Alma Mater Studiorum · Università di Bologna

facoltà di scienze matematiche, fisiche e naturali

Corso di Laurea Triennale in Matematica

MODULI SEMISEMPLICI E TEOREMA DI WEDDERBURN-ARTIN

Tesi di Laurea in Complementi di Algebra 1

Relatore:
Chiar.ma Prof.
Fioresi Rita

Presentata da:
Corbucci Giulia

Sessione I
Anno Accademico 2010/2011

Introduzione

Lo scopo di questa tesi è arrivare a enunciare e dimostrare il teorema di Wedderburn-Artin:
"Ogni algebra semplice su di un campo K di dimensione finita è isomorfa a un anello di matrici".

Nel capitolo 1 definiamo le strutture di modulo e di algebra su di un anello e il concetto di rappresentazione di un'algebra, facendo alcuni esempi salienti tra i quali l'algebra di gruppo, che si ottiene a partire da un gruppo finito e un campo. Nel caso di moduli su anelli commutativi definiamo la struttura di anello delle frazioni, che generalizza la nozione di campo dei quozienti nel caso in cui l'anello considerato non sia un dominio di integrità, e il processo di localizzazione. Descriviamo infine i moduli semplici, cioè quei moduli che non hanno sottomoduli non banali, e il concetto di serie di composizione per un modulo e presentiamo il teorema di Jordan-Hölder.

Nel capitolo 2 introduciamo i moduli semisemplici, con particolare attenzione all'anello delle matrici su di un campo, e dimostriamo due importanti teoremi della teoria della rappresentazione: il teorema di Burnside e il teorema di Wedderburn-Artin, che conduce alla classificazione delle algebre semisemplici:
"Ogni K-algebra semisemplice si può scrivere come somma diretta di anelli di matrici".

Indice

Capitolo 1

Moduli

In questo capitolo presentiamo una prima parte di teoria dei moduli su anelli unitari arbitrari R non necessariamente commutativi.
Nelle prime tre sezioni definiamo le strutture di modulo, sottomodulo e morfismo facendo alcuni esempi e illustriamo anche l'importante processo di localizzazione per moduli su anelli commutativi.
Nelle ultime sezioni trattiamo i moduli semplici mostrando il Lemma di Schur e le condizioni sulle catene.

1.1 Moduli, morfismi, sottomoduli

In questa sezione definiamo la nozione di modulo in due modi equivalenti introducendo anche il concetto di algebra e di rappresentazione. Passiamo poi a definire i morfismi di moduli, i sottomoduli, i quozienti e infine alcuni esempi.

Definizione 1.1. Si definisce *R-modulo sinistro* una coppia (M, μ) dove:

- $\mu : R \times M \to M$, $\mu(a, x) = ax$ è un'applicazione con le seguenti

proprietà: per ogni $x, y \in M$, per ogni $a, b \in R$

$$\begin{aligned} 1 \cdot x &= x; \\ (ab)x &= a(bx); \\ (a+b)x &= ax + bx; \\ a(x+y) &= ax + ay; \end{aligned}$$

- $(M, +)$ è un gruppo abeliano, quindi per ogni $x, y \in M$, $x + y \in M$ e valgono le seguenti proprietà: per ogni $x, y, z \in M$

$$\begin{aligned} x + y &= y + x; \\ (x + y) + z &= x + (y + z); \\ \text{esiste } 0 \in M \quad &\text{tale che} \quad 0 + x = x + 0 = x; \\ \text{esiste } -x \in M \quad &\text{tale che} \quad x + (-x) = 0. \end{aligned}$$

Si definisce *R-modulo destro* una coppia (M, ν) con M gruppo abeliano e $\nu : M \times R \to M$, $\nu(x, a) = xa$ applicazione con analoghe proprietà.

Definizione 1.2. Siano M, N due R-moduli. Un'applicazione $f : M \to N$ è un *morfismo di R-moduli* se: per ogni $x, y \in M$, per ogni $a \in R$

$$\begin{aligned} f(x + y) &= f(x) + f(y); \\ f(ax) &= af(x). \end{aligned}$$

Se $M = N$ si parla di *endomorfismo*. Se l'applicazione è biunivoca è detta *isomorfismo* di R-moduli.
Indichiamo con $\mathrm{End}_R M$ l'insieme degli endomorfismi su M.

È possibile dare una definizione equivalente di R-modulo nel modo seguente.

Proposizione 1.3. *M è un R-modulo se e solo se:*

- *$(M,+)$ è un gruppo abeliano;*

- *esiste un morfismo di anelli* $\quad \phi : R \to End_R(M), \quad \phi(a) = \psi_a.$

Dimostrazione. ($\Rightarrow$) Se M è un R-modulo allora è un gruppo abeliano. Consideriamo

$$\begin{aligned} \phi : R &\to \mathrm{End}_R(M) \\ a &\mapsto \psi_a \end{aligned}$$

con $\psi_a(m) = am$.
Per le proprietà di R-modulo si ha che: per ogni $a, b \in R$

- $\phi(1) = \psi_1 = Id$;
- $\phi(a+b) = \psi_{a+b} = \psi_a + \psi_b$, infatti $\psi_{a+b}(m) = (a+b)m = am + bm = \psi_a(m) + \psi_b(m) \quad \forall m \in M$;
- $\phi(ab) = \psi_{ab} = \psi_a \circ \psi_b$, infatti $\psi_{ab} = (ab)m = a(bm) = (\psi_a \circ \psi_b)(m) \quad \forall m \in M$.

