si chiamano *anelli quasi-di-Frobenius*.

8. Anelli semisemplici

Situazione 8.1. Sia A un anello commutativo.

Seguiamo Rotman, pagg.154-157.

Definizione 8.2. Un A-modulo M si dice *semisemplice*, se è somma diretto di A-moduli semplici (def. 2.15).

A si dice *semisemplice*, se è semisemplice come A-modulo.

Proposizione 8.3. *Un A-modulo M è semisemplice se e solo se ogni sottomodulo di M è un sommando diretto.*

<u>Dimostrazione.</u> (1) Sia M un A-modulo semisemplice. Allora $M = \bigoplus\limits_{j \in J} S_j$ dove S_j sono A-moduli semplici. Per $I \subseteq J$, definiamo $S_I = \bigoplus\limits_{j \in I} S_j$. Sia N un sottomodulo di M. Per il lemma di Zorn esiste $I \subseteq J$ massimale rispetto alla condizione $S_I \cap N = \{0\}$.

Se dimostriamo che $S_j \subseteq N + S_I$ per ogni $j \in J$ allora $M = N \oplus S_I$. Per $j \in I$ ovviamente $S_j \subseteq N + S_I$. Sia $j \notin I$, quindi per la massimalità di I abbiamo $(S_j + S_I) \cap N \neq \{0\}$ e quindi esistono $s_j \in S_j$, $s_I \in S_I$ e $n \in N$ tale che $s_j + s_I = n \neq 0$. Dunque $s_j = n - s_I \in (N + S_I) \cap S_j$ con $s_j \neq 0$ perché in tal caso avremmo $s_I = n \in N \cap S_I$ ma ciò è assurdo perchè $S_I \cap N = \{0\}$. Pertanto $S_j \subseteq N + S_I$.

(2) Sia M un A-modulo tale che ogni suo sottomodulo N è un sommando diretto.

(2a) Sia N un sottomodulo di M. Dimostriamo che N contiene un sottomodulo semplice. Sia $x \in N$, $x \neq 0$. Per il lemma di Zorn esiste un sottomodulo Z di N tale che $x \notin Z$. Per ipotesi Z è sommando diretto di M e quindi di N. Esiste perciò Y tale che $N = Z \oplus Y$ ed Y è semplice. Infatti se così non fosse esisterebbero Y', Y'' tali che $Y = Y' \oplus Y''$ e quindi $N = Z \oplus Y' \oplus Y''$. Ma essendo $x \notin Z = (Z \oplus Y') \cap (Z \oplus Y'')$ allora $Z \oplus Y'$ o $Z \oplus Y''$ non contengono x e ciò contraddice la massimalità di Z.

Esiste dunque per il lemma di Zorn una famiglia $\bigcirc\limits_{k \in K} S_k$ di sottomoduli semplici di M massimale rispetto alla condizione $D = \bigoplus\limits_{k \in K} S_k$. Per ipotesi esiste E sottomodulo di M tale che $M = D \oplus E$. Se $E = \{0\}$ abbiamo già concluso. Altrimenti $E = S \oplus E'$ dove S è un sottomodulo semplice per (2a). Ma allora possiamo aggiungere S alla famiglia $\bigcirc\limits_{k \in K} S_k$ contraddicendo la sua massimalità .

Corollario 8.4. *Ogni sottomodulo e ogni immagine omomorfa di un A-modulo semisemplice è semisemplice.*

<u>Dimostrazione.</u> (1) Sia N un sottomodulo di un A-modulo semisemplice M. Allora ogni sottomodulo di N è sommando diretto di M per la prop. 8.3 e quindi anche di N. Pertanto sempre per la prop. 8.3 N è semisemplice.

(2) Sia $\alpha : M \longrightarrow N$ un omomorfismo di A-moduli ed M è un A-modulo semisemplice. Sia K un sottomodulo di $\alpha(M)$. Dunque esiste E sottomodulo di M tale che $\alpha(E) = K$.

