MODULI SU UN ANELLO

ALBERTO CANONACO

23 marzo 2023

Gli anelli saranno sempre con unità, ma non necessariamente commutativi. In particolare, A denoterà sempre un anello e K un campo. All'inizio di ogni sezione verrà indicato se ci sono ulteriori assunzioni su A.

1. Moduli

Definizione 1.1. Un *A-modulo* è il dato di un gruppo abeliano $(M, +)$ e di una funzione (detta di *moltiplicazione per scalari*)

$$A \times M \to M$$
$$(a, x) \mapsto ax$$

tali che siano soddisfatti i seguenti assiomi per ogni $a, b \in A$ e per ogni $x, y \in M$:

(1) $a(x + y) = ax + ay$;
(2) $(a + b)x = ax + bx$;
(3) $(ab)x = a(bx)$;
(4) $1_A x = x$.

Con usuale abuso di notazione, un A-modulo come sopra verrà spesso indicato solo con M, sottintendendo sia l'operazione di gruppo che la moltiplicazione per scalari. Se poi l'anello A è chiaro dal contesto, a volte si dirà semplicemente modulo, senza specificare A-modulo.

Esempio 1.2. Un K-modulo è precisamente un K-spazio vettoriale.

Dati due gruppi abeliani $(G, +)$ e $(G', +)$, ricordiamo che l'insieme degli omomorfismi di gruppi da G a G' forma un gruppo abeliano $\mathrm{Hom}(G, G')$ con l'operazione $f + g$ (per ogni $f, g \in \mathrm{Hom}(G, G')$) definita da $(f + g)(x) := f(x) + g(x)$ per ogni $x \in G$. Inoltre $\mathrm{End}(G) := \mathrm{Hom}(G, G)$ (cioè l'insieme degli endomorfismi di G) è anche un anello con il prodotto fg dato dalla composizione $f \circ g$.

Osservazione 1.3. Se M è un A-modulo e indichiamo (per ogni $a \in A$) con $\alpha(a) \colon M \to M$ la funzione $x \mapsto ax$, gli assiomi della Definizione 1.1 si traducono come segue (per ogni $a, b \in A$):

(1) $\alpha(a) \in \mathrm{End}(M)$;
(2) $\alpha(a + b) = \alpha(a) + \alpha(b)$;
(3) $\alpha(ab) = \alpha(a) \circ \alpha(b)$;
(4) $\alpha(1_A) = \mathrm{id}_M = 1_{\mathrm{End}(M)}$.

Dunque $\alpha \colon A \to \mathrm{End}(M)$ risulta un omomorfismo di anelli, ed è chiaro che, viceversa, dato un gruppo abeliano $(M, +)$ e un omomorfismo di anelli $\alpha \colon A \to \mathrm{End}(M)$, M diventa un A-modulo con moltiplicazione per scalari

definita da $ax := \alpha(a)(x)$ per ogni $a \in A$ e per ogni $x \in M$. In altre parole, dare una struttura di A-modulo a un gruppo abeliano $(M, +)$ equivale a dare un omomorfismo di anelli $A \to \mathrm{End}(M)$.

Esempio 1.4. Ogni gruppo abeliano $(G, +)$ ammette un'unica struttura di $\mathbb{Z}$-modulo, in cui ng (per $n \in \mathbb{Z}$ e $g \in G$) va inteso nello stesso senso della notazione introdotta in teoria dei gruppi per i gruppi abeliani additivi. Ciò può essere verificato facilmente a partire dalla Definizione 1.1, o può essere dedotto immediatamente dall'Osservazione 1.3, ricordando che per ogni anello B (in questo caso $B = \mathrm{End}(G)$) esiste un unico omomorfismo di anelli $\mathbb{Z} \to B$, definito da $n \mapsto n1_B$.

Osservazione 1.5. Come per gli spazi vettoriali, segue dagli assiomi (e si può vedere più direttamente usando l'Osservazione 1.3 e le proprietà degli omomorfismi di gruppi) che in un A-modulo M si ha (per ogni $a, b \in A$ e per ogni $x, y \in M$): $a0_M = 0_M$, $a(x - y) = ax - ay$, $0_A x = 0_M$ e $(a - b)x = ax - bx$.

Esempio 1.6. Il gruppo abeliano additivo banale $\{0\}$ è sempre un A-modulo (detto ancora *banale* o *nullo*) con moltiplicazione per scalari data dall'unica funzione $A \times \{0\} \to \{0\}$. Se inoltre $1_A = 0_A$ (quindi $A = \{0\}$ è l'anello banale), allora ogni A-modulo M è banale: infatti, per ogni $x \in M$ si ha $x = 1_A x = 0_A x = 0_M$.

Esempio 1.7. Risulta evidente dalle definizioni di anello e di modulo che il gruppo abeliano $(A, +)$ è un A-modulo con moltiplicazione per scalari $A \times A \to A$ data dalla moltiplicazione di A. In generale questa può non essere l'unica struttura di A-modulo su $(A, +)$, ma in seguito A verrà sempre considerato come A-modulo in questo modo.

Osservazione 1.8. Quello che abbiamo chiamato modulo andrebbe più correttamente chiamato *modulo sinistro*: esiste infatti un'analoga nozione di *modulo destro*. Per la precisione, un A-modulo destro è il dato di un gruppo abeliano $(M, +)$ e di una funzione $M \times A \to M$, $(x, a) \mapsto xa$ tali che siano soddisfatti i seguenti assiomi per ogni $a, b \in A$ e per ogni $x, y \in M$:

(1) $(x + y)a = xa + ya$;
(2) $x(a + b) = xa + xb$;
(3) $x(ab) = (xa)b$;
(4) $x1_A = x$.

È importante notare che la differenza sostanziale tra moduli sinistri e moduli destri non è tanto nel fatto che gli scalari vengano scritti a sinistra o a destra, quanto piuttosto nel diverso significato dell'assioma (3). In effetti, dato un A-modulo sinistro M, si potrebbe pensare di ottenere su $(M, +)$ una struttura di A-modulo destro semplicemente definendo $xa := ax$ per ogni $a \in A$ e per ogni $x \in M$. Mentre è immediato verificare che ciascuno degli assiomi (1), (2) e (4) di modulo sinistro implica il corrispondente assioma di modulo destro, lo stesso non vale in generale per l'assioma (3). Infatti, poiché $x(ab) = (ab)x$ e $(xa)b = b(xa) = b(ax) = (ba)x$, M diventa veramente un A-modulo destro se e solo se $(ab)x = (ba)x$ per ogni $a, b \in A$ e per ogni $x \in M$. Tale condizione non è verificata se A non è commutativo e per esempio $M = A$ come A-modulo sinistro (basta prendere $x = 1_A$ e $a, b \in A$

tali che $ab \neq ba$). D'altra parte dovrebbe essere chiaro che in questo modo M diventa sempre invece un A^{op}-modulo destro.[1] Ne segue che la teoria degli A-moduli sinistri (rispettivamente destri) coincide con quella degli A^{op}-moduli destri (rispettivamente sinistri), e che per studiare i moduli sinistri o destri su un anello generico ci si può limitare per esempio a quelli sinistri. Va detto che in certi contesti può comunque essere necessario distinguere tra moduli sinistri e moduli destri: ciò succede per esempio quando si lavora con uno specifico anello non commutativo o quando si ha che fare con i cosiddetti "bimoduli" (cioè gruppi abeliani dotati simultaneamente di una struttura di modulo sinistro e di una di modulo destro, con un'opportuna condizione di compatibilità tra le due). Poiché in seguito non ci troveremo mai in situazioni di questo genere, per i nostri scopi potremo limitarci, senza perdita di generalità, a considerare solo moduli sinistri, che continueremo a chiamare semplicemente moduli per brevità.

2. Sottomoduli

Definizione 2.1. Un *A-sottomodulo* (o semplicemente un sottomodulo, se non c'è pericolo di confusione su A) di un A-modulo M è un sottogruppo (additivo) N di M tale che $ax \in N$ per ogni $a \in A$ e per ogni $x \in N$.

Esempio 2.2. Un K-sottomodulo di un K-spazio vettoriale V (si veda l'Esempio 1.2) è precisamente un K-sottospazio vettoriale di V.

Esempio 2.3. Se $(G, +)$ è un gruppo abeliano (visto come $\mathbb{Z}$-modulo, come spiegato nell'Esempio 1.4), ogni sottogruppo H di G è uno $\mathbb{Z}$-sottomodulo di G. Infatti $nx \in \langle x \rangle \subseteq H$ per ogni $n \in \mathbb{Z}$ e per ogni $x \in H$.

Esempio 2.4. $\{0\}$ e M sono sottomoduli di M (detti *banali*) per ogni modulo M.

Esempio 2.5. Segue subito dalle definizioni che gli A-sottomoduli di A (si veda l'Esempio 1.7) sono gli ideali sinistri[2] di A. In particolare, se A è commutativo, gli A-sottomoduli di A sono gli ideali di A.

Osservazione 2.6. Come per gli ideali sinistri in un anello, per dimostrare che un sottoinsieme N di un A-modulo M è un sottomodulo di M è sufficiente verificare che $N \neq \emptyset$ e che $x + y, ax \in N$ per ogni $x, y \in N$ e per ogni $a \in A$ (la chiusura rispetto agli opposti segue dal fatto che $-x = (-1_A)x$).

Definizione-Proposizione 2.7. *Sia M un A-modulo e siano $N_\lambda \subseteq M$ dei sottomoduli (con $\lambda \in \Lambda$). Allora $\bigcap_{\lambda\in\Lambda} N_\lambda$ e*

$$\sum_{\lambda\in\Lambda} N_\lambda := \left\{ \sum_{\lambda\in\Lambda} x_\lambda \,:\, x_\lambda \in N_\lambda \ \forall\, \lambda \in \Lambda,\ \#\{\lambda \in \Lambda \,:\, x_\lambda \neq 0\} < \infty \right\}$$

sono sottomoduli di M.

[1] A^{op} indica l'*anello opposto* di A, cioè l'anello che come gruppo additivo coincide con $(A, +)$, ma in cui il prodotto ab è definito come il prodotto ba in A. Si osservi che vale sempre $(A^{op})^{op} = A$ e che $A^{op} = A$ se e solo se A è commutativo.

[2] Ovviamente questo dipende dal fatto che per modulo intendiamo modulo sinistro (si veda l'Osservazione 1.8); se considerassimo invece moduli destri, gli A-sottomoduli di A sarebbero gli ideali destri di A.

Dimostrazione. Esercizio. □

Definizione-Proposizione 2.8. *Se $I \subseteq A$ è un ideale sinistro, M è un A-modulo e $U \subseteq M$ è un sottoinsieme, il* prodotto

$$IU := \left\{ \sum_{i=1}^{n} a_i x_i \,:\, n \in \mathbb{N},\ a_i \in I,\ x_i \in U\ \forall\, i = 1, \dots, n \right\}$$

è un sottomodulo di M. In particolare AU e IM sono sottomoduli di M.

Dimostrazione. Esercizio. □

Definizione-Proposizione 2.9. *Se M è un A-modulo, $N \subseteq M$ è un sottomodulo e $U \subseteq M$ è un sottoinsieme, allora*

$$(N : U) := \{a \in A \,:\, ax \in N\ \forall\, x \in U\}$$

*è un ideale sinistro di A; in particolare $(\{0\} : U)$ è un ideale sinistro di A, detto l'*annullatore di U *e denotato* $\mathrm{Ann}_A(U)$*, o semplicemente* $\mathrm{Ann}(U)$*.*

Se poi $P \subseteq M$ è un altro sottomodulo, $(N : P)$ è un ideale (bilatero) di A; in particolare $\mathrm{Ann}(P)$ *è un ideale di A.*

Dimostrazione. Esercizio. □

Osservazione 2.10. Se $x \in M$, si scriverà Ix invece di $I\{x\}$; chiaramente $Ix = \{ax \,:\, a \in I\}$. Analogamente si scriverà $(N : x)$ (rispettivamente $\mathrm{Ann}(x)$) invece di $(N : \{x\})$ (rispettivamente $\mathrm{Ann}(\{x\})$).

Osservazione 2.11. Per ogni A-modulo M si ha per definizione $\mathrm{Ann}(M) = \ker(\alpha)$, dove $\alpha \colon A \to \mathrm{End}(M)$ è l'omomorfismo di anelli che definisce la struttura di A-modulo su M (si veda l'Osservazione 1.3).

Definizione-Proposizione 2.12. *Sia M un A-modulo e sia $U \subseteq M$ un sottoinsieme. Il sottomodulo di M* generato da *U, denotato $\langle U \rangle_A$, può essere definito equivalentemente in uno dei modi seguenti:*

(1) *AU;*
(2) *$\sum_{x \in U} Ax$;*
(3) *l'intersezione degli A-sottomoduli di M contenenti U;*
(4) *il più piccolo A-sottomodulo di M contenente U.*

Dimostrazione. Esercizio. □

Esempio 2.13. Se A è commutativo e $M = A$, $\langle U \rangle_A = (U)$ coincide con l'ideale generato da U.

Osservazione 2.14. Se non c'è pericolo di confusione con il sottogruppo generato da U, a volte si scrive $\langle U \rangle$ invece di $\langle U \rangle_A$. Si noti che le due nozioni coincidono quando $A = \mathbb{Z}$ (o anche $A = \mathbb{Z}/n\mathbb{Z}$ per qualche intero positivo n), ma non in generale.

Definizione 2.15. Sia M un A-modulo. Si dice che un sottoinsieme $U \subseteq M$ è un *insieme di generatori* di M o che U *genera* M (come A-modulo) se $M = \langle U \rangle_A$. Si dice che M è un A-modulo *finitamente generato* (rispettivamente *ciclico*) se è generato da un insieme finito (rispettivamente costituito da un solo elemento).

Esempio 2.16. $\{0\} = \langle 0 \rangle_A$ e $A = \langle 1 \rangle_A$ sono A-moduli ciclici.

Osservazione 2.17. Se A è commutativo, un ideale di A è finitamente generato (rispettivamente principale) come ideale se e solo se è finitamente generato (rispettivamente ciclico) come A-modulo. Analogamente, un gruppo abeliano $(G, +)$ è finitamente generato (rispettivamente ciclico) come gruppo se e solo G è finitamente generato (rispettivamente ciclico) come $\mathbb{Z}$-modulo.

Definizione 2.18. Un modulo è *semplice* se non è nullo e i suoi unici sottomoduli sono quelli banali.

Esempio 2.19. A è un A-modulo semplice se e solo se A è un anello con divisione. Infatti A è un A-modulo semplice se e solo non è nullo e i suoi unici ideali sinistri sono quelli banali. È ben noto che questo è vero se A è un anello con divisione. Viceversa, se gli unici ideali sinistri di $A \neq \{0\}$ sono $\{0\}$ e A, allora per ogni $a \in A \setminus \{0\}$ l'ideale sinistro Aa, non essendo $\{0\}$, deve essere A. Quindi esiste $a' \in A$ tale che $a'a = 1$. Chiaramente anche $a' \neq 0$, e analogamente esiste $a'' \in A$ tale che $a''a' = 1$. Poiché $a'' = a''(a'a) = (a''a')a = a$, ciò dimostra che $a \in A^*$ (con $a^{-1} = a'$).

Osservazione 2.20. Anche se non ce ne occuperemo, è bene sapere che un anello A si dice *semplice* (come anello, non come A-modulo), se $A \neq \{0\}$ e gli unici ideali (bilateri) di A sono $\{0\}$ e A. Mentre è ovviamente vero che se A è semplice come A-modulo è anche semplice come anello, il viceversa vale se A è commutativo, ma non in generale. Per esempio, si può dimostrare che l'anello $\mathrm{M}_n(A)$ delle matrici $n \times n$ a coefficienti in un anello con divisione A è semplice come anello, ma non come modulo su se stesso se $n > 1$.

Osservazione 2.21. Un gruppo si dice *semplice* se è non banale e i suoi unici sottogruppi normali sono quelli banali. Chiaramente un gruppo abeliano (additivo) è semplice come gruppo se e solo se lo è come $\mathbb{Z}$-modulo.

3. Omomorfismi di moduli

Definizione 3.1. Siano M e N due A-moduli. Una funzione $f\colon M \to N$ è un *omomorfismo di A-moduli* (si dice anche che f è *A-lineare*) se f è un omomorfismo di gruppi additivi tale che $f(ax) = af(x)$ per ogni $a \in A$ e per ogni $x \in M$.

Esempio 3.2. Se V e W sono due K-spazi vettoriali, una funzione $V \to W$ è un omomorfismo di K-moduli se e solo se è un omomorfismo di K-spazi vettoriali.

Esempio 3.3. Se $(G, +)$ e $(G', +)$ sono gruppi abeliani (visti come $\mathbb{Z}$-moduli), ogni omomorfismo di gruppi $G \to G'$ è $\mathbb{Z}$-lineare.