Quindi ϕ è un morfismo di anelli.

($\Leftarrow$) Data

$$\begin{aligned} \phi : R &\to \mathrm{End}_R(M) \\ a &\mapsto \psi_a \end{aligned}$$

con $\psi_a(m)$ endomorfismo di M come gruppo abeliano, definiamo

$$\begin{aligned} \mu : R \times M &\to M \\ (a, m) &\mapsto am := \psi_a(m) \end{aligned}$$

Poichè ϕ è morfismo di anelli vale: per ogni $m, n \in M$, per ogni $a, b \in R$

- $1 \cdot m = \psi_1(m) = Id(m) = m$;
- $(ab)m = \psi_{ab}(m) = (\psi_a \circ \psi_b)(m) = \psi_a(bm) = a(bm)$;
- $(a+b)m = \psi_{a+b}(m) = \psi_a(m) + \psi_b(m) = am + bm$;

- $a(m+n) = \psi_a(m+n) = \psi_a(m) + \psi_a(n) = am + an$;

quindi M è un R-modulo. □

Grazie a questa proposizione possiamo ridefinire la nozione di R-modulo introducendo il concetto di rappresentazione di R. Definiamo prima la struttura di R-algebra.

Definizione 1.4. Una *R-algebra* A è un R-modulo munito di un'operazione bilineare $* : A \times A \to A$ chiamata *moltiplicazione* tale che $(A, +, *)$ sia un anello.

Osservazione 1.5 (moduli ottenuti per restrizione di scalari)**.** Siano A, B due anelli e $f : A \to B$ un morfismo di anelli. Se N è un B-modulo, allora è anche un A-modulo con l'operazione di moltiplicazione per elementi di A definita nel modo seguente:

$$a \cdot n := f(a) \cdot n \quad \text{per ogni } a \in A, \text{ per ogni } n \in N$$

e si dice modulo ottenuto dal B-modulo N per *restrizione di scalari*. In particolare B ha una struttura di A-modulo.

Esempio 1.6. Un esempio importante di R-algebra si ha considerando un morfismo di anelli $f : R \to A$: A diventa una R-algebra considerando la struttura di R-modulo ottenuta per restrizione di scalari

$$a \cdot x := f(a) \cdot x \quad \text{per ogni } a \in R, \text{ per ogni } x \in A$$

dove l'ultima operazione è la moltiplicazione in A.

Definizione 1.7. Sia K un campo, R una K-algebra, L un K-spazio vettoriale.
Una *rappresentazione* di R è un morfismo di algebre

$$\begin{aligned} \psi : R &\to End_K(L) \\ a &\mapsto \phi_a \end{aligned}$$

cioè un'applicazione tale che:

$$\begin{aligned} \phi_1 &= Id \quad \text{(applicazione identica)}; \\ \phi_{\alpha a} &= \alpha\phi_a \quad \forall\alpha \in K,\ \forall a \in R; \\ \phi_{a+b} &= \phi_a + \phi_b \quad \forall a, b \in R; \\ \phi_{ab} &= \phi_a\phi_b \quad \forall a, b \in R. \end{aligned}$$

La proposizione 1.3 ci dice dunque che possiamo equivalentemente interpretare un R-modulo M come rappresentazione di R.

Introduciamo infine i concetti di sottomodulo e quoziente.

Definizione 1.8. Sia M un R-modulo. N è un *sottomodulo* di M se è un sottogruppo ed è a sua volta un R-modulo con l'operazione di moltiplicazione indotta da M.
Se N è un sottomodulo di M, M/N è un gruppo abeliano e con la struttura ereditata da M

$$a(m + N) = am + N \quad \forall a \in R, \forall m \in M$$

si ha che M/N è a sua volta un R-modulo chiamato *quoziente*.

1.2 Esempi

Esempio 1.9. Un anello R è un modulo su se stesso in cui la moltiplicazione ax è definita come il prodotto nell'anello. In questo caso tutti e soli i suoi sottomoduli sono i suoi ideali.
Se R è un anello non commutativo i suoi sottomoduli sono tutti e soli i suoi ideali sinistri.
Se K è un campo, i K-moduli sono i K-spazi vettoriali.

Esempio 1.10. Ogni gruppo abeliano $(G, +)$ è uno $\mathbb{Z}$-modulo con

l'operazione di moltiplicazione data da:

$$\begin{aligned} f : \mathbb{Z} \times G &\to G \\ (m, a) &\mapsto ma = \underbrace{a + \cdots + a}_{\text{m volte}} \end{aligned}$$

Esempio 1.11. Sia R un anello commutativo e siano M e N due R-moduli. Se indichiamo con $\mathrm{Hom}_R(M, N)$ l'insieme dei morfismi da M a N e definiamo per ogni $m \in M$, per ogni $a \in R$, per ogni $f, g \in \mathrm{Hom}_R(M, N)$

$$(f + g)(m) = f(m) + g(m)$$

$$(af)(m) = af(m)$$

allora sono verificate tutte le proprietà di R-modulo.
Se R non è commutativo e M e N sono R-moduli sinistri non si può sempre definire il prodotto di $\phi \in \mathrm{Hom}_R(M, N)$ con $a \in R$. Infatti in generale l'applicazione $x \mapsto a\phi(x)$ non è un morfismo da M a N. Per esempio non è sempre verificata la proprietà per cui per ogni $b \in R$, per ogni $x \in M$,

$$(a\phi)(bx) = b((a\phi)(x))$$

in quanto $(a\phi)(bx) = a\ \phi(bx) = ab\ \phi(x)$.

