PARTE QUARTA
Teoria algebrica dei numeri

Lezione 17

Prerequisiti: Anelli. Spazi vettoriali.

Cenni sui moduli.

Sia A un anello commutativo unitario.

Definizione 17.1 Si dice *modulo (sinistro)* su A (o semplicemente, *A-modulo*) ogni gruppo additivo abeliano $(M,+)$ dotato di un'applicazione (*prodotto esterno*)

$$\cdot : A \times M \to M$$
$$(a,m) \mapsto am$$

che gode delle seguenti proprietà:

i) per ogni $a,b \in A, m \in M$, $(a+b)m = am + bm$
ii) per ogni $a \in A, m,n \in M$, $a(m+n) = am + an$
iii) per ogni $a,b \in A, m \in M$, $(ab)m = a(bm)$
iv) per ogni $m \in M$, $1m = m$.

Nota Per comodità, indicheremo con 0 l'elemento neutro di M, benché questo sia il simbolo usato anche per lo zero dell'anello A. Il contesto permetterà, di volta in volta, di dare la giusta interpretazione.

Esercizio 17.2* Provare che
a) per ogni $a \in A$ $a0 = 0$ (qui 0 indica lo zero di M.)
b) per ogni $m \in M$, $0m = 0$ (qui 0 indica lo zero di A a primo membro, lo zero di M a secondo membro).

Osservazione 17.3 Se A è un campo, la nozione di modulo su A coincide con quella di spazio vettoriale su A.

Esempi 17.4
a) L'anello commutativo unitario A è un modulo su se stesso (detto *modulo regolare*): il prodotto esterno è il prodotto di A.
b) Più in generale, A è un modulo su ogni suo sottoanello unitario.
c) La nozione di **Z**-modulo coincide con quella di gruppo abeliano.

Definizione 17.5 Sia M un A-modulo. Un sottogruppo N del gruppo additivo M si dice un *sottomodulo* (o, più precisamente, *sotto-A-modulo*) di M se, per ogni $a \in A, n \in N$, $an \in N$ (in altri termini, se è chiuso rispetto al prodotto esterno).

Esempi 17.6
a) Sono sottomoduli di un A-modulo M: M e $\{0\}$ (quest'ultimo è detto anche *sottomodulo nullo.*)

b) I sottomoduli di A sono i suoi ideali.

c) Dato un modulo M, per ogni ideale I di A l'insieme $IM = \{\sum_{i=1}^{n} a_i m_i \,|\, a_i \in I, m_i \in M, n \in \mathbf{N}\}$ è un sottomodulo di M.

Definizione 17.7 Dato un sottoinsieme S dell'A-modulo M, si dice *sottomodulo generato da S* il più piccolo sottomodulo di M contenente S.

Nota Il sottomodulo generato dall'insieme vuoto è il sottomodulo nullo.

Lasciamo al lettore la facile dimostrazione della seguente:

Proposizione 17.8 Il sottomodulo di M generato dal sottoinsieme S è

$$\left\{ \sum_{i=1}^{n} a_i s_i \,\middle|\, n \in \mathbf{N}, a_i \in A, s_i \in S \right\}.$$

Se $S = \{s_1,...,s_n\}$, indicheremo tale sottomodulo anche come $\sum_{i=1}^{n} As_i$.

Ai moduli si estendono le seguenti nozioni, note dalla teoria degli spazi vettoriali.

Definizione 17.9 Sia M un A-modulo, sia S un suo sottoinsieme. Si dice che

a) S è *libero*, se, per ogni $n \in \mathbf{N}, s_1,...,s_n \in S$ a due a due distinti e $a_1,...,a_n \in A$ tali che $\sum_{i=1}^{n} a_i s_i = 0$, si ha che $a_i = 0$ per ogni $i = 1,...,n$. In tal caso si dice anche che gli elementi di S sono *linearmente indipendenti*.

b) S è *un sistema di generatori* per M se il sottomodulo generato da S coincide con M, ossia, se per ogni $m \in M$ esistono $n \in \mathbf{N}, s_1,...,s_n \in S, a_1,...,a_n \in A$ tali che $m = \sum_{i=1}^{n} a_i s_i$.

c) S è una *base* di M se è libero ed è un sistema di generatori per M.

M si dice *finitamente generato* (*f.g.*) se ammette un sistema di generatori finito.

Nota Un elemento m di M si dice *libero* se $\{m\}$ è libero. Un elemento del modulo regolare A è libero se e solo se non è un divisore di zero.

Osservazione 17.10 Contrariamente a quanto avviene per gli spazi vettoriali, in un modulo
a) non sempre esiste una base;
b) un sistema di generatori minimale non è necessariamente una base;
c) un insieme libero massimale non è necessariamente una base;
d) i sistemi di generatori minimali non hanno necessariamente la stessa cardinalità.
e) gli insiemi liberi massimali non hanno necessariamente la stessa cardinalità.