Esempio 3.4. La funzione nulla $M \to N$ (definita da $x \mapsto 0_N$ per ogni $x \in M$) è un omomorfismo di moduli (detto *banale* o *nullo*) per ogni coppia di moduli M e N.

Esempio 3.5. Se M è un A-modulo e $N \subseteq M$ è un sottomodulo, la funzione di inclusione $N \to M$ è A-lineare (e iniettiva).

Esempio 3.6. Per ogni A-modulo M e per ogni $x \in M$ esiste un'unica funzione A-lineare $f_x\colon A \to M$ tale che $f_x(1_A) = x$ (definita da $f_x(a) := ax$ per ogni $a \in A$).

Osservazione 3.7. La composizione di funzioni A-lineari è A-lineare.

Osservazione 3.8. Come è noto dalla teoria dei gruppi, una funzione A-lineare $f\colon M \to N$ è iniettiva se e solo se $\ker(f) := f^{-1}(0_N) = \{0_M\}$. D'altra parte è ovvio che f è suriettiva se e solo se $\mathrm{im}(f) := f(M) = N$.

Definizione 3.9. Siano M e N due A-moduli. Una funzione $M \to N$ è un *isomorfismo di A-moduli* se è un omomorfismo biunivoco di A-moduli. Si dice che M e N sono *isomorfi* (come A-moduli) e si indica con $M \cong N$ se esiste un isomorfismo (di A-moduli) $M \to N$.

Osservazione 3.10. Se $f\colon M \to N$ e $g\colon N \to P$ sono isomorfismi di moduli, anche $g \circ f\colon M \to P$, $f^{-1}\colon N \to M$ e $\mathrm{id}_M\colon M \to M$ lo sono. Dunque l'isomorfismo di moduli è una relazione di equivalenza. Inoltre un omomorfismo di moduli $f\colon M \to N$ è un isomorfismo se e solo se esiste un omomorfismo di moduli $f'\colon N \to M$ tale che $f' \circ f = \mathrm{id}_M$ e $f \circ f' = \mathrm{id}_N$.

Proposizione 3.11. *Sia $f\colon M \to N$ un omomorfismo di A-moduli.*

1. *Se M' è un sottomodulo di M, allora $f(M')$ è un sottomodulo di N. In particolare* $\mathrm{im}(f)$ *è un sottomodulo di N.*
2. *Se N' è un sottomodulo di N, allora $f^{-1}(N')$ è un sottomodulo di M. In particolare* $\ker(f)$ *è un sottomodulo di M.*
3. *Per ogni sottoinsieme $U \subseteq M$ si ha $f(\langle U\rangle_A) = \langle f(U)\rangle_A$. In particolare, se f è suriettivo e M è finitamente generato (rispettivamente ciclico), allora N è finitamente generato (rispettivamente ciclico).*

Dimostrazione. Esercizio. □

Osservazione 3.12. Se $f\colon M \to N$ è un omomorfismo iniettivo di A-moduli, allora $M \cong \mathrm{im}(f)$.

Definizione-Proposizione 3.13. *Per ogni coppia di A-moduli M e N*

$$\mathrm{Hom}_A(M,N) := \{f \in \mathrm{Hom}(M,N) \,:\, f \text{ è } A\text{-lineare}\}$$

è un sottogruppo di $\mathrm{Hom}(M,N)$ *e* $\mathrm{End}_A(M) := \mathrm{Hom}_A(M,M)$ *è un sottoanello di* $\mathrm{End}(M)$*. Se inoltre A è commutativo, allora* $\mathrm{Hom}_A(M,N)$ *(e quindi in particolare* $\mathrm{End}_A(M)$*) è un A-modulo con moltiplicazione per scalari af (per ogni $a \in A$ e per ogni $f \in \mathrm{Hom}_A(M,N)$) definita da*

$$(af)(x) := af(x) = f(ax)\ \forall\, x \in M.$$

Dimostrazione. Esercizio. □

4. Moduli quoziente

Proposizione 4.1. *Sia M un A-modulo e sia $M' \subseteq M$ un sottomodulo. Il gruppo abeliano (additivo) M/M' con moltiplicazione per scalari*

$$A \times M/M' \to M/M'$$
$$(a, x + M') \mapsto ax + M'$$

è un A-modulo. Inoltre la proiezione al quoziente $\pi\colon M \to M/M'$, $x \mapsto x + M'$ è A-lineare, suriettiva e $\ker(\pi) = M'$.

Dimostrazione. Esercizio. □

Esempio 4.2. $M/M \cong \{0\}$ e $M/\{0\} \cong M$ per ogni modulo M (nel secondo caso $\pi\colon M \to M/\{0\}$ è un isomorfismo).

Esempio 4.3. A/I è un A-modulo per ogni ideale sinistro I di A.

Osservazione 4.4. Se M è un modulo finitamente generato (rispettivamente ciclico) e M' è un sottomodulo di M, anche M/M' è finitamente generato (rispettivamente ciclico): ciò segue dalla Proposizione 3.11, applicata alla proiezione al quoziente $\pi\colon M \to M/M'$.

Proposizione 4.5. *Sia M un modulo e sia $M' \subseteq M$ un sottomodulo. I sottomoduli di M/M' sono tutti e soli della forma M''/M' con $M'' \subseteq M$ sottomodulo tale che $M' \subseteq M''$.*

Dimostrazione. Esercizio. □

Indicando sempre con $\pi\colon M \to M/M'$ la proiezione al quoziente, il risultato seguente mostra che per ogni altro A-modulo N la funzione

$$\mathrm{Hom}_A(M/M', N) \to \mathrm{Hom}_A(M, N)$$
$$g \mapsto g \circ \pi$$

è iniettiva con immagine $\{f \in \mathrm{Hom}_A(M,N) \,:\, M' \subseteq \ker(f)\}$.

Teorema di omomorfismo (per moduli)**.** *Sia $f\colon M \to N$ un omomorfismo di moduli e sia $M' \subseteq \ker(f)$ un sottomodulo. Allora esiste un unico omomorfismo di moduli $g\colon M/M' \to N$ tale che $g(x + M') = f(x)$ per ogni $x \in M$. Inoltre $\mathrm{im}(g) = \mathrm{im}(f)$ (in particolare g è suriettivo se e solo se f lo è) e $\ker(g) = \ker(f)/M'$ (in particolare g è iniettivo se e solo se $M' = \ker(f)$).*

Dimostrazione. Esercizio. □

Primo teorema di isomorfismo (per moduli)**.** *Sia $f\colon M \to N$ un omomorfismo di moduli. Allora $\mathrm{im}(f) \cong M/\ker(f)$ (come moduli).*

Dimostrazione. Esercizio. □

Secondo teorema di isomorfismo (per moduli)**.** *Sia M un modulo e siano $M', M'' \subseteq M$ sottomoduli. Allora $M'/(M' \cap M'') \cong (M' + M'')/M''$ (come moduli).*

Dimostrazione. Esercizio. □

Terzo teorema di isomorfismo (per moduli)**.** *Sia M un modulo e siano $M'' \subseteq M' \subseteq M$ sottomoduli. Allora $(M/M'')/(M'/M'') \cong M/M'$ (come moduli).*

Dimostrazione. Esercizio. □

Lemma 4.6. *Se I è un ideale sinistro di A, allora $\mathrm{Ann}_A(A/I) \subseteq I$. Inoltre $\mathrm{Ann}_A(A/I) = I$ se e solo se I è un ideale (bilatero) di A.*

Dimostrazione. Se $a \in \mathrm{Ann}_A(A/I)$, si ha $a(1+I) = a+I = I$, per cui $a \in I$: questo dimostra $\mathrm{Ann}_A(A/I) \subseteq I$. Poiché $\mathrm{Ann}_A(A/I)$ è un ideale (per la Definizione-Proposizione 2.9), è ovvio che I è un ideale se $\mathrm{Ann}_A(A/I) = I$. Resta quindi da verificare che $I \subseteq \mathrm{Ann}_A(A/I)$ se I è un ideale. In effetti, dato $b \in I$, per ogni $a \in A$ si ha $b(a + I) = ba + I = I$ (perché $ba \in I$), il che dimostra che $b \in \mathrm{Ann}_A(A/I)$. □

Proposizione 4.7. *Un A-modulo M è ciclico se e solo se è isomorfo a A/I per qualche ideale sinistro I di A; inoltre, se $M = \langle x \rangle_A$, allora $M \cong A/\mathrm{Ann}_A(x)$. Se A è commutativo e I e J sono due ideali di A, allora $A/I \cong A/J$ (come A-moduli) se e solo se $I = J$.*

Dimostrazione. Segue dall'Esempio 2.16 e dall'Osservazione 4.4 che A/I è ciclico per ogni ideale sinistro I di A.

Viceversa, se $M = \langle x \rangle_A$ è un A-modulo ciclico, la funzione A-lineare $f_x \colon A \to M$ dell'Esempio 3.6 è tale che $\mathrm{im}(f_x) = \langle x \rangle_A = M$. Per il primo teorema di isomorfismo si ha $M = \mathrm{im}(f_x) \cong A/\ker(f_x)$, e per definizione $\ker(f_x) = \mathrm{Ann}_A(x)$.

Se A è commutativo, $\mathrm{Ann}_A(A/I) = I$ e $\mathrm{Ann}_A(A/J) = J$ per il Lemma 4.6. Dunque $I = J$ se $A/I \cong A/J$, dato che moduli isomorfi hanno chiaramente lo stesso annullatore. □

Corollario 4.8. *Un A-modulo è semplice se e solo se è isomorfo a A/I per qualche ideale sinistro massimale[3] I di A; in particolare, esiste un A-modulo semplice se $A \neq \{0\}$.[4] Se A è commutativo e I e J sono due ideali massimali di A, allora $A/I \cong A/J$ (come A-moduli) se e solo se $I = J$.*

Dimostrazione. Un A-modulo semplice M è necessariamente ciclico, generato da ogni $x \in M \setminus \{0\}$: infatti il sottomodulo $\langle x \rangle_A$ di M, non potendo essere $\{0\}$, deve essere M. Tenendo conto della Proposizione 4.7, basta allora dimostrare che, se I è un ideale sinistro di A, allora A/I è un A-modulo semplice se e solo se I è massimale. Ciò segue subito dalla Proposizione 4.5. □

Esempio 4.9. Se A è un anello con divisione, gli unici ideali sinistri di A sono $\{0\}$ e A. Segue allora dalla Proposizione 4.7 e dal Corollario 4.8 che, a meno di isomorfismo, gli unici A-moduli ciclici sono $A \cong A/\{0\}$ e $\{0\} \cong A/A$, e l'unico A-modulo semplice è A.

Esempio 4.10. Se $A = \mathbb{Z}$ dalla Proposizione 4.7 si ritrova il ben noto fatto che (a meno di isomorfismo) i gruppi (abeliani) ciclici sono tutti e soli della forma $\mathbb{Z}/n\mathbb{Z}$ con $n \in \mathbb{N}$, e che tali gruppi sono a due a due non isomorfi. D'altra parte, dal Corollario 4.8 segue che i gruppi abeliani semplici sono tutti e soli della forma $\mathbb{Z}/p\mathbb{Z}$ con p numero primo, e che tali gruppi sono a due a due non isomorfi. Il problema di classificare i gruppi non abeliani semplici è invece enormemente più complicato.

Osservazione 4.11. Se A è commutativo e I e J sono due ideali (massimali) distinti di A, è possibile che $A/I \cong A/J$ come anelli. Questo succede per esempio se $A = K[X]$, $I = (X)$ e $J = (X-1)$, nel qual caso $A/I \cong A/J \cong K$ come anelli.

5. Prodotti e somme dirette di moduli

Definizione-Proposizione 5.1. *Sia M_λ ($\lambda \in \Lambda$) un insieme di A-moduli.*

[3] Ovviamente si dice che un ideale sinistro I di A è *massimale* se $I \neq A$ e gli unici ideali sinistri di A contenenti I sono I e A.

[4] Con lo stesso argomento del caso commutativo si dimostra che, se $A \neq \{0\}$, esiste un ideale sinistro massimale di A, e più in generale che, se $I \subsetneq A$ è un ideale sinistro, esiste un ideale sinistro massimale di A contenente I.

(1) *Il* prodotto *degli M_λ è il prodotto cartesiano $\prod_{\lambda\in\Lambda} M_\lambda$ con la struttura di A-modulo definita da*

$$(x_\lambda)_{\lambda\in\Lambda} + (y_\lambda)_{\lambda\in\Lambda} := (x_\lambda + y_\lambda)_{\lambda\in\Lambda}, \qquad a(x_\lambda)_{\lambda\in\Lambda} := (ax_\lambda)_{\lambda\in\Lambda}$$

per ogni $(x_\lambda)_{\lambda\in\Lambda}, (y_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} M_\lambda$ e per ogni $a \in A$.

(2) *Il* coprodotto *(o la* somma diretta*) degli M_λ è il sottomodulo di $\prod_{\lambda\in\Lambda} M_\lambda$ denotato $\coprod_{\lambda\in\Lambda} M_\lambda$ o $\bigoplus_{\lambda\in\Lambda} M_\lambda$ e costituito dagli $(x_\lambda)_{\lambda\in\Lambda}$ tali che $\#\{\lambda \in \Lambda : x_\lambda \neq 0\} < \infty$.*

Dimostrazione. Esercizio. □

Osservazione 5.2. Chiaramente $\bigoplus_{\lambda\in\Lambda} M_\lambda = \prod_{\lambda\in\Lambda} M_\lambda$ se e solo se l'insieme $\{\lambda \in \Lambda : M_\lambda \neq \{0\}\}$ è finito (il che è vero in particolare se Λ è finito). Nel caso in cui $M_\lambda = M$ per ogni $\lambda \in \Lambda$, si può scrivere M^Λ (rispettivamente $M^{(\Lambda)}$) invece di $\prod_{\lambda\in\Lambda} M$ (rispettivamente $\bigoplus_{\lambda\in\Lambda} M$). Se poi $\#\Lambda = n < \infty$, si scrive di solito M^n invece di $M^\Lambda = M^{(\Lambda)}$.

Il risultato seguente mostra che prodotto e coprodotto di moduli soddisfano ciascuno una *proprietà universale*, "duale" una dell'altra.

Proposizione 5.3. *Sia M_λ ($\lambda \in \Lambda$) un insieme di A-moduli.*

(1) *Per ogni $\mu \in \Lambda$ la proiezione $\mathrm{pr}_\mu \colon \prod_{\lambda\in\Lambda} M_\lambda \to M_\mu$, $(x_\lambda)_{\lambda\in\Lambda} \mapsto x_\mu$ è A-lineare. Inoltre, date funzioni A-lineari $f_\mu \colon M \to M_\mu$ per ogni $\mu \in \Lambda$, esiste un'unica funzione A-lineare $f \colon M \to \prod_{\lambda\in\Lambda} M_\lambda$ tale che $f_\mu = \mathrm{pr}_\mu \circ f$ per ogni $\mu \in \Lambda$.*

(2) *Per ogni $\mu \in \Lambda$ l'inclusione $\mathrm{in}_\mu \colon M_\mu \to \bigoplus_{\lambda\in\Lambda} M_\lambda$, $x \mapsto (x_\lambda)_{\lambda\in\Lambda}$ con $x_\mu := x$ e $x_\lambda := 0$ se $\lambda \neq \mu$ è A-lineare. Inoltre, date funzioni A-lineari $f_\mu \colon M_\mu \to M$ per ogni $\mu \in \Lambda$, esiste un'unica funzione A-lineare $f \colon \bigoplus_{\lambda\in\Lambda} M_\lambda \to M$ tale che $f_\mu = f \circ \mathrm{in}_\mu$ per ogni $\mu \in \Lambda$.*

Dimostrazione. (1) È immediato verificare che pr_μ è A-lineare per ogni $\mu \in \Lambda$. È anche chiaro che, insiemisticamente, date funzioni (non necessariamente A-lineari) $f_\mu \colon M \to M_\mu$ per ogni $\mu \in \Lambda$, esiste un'unica funzione $f \colon M \to \prod_{\lambda\in\Lambda} M_\lambda$ tale che $f_\mu = \mathrm{pr}_\mu \circ f$ per ogni $\mu \in \Lambda$, definita da $f(x) := (f_\lambda(x))_{\lambda\in\Lambda}$ per ogni $x \in M$. Per concludere basta allora verificare che f è A-lineare se (e solo se) $\mathrm{pr}_\mu \circ f$ è A-lineare per ogni $\mu \in \Lambda$, il che segue subito dal fatto che la struttura di A-modulo su $\prod_{\lambda\in\Lambda} M_\lambda$ è definita componente per componente.