Esempio 1.12. Dati due R-moduli M e N e un morfismo $f : M \to N$, allora si ha che:

$$\mathrm{Ker}(f) = \{m \in M |\ f(m) = 0\} \quad \text{è un sottomodulo di } M;$$

$$\mathrm{Im}(f) = \{n \in N |\ \exists m \in M \text{ tale che } f(m) = n\} \quad \text{è un sottomodulo di } N.$$

Esempio 1.13. Sia G un gruppo finito e K un campo. Possiamo definire una K-algebra chiamata *algebra di gruppo* in questo modo:

$$K[G] := \left\{ \sum_{g \in G} \alpha_g g \mid \alpha_g \in K \right\}.$$

Si tratta delle somme formali di elementi in G a coefficienti in K.
Dato un K-spazio vettoriale V si dice che G agisce su V se esiste

$$\begin{aligned} \phi : (G, \cdot) &\rightarrow (\mathrm{Aut}_K(V), \circ) \\ g &\mapsto \phi_g \end{aligned}$$

morfismo di gruppi, quindi tale che per ogni $g_1, g_2 \in G$, $\phi_{g_1 \cdot g_2} = \phi_{g_1} \circ \phi_{g_2}$, dove $\mathrm{Aut}_K(V)$ denota il gruppo degli automorfismi su V.
Questo morfismo induce un altro morfismo

$$\begin{aligned} \tilde{\phi} : K[G] &\rightarrow \mathrm{End}_K(V) \\ \sum_{g \in G} \alpha_g g &\mapsto \sum_{g \in G} \alpha_g \, \phi_g. \end{aligned}$$

dove $\mathrm{End}_K(V)$ denota l'anello degli endomorfismi su V.
I $K[G]$-moduli sono le K-rappresentazioni di G, ovvero le applicazioni

$$\begin{aligned} \psi : G &\rightarrow \mathrm{Aut}_K(V) \\ g &\mapsto \psi_g \end{aligned}$$

tali che $\quad \forall g_1, g_2 \in G$

$$\begin{aligned} \psi_1 &= id; \\ \psi_{g_1} \circ \psi_{g_2} &= \psi_{g_1 \cdot g_2}. \end{aligned}$$

Equivalentemente i $K[G]$-moduli corrispondono anche alle rappresentazioni dell'algebra $K[G]$.

1.3 Localizzazione

Consideriamo ora un anello R commutativo unitario. Sia $S \subseteq A$ un sottoinsieme moltiplicativamente chiuso, $1 \in S$. Definiamo la seguente relazione su $A \times S$:

$$(a, s) \sim (a', s') \Leftrightarrow \text{esiste } t \in S \text{ tale che } (as' - a's)t = 0. \tag{1.1}$$

Si verifica facilmente che 1.1 è una relazione di equivalenza.
Indichiamo l'insieme delle classi di equivalenza con

$$S^{-1}A := \frac{A \times S}{\sim} = \left\{ [(a,s)] =: \frac{a}{s}, a \in A, s \in S \right\}$$

e definiamo le operazioni seguenti:

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &:= \frac{at+bs}{st}, \quad 0 = \frac{0}{1} \\ \frac{a}{s} \cdot \frac{b}{t} &:= \frac{ab}{st}. \end{aligned}$$

$(S^{-1}A, +, \cdot)$ è un anello commutativo unitario chiamato *anello delle frazioni* di A rispetto a S.

Osservazione 1.14. Se A è un dominio di integrità e $S = A - \{0\}$ allora $S^{-1}A$ è il campo dei quozienti di A.

Osservazione 1.15. Consideriamo il morfismo di anelli

$$\begin{aligned} f : A &\to S^{-1}A \\ a &\mapsto \frac{a}{1}. \end{aligned}$$

f gode delle tre proprietà seguenti:

1. se $f(a) = 0$ allora esiste $s \in S$ tale che $as = 0$;
2. per ogni $s \in S$, $f(s)$ è invertibile e ha inverso $\frac{1}{s}$;
3. ogni elemento di $S^{-1}A$ è della forma $f(a)f(s)^{-1}$.

Nella prossima proposizione vediamo che le proprietà (1), (2), (3) caratterizzano l'anello delle frazioni.