Inoltre per la prop. 8.3 $M = E \oplus Y$ per un qualche sottomodulo Y di M. Pertanto anche $K = \alpha(E)$ è sommando diretto di $\alpha(M)$.

Lemma 8.5. *Per ogni $\lambda \in \Lambda$ sia I_λ un ideale di A. Si abbia $A = \bigoplus\limits_{\lambda\in\Lambda} I_\lambda$. Allora $I_\lambda \neq 0$ solo per un numero finito di indici $\lambda \in \Lambda$.*

Dimostrazione. Siccome ogni elemento di una somma diretta ha un supporto finito esistono $e_1 \in I_1, \dots, e_n \in I_n$ tali che $1 = e_1 + \dots + e_n$. Se $a \in I_\lambda$ per $\lambda \neq 1, \dots, n$ allora

$$a = a1 = ae_1 + \dots + ae_n \in I_\lambda \cap (I_1 \oplus \dots \oplus I_n) = \{0\}.$$

Dunque $I_\lambda = 0$ per $\lambda \neq 1, \dots, n$.

Osservazione 8.6. I sottomoduli semplici di A sono esattamente gli ideali generalizzati minimali di A.

Corollario 8.7. *Se A è semisemplice, allora A è somma diretta di un numero finito di ideali generalizzati minimali.*

Dimostrazione. Sia A un A-modulo semisemplice. Allora A è somma diretta di A-moduli semplici. Ma ogni A-modulo semplice è un ideale minimale generalizzato di A. Dunque, siccome per il lemma 8.5 A è somma diretta di un numero finito di ideali, A è somma diretta di un numero finito di ideali minimali generalizzati.

Proposizione 8.8. *Sono equivalenti:*

(1) A è semisemplice

(2) Ogni A-modulo è semisemplice.

(3) Ogni A-modulo è iniettivo.

(4) Ogni ideale di A è un A-modulo iniettivo.

(5) Ogni A-modulo è proiettivo.

(6) Ogni successione esatta $0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0$ di A-moduli si spezza.

Dimostrazione. (1) $\Longrightarrow$ (2): Sia M un A-modulo. Essendo A semisemplice come A-modulo, ogni A-modulo libero è semisemplice, ma M è immagine omomorfa di un modulo libero per la prop. 3.34 e quindi M è semisemplice per il cor. 8.4.

(2) $\Longrightarrow$ (3): Sia Q un A-modulo tale che la successione $0 \longrightarrow Q \xrightarrow{\varphi} M$ è esatta. M è un A-modulo semisemplice, quindi per la prop. 8.3 ogni suo sottomodulo è sommando diretto. Quindi $\operatorname{Im}\varphi$ è sommando diretto, pertanto la successione si spezza e Q è iniettivo.

(3) $\Longrightarrow$ (4): I sottomoduli di A come A-modulo sono A-moduli iniettivi quindi ideali iniettivi.

(4) $\Longrightarrow$ (1): I sottomoduli di A sono ideali iniettivi quindi per la prop. 7.8 sono sommandi diretti. Quindi per la prop. 8.3 R è semisemplice

(3) $\Longrightarrow$ (5): Sia P un A-modulo e $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$ una successione esatta. Essendo M iniettivo la successione si spezza e quindi P è proiettivo.

(5) $\Longrightarrow$ (6): Data la successione esatta $0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0$ di A-moduli, per ipotesi M_2 è proiettivo quindi per la prop. 5.47 la successione si spezza.

(6) $\Longrightarrow$ (1): Sia M un sottomodulo di A. La successione esatta $0 \longrightarrow M \longrightarrow A \longrightarrow A/M \longrightarrow 0$ si spezza quindi M è sommando diretto di A.

9. Anelli ereditari

Situazione 9.1. Sia A un anello commutativo.

Seguiamo Rotman, pagg. 161-169.

Definizione 9.2. A si dice *ereditario*, se ogni ideale di A è proiettivo.