(2) È immediato verificare che in_μ è A-lineare per ogni $\mu \in \Lambda$. Date poi funzioni A-lineari $f_\mu \colon M_\mu \to M$ per ogni $\mu \in \Lambda$, se esiste una funzione A-lineare $f \colon \bigoplus_{\lambda\in\Lambda} M_\lambda \to M$ tale che $f_\mu = f \circ \mathrm{in}_\mu$ per ogni $\mu \in \Lambda$, deve essere

$$f((x_\lambda)_{\lambda\in\Lambda}) = f\left(\sum_{\lambda\in\Lambda} \mathrm{in}_\lambda(x_\lambda)\right) = \sum_{\lambda\in\Lambda} f(\mathrm{in}_\lambda(x_\lambda)) = \sum_{\lambda\in\Lambda} f_\lambda(x_\lambda)$$

per ogni $(x_\lambda)_{\lambda\in\Lambda} \in \bigoplus_{\lambda\in\Lambda} M_\lambda$ (si noti che tali somme possibilmente infinite hanno senso perché, per definizione di $\bigoplus_{\lambda\in\Lambda} M_\lambda$, solo un numero finito di addendi sono non nulli). Per concludere basta osservare che f è effettivamente A-lineare se è definita da $f((x_\lambda)_{\lambda\in\Lambda}) := \sum_{\lambda\in\Lambda} f_\lambda(x_\lambda)$ per ogni $(x_\lambda)_{\lambda\in\Lambda} \in \bigoplus_{\lambda\in\Lambda} M_\lambda$.

□

Esempio 5.4. Se Λ è infinito e $M_\lambda \neq \{0\}$ per ogni $\lambda \in \Lambda$, allora l'A-modulo $M := \bigoplus_{\lambda\in\Lambda} M_\lambda$ non è finitamente generato (dunque, se $A \neq \{0\}$, esistono sempre A-moduli non finitamente generati, per esempio $A^{(\Lambda)}$ con Λ infinito). Infatti, posto $\mathrm{Supp}(x) := \{\lambda \in \Lambda : \mathrm{pr}_\lambda(x) \neq 0\}$ per ogni $x \in M$ (si noti che $\mathrm{Supp}(x)$ è finito per definizione di somma diretta), si ha chiaramente $\mathrm{Supp}(x) \subseteq \mathrm{Supp}(U) := \bigcup_{y\in U} \mathrm{Supp}(y)$ per ogni $U \subseteq M$ e per ogni $x \in \langle U\rangle_A$. Ora, se U è finito, anche $\mathrm{Supp}(U)$ lo è, dunque esiste $\mu \in \Lambda \setminus \mathrm{Supp}(U)$ ed esiste $x \in M$ tale che $\mathrm{pr}_\mu(x) \neq 0$ (per esempio $x = \mathrm{in}_\mu(z)$ con $z \in M_\mu \setminus \{0\}$), cioè $\mu \in \mathrm{Supp}(x)$. Dunque $x \notin \langle U\rangle_A$, il che dimostra che M non è generato da U, e quindi non è finitamente generato.

Esempio 5.5. Se N_λ (con $\lambda \in \Lambda$) sono sottomoduli di un modulo M, per la Proposizione 5.3 esiste un unico omomorfismo $f\colon \bigoplus_{\lambda\in\Lambda} N_\lambda \to M$ tale che $f \circ \mathrm{in}_\mu\colon N_\mu \to M$ è l'inclusione naturale per ogni $\mu \in \Lambda$. Tenendo conto della definizione esplicita di f data nella dimostrazione della Proposizione 5.3, risulta chiaro che $\mathrm{im}(f) = \sum_{\lambda\in\Lambda} N_\lambda$. Se f è iniettiva, si ha dunque $\sum_{\lambda\in\Lambda} N_\lambda \cong \bigoplus_{\lambda\in\Lambda} N_\lambda$ e, con leggero abuso di notazione, si indicherà con $\bigoplus_{\lambda\in\Lambda} N_\lambda$ il sottomodulo $\sum_{\lambda\in\Lambda} N_\lambda$ di M. Si noti che f è iniettiva se e solo se $N_\mu \cap (\sum_{\lambda\in\Lambda\setminus\{\mu\}} N_\lambda) = \{0\}$ per ogni $\mu \in \Lambda$.

Osservazione 5.6. Se $M \cong \bigoplus_{\lambda\in\Lambda} M_\lambda$, l'immagine (attraverso tale isomorfismo) N_λ di ciascun $\mathrm{in}_\lambda(M_\lambda)$ è un sottomodulo di M e $N_\lambda \cong M_\lambda$. Risulta chiaramente $M = \bigoplus_{\lambda\in\Lambda} N_\lambda$.

Osservazione 5.7. Se N_1 e N_2 sono sottomoduli di un modulo M tali che $M = N_1 \oplus N_2$ (cioè $N_1 \cap N_2 = \{0\}$ e $N_1 + N_2 = M$), allora $M/N_1 \cong N_2$ (e $M/N_2 \cong N_1$). Infatti $\mathrm{pr}_2\colon M = N_1 \oplus N_2 = N_1 \times N_2 \to N_2$ è un omomorfismo suriettivo con $\ker(\mathrm{pr}_2) = N_1$. L'isomorfismo cercato segue allora dal primo teorema di isomorfismo per moduli.

6. Moduli liberi

In questa sezione assumiamo $A \neq \{0\}$.

Definizione 6.1. Un sottoinsieme U di un A-modulo M è *linearmente indipendente* se, dati $x_1, \dots, x_n \in U$ distinti e $a_1, \dots, a_n \in A$, si ha $\sum_{i=1}^n a_i x_i = 0_M$ se e solo se $a_1 = \cdots = a_n = 0_A$. Si dice che U è una *base* di M se U è linearmente indipendente e genera M.

Definizione 6.2. Un A-modulo è *libero* se ha una base.

Esempio 6.3. Per ogni insieme Λ l'A-modulo $A^{(\Lambda)}$ è libero: chiaramente una sua base è $\{e_\lambda := \mathrm{in}_\lambda(1_A) : \lambda \in \Lambda\}$.

Proposizione 6.4. *Sia L un A-modulo libero e sia $\{y_\lambda : \lambda \in \Lambda\}$ una sua base con $y_\lambda \neq y_\mu$ se $\lambda \neq \mu$. Dato un altro A-modulo M e dati $x_\lambda \in M$ per ogni $\lambda \in \Lambda$, esiste un'unica funzione A-lineare $f\colon L \to M$ tale che $f(y_\lambda) = x_\lambda$ per ogni $\lambda \in \Lambda$. Inoltre f è suriettiva se e solo se $\{x_\lambda : \lambda \in \Lambda\}$ genera M e f è iniettiva se e solo se $\{x_\lambda : \lambda \in \Lambda\}$ è linearmente indipendente e $x_\lambda \neq x_\mu$ se $\lambda \neq \mu$.*

Dimostrazione. Esercizio. □

Corollario 6.5. *Ogni A-modulo è isomorfo a un quoziente di $A^{(\Lambda)}$ (quindi di un A-modulo libero, grazie all'Esempio 6.3) per qualche insieme Λ. Inoltre un A-modulo è finitamente generato se e solo se è isomorfo a un quoziente di A^n per qualche $n \in \mathbb{N}$.*

Dimostrazione. Dato un A-modulo M, esistono elementi $x_\lambda \in M$ (con $\lambda \in \Lambda$) tali che $M = \langle x_\lambda : \lambda \in \Lambda \rangle_A$ (per esempio, si può scegliere $\Lambda = M$ e $x_\lambda = \lambda$ per ogni $\lambda \in M$). Ricordando l'Esempio 6.3, per la Proposizione 6.4 esiste un omomorfismo $f\colon A^{(\Lambda)} \to M$ tale che $f(e_\lambda) = x_\lambda$ per ogni $\lambda \in \Lambda$; inoltre f è suriettivo. Per il primo teorema di isomorfismo per moduli questo implica che $M \cong A^{(\Lambda)}/\ker(f)$. Se poi M è finitamente generato, si può prendere Λ finito, per cui $A^{(\Lambda)} = A^n$ con $n = \#\Lambda$. D'altra parte, se $M \cong A^n/N$ per qualche $n \in \mathbb{N}$ e qualche sottomodulo N di A^n, allora esiste un omomorfismo suriettivo $A^n \to M$. Tenendo conto che A^n è finitamente generato (sempre per lEsempio 6.3), anche M lo è per la Proposizione 3.11. □

Corollario 6.6. *Un A-modulo è libero se e solo se è isomorfo a $A^{(\Lambda)}$ per qualche insieme Λ. Più precisamente, un A-modulo è isomorfo a $A^{(\Lambda)}$ se e solo se ha una base di cardinalità $\#\Lambda$.*

Dimostrazione. Il fatto che un A-modulo isomorfo a $A^{(\Lambda)}$ abbia una base di cardinalità $\#\Lambda$ segue subito dall'Esempio 6.3, tenendo conto che chiaramente un isomorfismo manda una base in una base. Viceversa, se un A-modulo M ha una base di cardinalità $\#\Lambda$, si può ovviamente scrivere tale base come $\{x_\lambda : \lambda \in \Lambda\}$ con $x_\lambda \neq x_\mu$ se $\lambda \neq \mu$. Per la Proposizione 6.4 esiste allora un'unica funzione A-lineare $f\colon A^{(\Lambda)} \to M$ tale che $f(e_\lambda) = x_\lambda$ per ogni $\lambda \in \Lambda$; inoltre f è un isomorfismo. □

Esempio 6.7. Se $n > 1$ è un intero, lo $\mathbb{Z}$-modulo $\mathbb{Z}/n\mathbb{Z}$ non è libero. Infatti $\mathbb{Z}/n\mathbb{Z}$ non è isomorfo a $\mathbb{Z}^{(\Lambda)}$ per nessun insieme Λ, dato che $\mathbb{Z}^{(\Lambda)}$ è banale se $\Lambda = \emptyset$, e altrimenti è infinito.

Proposizione 6.8. *Tutti gli A-moduli sono liberi se e solo se A è un anello con divisione.*

Dimostrazione. Se A è un anello con divisione, va dimostrato che ogni A-modulo M ha una base. Sia $\mathcal{U}$ l'insieme di tutti i sottoinsiemi linearmente indipendenti di M, e ordiniamo $\mathcal{U}$ rispetto all'inclusione (cioè, se $U, U' \in \mathcal{U}$, definiamo $U \leq U'$ se e solo se $U \subseteq U'$). Chiaramente $\mathcal{U} \neq \emptyset$ (in ogni caso $\emptyset \in \mathcal{U}$). Inoltre ogni catena $\{U_\lambda : \lambda \in \Lambda\}$ di $\mathcal{U}$ ha un maggiorante in $\mathcal{U}$, cioè $U := \bigcup_{\lambda\in\Lambda} U_\lambda$ (ovviamente $U \subseteq M$, ed è facile vedere che U è linearmente indipendente). Per il lemma di Zorn esiste allora $U \in \mathcal{U}$ massimale, e basta dimostrare che U (che per definizione è linearmente indipendente) è una base di M. Supponiamo per assurdo che $M' := \langle U \rangle_A \subsetneq M$ e sia $x \in M \setminus M'$. Per la massimalità di U, l'insieme $U \cup \{x\}$ non è linearmente indipendente, dunque esistono $x_1, \ldots, x_n \in U$ distinti e $a, a_1, \ldots, a_n \in A$ non tutti nulli tali che $ax + \sum_{i=1}^n a_i x_i = 0$. L'indipendenza lineare di U implica $a \neq 0$, e dunque $x = -a^{-1} \sum_{i=1}^n a_i x_i \in M'$, assurdo.

Se viceversa ogni A-modulo è libero, sia M un A-modulo semplice (M esiste per il Corollario 4.8). Poiché M è libero, per il Corollario 6.6 esiste un insieme Λ tale che $A^{(\Lambda)} \cong M$. Allora anche $A^{(\Lambda)}$ è semplice, e perciò non

può essere né $\Lambda = \emptyset$ (perché $A^0 = \{0\}$) né $\#\Lambda > 1$ (perché in quel caso ogni singola componente di $A^{(\Lambda)}$ costituisce un sottomodulo non banale, isomorfo a A). Dunque $A^{(\Lambda)} \cong A$ è un A-modulo semplice, il che implica che A è un anello con divisione per l'Esempio 2.19. □

Per la dimostrazione della Proposizione 6.9 nel caso non finitamente generato assumeremo la conoscenza dei seguenti risultati di teoria degli insiemi.

- Se Λ e Λ' sono due insiemi tali che $\#\Lambda \leq \#\Lambda'$ (cioè esiste una funzione iniettiva $\Lambda \to \Lambda'$) e $\#\Lambda' \leq \#\Lambda$, allora $\#\Lambda = \#\Lambda$.
- Se Λ è un insieme infinito, allora $\#\Lambda = \#(\Lambda \times \mathbb{N})$.

Proposizione 6.9. *Se A è un anello con divisione, tutte le basi di un A-modulo (necessariamente libero per la Proposizione 6.8) hanno la stessa cardinalità.*

Dimostrazione. Per il Corollario 6.6 basta dimostrare che, se Λ e Λ' sono insiemi tali che $A^{(\Lambda')} \cong A^{(\Lambda)}$ come A-moduli, allora $\#\Lambda = \#\Lambda'$. Per ogni $\lambda \in \Lambda$ (rispettivamente $\lambda' \in \Lambda'$) sia $e_\lambda := \mathrm{in}_\lambda(1) \in A^{(\Lambda)}$ (rispettivamente $e_{\lambda'} := \mathrm{in}_{\lambda'}(1) \in A^{(\Lambda')}$) e sia $f\colon A^{(\Lambda')} \to A^{(\Lambda)}$ un isomorfismo di A-moduli.

Se almeno uno tra Λ e Λ' è finito, si può supporre $\Lambda' = \{1, \dots, n\}$ (quindi $A^{(\Lambda')} = A^n$) per qualche $n \in \mathbb{N}$, e va dimostrato che $\#\Lambda = n$. Procediamo per induzione su n: il caso $n = 0$ essendo banale, possiamo assumere che $n > 0$ e che $A^{(\tilde{\Lambda})} \cong A^{n-1}$ (per qualche insieme $\tilde{\Lambda}$) implichi $\#\tilde{\Lambda} = n - 1$. Chiaramente $A^n = M \oplus N$ con $M := \langle e_1, \dots, e_{n-1} \rangle_A \cong A^{n-1}$ e $N := \langle e_n \rangle_A \cong A$. Poiché $f(e_n) \neq 0$ (essendo $e_n \neq 0$ e f iniettivo), esiste $\mu \in \Lambda$ tale che $c := \mathrm{pr}_\mu(f(e_n)) \neq 0$. Posto $\tilde{\Lambda} := \Lambda \setminus \{\mu\}$, sia $M' := \langle e_\lambda : \lambda \in \tilde{\Lambda} \rangle_A \cong A^{(\tilde{\Lambda})}$ e $N' := f(N) = \langle f(e_n) \rangle_A$ (l'uguaglianza segue dalla Proposizione 3.11), e osserviamo che $N' \cong A$ per l'Esempio 4.9. Vogliamo intanto dimostrare che

$$A^{(\Lambda)} = M' \oplus N'. \tag{6.1}$$

Sia infatti $x \in M' \cap N'$: esiste $a \in A$ tale che $x = af(e_n)$ (perché $x \in N'$) e $\mathrm{pr}_\mu(x) = 0$ (perché $x \in M'$). Ne segue che $0 = \mathrm{pr}_\mu(af(e_n)) = ac$, per cui $a = 0$ (dato che $c \neq 0$); dunque $x = 0$, e ciò dimostra che $M' \cap N' = \{0\}$. D'altra parte, se $y \in A^{(\Lambda)}$, esiste $a = \mathrm{pr}_\mu(y)c^{-1} \in A$ tale che $\mathrm{pr}_\mu(y) = ac = \mathrm{pr}_\mu(af(e_n))$, e quindi $y = y - af(e_n) + af(e_n)$ con $y - af(e_n) \in M'$ (perché $\mathrm{pr}_\mu(y - af(e_n)) = 0$) e $af(e_n) \in N'$. Pertanto $M' + N' = A^{(\Lambda)}$, il che conclude la dimostrazione di (6.1). Si ottiene allora (ricordando l'Osservazione 5.7) $A^{(\Lambda)}/N' \cong M'$, e analogamente $A^n/N \cong M$. Si ha dunque

$$A^{n-1} \cong M \cong A^n/N \cong f(A^n)/f(N) = A^{(\Lambda)}/N' \cong M' \cong A^{(\tilde{\Lambda})},$$

da cui segue $\#\tilde{\Lambda} = n - 1$ per l'ipotesi induttiva, e perciò $\#\Lambda = n$.