Proposizione 1.16. *Sia $g : A \to B$ un morfismo di anelli tale che per ogni $s \in S$, con $S \subseteq A$ sottoinsieme moltiplicativamente chiuso, $g(s)$ sia invertibile in B. Allora esiste un unico morfismo di anelli $h : S^{-1}A \to B$ tale che $g = h \circ f$.*

Dimostrazione. Unicità. Sia f il morfismo definito nell'osservazione 1.15. Se h è tale che $g = h \circ f$, allora $h\left(\frac{a}{1}\right) = h(f(a)) = g(a)$ per ogni $a \in A$ e $h\left(\frac{1}{s}\right) = h\left(\left(\frac{s}{1}\right)^{-1}\right) = h\left(\frac{s}{1}\right)^{-1} = g(s)^{-1}$ per ogni $s \in S$. Allora

$$h\left(\frac{a}{s}\right) = h\left(\frac{a}{1}\right) h\left(\frac{s}{1}\right)^{-1} = g(a)g(s)^{-1}$$

e quindi h è univocamente determinata da g.
Esistenza. Sia $h\left(\frac{a}{s}\right) = g(a)g(s)^{-1}$. Allora h è un morfismo di anelli se è ben definito sulle classi di equivalenza. Supponiamo $\frac{a}{s} = \frac{a'}{s'}$, allora esiste $t \in S$ tale che $(as' - a's)t = 0$, quindi applicando g si ha

$$[g(a)g(s') - g(a')g(s)]\, g(t) = 0$$

dove $g(t)$ è invertibile per ipotesi. Moltiplicando per $g(s')^{-1}g(s)^{-1}$ otteniamo $g(a)g(s)^{-1} = g(a')g(s')^{-1}$, cioè $h\left(\frac{a}{s}\right) = h\left(\frac{a'}{s'}\right)$. □

Corollario 1.17. *Sia $g : A \to B$ un morfismo di anelli tale che:*

1. *se $s \in S$, con $S \subseteq A$ sottoinsieme moltiplicativamente chiuso, allora $g(s)$ è invertibile in B;*
2. *se $g(a) = 0$ allora esiste $s \in S$ tale che $as = 0$;*
3. *ogni elemento di B è della forma $g(a)g(s)^{-1}$;*

allora esiste un unico isomorfismo di anelli $h : S^{-1}A \to B$ tale che $g = h \circ f$.

Dimostrazione. Basta dimostrare che il morfismo h definito in 1.16 è un isomorfismo. Per l'ipotesi 3. h è suriettiva. Consideriamo ora il nucleo di h: $\mathrm{Ker}(h) = \left\{\frac{a}{s} \mid g(a)g(s)^{-1} = 0\right\} = \left\{\frac{a}{s} \mid g(a) = 0\right\}$ per l'ipotesi 1. Allora $\mathrm{Ker}(h) = \left\{\frac{a}{s} \mid \text{esiste } t \in S \text{ tale che } at = 0\right\}$ per l'ipotesi 2. Così $\mathrm{Ker}(h) = \left\{\frac{0}{1}\right\}$ e h è iniettiva. □

In questo modo abbiamo verificato che l'anello delle frazioni è l'unico anello, a meno di isomorfismi, che soddisfa le proprietà dell'osservazione 1.15.

Osservazione 1.18. Un anello A si dice *locale* se ha un solo ideale massimale $\mathfrak{m}$. Si dimostra che: *A è locale con massimale $\mathfrak{m}$ se e solo se per ogni $x \in A - \mathfrak{m}$, x è invertibile.*

Esempio 1.19. Sia A un dominio di integrità e $\mathfrak{p}$ un suo ideale primo. Definiamo

$$A_{\mathfrak{p}} := (A - \mathfrak{p})^{-1}A = \left\{ \frac{a}{s},\ a \in A, s \notin \mathfrak{p} \right\}.$$

La definizione è ben posta perchè se $\mathfrak{p}$ è primo, $S = (A - \mathfrak{p})$ è moltiplicativamente chiuso (infatti $xp \notin \mathfrak{p} \Leftrightarrow x \notin \mathfrak{p}, y \notin \mathfrak{p}$). Consideriamo

$$\begin{aligned} f : A &\rightarrow A_{\mathfrak{p}} \\ \mathfrak{p} &\mapsto \tilde{\mathfrak{p}} = \left\{ \frac{x}{y},\ x \in \mathfrak{p}, y \notin \mathfrak{p} \right\}. \end{aligned}$$

$\tilde{\mathfrak{p}}$ è un ideale di $A_{\mathfrak{p}}$, infatti:
$\tilde{\mathfrak{p}} = \left\langle \left\{ \frac{x}{1},\ x \in \mathfrak{p} \right\} \right\rangle$ e se $\frac{a}{s} \in A_{\mathfrak{p}}$ e $\frac{x}{y} \in \tilde{\mathfrak{p}}$ allora $\frac{a}{s} \cdot \frac{x}{y} = \frac{ax}{sy} \in \tilde{\mathfrak{p}}$. Inoltre vale che se $\frac{a}{s} \in A_{\mathfrak{p}} - \tilde{\mathfrak{p}}$, cioè $a \notin \mathfrak{p}, s \notin \mathfrak{p}$, allora è invertibile con inverso $\left(\frac{a}{s}\right)^{-1} = \frac{s}{a}$. Così per l'osservazione 1.18 l'anello $A_{\mathfrak{p}}$ è un anello locale.
Questa procedura che associa a A e $\mathfrak{p}$ l'anello locale $A_{\mathfrak{p}}$ si dice *localizzazione* di A in $\mathfrak{p}$.

1.4 Moduli semplici

In questa sezione tratteremo i moduli semplici insieme ad alcuni esempi salienti e dimostreremo il Lemma di Schur, di importanza capitale nella teoria della rappresentazione.