A si dice di *Dedekind*, se è ereditario e integro.

Osservazione 9.3. Se A è semisemplice, allora A è ereditario.

Osservazione 9.4. Ogni anello ad ideali principali è di Dedekind.

Dimostrazione. Sia A un anello ad ideali principali. Allora A è un dominio commutativo. Resta da verificare che ogni ideale di A è proiettivo. Ma ogni ideale di A è del tipo Ar con $r \in A$ e quindi isomorfo ad A e perciò libero e proiettivo, quando $r \neq 0$.

Teorema 9.5 (Kaplansky). *A sia ereditario ed M un A-modulo che sia sottomodulo di un A-modulo libero. Allora M è isomorfo a una somma diretta di ideali di A.*

Dimostrazione. Siano L un A-modulo libero con $\{l_k \mid k \in K\}$ una base di L e M un sottomodulo di L. Per l'assioma della scelta possiamo assumere che K è ben ordinato e definire, denotando con 0 l'elemento più piccolo di K rispetto al buon ordine considerato, partendo da $F_0 = \{0\}$:

$$L_k := \bigoplus_{i<k} Al_i \quad \text{e} \quad \overline{L_k} := \bigoplus_{i\leq k} Al_i = L_k \oplus Al_k$$

Da ciò segue $\overline{L_0} = Al_0$. Ogni elemento $m \in M \cap \overline{L_k}$ ha un'unica espressione $m = b + a_m l_k$ dove $b \in L_k$ e $a_m \in A$. Perciò l'applicazione $\varphi_k := \bigcirc_m a_m : M \cap \overline{L_k} \longrightarrow A$ è ben definita. Abbiamo una sequenza esatta

$$0 \longrightarrow M \cap F_k \longrightarrow M \cap \overline{L_k} \longrightarrow \operatorname{Im} \varphi_k \longrightarrow 0$$

Siccome per ipotesi l'ideale $\operatorname{Im} \varphi_k$ è proiettivo, la successione si spezza, per cui $M \cap \overline{L_k} = (M \cap L_k) \oplus C_k$, dove $C_k \cong \operatorname{Im} \varphi_k$. Dimostriamo ora che $M = \bigoplus_{k\in K} C_k$.

(1) Dimostriamo che $M = A \bigcup_{k\in K} C_k$. Essendo $L = \bigcup_{k\in K} \overline{L_k}$, ogni $m \in M$ appartiene a qualche $\overline{L_k}$; sia $\mu(m)$ il più piccolo indice k con $m \in \overline{L_k}$. Definiamo $C = A \bigcup_{k\in K} C_k \subseteq M$. Se $C \neq M$, allora $J = \{\mu(m) \mid m \in M \setminus C\} \neq 0$. Sia $j \in J$ il più piccolo elemento di J e $y \in M \setminus C$ tale che $\mu(y) = j$. Essendo $y \in M \cap \overline{L_j} = (M \cap L_j) \oplus C_j$, $y = b + c$ dove $b \in M \cap F_j$ e $c \in C_j$. Dunque $b = y - c \in M$, $b \notin C$ e $\mu(b) < j$, in contraddizione con la minimalità di j.

(2) Dimostriamo che la somma è diretta. Supponiamo che $c_1 + \ldots + c_n = 0$ dove $c_i \in C_{k_i}$, $k_1 < \ldots < k_n$, e k_n è minimale. Dunque

$$c_1 + \ldots + c_{n-1} = -c_n \in (M \cap L_{k_n}) \cap C_{k_n} = \{0\}.$$

Pertanto $c_n = 0$, in contraddizione con la minimalità di k_n.