Se invece sia Λ che Λ' sono infiniti, per ogni $\lambda' \in \Lambda'$ sia (usando la notazione dell'Esempio 5.4) $\Lambda_{\lambda'} := \mathrm{Supp}(f(e_{\lambda'})) \subset \Lambda$. Chiaramente $\mathrm{Supp}(f(x')) \subseteq \bigcup_{\lambda' \in \Lambda'} \Lambda_{\lambda'}$ per ogni $x' \in A^{(\Lambda')}$, e da ciò segue facilmente (grazie anche alla suriettività di f) che $\Lambda = \bigcup_{\lambda' \in \Lambda'} \Lambda_{\lambda'}$. Tenendo conto che ogni $\Lambda_{\lambda'}$ è finito, se ne deduce che

$$\#\Lambda = \# \bigcup_{\lambda' \in \Lambda'} \Lambda_{\lambda'} \leq \# \coprod_{\lambda' \in \Lambda'} \Lambda_{\lambda'} \leq \# \coprod_{\lambda' \in \Lambda'} \mathbb{N} = \#(\Lambda' \times \mathbb{N}) = \#\Lambda'.$$

Per simmetria vale anche $\#\Lambda' \leq \#\Lambda$, e quindi $\#\Lambda = \#\Lambda'$. □

Osservazione 6.10. Per A qualunque non è sempre vero che tutte le basi di un A-modulo libero M abbiano la stessa cardinalità. Nei casi in cui questo è vero (per esempio se A è un anello con divisione, come si è appena visto), tale cardinalità comune si chiama *rango* di M e si indica con $\mathrm{rk}_A(M)$ (o semplicemente $\mathrm{rk}(M)$). Il rango di un K-spazio vettoriale V è meglio noto come *dimensione* di V e si indica con $\dim_K(V)$ (o semplicemente $\dim(V)$).

Esempio 6.11. È possibile dimostrare che, se V è un K-spazio vettoriale di dimensione infinita, allora per l'anello (non commutativo) $A := \mathrm{End}_K(V)$ vale $A \cong A^2$ (come A-moduli).

7. Restrizione ed estensione degli scalari

Se $f\colon A \to B$ è un omomorfismo di anelli, è immediato verificare che ogni B-modulo M è in modo naturale un A-modulo con moltiplicazione per scalari definita da $ax := f(a)x$ per ogni $a \in A$ e per ogni $x \in M$ (in particolare, B stesso è un A-modulo). Si dice anche che la struttura indotta di A-modulo su M è ottenuta da quella di B-modulo per *restrizione degli scalari*[5] attraverso f. Si noti che, se la struttura di B-modulo su M è data dall'omomorfismo di anelli $\beta\colon B \to \mathrm{End}(M)$, quella indotta di A-modulo è data da $\beta \circ f\colon A \to \mathrm{End}(M)$. È anche evidente che ogni B-sottomodulo di M è pure un A-sottomodulo, e che, se N è un altro B-modulo e $g\colon M \to N$ è B-lineare, allora g è anche A-lineare.

Osservazione 7.1. Dato $U \subseteq M$, si ha chiaramente $\langle U\rangle_A \subseteq \langle U\rangle_B$, e quindi $\langle U\rangle_B = M$ se $\langle U\rangle_A = M$. In particolare, M è finitamente generato come B-modulo se lo è come A-modulo. In generale non vale il viceversa: infatti B è sempre finitamente generato (anche ciclico) come B-modulo, ma non necessariamente come A-modulo (per esempio, se $f\colon A \to B = A[X]$ è l'omomorfismo di inclusione, dato che $A[X] \cong A^{(\mathbb{N})}$ come A-modulo).

Esiste anche un'altra procedura (più complicata), detta di *estensione degli scalari* attraverso un omomorfismo di anelli $f\colon A \to B$, che permette di passare da A-moduli (e omomorfismi di A-moduli) a B-moduli (e omomorfismi di B-moduli). Ce ne occuperemo solo nel caso particolare (e facile da trattare) in cui l'omomorfismo di anelli è una proiezione al quoziente $\pi\colon A \to A/I$ (con I ideale bilatero di A).

Notiamo intanto che, se M è un A/I-modulo, allora (vedendo M come A-modulo per restrizione degli scalari attraverso π) ovviamente $IM = \{0\}$, cioè $I \subseteq \mathrm{Ann}_A(M)$. Viceversa, se M è un A-modulo tale che $IM = \{0\}$, è molto facile verificare che M è anche un A/I-modulo con moltiplicazione per scalari definita da $(a + I)x := ax$ per ogni $a \in A$ e per ogni $x \in M$. In effetti, se la struttura di A-modulo su M è definita dall'omomorfismo di anelli $\alpha\colon A \to \mathrm{End}(M)$, quella di A/I-modulo è definita dall'omomorfismo di anelli $\alpha'\colon A/I \to \mathrm{End}(M)$ indotto da α (cioè tale che $\alpha'(a + I) = \alpha(a)$ per ogni $a \in A$) grazie al teorema di omomorfismo per anelli, che può essere applicato perché $I \subseteq \ker(\alpha) = \mathrm{Ann}_A(M)$.

[5] Il termine è veramente appropriato solo quando f è un'inclusione di A come sottoanello di B, ma si può usare anche quando f non è iniettivo.

Osservazione 7.2. Se M è un A/I-modulo (e quindi un A-modulo tale che $IM = \{0\}$), è chiaro che gli A/I-sottomoduli di M coincidono con gli A-sottomoduli di M. Se poi N è un altro A/I-modulo, una funzione $M \to N$ è A-lineare se e solo se è A/I-lineare; ne segue anche che $M \cong N$ come A-moduli se e solo se $M \cong N$ come A/I-moduli.

In generale, se M è un A-modulo qualunque, l'A-modulo M/IM soddisfa chiaramente $I(M/IM) = \{0\}$, e dunque è in modo naturale un A/I-modulo per quanto visto sopra. Si dice appunto che l'A/I-modulo M/IM è ottenuto da M per estensione degli scalari attraverso $\pi\colon A \to A/I$. Inoltre ogni omomorfismo di A-moduli $g\colon M \to N$ induce un omomorfismo $\overline{g}\colon M/IM \to N/IN$, $x + IM \mapsto g(x) + IN$ di A-moduli, e quindi anche di A/I-moduli per l'Osservazione 7.2. L'esistenza di $\overline{g}$ segue dal teorema di omomorfismo per moduli, applicato a $M \xrightarrow{g} N \xrightarrow{p} N/IN$ (dove p indica la proiezione al quoziente). Si noti che $IM \subseteq \ker(p \circ g)$ perché chiaramente $g(IM) \subseteq IN$.

Osservazione 7.3. È chiaro che, se una funzione A-lineare $g\colon M \to N$ è suriettiva, anche $\overline{g}\colon M/IM \to N/IN$ lo è. È vero inoltre che, se g è un isomorfismo, anche $\overline{g}$ lo è e $\overline{g}^{-1} = \overline{g^{-1}}$. È infatti facile vedere che

$$\overline{g^{-1}} \circ \overline{g} = \overline{g^{-1} \circ g} = \overline{\mathrm{id}_M} = \mathrm{id}_{M/IM}$$

e analogamente $\overline{g} \circ \overline{g^{-1}} = \mathrm{id}_{N/IN}$. Non è invece sempre vero che, se g è iniettiva, anche $\overline{g}$ lo è (dunque, in generale, se $M' \subseteq M$ è un sottomodulo, non si può identificare M'/IM' con un sottomodulo di M/IM).

Esempio 7.4. Se $A = \mathbb{Z}$, $n > 1$ è un intero, $I = n\mathbb{Z}$ e $M = N = \mathbb{Z}$, l'omomorfismo $g\colon \mathbb{Z} \to \mathbb{Z}$, $a \mapsto na$ è iniettivo, ma $\overline{g}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ è l'omomorfismo nullo, che non è iniettivo.

Osservazione 7.5. Se $M = \bigoplus_{\lambda \in \Lambda} M_\lambda$ come A-moduli, è facile vedere che $M/IM \cong \bigoplus_{\lambda \in \Lambda} M_\lambda/IM_\lambda$ come A-moduli, e quindi anche come A/I-moduli per l'Osservazione 7.2.

Lemma 7.6. *Se il rango di ogni A/I-modulo libero è ben definito, allora il rango di ogni A-modulo libero è ben definito.*

Dimostrazione. Ricordando il Corollario 6.6, la tesi è che, se Λ e Λ' sono due insiemi tali che $A^{(\Lambda)} \cong A^{(\Lambda')}$ (come A-moduli), allora $\#\Lambda = \#\Lambda'$. Dall'isomorfismo dato segue $A^{(\Lambda)}/IA^{(\Lambda)} \cong A^{(\Lambda')}/IA^{(\Lambda')}$ (come A/I-moduli) per l'Osservazione 7.3. Poiché $A^{(\Lambda)}/IA^{(\Lambda)} \cong (A/I)^{(\Lambda)}$ e $A^{(\Lambda')}/IA^{(\Lambda')} \cong (A/I)^{(\Lambda')}$ per l'Osservazione 7.5, si ottiene allora $(A/I)^{(\Lambda)} \cong (A/I)^{(\Lambda')}$ (come A/I-moduli), e dunque $\#\Lambda = \#\Lambda'$ grazie all'ipotesi. □

Corollario 7.7. *Se A è un anello commutativo non banale, il rango di ogni A-modulo libero è ben definito.*

Dimostrazione. Sia $I \subsetneq A$ un ideale massimale. Poiché A/I è un campo, il rango di ogni A/I-modulo libero è ben definito per la Proposizione 6.9. La tesi segue allora dal Lemma 7.6. □

8. Algebre

In questa sezione assumiamo che A sia commutativo.

Definizione 8.1. Una *A-algebra* è il dato di un anello B e di un omomorfismo di anelli $A \to Z(B)$.[6]

Con abuso di notazione spesso si dice semplicemente che un anello B è una A-algebra, soprattutto quando non ci sono dubbi sull'omomorfismo di anelli $A \to Z(B)$ (in particolare, quando A è un sottoanello di $Z(B)$).

Osservazione 8.2. Se B è una A-algebra, B è anche un A-modulo (per restrizione degli scalari) e chiaramente

$$a(bb') = (ab)b' = b(ab') \tag{8.1}$$

per ogni $a \in A$ e per ogni $b, b' \in B$. Viceversa, è facile dimostrare che, se B è un anello con una struttura di A-modulo che verifica (8.1), allora B è una A-algebra definita dall'omomorfismo di anelli $A \to Z(B)$, $a \mapsto a1_B$.

Esempio 8.3. Dare una struttura di A-algebra a un anello commutativo B equivale a dare un omomorfismo di anelli $A \to B$. In particolare, l'anello dei polinomi $A[X_1, \ldots, X_n]$ è una A-algebra con l'omomorfismo di inclusione $A \to A[X_1, \ldots, X_n]$.

Esempio 8.4. Ogni anello B ha un'unica struttura di $\mathbb{Z}$-algebra. È infatti chiaro che l'immagine dell'unico omomorfismo di anelli $\mathbb{Z} \to B$ (definito da $n \mapsto n_B$) è contenuta in $Z(B)$.

Esempio 8.5. È molto facile vedere che per ogni $n > 0$ l'anello $\mathrm{M}_n(A)$ è una A-algebra con l'omomorfismo di anelli $A \to Z(\mathrm{M}_n(A))$ che manda $a \in A$ nella matrice con tutti a sulla diagonale e 0 al di fuori della diagonale.

Esempio 8.6. Sia M un A-modulo e sia $\alpha\colon A \to \mathrm{End}(M)$ il corrispondente omomorfismo di anelli. Essendo A commutativo, per ogni $a, b \in A$ e per ogni $x \in M$ si ha $\alpha(a)(bx) = abx = bax = b\alpha(a)(x)$, cioè $\mathrm{im}(\alpha) \subseteq \mathrm{End}_A(M)$. D'altra parte, dal fatto che ogni elemento di $\mathrm{End}_A(M)$ è A-lineare segue immediatamente che $\mathrm{im}(\alpha) \subseteq Z(\mathrm{End}_A(M))$. Dunque $\mathrm{End}_A(M)$ è in modo naturale una A-algebra.

Definizione 8.7. Siano $f\colon A \to Z(B)$ e $g\colon A \to Z(C)$ due A-algebre. Un omomorfismo di anelli $h\colon B \to C$ è un *omomorfismo di A-algebre* se $g(a) = h(f(a))$ per ogni $a \in A$. Un *isomorfismo di A-algebre* è un omomorfismo biunivoco di A-algebre.

Osservazione 8.8. La composizione di omomorfismi (rispettivamente isomorfismi) di algebre è un omomorfismo (rispettivamente isomorfismo). Inoltre l'identità di un'algebra e l'inverso di un isomorfismo di algebre sono isomorfismi; dunque l'isomorfismo di algebre è una relazione di equivalenza. Inoltre un omomorfismo di algebre $h\colon B \to C$ è un isomorfismo se e solo se esiste un omomorfismo $h'\colon C \to B$ tale che $h' \circ h = \mathrm{id}_B$ e $h \circ h' = \mathrm{id}_C$.

Esempio 8.9. Ogni omomorfismo di anelli è un omomorfismo di $\mathbb{Z}$-algebre.

Esempio 8.10. Se $f\colon A \to Z(B)$ è una A-algebra, per ogni $b \in B$ esiste un unico omomorfismo di A-algebre $g\colon A[X] \to B$ tale che $g(X) = b$. È chiaro

[6] Ricordiamo che il *centro* $Z(B) := \{c \in B : cb = bc \ \forall\, b \in B\}$ è un sottoanello di B.

infatti che, se esiste, g deve essere definito da

$$g\left(\sum_{i\geq 0} a_i X^i\right) := \sum_{i\geq 0} f(a_i)b^i = \sum_{i\geq 0} a_i b^i$$

(dove nell'ultimo termine si usa la struttura di A-modulo su B) per ogni $\sum_{i\geq 0} a_i X^i \in A[X]$, ed è facile vedere che, con questa definizione, g è veramente un omomorfismo di A-algebre.

Esempio 8.11. Se L è un A-modulo libero di rango $n > 0$, le A-algebre $\mathrm{End}_A(L)$ e $\mathrm{M}_n(A)$ sono isomorfe. In effetti, scelta una base di L, un isomorfismo si ottiene mandando un elemento di $\mathrm{End}_A(L)$ nella matrice associata rispetto alla base.

9. Moduli noetheriani

Definizione-Proposizione 9.1. *Un A-modulo M è* noetheriano *se soddisfa una delle (e quindi tutte le) seguenti condizioni equivalenti.*

1. *Ogni successione crescente $\cdots \subseteq N_i \subseteq N_{i+1} \subseteq \cdots$ $(i \in \mathbb{N})$ di sottomoduli di M è stazionaria, cioè esiste $k \in \mathbb{N}$ tale che $N_i = N_k$ per ogni $i \geq k$.*
2. *Ogni sottoinsieme non vuoto dell'insieme dei sottomoduli di M ha un elemento massimale (rispetto all'inclusione).*
3. *Ogni sottomodulo di M è finitamente generato.*

Dimostrazione. (1) $\implies$ (2) Sia $\{N_\lambda : \lambda \in \Lambda\}$ un insieme non vuoto (dunque $\Lambda \neq \emptyset$) di sottomoduli di M, e supponiamo per assurdo che non abbia elementi massimali. Possiamo allora trovare $\lambda_i \in \Lambda$ tali che $N_{\lambda_i} \subsetneq N_{\lambda_{i+1}}$ per ogni $i \in \mathbb{N}$: basta scegliere λ_0 arbitrariamente, poi per induzione, dato λ_i, esiste λ_{i+1} con la proprietà richiesta perché N_{λ_i} non è massimale. È chiaro allora che $\cdots \subsetneq N_{\lambda_i} \subsetneq N_{\lambda_{i+1}} \subsetneq \cdots$ $(i \in \mathbb{N})$ è una successione crescente e non stazionaria di sottomoduli di M, assurdo.

(2) $\implies$ (3) Se N è un sottomodulo di M, per ipotesi l'insieme (non vuoto perché contiene $\{0\}$) dei sottomoduli finitamente generati di N ha un elemento massimale $N' \subseteq N$, e basta dimostrare che $N' = N$. Se per assurdo non fosse così, esisterebbe $x \in N \setminus N'$, e quindi $N' \subsetneq N'' := N' + \langle x\rangle_A \subseteq N$. Se $N' = \langle x_1, \ldots, x_n\rangle_A$, si ha $N'' = \langle x_1, \ldots, x_n, x\rangle_A$, assurdo per la massimalità di N'.