Sia R un anello non necessariamente commutativo.

Definizione 1.20. Un R-modulo M si dice *semplice* se non ha sottomoduli propri non banali, quindi non ha altri sottomoduli tranne 0 e se stesso.
Un anello A si dice *semplice* se non ha ideali propri.

Esempio 1.21. Sia K un campo. Se V è un K-spazio vettoriale i suoi K-sottomoduli sono i sottospazi vettoriali. Gli unici K-moduli semplici sono i K-spazi vettoriali di dimensione 1.

Definizione 1.22. Si definisce *corpo* un anello D unitario in cui ogni elemento non nullo è invertibile, quindi per ogni $a \in D,\ a \neq 0$ esiste $b \in D$ tale che $a \cdot b = 1$.

Un campo è un corpo commutativo.

Esempio 1.23. Uno degli esempi più importanti di corpo è l'algebra dei *quaternioni* $\mathbb{H}$. Questa è una $\mathbb{R}$-algebra di dimensione 4 con base $1, i, j, k$ e con le seguenti regole di moltiplicazione:

- $1h = h$ per ogni $h \in \mathbb{H}$;
- $i^2 = j^2 = k^2 = -1$;
- $ij = k,\ jk = i,\ ki = j$ da cui deriva che $ji = -k,\ kj = -i,\ ik = -j$.

Dato un elemento $q \in \mathbb{H}$, $q = a+bi+cj+dk$, si definisce *modulo* di q il numero $|q| = \sqrt{a^2 + b^2 + c^2 + d^2}$ e *coniugato* di q il quaternione $\overline{q} = a - bi - cj - dk$. Si verifica facilmente che $q\overline{q} = \overline{q}q = |q|^2$ e $\overline{q_1 q_2} = \overline{q_2}\ \overline{q_1}$.
Da queste relazioni segue che se $q \in \mathbb{H},\ q \neq 0$ allora $q^{-1} = \dfrac{\overline{q}}{|q|^2}$ è l'inverso di q, tale che $qq^{-1} = q^{-1}q = 1$. Così $\mathbb{H}$ è un corpo.
Si osserva, poi, che l'algebra dei quaternioni contiene il campo dei numeri complessi $\mathbb{C}$ come elementi del tipo $a + bi$. In particolare

$$\mathbb{H} = \mathbb{C} \oplus \mathbb{C}j$$

quindi ogni quaternione $q = a + bi + cj + dk$ si scrive in modo unico come $q = z_1 + z_2 j$ con $z_1 = a + bi,\ z_2 = c + di \in \mathbb{C}$.

Esempio 1.24. Consideriamo l'anello delle matrici $n \times n$ su di un corpo D, $R = M_n(D)$, con $n > 1$ e $\forall k,\ 1 \leq k \leq n$, definiamo

$$I_k = \left\{ (a_{ij}) \in R |\ a_{ij} = 0 \quad \forall j \neq k \right\} = \left\{ \begin{pmatrix} 0 & \cdots & 0 & a_{1k} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nk} & 0 & \cdots & 0 \end{pmatrix} \in R \right\}$$

Si verifica direttamente che I_k è un R-modulo sinistro, sottomodulo di R, quindi R come modulo su se stesso non è semplice. Si vede però che come anello è semplice.
Vale il seguente risultato.

Teorema 1.25. *Sia A un anello. J è un ideale di $M_n(A)$ se e solo se $J = M_n(I)$ con I ideale di A.*

Dimostrazione. Si veda in [3], capitolo 3, esercizio III.2.8. □

Come per i campi vale che se D è un corpo allora ha solo gli ideali banali; così $M_n(D)$ è un anello semplice.

Un importante lemma legato ai moduli semplici è il seguente.

Proposizione 1.26 (Lemma di Schur)**.** *Siano M e N due R-moduli semplici. Un morfismo $f : M \to N$ o è un isomorfismo o è il morfismo nullo.*

Dimostrazione. Poichè $\mathrm{Ker}(f)$ e $\mathrm{Im}(f)$ sono sottomoduli rispettivamente di M e di N e M e N non hanno sottomoduli propri, allora si possono avere solo due possibilità:

1. $\mathrm{Ker}(f) = 0$, $\mathrm{Im}(f) = N$;
2. $\mathrm{Ker}(f) = M$, $\mathrm{Im}(f) = 0$.

Se vale (1) f è un isomorfismo, se vale (2) f è il morfismo nullo. □

1.5 Condizioni sulle catene

Dato un R-modulo M, una *catena di sottomoduli di M* è una successione $(M_i)_{0 \leq i \leq n}$ di sottomoduli di M tali che:

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

Il numero n è detto *lunghezza* della catena.

Definizione 1.27. Sia M un R-modulo. Una *serie di composizione di M* è una catena massimale di sottomoduli di M, ovvero una catena in cui non possono essere inseriti altri sottomoduli.

Ciò equivale a dire che ogni quoziente M_i/M_{i+1} è semplice. Infatti se $N \subseteq M_i/M_{i+1}$ fosse un sottomodulo proprio, allora la sua immagine N' tramite l'inversa della proiezione canonica $\pi : M_i \to M_i/M_{i+1}$ sarebbe un sottomodulo proprio $M_i \supset N' \supset M_{i+1}$ e si otterrebbe quindi una catena più lunga.