L'Osservazione 17.10 giustifica la seguente

Definizione 17.11 Un modulo si dice *libero* se ha una base.

Esempi 17.12 Sia A un anello non banale. Sono moduli liberi:
a) l'anello A come modulo su se stesso: una base è formata da 1;
b) per ogni intero positivo n, l'anello somma diretta A^n: una base è formata dalle n-uple

$$e_1 = (1,0,0,..,0,0), \quad e_2 = (0,1,0,...,0,0), \quad \ldots, \quad e_n = (0,0,0,...,0,1);$$

c) l'anello dei polinomi $A[x]$ nell'indeterminata x: una base è formata dagli elementi $1, x, x^2, ...$
d) il modulo nullo, che ha l'insieme vuoto come base.

Esempi 17.13 Non sono moduli liberi:
a) i gruppi $\mathbf{Z}_n$ come $\mathbf{Z}$-moduli: infatti $\mathbf{Z}_n$ non ha sottoinsiemi liberi non vuoti;
b) $\mathbf{Q}$ come $\mathbf{Z}$-modulo: infatti è facile vedere che, dato un sottoinsieme S di $\mathbf{Q}$, se S ha un solo elemento, non è un sistema di generatori, e se S ha almeno due elementi, non è libero.

La seguente proprietà stabilisce, però, un'importante analogia con gli spazi vettoriali. Ne daremo la dimostrazione a conclusione di questa lezione.

Proposizione 17.14 Le basi di un modulo libero hanno tutte la stessa cardinalità (detta *rango* del modulo).

Anche in un modulo libero, tuttavia, possono essere valide le affermazioni b), c) e d) dell'Osservazione 17.10. Lo dimostra il prossimo esempio.

Esempio 17.15 In base all'Esempio 17.12 a) $\mathbf{Z}$ è uno $\mathbf{Z}$-modulo libero di rango 1. Però:
- $\{2,3\}$ è un sistema di generatori minimale, ma non è una base;
- $\{2\}$ è un sottoinsieme libero massimale, ma non è una base;
- $\{2,3\}$ e $\{6,15,10\}$ sono sistemi di generatori minimali, aventi cardinalità diverse.

Diversamente da quanto avviene per gli spazi vettoriali, un sottomodulo di un modulo libero non è necessariamente libero.

Proposizione 17.16 Se un ideale dell'anello A è un A-modulo libero, allora è principale. Se A è integro, vale il viceversa.

Dimostrazione: Osserviamo che un sottoinsieme di A avente almeno due elementi a, b non è libero, in quanto ba-ab = 0. Quindi un ideale libero dell'anello A è necessariamente generato da un solo elemento, cioè è principale. Sia $I = (a)$. Se a = 0, allora I è libero in virtù dell'Esempio 17.12 d). Altrimenti, se A è integro, a è un elemento libero. Quindi $\{a\}$ è una base di I come A-modulo. □

Esempio 17.17 In base all'Esempio 17.11 c), $\mathbf{Z}[x]$ è uno $\mathbf{Z}[x]$-modulo libero. Però l'ideale $(2,x)$ non è uno $\mathbf{Z}[x]$-modulo libero, perché, come visto in Algebra 2, Esempio 16.12, non è un ideale principale.

Osservazione 17.18 Dalla Proposizione 17.16 non è possibile rimuovere l'ipotesi di integrità. Infatti, in $\mathbf{Z}_6$, l'ideale $([2]_6)$ non è uno $\mathbf{Z}_6$-modulo libero, perché nessuno dei suoi elementi è libero.

Per avere proprietà simili a quelle degli spazi vettoriali, è necessario considerare moduli liberi finitamente generati su domini ad ideali principali, ad esempio su $\mathbf{Z}$. Per questi vale il seguente teorema, che è conseguenza del Teorema di struttura per i moduli finitamente generati su $\mathbf{Z}$ (vedi Algebra 2, Lezione 27)

Teorema 17.19 Sia M un modulo libero finitamente generato su **Z**, e sia m il rango di M. Sia N un sottomodulo di M. Allora

a) N è libero, finitamente generato, di rango $n \le m$;
b) esiste un base $\{s_1,...,s_m\}$ di M ed esistono numeri interi $c_1,...,c_n$ tali che $\{c_1 s_1,...,c_n s_n\}$ sia una base di N;
c) L'indice $(M:N)$ è finito se e solo se $m = n$. In tal caso, se $\{a_1,...,a_m\}$ e $\{b_1,...,b_m\}$ sono basi di M ed N rispettivamente, allora esiste un matrice invertibile T di ordine m a coefficienti in **Z** tale che

$$\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = T \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}.$$

Inoltre, $(M:N) = |\det T|$.

Dimostrazione: [B], Theorem A.11.

Nota La condizione $m=n$ contenuta nella parte b) dell'enunciato non implica affatto che $M=N$. Basta pensare che, in base alla Proposizione 17.16, tutti i sottogruppi (ideali) di **Z** sono **Z**-moduli liberi di rango 1.