(3) $\implies$ (1) Data una successione crescente $\cdots \subseteq N_i \subseteq N_{i+1} \subseteq \cdots$ $(i \in \mathbb{N})$ di sottomoduli di M, è facile vedere che $N := \bigcup_{i\in\mathbb{N}} N_i$ è un sottomodulo di M, quindi per ipotesi ha un insieme finito di generatori, diciamo $\{x_1, \ldots, x_n\}$. Per ogni $j = 1, \ldots n$ esiste $i_j \in \mathbb{N}$ tale che $x_j \in N_{i_j}$. Posto $k := \max\{i_1, \ldots, i_n\}$, si ha allora $x_j \in N_k$ per ogni $j = 1, \ldots n$, e quindi $N = \langle x_1, \ldots, x_n\rangle_A \subseteq N_k$. Poiché d'altra parte $N_k \subseteq N_i \subseteq N$ per ogni $i \geq k$, concludiamo che $N_i = N_k$ per ogni $i \geq k$. □

Osservazione 9.2. Le condizioni (1) e (2) della Definizione-Proposizione 9.1 prendono il nome, rispettivamente, di *condizione della catena ascendente* e di *condizione massimale*. Riguardo alla prima si può notare che sembrerebbe più corretto chiamarla condizione della catena ascendente *numerabile*. Tuttavia l'abuso terminologico è del tutto innocuo perché (come è molto facile

vedere), se vale la (1), allora ogni catena ascendente (non necessariamente numerabile) è pure stazionaria.

Osservazione 9.3. Invertendo la relazione d'ordine (sull'insieme dei sottomoduli di M) data dall'inclusione, si ottengono delle varianti delle condizioni (1) e (2), dette, rispettivamente, *condizione della catena discendente* e *condizione minimale*. I moduli che soddisfano tali condizioni (ancora equivalenti) sono detti *artiniani*. D'altra parte per i moduli artiniani non esiste una caratterizzazione in qualche modo analoga alla condizione (3), il che li rende in un certo senso meno utili o interessanti di quelli noetheriani. Anche se non ci occuperemo dei moduli artiniani, si può comunque osservare che anche per essi valgono alcune delle proprietà che vedremo per quelli noetheriani (come la Proposizione 9.6).

Esempio 9.4. Chiaramente un modulo è noetheriano se ha un numero finito di sottomoduli. Questo succede per esempio se è semplice o finito.

Esempio 9.5. Ovviamente un modulo non finitamente generato non è noetheriano. Esistono però anche moduli finitamente generati non noetheriani. In particolare A è sempre un A-modulo finitamente generato (addirittura ciclico), ma non sempre noetheriano. Per esempio, se B è un anello non banale e Λ è un insieme infinito, è chiaro che nell'anello $A = B^\Lambda$ il B-sottomodulo $B^{(\Lambda)}$ è anche un A-sottomodulo (in effetti pure un ideale bilatero), e l'argomento nell'Esempio 5.4 può essere adattato molto facilmente per dimostrare che non è finitamente generato nemmeno come A-modulo.

Proposizione 9.6. *Sia M un A-modulo e sia M' un sottomodulo di M. Allora M è noetheriano se e solo se M' e M/M' sono noetheriani.*

Dimostrazione. Sia U_N l'insieme dei sottomoduli di un modulo N.

Supponiamo prima che M sia noetheriano. Ovviamente $U_{M'}$ è un sottoinsieme di U_M; d'altra parte, grazie alla Proposizione 4.5 anche $U_{M/M'}$ si può identificare al sottoinsieme $U'_{M/M'} := \{N \in U_M : M' \subseteq N\}$ di U_M; è inoltre chiaro che tale identificazione conserva le relazioni di inclusione. Se ne deduce immmediatamente che, se M soddisfa per esempio la condizione massimale, lo stesso vale per M' e per M/M'.

Supponiamo ora che M' e M/M' siano noetheriani e sia $\cdots \subseteq N_i \subseteq N_{i+1} \subseteq \cdots$ $(i \in \mathbb{N})$ una successione crescente di sottomoduli di M. Per ogni $i \in \mathbb{N}$ sia $N'_i := N_i \cap M' \in U_{M'}$ e $N''_i := N_i + M' \in U'_{M/M'}$. Per ipotesi esistono $k', k'' \in \mathbb{N}$ tali che $N'_i = N'_{k'}$ per ogni $i \geq k'$ e $N''_i = N''_{k''}$ per ogni $i \geq k''$, e vogliamo dimostrare che $N_i = N_k$ per ogni $i \geq k := \max\{k', k''\}$. Sia dunque $i \geq k$ e verifichiamo che $N_i \subseteq N_k$ (l'inclusione opposta vale per ipotesi). Dato $x \in N_i$, poiché $N_i \subseteq N''_i = N''_k$, esistono $x_k \in N_k$ e $x' \in M'$ tali che $x = x_k + x'$. Inoltre $x' = x - x_k \in N_i$ (essendo $x, x_k \in N_i$), per cui $x' \in N'_i = N'_k \subseteq N_k$. Concludiamo che $x = x_k + x' \in N_k$ (essendo $x_k, x' \in N_k$). □

Osservazione 9.7. Se $M' \subseteq M$ è un sottomodulo con M finitamente generato, anche M/M' lo è per Osservazione 4.4. È pure vero che, se M' e M/M' sono finitamente generati, anche M lo è: è facile vedere che, se $M' = \langle x'_1, \ldots, x'_m \rangle_A$ e $M/M' = \langle x_1 + M', \ldots, x_n + M' \rangle_A$, allora $M =$

$\langle x'_1, \ldots, x'_m, x_1, \ldots, x_n \rangle_A$. D'altra parte, come si è visto nell'Esempio 9.5, in generale non è vero che se M è finitamente generato anche M' lo è.

Corollario 9.8. *Siano M_i ($i = 1, \ldots, n$) A-moduli. Allora $\bigoplus_{i=1}^n M_i$ è noetheriano se e solo se M_i è noetheriano per ogni $i = 1, \ldots, n$.*

Dimostrazione. Se $M := \bigoplus_{i=1}^n M_i$ è noetheriano, per la Proposizione 9.6 anche ciascun M_i lo è, essendo (isomorfo a) un sottomodulo di M. Viceversa, se ogni M_i è noetheriano, dimostriamo che anche M lo è per induzione su n. Il caso $n = 1$ essendo ovvio, supponiamo $n > 1$. Poiché sia M_n (per ipotesi) che $M' := \bigoplus_{i=1}^{n-1} M_i$ (per induzione) sono noetheriani, e ricordando che $M/M_n \cong M'$, ancora per la Proposizione 9.6 concludiamo che M è noetheriano. □

Corollario 9.9. *Tutti gli A-moduli finitamente generati sono noetheriani se e solo se A è un A-modulo noetheriano.*

Dimostrazione. Assumiamo che A sia un A-modulo noetheriano (il viceversa è ovvio). Per il Corollario 9.8 anche A^n è noetheriano per ogni $n \in \mathbb{N}$, e segue allora dalla Proposizione 9.6 che pure ogni quoziente di A^n è noetheriano. Per concludere basta ricordare che (grazie al Corollario 6.5) ogni A-modulo finitamente generato è isomorfo a un quoziente di A^n per qualche $n \in \mathbb{N}$. □

10. Anelli noetheriani

In questa sezione assumiamo che A sia commutativo.

Definizione 10.1. Si dice che A è *noetheriano* (come anello) se è un A-modulo noetheriano.

Osservazione 10.2. Nel caso non commutativo si dice che un anello B è *noetheriano a sinistra* se è noetheriano come B-modulo (sinistro); analogamente B è *noetheriano a destra* se B^{op} è noetheriano a sinistra. Si dice poi che B è *noetheriano* se lo è sia a sinistra che a destra. Molte proprietà che vedremo per anelli commutativi noetheriani valgono in effetti per anelli (non commutativi) noetheriani a sinistra.

Osservazione 10.3. Essendo commutativo, A è noetheriano se e solo se ogni suo ideale è finitamente generato, o, equivalentemente, se soddisfa la condizione della catena ascendente o la condizione massimale per gli ideali.

Osservazione 10.4. Se A è noetheriano, per il Corollario 9.9 un A-modulo è noetheriano se e solo se è finitamente generato.

Esempio 10.5. Ogni dominio a ideali principali è chiaramente noetheriano. In particolare $\mathbb{Z}$, K e $K[X]$ sono noetheriani.

Proposizione 10.6. *Se A è noetheriano e $I \subseteq A$ è un ideale, allora A/I è noetheriano.*

Dimostrazione. Essendo A un A-modulo noetheriano, anche A/I lo è per la Proposizione 9.6. D'altra parte, segue subito dall'Osservazione 7.2 che A/I è noetheriano come A-modulo se e solo se lo è come A/I-modulo. □

Teorema 10.7 (della base di Hilbert)**.** *Se A è noetheriano, anche l'anello dei polinomi $A[X]$ è noetheriano.*

Dimostrazione. Dato un ideale J di $A[X]$, sia

$$I := \{a \in A : \exists \sum_{i=0}^{d} a_i X^i \in J \text{ con } a_d = a\}.$$

È molto facile vedere che I è un ideale di A, quindi per ipotesi esistono $a_1, \ldots, a_n \in A$ tali che $I = \langle a_1, \ldots, a_n \rangle_A$. Per definizione di I, per ogni $i = 1, \ldots, n$ esiste $f_i = \sum_{j=0}^{d_i} a_{i,j} X^j \in J$ tale che $a_{i,d_i} = a_i$. Posto $d := \max\{d_1, \ldots, d_n\}$, sia $A[X]_{<d}$ il sottoinsieme di $A[X]$ costituito da 0 e dai polinomi di grado $< d$: chiaramente $A[X]_{<d}$ è un A-sottomodulo di $A[X]$ ed è un A-modulo libero di rango d (una sua base è $\{X^i : 0 \leq i < d\}$). Essendo A noetheriano, per il Corollario 9.8 $A[X]_{<d} \cong A^d$ è un A-modulo noetheriano, e quindi il suo A-sottomodulo $M := J \cap A[X]_{<d}$ è finitamente generato. Esistono allora $g_1, \ldots, g_m \in M$ tali che $M = \langle g_1, \ldots, g_m \rangle_A$, e vogliamo dimostrare che

$$J = J' := \langle f_1, \ldots, f_n, g_1, \ldots, g_m \rangle_{A[X]}.$$

L'altra inclusione essendo evidente, dobbiamo vedere che $J \subseteq J'$. Dato $f \in J$, possiamo supporre $f \neq 0$ e dimostriamo che $f \in J'$ per induzione su $l := \deg(f)$. Se $l < d$ si ha in effetti

$$f \in J \cap A[X]_{<d} = M = \langle g_1, \ldots, g_m \rangle_A \subseteq \langle g_1, \ldots, g_m \rangle_{A[X]} \subseteq J'.$$

Se $l \geq d$ e $f = \sum_{i=0}^{l} c_i X^i$, per definizione $c_l \in I$, dunque esistono $b_1, \ldots, b_n \in A$ tali che $c_l = \sum_{i=1}^{n} b_i a_i$. Allora $h := \sum_{i=1}^{n} b_i X^{l-d_i} f_i \in J' \subseteq J$ ha grado l e il suo coefficiente di grado l è proprio c_l. Ne segue che $f - h \in J$ soddisfa $f - h = 0$ o $\deg(f - h) < l$, e quindi, per ipotesi induttiva, $f - h \in J'$, da cui anche $f = (f - h) + h \in J'$. Ciò dimostra che $J = J'$ è un ideale finitamente generato, e pertanto $A[X]$ è noetheriano. □

Corollario 10.8. *Se A è noetheriano, $A[X_1, \ldots, X_n]$ è noetheriano per ogni $n \in \mathbb{N}$.*

Dimostrazione. Segue subito per induzione su n dal Teorema 10.7. □

Esempio 10.9. In particolare, $\mathbb{Z}[X_1, \ldots, X_n]$ e $K[X_1, \ldots, X_n]$ sono domini noetheriani per ogni $n \in \mathbb{N}$.

Esempio 10.10. Per l'Esempio 9.5 $A = B^\Lambda$ non è noetheriano se B è un anello commutativo non banale e Λ è infinito. Si noti che tale anello non è mai un dominio, ma esistono comunque anche domini non noetheriani. In effetti in generale si può definire l'anello $A[X_1, X_2, \ldots]$ dei polinomi in infinite variabili X_i ($i > 0$) a coefficienti in A: i suoi elementi sono ordinari polinomi che coinvolgono un numero finito di tali variabili, con somma e prodotto definiti nel solito modo. È facile vedere che $A[X_1, X_2, \ldots]$ non è noetheriano (se $A \neq 0$), perché $(X_1) \subsetneq (X_1, X_2) \subsetneq \cdots$ è una successione strettamente crescente di ideali. D'altra parte è chiaro che $A[X_1, X_2, \ldots]$ è un dominio se (e solo se) A lo è.

Osservazione 10.11. Se A è un sottoanello di un anello (commutativo) noetheriano B, non è detto che anche A sia noetheriano. Per esempio, si può prendere come A un qualunque dominio non noetheriano (che esiste per l'Esempio 10.10), visto come sottoanello del suo campo dei quozienti B.

11. Decomponibilità di moduli

Definizione 11.1. Sia M un A-modulo. Un sottomodulo M' di M è un *addendo diretto* di M se esiste un altro sottomodulo M'' di M (detto *complementare* di M' in M) tale che $M = M' \oplus M''$ (cioè $M' \cap M'' = \{0\}$ e $M' + M'' = M$).

Esempio 11.2. Poiché $M = M \oplus \{0\}$, i sottomoduli banali $\{0\}$ e M sono sempre addendi diretti di M.

Esempio 11.3. Se $n > 1$ è un intero, $n\mathbb{Z}$ non è un addendo diretto del gruppo abeliano (cioè dello $\mathbb{Z}$-modulo) $\mathbb{Z}$. Infatti, se lo fosse, un suo complementare sarebbe isomorfo a $\mathbb{Z}/n\mathbb{Z}$ per l'Osservazione 5.7, ma $\mathbb{Z}$ non contiene sottogruppi isomorfi a $\mathbb{Z}/n\mathbb{Z}$.

Proposizione 11.4. *Sia M un A-modulo e sia M' un sottomodulo di M. Indicando con $\pi\colon M \to M/M'$ la proiezione naturale, le seguenti condizioni sono equivalenti.*

1. *M' è un addendo diretto di M.*
2. *Esiste un omomorfismo $f\colon M \to M'$ tale che $f|_{M'} = \mathrm{id}_{M'}$.*
3. *Esiste un omomorfismo $g\colon M/M' \to M$ tale che $\pi \circ g = \mathrm{id}_{M/M'}$.*

Dimostrazione. (1) $\implies$ (2) Per definizione esiste un sottomodulo M'' di M tale che $M = M' \oplus M''$. Allora la proiezione sul primo fattore $f\colon M = M' \times M'' \to M'$ è un omomorfismo che soddisfa $f|_{M'} = \mathrm{id}_{M'}$.

(2) $\implies$ (3) Chiaramente $\tilde{f}\colon M \to M$, $x \mapsto x - f(x)$ è un omomorfismo tale che $\tilde{f}(x') = 0$ per ogni $x' \in M'$. Dunque $M' \subseteq \ker(\tilde{f})$, e per il teorema di omomorfismo per moduli esiste un unico omomorfismo $g\colon M/M' \to M$ tale che $g \circ \pi = \tilde{f}$. Per ogni $x \in M$, poiché $f(x) \in M' = \ker(\pi)$, si ha

$$\pi \circ g(\pi(x)) = \pi(g \circ \pi(x)) = \pi(\tilde{f}(x)) = \pi(x - f(x)) = \pi(x) - \pi(f(x)) = \pi(x),$$

il che dimostra (essendo π suriettiva) che $\pi \circ g = \mathrm{id}_{M/M'}$.

(3) $\implies$ (1) $M'' := \mathrm{im}(g)$ è un sottomodulo di M, e vogliamo dimostrare che è un complementare di M' in M. Se $x \in M' \cap M''$, esiste $y \in M/M'$ tale che $x = g(y)$ (perché $x \in M''$), quindi $y = \pi(g(y)) = \pi(x) = 0$ (perché $x \in M' = \ker(\pi)$). Ne segue che $x = g(y) = g(0) = 0$, cioè $M' \cap M'' = \{0\}$. D'altra parte, se $x \in M$, posto $x'' := g(\pi(x)) \in M''$ e $x' := x - x''$, si ha

$$\pi(x') = \pi(x - x'') = \pi(x) - \pi(x'') = \pi(x) - \pi(g(\pi(x))) = \pi(x) - \pi(x) = 0.$$

Dunque $x' \in \ker(\pi) = M'$ e $x = x' + x'' \in M' + M''$, cioè $M' + M'' = M$. □

Corollario 11.5. *Sia M un A-modulo e sia M' un sottomodulo di M tale che M/M' è libero. Allora M' è un addendo diretto di M.*

Dimostrazione. Sia $(y_\lambda)_{\lambda\in\Lambda}$ una base di M/M' con $y_\lambda \neq y_\mu$ se $\lambda \neq \mu$. Per ogni $\lambda \in \Lambda$ esiste $x_\lambda \in M$ tale che $y_\lambda = \pi(x_\lambda)$. Per la Proposizione 6.4 esiste un (unico) omomorfismo $g\colon M/M' \to M$ tale che $g(y_\lambda) = x_\lambda$ per ogni $\lambda \in \Lambda$. Si ha dunque $\pi(g(y_\lambda)) = \pi(x_\lambda) = y_\lambda$ per ogni $\lambda \in \Lambda$, e questo implica (per l'unicità data sempre dalla Proposizione 6.4) $\pi \circ g = \mathrm{id}_{M/M'}$. Segue allora dalla Proposizione 11.4 che M' è un addendo diretto di M. □

Esempio 11.6. Se A è un anello con divisione, ogni sottomodulo M' di un A-modulo M è un addendo diretto di M. In effetti ciò segue subito dal Corollario 11.5, tenendo conto che M/M' è libero per la Proposizione 6.8.