Vediamo ora un importante teorema sulle serie di composizione.

Teorema 1.28 (Jordan-Hölder)**.** *1. Sia M un R-modulo, allora tutte le serie di composizione di M hanno la stessa lunghezza (in particolare sono tutte finite o infinite). Inoltre ogni catena può essere estesa a una serie di composizione.*

2. Sia M un R-modulo di lunghezza finita n e siano $(M_i)_{0\leq i\leq n}$ e $(M'_i)_{0\leq i\leq n}$ due serie di composizione di M, allora esiste una corrispondenza biunivoca tra l'insieme dei quozienti $(M_{i-1}/M_i)_{0\leq i\leq n}$ e $\left(M'_{i-1}/M'_i\right)_{0\leq i\leq n}$ tale che i quozienti corrispondenti siano isomorfi.

Dimostrazione. 1. Indichiamo con $l(M)$ la lunghezza minima di una serie di composizione di M ($l(M) = +\infty$ se M non ha serie di composizione). Dimostriamo che se $N \subseteq M$ allora $l(N) \leq l(M)$ e $l(N) = l(M)$ se e solo se $N = M$.

Sia $(M_i)\,,\ M = M_0 \supset M_1 \supset \cdots \supset M_{l(M)} = 0$, una serie di composizione di M di lunghezza minima e consideriamo $M \cap N = N = (M_0 \cap N) \supset (M_1 \cap N) \supset \cdots \supset \left(M_{l(M)} \cap N\right) = 0$. Indichiamo con $N_i = N \cap M_i$ il sottomodulo di N. Poichè $N_{i-1}/N_i \subseteq M_{i-1}/M_i$ e quest'ultimo è un modulo semplice: o $N_{i-1}/N_i = M_{i-1}/M_i$, o $N_{i-1}/N_i = 0$ e quindi $N_{i-1} = N_i$. Allora, eliminando i sottomoduli ripetuti, otteniamo una serie di composizione di N con $l(N) \leq l(M)$. Se $l(N) = l(M) = n$ allora $N_{i-1}/N_i = M_{i-1}/M_i$ per ogni $i = 1, 2, \cdots, n$, quindi $M_{n-1} = N_{n-1}$, $M_{n-2} = N_{n-2}$, fino a $M = N$.

Dimostriamo ora che ogni catena di M ha lunghezza minore o uguale a $l(M)$. Sia $(M_{i-1}/M_i)_{0\leq i\leq k}$ una catena di lunghezza k. Per quanto appena dimostrato $l(M) > l(M_1) > \cdots > l(M_k) = 0$, quindi $l(M) \geq k$. Allora se consideriamo una serie di composizione di lunghezza k, $k \leq l(M)$ e quindi, per definizione di $l(M)$, $k = l(M)$. Così ogni serie di composizione di M ha lunghezza $l(M)$.
Infine consideriamo una qualunque catena di M. Se la sua lunghezza è $l(M)$ allora è una serie di composizione, se è minore non è massimale e quindi possiamo aggiungere altri sottomoduli fino a ottenere una serie di composizione di lunghezza $l(M)$.

2. Per la dimostrazione si veda in [2], capitolo 3, Teorema 3.3.11.

□

Capitolo 2

Moduli semisemplici e Teorema di Wedderburn-Artin

In questo capitolo definiamo i moduli semisemplici e mostriamo i principali risultati che portano alla dimostrazione del teorema di Wedderburn-Artin. In particolare dimostreremo il teorema di Burnside.

Sia R una K-algebra con unità, K un campo.
Tutti i moduli, se non specificato, sono da intendersi come R-moduli.

2.1 Moduli semisemplici

Iniziamo ricordando la definizione di modulo semplice e dando inoltre la definizione di modulo semisemplice.

Definizione 2.1. Un modulo M è *semplice* se non ha sottomoduli propri non banali.
Un anello A è *semplice* se non ha ideali propri.

Definizione 2.2. Un modulo M è detto *semisemplice* se soddisfa una delle tre condizioni equivalenti seguenti:

1. M è somma di una famiglia di sottomoduli semplici;

2. M è somma diretta di una famiglia di sottomoduli semplici;

3. ogni sottomodulo N di M è un addendo in una somma diretta, cioè esiste N' sottomodulo di M tale che $M = N \oplus N'$.

Un anello A è detto *semisemplice* se è semisemplice come modulo su se stesso.

Premettiamo alcuni lemmi per provare che queste condizioni sono equivalenti.