Corollario 9.6. *A sia ereditario. Allora ogni sottomodulo di un A-modulo proiettivo è proiettivo.*

Dimostrazione. Siano P un A-modulo proiettivo e S un sottomodulo di P. Per il teorema 6.6 P è sommando diretto di un modulo libero. Dunque S è sottomodulo di un modulo libero e quindi S è somma diretta di ideali, ognuno dei quali è proiettivo, per il teorema 9.5. Dunque S è proiettivo per il corollario 6.8.,

Corollario 9.7. *A sia un anello ad ideali principali.*

Allora ogni sottomodulo di un A-modulo libero è libero.

Dimostrazione. Siano L un A-modulo libero e M un sottomodulo di L. Utilizzando la dimostrazione del teorema 9.5, essendo $\{l_k \mid k \in K\}$ una base di L, allora $M = \bigoplus_{k \in K} C_k$ dove ogni C_k è isomorfo a un ideale di A. Essendo A un anello ad ideali principali, ogni ideale diverso da zero è isomorfo ad A, quindi $C_k = 0$ o $C_k \cong A$. Dunque M è libero.

Corollario 9.8. *Sia A un anello ad ideali principali. Allora ogni A-modulo proiettivo è libero.*

Dimostrazione. Ogni A-modulo proiettivo è sottomodulo di un modulo libero e quindi per il cor. 9.7 è libero.

Lemma 9.9. *P è un A-modulo proiettivo se e solo se per ogni diagramma di R-moduli*

$$\begin{tikzcd} & P \arrow[d, "f"] & \\ Q \arrow[r] & Q'' \arrow[r] & 0 \end{tikzcd}$$

in cui Q è iniettivo e la riga è esatta, esiste un omomorfismo $\beta : P \longrightarrow Q$ che rende commutativo il diagramma

$$\begin{tikzcd} & P \arrow[d, "f"] \arrow[dl, "\beta"'] & \\ Q \arrow[r] & Q'' \arrow[r] & 0 \end{tikzcd}$$

Dimostrazione. (1) Se P è proiettivo l'implicazione è ovvia.

(2) P abbia la proprietà richiesta. Per dimostrare che P è proiettivo basta verificare che esiste $g : P \longrightarrow A$ tale che il seguente diagramma

$$\begin{tikzcd} & & & P \arrow[d, "f"] \arrow[dl, "g"'] & \\ 0 \arrow[r] & A' \arrow[r, "i"'] & A \arrow[r, "\tau"'] & A'' \arrow[r] & 0 \end{tikzcd}$$

sia commutativo. Per il teorema 7.31 esistono un modulo iniettivo Q e un' inclusione $i : A \longrightarrow Q$. Si può quindi considerare il diagramma

$$\begin{tikzcd}
 & & P \arrow[d, "f"] & \\
0 \arrow[r] & A' \arrow[r, "i"] \arrow[d, "l"] & A \arrow[r, "\tau"] \arrow[d, "\sigma"] & A'' \arrow[r] \arrow[d, "\rho"] & 0 \\
0 \arrow[r] & A' \arrow[r, "\sigma i"'] & Q \arrow[r, "\nu"'] & Q'' \arrow[r] & 0
\end{tikzcd}$$

dove $Q'' =$ e ν è una mappa naturale. Per ipotesi esiste $\gamma : P \longrightarrow Q$ tale che $\nu\gamma = \rho f$. Per completare la dimostrazione dobbiamo dimostrare che $\operatorname{Im}\gamma \subset \operatorname{Im}\sigma$. Se $x \in P$, scegliamo $a \in A$ con $\tau a = fx$. Dunque $\nu\gamma x = \rho f x = \rho\tau a = \nu\sigma a$, dunque $\gamma x - \sigma a \in \operatorname{Ker}\nu = \operatorname{Im}\sigma i$. Perciò esiste $a' \in A'$ con $\gamma x - \sigma a = \sigma i a'$, e quindi $\gamma x = \sigma(a + ia') \in \operatorname{Im}\sigma$.

Teorema 9.10 (Cartan-Eilenberg). *Sono equivalenti:*

(1) A è ereditario.

(2) Ogni sottomodulo di un A-modulo proiettivo è proiettivo.