Definizione 11.7. Un modulo M è *indecomponibile* se $M \neq \{0\}$ e gli unici addendi diretti di M sono $\{0\}$ e M.

Esempio 11.8. Un modulo semplice è ovviamente indecomponibile.

Esempio 11.9. Per quanto visto nell'Esempio 11.3, $\mathbb{Z}$ è uno $\mathbb{Z}$-modulo indecomponibile ma non semplice.

Un possibile approccio al problema di classificare (a meno di isomorfismo) i moduli su un anello è quello di stabilire se ogni modulo M si può decomporre come somma diretta di moduli indecomponibili, ed eventualmente se tale decomposizione è *essenzialmente unica*. Naturalmente con questo intendiamo che, se $M \cong \bigoplus_{\lambda\in\Lambda} M_\lambda \cong \bigoplus_{\lambda'\in\Lambda'} N_{\lambda'}$, con M_λ e $N_{\lambda'}$ indecomponibili per ogni $\lambda \in \Lambda$ e per ogni $\lambda' \in \Lambda'$, allora esiste una funzione biunivoca $\sigma\colon \Lambda \to \Lambda'$ tale che $M_\lambda \cong N_{\sigma(\lambda)}$ per ogni $\lambda \in \Lambda$. Anche nei casi in cui si riesce a dimostrare questo, rimane poi il problema di classificare (a meno di isomorfismo) i moduli indecomponibili.

Esempio 11.10. Quanto detto sopra funziona particolarmente bene se A è un anello con divisione. In tal caso, infatti, ogni A-modulo è libero (per la Proposizione 6.8), e quindi è isomorfo a una somma diretta di copie di A (per il Corollario 6.6) in modo essenzialmente unico (per la Proposizione 6.9). Inoltre A è l'unico A-modulo indecomponibile, a meno di isomorfismo: in effetti A è un A-modulo semplice e quindi indecomponibile per l'Esempio 2.19; d'altra parte è chiaro che (su ogni anello) un A-modulo libero indecomponibile deve avere rango 1, cioè deve essere isomorfo a A.

Proposizione 11.11. *Ogni modulo noetheriano è somma diretta finita di moduli indecomponibili (e noetheriani).*

Dimostrazione. Supponiamo per assurdo che esista un modulo noetheriano $M = M_0$ che non è somma diretta finita di moduli indecomponibili. In particolare M_0 non è nullo e non è indecomponibile, quindi esistono due sottomoduli non nulli M_1 e M_1' di M_0 tali che $M_0 = M_1 \oplus M_1'$. Inoltre almeno uno tra M_1 e M_1' non è somma diretta finita di indecomponibili (altrimenti anche M_0 lo sarebbe), e possiamo supporre che M_1 non lo sia. Proseguendo induttivamente allo stesso modo, dato M_i (per qualche $i \in \mathbb{N}$) che non è somma diretta finita di indecomponibili, possiamo trovare due sottomoduli non nulli M_{i+1} e M_{i+1}' di M_i tali che $M_i = M_{i+1} \oplus M_{i+1}'$ e con M_{i+1} che ancora non è somma diretta finita di indecomponibili. Ponendo (per ogni $i \in \mathbb{N}$) $N_i := \sum_{j=1}^{i} M_j'$, è chiaro per costruzione che $N_i = \bigoplus_{j=1}^{i} M_j'$ (risulta in effetti $M = \bigoplus_{j=1}^{i} M_j' \oplus M_i$). In particolare gli N_i sono allora sottomoduli di M tali che $N_i \subsetneq N_{i+1}$ per ogni $i \in \mathbb{N}$, assurdo perché M è noetheriano. Dunque M è somma diretta finita di moduli indecomponibili, e il fatto che tali moduli indecomponibili siano anche noetheriani segue subito dalla Proposizione 9.6. □

Osservazione 11.12. Un modulo non noetheriano non è sempre somma diretta (eventualmente infinita) di moduli indecomponibili. Si può per esempio dimostrare che, se A è un dominio a ideali principali ma non un campo e Λ è un insieme infinito, allora A^Λ non è somma diretta di indecomponibili.

Osservazione 11.13. Anche assumendo che A sia un dominio noetheriano, in generale la decomposizione di un A-modulo noetheriano come somma diretta finita di indecomponibili non è essenzialmente unica (nemmeno il numero di addendi della somma diretta è univocamente determinato). Vedremo però che l'unicità vale se A è un dominio a ideali principali.

Esempio 11.14. Anche su un dominio a ideali principali possono esistere moduli indecomponibili non noetheriani. Per esempio, è facile vedere che $\mathbb{Q}$ è uno $\mathbb{Z}$-modulo non finitamente generato e quindi non noetheriano. D'altra parte $\mathbb{Q}$ è uno $\mathbb{Z}$-modulo indecomponibile: se H_1 e H_2 sono due sottogruppi non nulli di $\mathbb{Q}$, sia $\frac{a_i}{b_i} \in H_i \setminus \{0\}$ (con $a_i, b_i \in \mathbb{Z} \setminus \{0\}$) per $i = 1, 2$. Allora $0 \neq a_1 a_2 = a_{3-i} b_i \frac{a_i}{b_i} \in H_i$ per $i = 1, 2$, cioè $H_1 \cap H_2 \neq \{0\}$.

12. Moduli su un dominio

In questa sezione assumiamo che A sia un dominio.

Definizione 12.1. Sia M un A-modulo. Un elemento $x \in M$ si dice *di torsione* se $\mathrm{Ann}(x) \neq \{0\}$ (cioè se esiste $a \in A \setminus \{0\}$ tale che $ax = 0$). Posto $\mathrm{T}(M) := \{x \in M : x \text{ è di torsione}\}$, si dice che M è *di torsione* se $\mathrm{T}(M) = M$, si dice invece che M è *senza torsione* se $\mathrm{T}(M) = \{0\}$.

Esempio 12.2. Il modulo nullo è l'unico sia di torsione che senza torsione.

Esempio 12.3. Ogni modulo libero è chiaramente senza torsione. In particolare ogni spazio vettoriale su un campo è senza torsione.

Esempio 12.4. Se $(G, +)$ è un gruppo abeliano (visto come $\mathbb{Z}$-modulo), si ha $\mathrm{T}(G) = \{g \in G : \mathrm{ord}(g) < \infty\}$. In particolare ogni gruppo abeliano finito è di torsione.

Lemma 12.5. *Se M è un modulo, $\mathrm{T}(M)$ è un sottomodulo (ovviamente di torsione) di M e $M/\mathrm{T}(M)$ è senza torsione.*

Dimostrazione. Ovviamente $0 \in \mathrm{T}(M)$. Se $x, y \in \mathrm{T}(M)$, siano $a \in \mathrm{Ann}(x)$ e $b \in \mathrm{Ann}(y)$ con $a, b \neq 0$. Si ha allora $ab(x + y) = bax + aby = 0$ e $ab \neq 0$, cioè $x + y \in \mathrm{T}(M)$. È inoltre chiaro che $\mathrm{Ann}(x) \subseteq \mathrm{Ann}(ax)$ per ogni $x \in M$ e per ogni $a \in A$, e quindi $ax \in \mathrm{T}(M)$ se $x \in \mathrm{T}(M)$. Ciò conclude la dimostrazione del fatto che $\mathrm{T}(M)$ è un sottomodulo di M. Sia poi $x \in M$ tale che $\overline{x} := x + \mathrm{T}(M)$ è di torsione in $M/\mathrm{T}(M)$. Per definizione esiste $a \in A \setminus \{0\}$ tale che $a\overline{x} = \overline{ax} = \overline{0}$, cioè $ax \in \mathrm{T}(M)$. Esiste allora $b \in A \setminus \{0\}$ tale che $bax = 0$, il che dimostra (essendo $ba \neq 0$) che $x \in \mathrm{T}(M)$, cioè $\overline{x} = \overline{0}$. Questo dimostra che $M/\mathrm{T}(M)$ è senza torsione. □

Osservazione 12.6. Se M è di torsione (rispettivamente senza torsione), banalmente anche ogni sottomodulo M' di M lo è. È inoltre chiaro che, se M è di torsione, pure M/M' lo è, ma, se M è senza torsione, non è detto che M/M' lo sia. Per esempio, $\mathbb{Z}$ è un gruppo abeliano senza torsione, ma $\mathbb{Z}/n\mathbb{Z}$ non lo è per $n > 1$.

Lemma 12.7. *Sia M un modulo noetheriano e senza torsione. Allora M è isomorfo a un sottomodulo di un modulo libero di rango finito.*[7]

[7] Ricordiamo che il rango di un modulo libero è ben definito per il Corollario 7.7.

Dimostrazione. Per la condizione massimale esiste un sottomodulo M' di M che sia massimale tra i sottomoduli liberi di M (l'insieme di tali sottomoduli è non vuoto perché contiene $\{0\}$). Inoltre M' ha rango finito perché è finitamente generato (essendo sottomodulo del modulo noetheriano M). Osserviamo intanto che $(M' : x) \neq \{0\}$ per ogni $x \in M$. Se infatti esistesse $x \in M$ tale che $(M' : x) = \{0\}$, il sottomodulo Ax di M sarebbe libero di rango 1 (con base $\{x\}$) e $M' \cap Ax = \{0\}$, per cui $M'' := M' + Ax = M' \oplus Ax$ sarebbe un sottomodulo libero di M tale che $M' \subsetneq M''$, contro la massimalità di M'. In particolare, scelto un insieme $\{x_1, \dots, x_n\}$ di generatori di M (che è finitamente generato perché noetheriano), per ogni $i = 1, \dots, n$ esiste $a_i \in A \setminus \{0\}$ tale che $a_i x_i \in M'$. Posto $a := \prod_{i=1}^{n} a_i \in A \setminus \{0\}$, si ha anche $ax_i \in M'$ per ogni $i = 1, \dots, n$, e ne segue facilmente che $ax \in M'$ per ogni $x \in M$. Essendo $f \colon M \to M$, $x \mapsto ax$ un omomorfismo iniettivo (perché M è senza torsione), si conclude che $M \cong \mathrm{im}(f)$ e che $\mathrm{im}(f)$ è un sottomodulo del modulo libero di rango finito M'. □

Esempio 12.8. In generale un modulo senza torsione non è isomorfo a un sottomodulo di un modulo libero. Per esempio, il gruppo abeliano $\mathbb{Q}$ è chiaramente senza torsione, ma non è isomorfo a un sottogruppo di un gruppo abeliano libero. Se lo fosse, esisterebbe infatti un omomorfismo iniettivo $f \colon \mathbb{Q} \to \mathbb{Z}^{(\Lambda)}$ per qualche insieme Λ. Essendo $f(1) \neq 0$ per l'iniettività di f, esisterebbe $\mu \in \Lambda$ tale che $a := \mathrm{pr}_\mu(f(1)) \in \mathbb{Z} \setminus \{0\}$. Si avrebbe allora

$$a = \mathrm{pr}_\mu(f(1)) = \mathrm{pr}_\mu(f(2a\frac{1}{2a})) = 2a\mathrm{pr}_\mu(f(\frac{1}{2a})),$$

che è impossibile in $\mathbb{Z}$.

Lemma 12.9. *Ogni ideale non nullo di A è indecomponibile; in particolare A è indecomponibile.*

Dimostrazione. Supponendo per assurdo che un ideale non nullo I di A non sia indecomponibile, si avrebbe $I = I' \oplus I''$ con $I', I'' \neq \{0\}$. Essendo A-sottomoduli di I, I' e I'' sarebbero però ideali di A, e dunque, presi $a' \in I' \setminus \{0\}$ e $a'' \in I'' \setminus \{0\}$, si avrebbe $0 \neq a'a'' \in I'I'' \subseteq I' \cap I''$, assurdo. □

Corollario 12.10. *Un ideale di A è principale se e solo se è un modulo libero; inoltre in tal caso il suo rango è 0 o 1.*

Dimostrazione. Sia I un ideale di A. Se $I = (a)$ è principale, allora $I = \{0\}$ (se $a = 0$) o $I \cong A$ (se $a \neq 0$, nel qual caso $A \to I$, $b \mapsto ba$ è un isomorfismo), per cui I è libero e $\mathrm{rk}(I)$ vale 0 nel primo caso e 1 nel secondo. Viceversa, se I è libero, possiamo supporre $I \neq \{0\}$. Quindi I è indecomponibile per il Lemma 12.9, per cui deve essere $\mathrm{rk}(I) = 1$; in particolare allora I è un modulo ciclico, cioè un ideale principale. □

Esempio 12.11. Un modulo noetheriano senza torsione non è sempre libero. Per esempio, se A è noetheriano ma non a ideali principali, ogni ideale (noetheriano per la Proposizione 9.6 e chiaramente senza torsione) non principale di A non è libero per il Corollario 12.10. Si noti che un tale ideale non è nemmeno somma diretta di moduli ciclici, essendo indecomponibile per il Lemma 12.9. Un esempio esplicito è dato da $A = \mathbb{Z}[X]$ e $I = (2, X)$.

13. Moduli su un dominio a ideali principali

In questa sezione assumiamo che A sia un dominio a ideali principali ma non un campo (per esempio, $A = \mathbb{Z}$ o $A = K[X]$). Ricordiamo che, essendo A noetheriano, un A-modulo è finitamente generato se e solo se è noetheriano per l'Osservazione 10.4.

Lemma 13.1. *Sia M un modulo libero di rango finito. Se M' è un sottomodulo di M, allora M' è libero e $\mathrm{rk}(M') \leq \mathrm{rk}(M)$.*

Dimostrazione. Posto $n := \mathrm{rk}(M)$, per il Corollario 6.6 possiamo supporre $M = A^n$. Procedendo per induzione su n, il caso $n = 0$ è banale perché $M = M' = \{0\}$. Se $n > 0$, identifichiamo A^{n-1} con $\ker(\mathrm{pr}_n)$ e poniamo $M'' := A^{n-1} \cap M'$ e $I := \mathrm{pr}_n(M')$. Per l'ipotesi induttiva M'' è libero e $\mathrm{rk}(M'') \leq \mathrm{rk}(A^{n-1}) = n - 1$; inoltre I, essendo un ideale (principale) di A, è libero per il Corollario 12.10 e $\mathrm{rk}(I) \leq 1$. Ora $f := \mathrm{pr}_n|_{M'} \colon M' \to A$ è un omomorfismo tale che $\mathrm{im}(f) = I$ e $\ker(f) = \ker(\mathrm{pr}_n) \cap M' = M''$, quindi $I \cong M'/M''$ per il primo teorema di isomorfismo per moduli. Poiché I è libero, segue dal Corollario 11.5 e dall'Osservazione 5.7 che $M' \cong M'' \oplus I$. Si conclude allora che M' è libero e $\mathrm{rk}(M') = \mathrm{rk}(M'') + \mathrm{rk}(I) \leq n$. □

Osservazione 13.2. Usando il lemma di Zorn non è difficile dimostrare che il Lemma 13.1 vale anche senza assumere che il rango di M sia finito.

Proposizione 13.3. *Sia M un modulo finitamente generato e senza torsione. Allora M è libero di rango finito.*

Dimostrazione. Per il Lemma 12.7 M è isomorfo a un sottomodulo di un modulo libero di rango finito. Allora M è libero di rango finito per il Lemma 13.1. □

Osservazione 13.4. L'Esempio 12.8 (in cui $A = \mathbb{Z}$ e $M = \mathbb{Q}$) mostra in particolare che esistono moduli senza torsione ma non liberi.

Corollario 13.5. *Sia M un modulo finitamente generato. Allora esiste un sottomodulo libero di rango finito L di M tale che $M = \mathrm{T}(M) \oplus L$.*

Dimostrazione. Per il Lemma 12.5 $M/\mathrm{T}(M)$ è senza torsione; inoltre è finitamente generato per l'Osservazione 4.4. Allora $M/\mathrm{T}(M)$ è libero di rango finito per la Proposizione 13.3. Per il Corollario 11.5 esiste dunque un sottomodulo L di M tale che $M = \mathrm{T}(M) \oplus L$, e L è libero di rango finito perché $L \cong M/\mathrm{T}(M)$ per l'Osservazione 5.7. □

Osservazione 13.6. Mentre è unico a meno di isomorfismo, L nell'enunciato del Corollario 13.5 non è unico come sottomodulo di M, in generale. Per esempio, se $A = \mathbb{Z}$ e $M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$, risulta $\mathrm{T}(M) = \langle(\bar{1}, 0)\rangle$ e si può prendere come L sia $\langle(\bar{0}, 1)\rangle$ che $\langle(\bar{1}, 1)\rangle$.