Lemma 2.3. *Sia M un modulo. Se $M = \sum_{i \in I} M_i$ è somma (non necessariamente diretta) di sottomoduli semplici M_i allora esiste $J \subset I$ tale che $M = \bigoplus_{j \in J} M_j$ sia una somma diretta di sottomoduli semplici M_j.*

Dimostrazione. Sia J un sottoinsieme massimale di I tale che la somma $\sum_{j \in J} M_j$ sia diretta. Per provare che questa è uguale a M basta verificare che ogni sottomodulo M_i vi appartiene. $\sum_{j \in J} M_j \cap M_i$ è un sottomodulo di M_i e quindi è o 0 o M_i; se fosse 0 allora potremmo aggiungere M_i alla somma e J non sarebbe massimale. Quindi ogni sottomodulo è contenuto nella somma e $M = \bigoplus_{j \in J} M_j$. □

Lemma 2.4. *Sia M un modulo tale che valga la condizione (3) della definizione 2.2. Allora ogni sottomodulo non nullo di M contiene un sottomodulo semplice.*

Dimostrazione. Sia $v \in M, v \neq 0$; Rv è un sottomodulo di M. Consideriamo il morfismo $R \to Rv \subset M$ il cui nucleo è un ideale sinistro $L \neq R$. Allora esiste un ideale massimale sinistro $I \neq R$ tale che $L \subset I$, così I/L è un sottomodulo massimale di R/L e considerando l'isomorfismo $R/L \to Rv$ si ha che Iv è un sottomodulo massimale di Rv. Per l'ipotesi su M esiste un sottomodulo J tale che $M = Iv \oplus J$. Così $Rv = Iv \oplus (J \cap Rv)$, infatti ogni elemento $x \in Rv \subset M$ si può scrivere in modo unico come $x = av + x'$ con $a \in I, x' \in J$ dove $x' = x - av$ appartiene anche a Rv e quindi $x' \in J \cap Rv$. Poichè Iv è massimale in Rv il sottomodulo $J \cap Rv$ deve essere semplice. □

Dimostrazione delle equivalenze di 2.2. (1) $\Rightarrow$ (2): segue dal lemma 2.3.
(2) $\Rightarrow$ (3): sia N un sottomodulo di M e J un un sottoinsieme massimale di I tale che $N + \bigoplus_{j\in J} M_j$ sia una somma diretta. Indichiamo $N' = \bigoplus_{j\in J} M_j$. Per provare che questa somma è uguale a M basta provare che ogni M_i vi appartiene. Consideriamo $M_i \cap (N \oplus N')$, questo è un sottomodulo di M_i quindi è o 0 o M_i: se fosse 0 allora potremmo aggiungere M_i alla somma e J non sarebbe massimale, così ogni M_i è contenuto nella somma e $M = N \oplus N'$.
(3) $\Rightarrow$ (1): sia N il sottomodulo di M somma di tutti i sottomoduli semplici di M. Se $N \neq M$ allora esiste $N' \neq 0$ tale che $M = N \oplus N'$ e, per il lemma 2.4 esiste un sottomodulo di N' semplice. Questo contraddice la definizione di N, così $N = M$. □

Esempio 2.5. Riprendiamo l'esempio 1.24. $M_n(K)$ è semplice come anello, ma non come modulo su se stesso perchè $\{I_k\}_{1\leq k\leq n}$ è una famiglia di sottomoduli semplici. Possiamo però scrivere $M_n(K) = \bigoplus_{1\leq k\leq n} I_k$, così $M_n(K)$ è semisemplice.
Se prendiamo V, K-spazio vettoriale di dimensione n, allora $\mathrm{End}_K(V) \cong M_n(K)$ e quindi valgono le stesse considerazioni.

Proposizione 2.6. *Sia M un modulo semisemplice. Allora ogni suo sottomodulo N è semisemplice.*

Dimostrazione. Sia N un sottomodulo e N_0 la somma di tutti i sottomoduli semplici di N. Scriviamo $M = N_0 \oplus N_0'$. Ogni elemento $x \in N$ si scrive in modo unico come $x = x_0 + x_0'$ con $x_0 \in N_0, x_0' \in N_0'$, e quindi $x_0' = x - x_0 \in N$. Così $N = N_0 \oplus (N \cap N_0')$, ma allora deve essere $N = N_0$ semisemplice. □

2.2 Teorema di Burnside

In questa sezione dimostriamo il teorema di Burnside, fondamentale per comprendere la struttura delle algebre e per la dimostrazione del teorema di Wedderburn-Artin.

Definizione 2.7. Un'algebra A si dice *semplice* se è semplice come anello, quindi se gli unici ideali bilateri sono 0 e A.

Riprendiamo il concetto di rappresentazione di un'algebra.
In particolare abbiamo visto nel capitolo 1, con la proposizione 1.3 e la definizione 1.7, che se ρ è una rappresentazione di una K-algebra A su un K-spazio vettoriale V, allora possiamo considerare in modo naturale V come A-modulo.
Se $U \subset V$ è un sottospazio vettoriale tale che $\rho(a)U \subset U$ per ogni $a \in A$ allora U è detto *invariante* per la rappresentazione ρ e si definisce la rappresentazione (ρ_U, U) restringendo $\rho(A)$ a U. I sottospazi invarianti corrispondono ai sottomoduli.
Se gli unici sottospazi invarianti sono V e 0 la rappresentazione è detta *irriducibile*. Le rappresentazioni irriducibili corrispondono ai moduli semplici.
Le rappresentazioni corrispondenti ai moduli semisemplici si dicono *completamente irriducibili*.