Definizione 17.20 Un'applicazione $f : M \to N$ tra A-moduli si dice un *omomorfismo di A-moduli* (o *applicazione A-lineare*) se è un omomorfismo di gruppi additivi tale che, per ogni $a \in A, m \in M$,

$$f(am) = af(m).$$

Esercizio 17.21* Provare che l'immagine (la controimmagine) di un sottomodulo del modulo di partenza (di arrivo) è un sottomodulo del modulo di arrivo (di partenza).

In particolare, il nucleo di un omomorfismo di moduli è un sottomodulo del modulo di partenza.

Concludiamo questa sezione introduttiva con la struttura di modulo quoziente. Dati un A-modulo M ed un suo sottomodulo N, il gruppo quoziente M/N può essere dotato di una struttura di A-modulo definendo il prodotto esterno nel seguente modo: per ogni $a \in A, m \in M$ si pone

$$a(N+m) = N + am.$$

Si verifica facilmente che tale definizione è ben posta.

Definizione 17.22 Il gruppo quoziente M/N dotato del prodotto esterno definito sopra si dice *modulo quoziente di M rispetto ad N* (detto, per brevità, anche *M su N,* oppure *M modulo N*).

La suriezione canonica

$$\pi : M \to M/N$$
$$m \mapsto N + m$$

com'è facile vedere, è un omomorfismo di moduli.

Ai moduli, agli omomorfismi di moduli ed ai moduli quoziente si estendono in maniera naturale le principali proprietà valide per i gruppi (ad esempio, i Teoremi di isomorfismo, di corrispondenza, e molti altri) e le principali costruzioni (somma diretta, prodotto diretto). Le richiameremo, di volta in volta, quando ci occorreranno.

Per ora, diamo invece un risultato che appartiene esclusivamente alla teoria dei moduli, e che ci sarà utile per dimostrare la Proposizione 17.14.

Lemma 17.23 Sia I un ideale dell'anello A e sia M un A-modulo. Allora M/IM è un modulo su A/I mediante il prodotto esterno definito come segue: per ogni $a \in A, m \in M$,

$$(I + a)(IM + m) = IM + am .$$

Dimostrazione: È sufficiente dimostrare che la definizione è ben posta: dopo di ciò, gli assiomi di modulo seguono banalmente da quelli soddisfatti da M. Siano $a' \in A, m' \in M$ tali che

$$I + a' = I + a, \qquad IM + m' = IM + m.$$

Allora si deduce facilmente che

$$a'm' - am = a'm' - a'm + a'm - am = a'(m' - m) + (a' - a)m \in IM . \square$$

Siamo ora in grado di dare la

Dimostrazione della Proposizione 17.14: Sia M un modulo libero sull'anello A. Sia B una sua base. Supporremo, per semplicità, che B sia finito, $B = \{x_1, ..., x_n\}$. Sia I un ideale massimale di A (esistente come conseguenza del Lemma di Zorn, vedi, ad esempio, [AM], Teorema 1.3.). Allora A/I è un campo (vedi Algebra 2, Proposizione 18.10), e alla luce del Lemma 17.23, M/IM è uno spazio vettoriale su A/I. Detta $\pi : M \to M/IM$ la suriezione canonica, è facile vedere che $\pi(B)$ è un sistema di generatori di M/IM su A/I. Proviamo che $\pi(B)$ è anche un insieme libero. Siano $a_1, ..., a_n \in A$ tali che

$$\sum_{i=1}^{n} (I + a_i)(IM + x_i) = IM + 0 . \qquad (1)$$

Allora $\sum_{i=1}^{n} a_i x_i \in IM$, quindi esistono $b_1, ..., b_n \in I$ tali che

$$\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} b_i x_i .$$

Per l'unicità della rappresentazione, segue che, per ogni $i = 1,...,n$, $a_i = b_i$, quindi $I + a_i = I$. Segue che i coefficienti della combinazione lineare in (1) sono tutti nulli. Ciò prova che $\pi(B)$ è una base di M/IM su A/I, quindi

$$n = \dim_{A/I} M / IM .$$

Ciò prova che tutte le basi di *M* su *A* hanno lo stesso numero *n* di elementi. □

Supponiamo che l'*A*-modulo M ammetta un sistema di generatori finito $S = \{s_1,...,s_n\}$. Consideriamo l'applicazione

$$\begin{aligned} \varphi &: A^n \to M \\ (a_1,...,a_n) &\mapsto \sum_{i=1}^{n} a_i s_i \end{aligned} .$$

Questa è evidentemente un omomorfismo di *A*-moduli suriettivo, che è iniettivo se e solo se *S* è una base. In base al teorema fondamentale di omomorfismo per moduli segue

Proposizione 17.24 Ogni *A*-modulo generato da *n* elementi è isomorfo ad un quoziente di A^n.