(3) Ogni quoziente di un A-modulo iniettivo è iniettivo.

Dimostrazione. (1) $\Longrightarrow$ (2): Segue dal cor. 9.6.

(2) $\Longrightarrow$ (1): A è un A-modulo libero e quindi proiettivo. Dunque, i suoi sottomoduli (che sono i suoi ideali) sono proiettivi, quindi A è ereditario.

(3) $\Longrightarrow$ (2): Consideriamo il diagramma

$$\begin{tikzcd}
P \arrow[d, "k"'] & P' \arrow[l, "j"] \arrow[d, "f"] & 0 \arrow[l] \\
Q \arrow[r, "r"] & Q'' \arrow[r] & 0
\end{tikzcd}$$

dove le righe sono esatte, P è proiettivo e Q è iniettivo. Per il lemma 9.9 è sufficiente dimostrare che esiste un omomorfismo $g : P' \longrightarrow Q$ con $rg = f$. Per ipotesi Q'' è iniettivo quindi esiste un omomorfismo $h : P \longrightarrow Q''$ tale che $hj = f$. Inoltre essendo P proiettivo esiste $k : P \longrightarrow Q$ con $rk = h$. Definiamo ora $g = kj : P' \longrightarrow Q$. g è l'omomorfismo richiesto: infatti $rg = r(kj) = hj = f$.

(2) $\Longrightarrow$ (3): Nello stesso modo, per dualità .

Proposizione 9.11. *A sia integro. Allora A è di Dedekind se e solo se ogni A-modulo divisibile è iniettivo.*

Dimostrazione. (1) Ogni A-modulo divisibile sia iniettivo. Sia E un A-modulo iniettivo. Allora per l'oss. 7.20 E è divisibile. Sia E'' un quoziente di E, siccome ogni quoziente di un modulo divisibile è divisibile allora, E'' per ipotesi è iniettivo e quindi per il teorema 9.10 A è di Dedekind.

(2) Sia A un anello di Dedekind e E un A-modulo divisibile. Utilizzando il teorema 7.14, dato il diagramma

$$\begin{tikzcd} & E \\ 0 \arrow[r] & I \arrow[u, "f"] \arrow[r, "i"] & A \end{tikzcd}$$

dove I è un ideale di A, basta dimostrare che esiste un omomorfismo $g : A \longrightarrow E$ che è estensione di i. Possiamo assumere che I sia diverso da zero e quindi invertibile. Esistono quindi $a_1, \ldots, a_n \in I$ e $q_1, \ldots, q_n \in \mathcal{K}(A)$ con $q_i I \subset A$ e $1 = \sum q_i a_i$. Essendo E divisibile esistono $e_i \in E$ tali che $f(a_i) = a_i e_i$. Sia $b \in I$, allora

$$f(b) = f(\sum q_i a_i b) = \sum (q_i b) a_i e_i = b \sum (q_i a_i) e_i$$

Sia $e := \sum (q_i a_i) e_i = e$. Allora $e \in E$, inoltre $fb = be$ per ogni $b \in I$. Ciò permette di definire $g := \bigcirc_r re : A \longrightarrow E$. In questo modo con g otteniamo un' estensione di f e vediamo che E è iniettivo.

Bibliografia

J. Dauns: Modules and rings. Cambridge UP 2008.

C. Dolcini: Concetti fondamentali della teoria degli anelli. Tesi Ferrara, 1988.

D. Dummit/R. Foote: Abstract algebra. Wiley 2004.

K. Goodearl/R. Warfield: An introduction to noncommutative noetherian rings. Cambridge UP 2004.

T. Lam [LMR]: Lectures on modules and rings. Springer 1999.

T. Lam [FCNR]: A first course in noncommutative rings. Springer 2001.

J. Lambek: Lectures on rings and modules. AMS Chelsea 2009.

C. Menini: Module theory. Appunti 2011.

J. Rotman: An introduction to homological algebra. Springer 2009.