Indicheremo con $\mathrm{Max}(A)$ l'insieme (non vuoto) degli ideali massimali di A. Ricordiamo che $\mathrm{Max}(A)$ coincide con l'insieme degli ideali primi di A, escluso $\{0\}$, e che per ogni $P \in \mathrm{Max}(A)$ esiste (unico a meno di associati) $p \in A$ irriducibile tale che $P = (p)$. Inoltre, A è anche un dominio a fattorizzazione unica, e da ciò segue che per ogni ideale (principale) non nullo I di A esistono unici $P_1, \ldots, P_k \in \mathrm{Max}(A)$ distinti e $n_1, \ldots, n_k > 0$ tali che $I = \prod_{i=1}^{k} P_i^{n_i}$.

Definizione-Proposizione 13.7. *Sia M un A-modulo e sia $P = (p) \in \mathrm{Max}(A)$. Un elemento $x \in M$ si dice* di P-torsione *(o di p-torsione) se $\mathrm{Ann}(x) = P^n$ per qualche $n \in \mathbb{N}$, o, equivalentemente, se esiste $m \in \mathbb{N}$ tale che $p^m x = 0$. Inoltre $\mathrm{T}_P(M) := \{x \in M : x \text{ è di } P\text{-torsione}\}$ (indicato anche con $\mathrm{T}_p(M)$) è un sottomodulo (ovviamente di torsione) di M, e si dice che M è* di P-torsione *(o di p-torsione) se $\mathrm{T}_P(M) = M$.*

Dimostrazione. È chiaro che, se $\mathrm{Ann}(x) = P^n$ per qualche $n \in \mathbb{N}$, allora $p^n x = 0$. Viceversa, se esiste $m \in \mathbb{N}$ tale che $p^m x = 0$, si ha $p^m \in \mathrm{Ann}(x)$, e quindi $P^m = (p^m) \subseteq \mathrm{Ann}(x)$. Poiché gli unici ideali di A contenenti P^m sono quelli della forma P^n con $0 \leq n \leq m$, se ne deduce che $\mathrm{Ann}(x)$ deve essere uno di questi. La verifica che $\mathrm{T}_P(M)$ è un sottomodulo di M è facile e simile a quella per $\mathrm{T}(M)$ nella dimostrazione del Lemma 12.5. □

Proposizione 13.8. *Se M è un modulo, $\mathrm{T}(M) = \bigoplus_{P \in \mathrm{Max}(A)} \mathrm{T}_P(M)$.*

Dimostrazione. Ovviamente $\mathrm{T}_P(M) \subseteq \mathrm{T}(M)$ per ogni $P \in \mathrm{Max}(A)$. Fissato $Q = (q) \in \mathrm{Max}(A)$, sia $N_Q := \sum_{P \in \mathrm{Max}(A) \setminus \{Q\}} \mathrm{T}_P(M)$ e sia $x \in \mathrm{T}_Q(M) \cap N_Q$. Poiché $x \in \mathrm{T}_Q(M)$, esiste $n \in \mathbb{N}$ tale che $\mathrm{Ann}(x) = Q^n$. D'altronde, il fatto che $x \in N_Q$ significa che esistono $P_1, \ldots, P_k \in \mathrm{Max}(A) \setminus \{Q\}$ distinti e $x_i \in \mathrm{T}_{P_i}(M)$ (per $i = 1, \ldots, k$) tali che $x = \sum_{i=1}^k x_i$. Per ogni $i = 1, \ldots, k$ esiste $m_i \in \mathbb{N}$ tale che $p_i^{m_i} x_i = 0$ (con $P_i = (p_i)$), e quindi, posto $a := \prod_{i=1}^k p_i^{m_i}$, anche $a x_i = 0$. Da questo segue chiaramente $ax = 0$, per cui $a \in \mathrm{Ann}(x) = (q^n)$. Per l'unicità della fattorizzazione in A deve essere allora $n = 0$, e quindi $x = 0$. Ciò dimostra $\mathrm{T}_Q(M) \cap N_Q = \{0\}$, e pertanto

$$N := \sum_{P \in \mathrm{Max}(A)} \mathrm{T}_P(M) = \bigoplus_{P \in \mathrm{Max}(A)} \mathrm{T}_P(M) \subseteq \mathrm{T}(M).$$

Resta da dimostrare che $\mathrm{T}(M) \subseteq N$. Dato $x \in \mathrm{T}(M)$, esistono unici $P_1, \ldots, P_k \in \mathrm{Max}(A)$ distinti e $n_1, \ldots, n_k > 0$ tali che $\mathrm{Ann}(x) = \prod_{i=1}^k P_i^{n_i}$. Dimostriamo che $x \in N$ per induzione su k: il caso $k = 0$ è ovvio perché risulta $x = 0$. Supponiamo allora $k > 0$ e, posto $P_i = (p_i)$, siano $a := \prod_{i=1}^{k-1} p_i^{n_i}$ e $b := p_k^{n_k}$. Dato che $\mathrm{mcd}(a, b) = 1$, esistono $c, d \in A$ tali che $ac + bd = 1$, per cui $x = y + z$ con $y := acx$ e $z := bdx$. Ora, $by = bacx = 0$ (perché $ab \in \mathrm{Ann}(x)$), e questo significa che y è di P_k-torsione, cioè $y \in \mathrm{T}_{P_k}(M) \subseteq N$. Analogamente $az = abdx = 0$, per cui $(a) = \prod_{i=1}^{k-1} P_i^{n_i} \subseteq \mathrm{Ann}(z)$. Da ciò segue che $\mathrm{Ann}(z) = \prod_{i=1}^{k-1} P_i^{m_i}$ con $0 \leq m_i \leq n_i$ per $i = 1, \ldots, k-1$. Per l'ipotesi induttiva si ha allora $z \in N$, e quindi anche $x = y + z \in N$. □

Lemma 13.9. *Sia $P \in \mathrm{Max}(A)$ e sia M un modulo finitamente generato e di P-torsione. Allora esiste $x \in M$ tale che $\mathrm{Ann}(M) = \mathrm{Ann}(x) = P^n$ per qualche $n \in \mathbb{N}$. Inoltre $\langle x \rangle_A$ è un addendo diretto di M.*

Dimostrazione. Se $M = \langle x_1, \ldots, x_k \rangle_A$, per ogni $i = 1, \ldots, k$ esiste $n_i \in \mathbb{N}$ tale che $\mathrm{Ann}(x_i) = P^{n_i}$. Posto $P = (p)$ e $n := \max\{n_1, \ldots, n_k\}$, si ha $p^n x_i = 0$ per ogni $i = 1, \ldots, k$, da cui segue facilmente che $p^n \in \mathrm{Ann}(M)$, cioè $P^n \subseteq \mathrm{Ann}(M)$. D'altra parte esiste $j \in \{1, \ldots, k\}$ tale che $n = n_j$, per cui $x := x_j$ soddisfa $\mathrm{Ann}(x) = P^n$. Poiché ovviamente $\mathrm{Ann}(M) \subseteq \mathrm{Ann}(x)$, otteniamo che $\mathrm{Ann}(M) = \mathrm{Ann}(x) = P^n$.

Per la condizione massimale esiste un sottomodulo M' di M massimale rispetto alla proprietà che $\langle x \rangle_A \cap M' = \{0\}$ (l'insieme di tali sottomoduli è

non vuoto perché contiene $\{0\}$). Posto $N := \langle x\rangle_A + M' = \langle x\rangle_A \oplus M'$, per concludere che $\langle x\rangle_A$ è un addendo diretto di M basta ovviamente dimostrare che $N = M$. Supponiamo per assurdo che $N \subsetneq M$, e sia $y \in M \setminus N$. Posto $M'_a := M' + \langle y - ax\rangle_A$ per ogni $a \in A$, si ha $M' \subsetneq M'_a$ perché $y - ax \notin N$ (dato che $x \in N$ mentre $y \notin N$), e quindi $y - ax \notin M'$. Per arrivare a un assurdo, contraddicendo la massimalità di M', basta perciò dimostrare che esiste $a \in A$ tale che $\langle x\rangle_A \cap M'_a = \{0\}$. Poiché $(N : y) \supseteq \mathrm{Ann}(y) \supseteq \mathrm{Ann}(M) = P^n$, deve essere $(N : y) = P^m$ con $0 \leq m \leq n$. In particolare $p^m y \in N$, per cui esistono $b \in A$ e $x' \in M'$ tali che $p^m y = bx + x'$. Dall'uguaglianza

$$0 = p^n y = p^{n-m} p^m y = p^{n-m}(bx + x') = p^{n-m} bx + p^{n-m} x'$$

segue $p^{n-m} bx = -p^{n-m} x' \in \langle x\rangle_A \cap M' = \{0\}$, quindi $p^{n-m} b \in \mathrm{Ann}(x) = (p^n)$. Allora $b = p^m c$ per qualche $c \in A$, e per concludere basta dimostrare che $\langle x\rangle_A \cap M'_c = \{0\}$. Per ogni $z \in \langle x\rangle_A \cap M'_c$ esistono $z' \in M'$ e $a \in A$ tali che $z = z' + a(y - cx)$ (perché $z \in M'_c$). Poiché $z, x \in \langle x\rangle_A \subseteq N$ e $z' \in M' \subseteq N$, anche $ay = z - z' + acx \in N$, cioè $a \in (N : y) = (p^m)$, per cui $a = a' p^m$ per qualche $a' \in A$. Dato che $p^m y = bx + x'$ e $p^m c = b$, si ottiene

$$z = z' + a' p^m y - a' p^m cx = z' + a'(bx + x') - a' bx = z' + a' x' \in M',$$

il che dimostra che $z \in \langle x\rangle_A \cap M' = \{0\}$. □

Proposizione 13.10. *Un A-modulo finitamente generato è indecomponibile se e solo se è isomorfo a A o a A/P^n per qualche $P \in \mathrm{Max}(A)$ e $n > 0$.*

Dimostrazione. A è indecomponibile per il Lemma 12.9. Se $P \in \mathrm{Max}(A)$ e $n > 0$, per la Proposizione 4.5 gli A-sottomoduli di A/P^n sono tutti e soli della forma I/P^n, dove I è un ideale di A tale che $P^n \subseteq I$, cioè $I = P^i$ con $0 \leq i \leq n$. Poiché $P^i \subseteq P^j$ se $i \geq j$, si ha chiaramente (per $0 \leq i, j \leq n$) $P^i/P^n + P^j/P^n = A/P^n$ se e solo se $i = 0$ o $j = 0$. Da ciò segue subito che gli unici addendi diretti di A/P^n sono quelli banali, cioè A/P^n è indecomponbile.

Viceversa, sia M un modulo finitamente generato e indecomponibile. Per il Corollario 13.5 esiste un sottomodulo libero (di rango finito) L di M tale che $M = \mathrm{T}(M) \oplus L$. Per l'indecomponibilità di M deve essere $\mathrm{T}(M) = 0$ e $M = L$ o $L = 0$ e $M = \mathrm{T}(M)$. Nel primo caso $M = L$ è libero e indecomponibile, quindi necessariamente di rango 1, cioè $M \cong A$. Nel secondo caso $M = \mathrm{T}(M) = \bigoplus_{P \in \mathrm{Max}(A)} \mathrm{T}_P(M)$ per la Proposizione 13.8. Di nuovo, l'indecomponibilità di M implica che esiste unico $P \in \mathrm{Max}(A)$ tale che $M = \mathrm{T}_P(M)$. Per il Lemma 13.9 esiste $x \in M$ tale che $\mathrm{Ann}(M) = \mathrm{Ann}(x) = P^n$ (con $n \in \mathbb{N}$) e $\langle x\rangle_A$ è un addendo diretto di M. Essendo M indecomponibile (quindi in particolare non nullo) deve essere $n > 0$, $x \neq 0$ e $M = \langle x\rangle_A$. Si conclude allora che $M \cong A/\mathrm{Ann}(x) = A/P^n$ per la Proposizione 4.7. □

Possiamo ora dimostrare una versione del *teorema di struttura per moduli finitamente generati su un dominio a ideali principali.*

Teorema 13.11. *Sia M un A-modulo finitamente generato. Allora esistono unici $l \in \mathbb{N}$ e $l_{P,n} \in \mathbb{N}$ per ogni $P \in \mathrm{Max}(A)$ e per ogni $n > 0$ tali che*

$$M \cong \bigoplus_{P \in \mathrm{Max}(A),\, n > 0} (A/P^n)^{l_{P,n}} \bigoplus A^l \tag{13.1}$$

e $\#\{(P,n) \in \mathrm{Max}(A) \times \mathbb{N}_{>0} : l_{P,n} > 0\} < \infty$.

Dimostrazione. L'esistenza della decomposizione cercata è garantita dalla Proposizione 11.11, tenendo conto che, a meno di isomorfismo, gli A-moduli noetheriani (cioè finitamente generati) indecomponibili sono precisamente A e A/P^n (con $P \in \mathrm{Max}(A)$ e $n > 0$) per la Proposizione 13.10.

Per quanto riguarda l'unicità, se vale (13.1) e chiamiamo M' il membro di destra, è ovvio che $\mathrm{T}(M')$ è dato dalla prima sommatoria, per cui (ricordando l'Osservazione 5.7) $M/\mathrm{T}(M) \cong M'/\mathrm{T}(M') \cong A^l$. Pertanto $l = \mathrm{rk}(M/\mathrm{T}(M))$ è univocamente determinato da $M/\mathrm{T}(M)$ (e quindi da M) per il Corollario 7.7. Fissato poi $P \in \mathrm{Max}(A)$, si ha chiaramente $\mathrm{T}_P(M) \cong \mathrm{T}_P(M') = \bigoplus_{n>0}(A/P^n)^{l_n}$ (dove per brevità scriviamo l_n invece di $l_{P,n}$), e resta da dimostrare che gli l_n sono univocamente determinati da $\mathrm{T}_P(M)$ (e quindi da M). Per ogni A-modulo N e per ogni $i \in \mathbb{N}$ poniamo $E_i(N) := (P^iN)/(P^{i+1}N)$: poiché $P^{i+1}N = P(P^iN)$, l'A-modulo $E_i(N)$ è in modo naturale un $K := A/P$-spazio vettoriale. Per ogni $n > 0$ si ha chiaramente $P^i(A/P^n) = P^{\min\{i,n\}}/P^n$, e dunque

$$E_i(A/P^n) \cong P^{\min\{i,n\}}/P^{\min\{i+1,n\}} \cong \begin{cases} P^i/P^{i+1} & \text{se } i < n \\ \{0\} & \text{se } i \geq n \end{cases}$$

(per il terzo teorema di isomorfismo per moduli). D'altronde, tenendo conto dell'Osservazione 7.5, si ha

$$E_i(\mathrm{T}_P(M)) \cong E_i(\mathrm{T}_P(M')) \cong \bigoplus_{n>0} E_i(A/P^n)^{l_n}.$$

Poiché $\dim_K(P^i/P^{i+1}) = 1$ (se $P = (p)$, è facile vedere che $\{p^i + P^{i+1}\}$ è una base di P^i/P^{i+1}), si ottiene $\dim_K(E_i(\mathrm{T}_P(M))) = \sum_{n>i} l_n$, e pertanto

$$l_n = l_{P,n} = \dim_K(E_{n-1}(\mathrm{T}_P(M))) - \dim_K(E_n(\mathrm{T}_P(M)))$$

è univocamente determinato da $\mathrm{T}_P(M)$. □

Osservazione 13.12. Dato che A e A/P^n (con $P \in \mathrm{Max}(A)$ e $n > 0$) sono A-moduli ciclici, il Teorema 13.11 dice in particolare che ogni A-modulo finitamente generato M è somma diretta finita di A-moduli ciclici. Una tale decomposizione non è però essenzialmente unica. È infatti immediato verificare che, se I e J sono ideali coprimi di A (cioè $I + J = A$), l'isomorfismo di anelli (dato dal teorema cinese del resto) $A/IJ \to A/I \times A/J$, $a + IJ \mapsto (a + I, a + J)$ è anche un isomorfismo di A-moduli. Ne segue (per induzione su k) che se $P_1, \ldots, P_k \in \mathrm{Max}(A)$ sono distinti e $n_1, \ldots, n_k \in \mathbb{N}$, c'è un isomorfismo di A-moduli $A/\prod_{i=1}^k P_i^{n_i} \cong \bigoplus_{i=1}^k A/P_i^{n_i}$. Dunque nella decomposizione (13.1) si possono raggruppare termini di torsione relativi a ideali massimali distinti, e in generale questo può essere fatto in modi diversi. D'altra parte non è difficile dimostrare che esistono unici ideali $I_1 \subseteq \cdots \subseteq I_k \subsetneq A$ tali che $M \cong \bigoplus_{i=1}^k A/I_i$ (tra l'altro tale decomposizione richiede il minimo numero possibile di addendi ciclici). In effetti risulta $I_1 = \cdots = I_l = \{0\}$ e, se $\mathrm{T}(M) \neq \{0\}$, $I_{l+1} = \prod_{P \in \mathrm{Max}(A)} P^{m_P}$, dove $m_P = 0$ se $\mathrm{T}_P(M) = \{0\}$ e altrimenti $m_P = \max\{n > 0 : l_{P,n} > 0\}$; gli eventuali successivi I_i vengono poi determinati induttivamente in modo analogo.

Osservazione 13.13. Un A-modulo non finitamente generato non è in generale somma diretta di moduli ciclici. Un esempio esplicito è dato da $\mathbb{Q}$ (con $A = \mathbb{Z}$), che è indecomponibile (per l'Esempio 11.14) ma non ciclico.

14. Forma canonica di Jordan

Sia V un K-spazio vettoriale e sia $f \in \mathrm{End}_K(V)$. Segue dall'Esempio 8.6 e dall'Esempio 8.10 che esiste un unico omomorfismo di K-algebre $\beta\colon K[X] \to \mathrm{End}_K(V) \subseteq \mathrm{End}(V)$ tale che $\beta(X) = f$. Indicando con V_f il $K[X]$-modulo definito da β, è ovvio per definizione che il K-spazio vettoriale ottenuto da V_f per restrizione degli scalari è V e che $Xv = f(v)$ per ogni $v \in V_f = V$.

Viceversa, sia M un $K[X]$-modulo, dato da un omomorfismo di anelli $\beta\colon K[X] \to \mathrm{End}(M)$, e notiamo che (sempre grazie all'Esempio 8.6) $\mathrm{im}(\beta) \subseteq \mathrm{End}_{K[X]}(M) \subseteq \mathrm{End}_K(M)$. Dunque, indicando con V il K-spazio vettoriale ottenuto da M per restrizione degli scalari, la funzione $f\colon V \to V$, $v \mapsto Xv$ è K-lineare, ed è chiaro che $V_f = M$. Pertanto dare un $K[X]$-modulo equivale a dare una coppia costituita da un K-spazio vettoriale e da un suo endomorfismo K-lineare.

Osservazione 14.1. Segue subito dalla definizione che $W \subseteq V_f$ è un $K[X]$-sottomodulo se e solo se $W \subseteq V$ è un K-sottospazio vettoriale tale che $f(W) \subseteq W$.

Fissiamo una coppia (V, f) come sopra e assumiamo $\dim_K(V) < \infty$: essendo V un K-modulo finitamente generato, V_f è un $K[X]$-modulo finitamente generato per l'Osservazione 7.1. Per il Teorema 13.11 V_f è (in modo essenzialmente unico) una somma diretta finita di $K[X]$-moduli della forma $K[X]/(p)^n$ con $p \in K[X]$ irriducibile e $n > 0$ (si noti che non ci possono essere termini della forma $K[X]$ perché $\dim_K(K[X]) = \infty$). Per l'Osservazione 5.6 possiamo supporre che ciascuno di tali moduli sia proprio un sottomodulo di V_f. Tenendo conto dell'Osservazione 14.1, se ne deduce che si può trovare una base di V rispetto alla quale f è rappresentata da una matrice "diagonale a blocchi", in cui ciascun blocco rappresenta la restrizione di f ai vari sottomoduli dati dalla decomposizione.

Facendo l'ipotesi ulteriore che K sia algebricamente chiuso, i polinomi irriducibili di $K[X]$ sono solo quelli di primo grado, per cui si può supporre $p = X - a$ per qualche $a \in K$. Posto $W := K[X]/(X-a)^n$ possiamo dunque vedere W come K-sottospazio vettoriale di V tale che $f|_W\colon W \to W$ è definita da $f(\overline{g}) = X\overline{g}$ (dove $\overline{g} := g + (X-a)^n \in W$ per ogni $g \in K[X]$). È allora facile vedere che $\{w_i := \overline{(X-a)^{n-i}} \,:\, i = 1, \dots, n\}$ è una base di W e che $f(w_1) = aw_1$, mentre $f(w_i) = aw_i + w_{i-1}$ per $1 < i \leq n$. Quindi rispetto a tale base $f|_W$ è rappresentata dalla matrice $n \times n$

$$\begin{pmatrix} a & 1 & 0 & \cdots & \cdots & 0 \\ 0 & a & 1 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & 0 & a & 1 \\ 0 & \cdots & \cdots & \cdots & 0 & a \end{pmatrix} \tag{14.1}$$

detta *blocco di Jordan*. In conclusione, se K è algebricamente chiuso e $\dim_K(V) < \infty$, esiste una base di V rispetto alla quale f è rappresentata da

una matrice diagonale a blocchi in cui ogni blocco è appunto di Jordan. Tale matrice si dice *forma canonica di Jordan* di f: segue facilmente dall'unicità del Teorema 13.11 che essa è unica, a meno dell'ordine dei blocchi.

15. Gruppi abeliani finiti

Il Teorema 13.11 con $A = \mathbb{Z}$ fornisce una versione del *teorema di struttura dei gruppi abeliani finitamente generati.*

Teorema 15.1. *Sia G un gruppo abeliano finitamente generato. Allora, indicando con $\mathcal{P}$ l'insieme dei numeri primi, esistono unici $l \in \mathbb{N}$ e $l_{p,n} \in \mathbb{N}$ per ogni $p \in \mathcal{P}$ e per ogni $n > 0$ tali che*

$$G \cong \bigoplus_{p\in\mathcal{P},\, n>0} (\mathbb{Z}/p^n\mathbb{Z})^{l_{p,n}} \bigoplus \mathbb{Z}^l$$

e $\#\{(p,n) \in \mathcal{P} \times \mathbb{N}_{>0} \,:\, l_{p,n} > 0\} < \infty$. Inoltre G è finito se e solo se $l = 0$.

Corollario 15.2 (Teorema di Sylow per gruppi abeliani)**.** *Sia G un gruppo abeliano finito di ordine $\prod_{p\in\mathcal{P}} p^{n_p}$ (con $n_p \in \mathbb{N}$ quasi tutti 0). Allora per ogni $p \in \mathcal{P}$ esiste un unico sottogruppo H_p di G di ordine p^{n_p}; se inoltre H è un sottogruppo di G di ordine una potenza di p, allora $H \subseteq H_p$.*

Dimostrazione. Possiamo chiaramente supporre che $(G, +)$ sia un gruppo additivo. Posto $H_p := \mathrm{T}_p(G)$ per ogni $p \in \mathcal{P}$, per il Teorema 15.1 (e ricordando la Proposizione 13.8) si ha $G = \bigoplus_{p\in\mathcal{P}} H_p$ e ogni H_p è una somma diretta finita di gruppi ciclici di ordine potenze di p, per cui $\#H_p = p^{n'_p}$ per qualche $n'_p \in \mathbb{N}$. D'altra parte

$$\prod_{p\in\mathcal{P}} p^{n_p} = \#G = \#\left(\bigoplus_{p\in\mathcal{P}} H_p\right) = \prod_{p\in\mathcal{P}} \#H_p = \prod_{p\in\mathcal{P}} p^{n'_p},$$

e quindi $n'_p = n_p$ per ogni $p \in \mathcal{P}$. Per dimostrare l'ultima affermazione (che chiaramente implica anche l'unicità di H_p come sottogruppo di ordine p^{n_p}), basta osservare che, se H è un sottogruppo di G di ordine una potenza di p, allora per ogni $a \in H$ anche $\mathrm{ord}(a)$ è una potenza di p (per il teorema di Lagrange), e dunque a è un elemento di p-torsione, cioè $a \in H_p$. □

Osservazione 15.3. Indicando con $\mathrm{ab}(n)$ (per ogni intero positivo n) il numero di classi di isomorfismo di gruppi abeliani di ordine n, segue dal Teorema 15.1 e dal Corollario 15.2 che, se $n = \prod_{p\in\mathcal{P}} p^{n_p}$ (con $n_p \in \mathbb{N}$ quasi tutti 0), allora $\mathrm{ab}(n) = \prod_{p\in\mathcal{P}} \mathrm{ab}(p^{n_p})$. Inoltre $\mathrm{ab}(p^k)$ (per $k > 0$) non dipende da p, e in effetti $\mathrm{ab}(p^k) = \mathrm{p}(k)$, dove $\mathrm{p}(k)$ indica il numero di partizioni di k come somma di interi positivi. Per esempio, le partizioni di 4 sono 4, $3+1$, $2+2$, $2+1+1$, $1+1+1+1$, per cui $\mathrm{p}(4) = 5$.

Definizione 15.4. L'*esponente* di un gruppo finito G è il più piccolo intero positivo $\exp(G)$ tale che $g^{\exp(G)} = 1$ per ogni $g \in G$.

Osservazione 15.5. $\exp(G) = \mathrm{mcm}\{\mathrm{ord}(g) \,:\, g \in G\}$ per ogni gruppo finito G; segue inoltre dal teorema di Lagrange che $\exp(G) \mid \#G$.

Corollario 15.6. *Sia G un gruppo abeliano finito. Allora $\exp(G) = \#G$ se e solo se G è ciclico.*

Dimostrazione. Se $G = \langle g \rangle$ è ciclico, allora $\mathrm{ord}(g) = \#G$. Se ne deduce (tenendo conto dell'Osservazione 15.5) che $\exp(G)$ è sia un multiplo che un divisore di $\#G$, per cui $\exp(G) = \#G$. Supponiamo viceversa che $\exp(G) = \#G$. Per il Teorema 15.1 esistono degli interi positivi $l_1, \dots, l_s$ tali che $G \cong \bigoplus_{i=1}^{s} C_{l_i} = \prod_{i=1}^{s} C_{l_i}$ (dove C_{l_i} indica un gruppo ciclico di ordine l_i). Poiché (come è molto facile vedere) $\exp(G_1 \times G_2) = \mathrm{mcm}\{\exp(G_1), \exp(G_2)\}$ per ogni coppia di gruppi finiti G_1 e G_2, si ha

$$\prod_{i=1}^{s} l_i = \#G = \exp(G) = \mathrm{mcm}\{\exp(C_{l_1}), \dots, \exp(C_{l_s})\} = \mathrm{mcm}\{l_1, \dots, l_s\},$$

da cui segue che $l_1, \dots, l_s$ sono a due a due coprimi. Applicando il teorema cinese del resto per gruppi si ottiene allora (per induzione su s) che $G \cong \prod_{i=1}^{s} C_{l_i}$ è ciclico. □

Osservazione 15.7. Per un gruppo non abeliano finito può essere $\exp(G) = \#G$: questo succede per esempio se $G = S_3$.

Corollario 15.8. *Se A è un dominio, ogni sottogruppo finito di A^* è ciclico. In particolare, K^* è ciclico per ogni campo finito K (e quindi $\mathbb{Z}/p\mathbb{Z}^*$ è ciclico per ogni numero primo p).*

Dimostrazione. Se G è un sottogruppo di ordine n di A^* e $d = \exp(G)$, ogni elemento di G è radice in A del polinomio $X^d - 1 \in A[X]$. Poiché un polinomio di grado d ha al più d radici in un dominio, deve essere $n \leq d$, e quindi (ricordando che in ogni caso $d \leq n$ per l'Osservazione 15.5) $n = d$. Allora G è ciclico per il Corollario 15.6. □

16. Esercizi

(1) Sia $f\colon M \to N$ un omomorfismo di moduli, e siano $M' \subseteq M$ e $N' \subseteq N$ sottomoduli tali che $f(M') \subseteq N'$.
   (a) Dimostrare che esiste un unico omomorfismo $\overline{f}\colon M/M' \to N/N'$ tale che $\overline{f}(x + M') = f(x) + N'$ per ogni $x \in M$.
   (b) Indicando con $f'\colon M' \to N'$ la restrizione di f, dimostrare che, se f' e $\overline{f}$ sono iniettivi/suriettivi, anche f lo è.

(2) Siano M e N_λ ($\lambda \in \Lambda$) degli A-moduli. Dimostrare che la funzione

$$\begin{aligned} \mathrm{Hom}_A(M, \prod_{\lambda\in\Lambda} N_\lambda) &\to \prod_{\lambda\in\Lambda} \mathrm{Hom}_A(M, N_\lambda) \\ f &\mapsto (\mathrm{pr}_\lambda \circ f)_{\lambda\in\Lambda} \end{aligned}$$

è un isomorfismo di gruppi, e anche di A-moduli se A è commutativo.

(3) Siano M_λ ($\lambda \in \Lambda$) e N degli A-moduli. Dimostrare che la funzione

$$\begin{aligned} \mathrm{Hom}_A(\bigoplus_{\lambda\in\Lambda} M_\lambda, N) &\to \prod_{\lambda\in\Lambda} \mathrm{Hom}_A(M_\lambda, N) \\ f &\mapsto (f \circ \mathrm{in}_\lambda)_{\lambda\in\Lambda} \end{aligned}$$

è un isomorfismo di gruppi, e anche di A-moduli se A è commutativo.

(4) Sia M un modulo e sia f un endomorfismo di M.
   (a) Dimostrare che, se f è suriettivo e non iniettivo, allora $\ker(f) \subsetneq \ker(f^2)$.

(b) Dimostrare che, se M è noetheriano e f è suriettivo, allora f è anche iniettivo.
(c) Fornire un esempio in cui M è noetheriano e f è iniettivo ma non suriettivo.

(5) Siano A_1 e A_2 due anelli commutativi noetheriani. Ricordando che gli ideali di $A_1 \times A_2$ sono tutti e soli della forma $I_1 \times I_2$ con I_i ideale di A_i per $i = 1, 2$, dimostrare che $A_1 \times A_2$ è noetheriano.
(6) Sia A un anello commutativo e siano I e J due ideali di A. Dimostrare che $\mathrm{Hom}_A(A/I, A/J) \cong (J : I)/J$ come A-moduli. Dimostrare inoltre che $\mathrm{End}_A(A/I) \cong A/I$ come A-algebre.
(7) Un elemento e di un anello si dice *idempotente* se $e^2 = e$; 0 e 1 sono ovviamente idempotenti, detti *banali*. Sia $M \neq \{0\}$ un A-modulo.
(a) Dimostrare che, se $e \in \mathrm{End}_A(M)$ è idempotente, allora $M = \ker(e) \oplus \mathrm{im}(e)$.
(b) Dimostrare che M è indecomponibile se e solo se gli unici idempotenti di $\mathrm{End}_A(M)$ sono quelli banali.
(8) Sia $f\colon M \to N$ un omomorfismo di A-moduli. Dimostrare che $M \cong \ker(f) \oplus \mathrm{im}(f)$ se A è un dominio a ideali principali, M è finitamente generato e N è senza torsione.
(9) Sia A un dominio e consideriamo A come sottoanello del suo campo dei quozienti K.
(a) Dimostrare che A è un A-sottomodulo di K e che l'A-modulo K/A è di torsione.
(b) Dimostrare che, se A è a ideali principali ma non un campo e $P = (p) \in \mathrm{Max}(A)$, allora i sottomoduli $M_n := \langle \frac{1}{p^n} + A \rangle_A$ (per $n \in \mathbb{N}$) di K/A sono tali che $M_n \subsetneq M_{n+1}$ per ogni $n \in \mathbb{N}$.
(c) Con le ipotesi del punto precedente, dimostrare che l'A-modulo $\mathrm{T}_P(K/A)$ non è finitamente generato.
(10) Sia A un dominio a ideali principali ma non un campo. Sia inoltre N un sottomodulo non banale di A^2 e sia $M := A^2/N$.
(a) Dimostrare che, se $N \cong A^2$, allora M è di torsione.
(b) Dimostrare che, se M è senza torsione, allora $M \cong N \cong A$.
(11) Sia G un gruppo abeliano di ordine n e sia d un divisore positivo di n. Dimostrare che G ha un sottogruppo di ordine d.
(12) Sia $G := \mathbb{Z}/p^2\mathbb{Z} \oplus (\mathbb{Z}/p\mathbb{Z})^2$ (con p un numero primo) e sia H un sottogruppo di G di ordine p^2.
(a) Dimostrare che, se H è ciclico, allora H è un addendo diretto di G e $G/H \cong (\mathbb{Z}/p\mathbb{Z})^2$.
(b) È vero che, se H non è ciclico, allora $G/H \cong \mathbb{Z}/p^2\mathbb{Z}$?