Teorema 2.8 (di Burnside)**.** *Sia A una K-algebra, V un K-spazio vettoriale e ρ una rappresentazione irriducibile di A su V. Se V ha dimensione finita e $\rho(A) \neq 0$, allora $\rho(A) = End_K(V)$.*

Dimostrazione. Sia $B = \rho(A)$. B è un'algebra non nulla di dimensione finita contenuta in $\mathrm{End}(V)$, V è un B-modulo semplice perchè ρ è una rappresentazione irriducibile.
Premettiamo alcune osservazioni. Se $0 \neq v \in V$ allora $Bv \neq 0$, così

$$\{v \in V |\ Bv = 0\} = \{0\}. \tag{2.1}$$

Per ogni sottoinsieme $S \subset V$ definiamo

$$\mathrm{Ann}(S) = \{b \in B |\ bv = 0 \text{ per ogni } v \in S\}$$

un ideale sinistro di B chiamato *annichilatore*. Se C è un ideale sinistro di B e $v \in V$, allora Cv è un sottospazio invariante di V e quindi o $Cv = 0$ o $Cv = V$, per l'irriducibilità della rappresentazione.

Scegliamo ora un ideale sinistro $C_1 \subset B$ di dimensione minima e un vettore $v_1 \in V$ tale che $C_1 v_1 \neq 0$ e quindi

$$C_1 v_1 = V. \tag{2.2}$$

Definiamo

$$B_1 = \mathrm{Ann}\{v_1\}$$

e consideriamo l'applicazione

$$\begin{aligned} T_1 : C_1 &\rightarrow V \\ c &\mapsto cv_1. \end{aligned}$$

Allora $\mathrm{Ker}(T_1) = B_1 \cap C_1$ è un ideale sinistro proprio di C_1 e quindi è uguale a 0. Così, poichè C_1 è un B-modulo sinistro e $T_1 \in \mathrm{Hom}_B(C_1, V)$, $C_1 \cong V$ come B-modulo. Inoltre se $x \in B$ per l'equazione 2.2, esiste $y \in C_1$ tale che $xv_1 = yv_1$, quindi $x - y \in B_1$ e

$$B = B_1 \oplus C_1.$$

Se $B_1 \neq 0$ ripetiamo il ragionamento scegliendo $C_2 \subset B_1$ di dimensione minima e $v_2 \in V$ tale che $C_2 v_2 = V$. Definiamo $B_2 = \mathrm{Ann}\{v_1, v_2\} \subset B_1$ e consideriamo

$$\begin{aligned} T_2 : C_2 &\rightarrow V \\ c &\mapsto cv_2 \end{aligned}$$

con $\mathrm{Ker}(T_2) = B_2 \cap C_2 = 0$ e $C_2 \cong V$ come B-moduli tramite T_2. Così $B_1 = B_2 \oplus C_2$ e $B = B_2 \oplus C_1 \oplus C_2$.
Poichè la dimensione di B è finita questo processo di ricerca di ideali C_i termina dopo un numero finito di passi trovando gli ideali sinistri $C_1, \cdots, C_m$ e gli isomorfismi di B-moduli $T_i : C_i \xrightarrow{\cong} V$, definiti come sopra, tali che

$$B = C_1 \oplus \cdots \oplus C_m. \tag{2.3}$$

Se $\dim(V) = n$ allora $\dim B = mn$ e poichè $\dim B \leq \dim \mathrm{End}(V) = n^2$ allora $m \leq n$.

Per dimostrare il teorema è ora sufficiente mostrare che $m \geq n$. Consideriamo $x \in B$ e l'azione della moltiplicazione destra su C_j. Per l'equazione 2.3 un elemento di B è del tipo $v = (v_1, \cdots, v_m)$ ed esistono delle applicazioni $T_{ij}(x) : C_j \to C_i$ tali che

$$v \cdot x = \begin{pmatrix} T_{11}(x) & \cdots & T_{1m}(x) \\ \vdots & \ddots & \vdots \\ T_{m1}(x) & \cdots & T_{mm}(x) \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix}$$

Si verifica che le $T_{ij}(x)$ sono applicazioni lineari. Inoltre se $y \in C_j$ allora

$$y \cdot x = \begin{pmatrix} T_{11}(x) & \cdots & T_{1j}(x) & \cdots & T_{1m}(x) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ T_{j1}(x) & \cdots & T_{jj}(x) & \cdots & T_{jm}(x) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ T_{m1}(x) & \cdots & T_{mj}(x) & \cdots & T_{mm}(x) \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ y \\ \vdots \\ 0 \end{pmatrix} = \sum_{i=1}^{m} T_{ij}(x)y. \quad (2.4)$$

Così $T_{ij}(x) \in \mathrm{Hom}_B(C_j, C_i)$ come anche l'isomorfismo $T_i^{-1}T_j$, quindi per il lemma di Schur esistono degli scalari in $\mu_{ij} \in K$ tali che

$$T_{ij}(x) = \mu_{ij}(x)T_i^{-1}T_j \quad \text{per ogni } i, j = 1, \cdots, m.$$

Definiamo $\mu(x)$ la matrice $(\mu_{ij}(x))$, allora $\mu(x) : B \to M_m(K)$ è un'applicazione lineare. Se $\mu(x) = 0$ allora $Bx = 0$, $Bxv = 0$ per ogni $v \in V$ e quindi $xv = 0$ per ogni $v \in V$. Allora, per l'osservazione 2.1 della dimostrazione, questo implica $x = 0$. Così l'applicazione μ è iniettiva e $mn = \dim B \leq \dim M_m(K) = m^2$, quindi $n \leq m$. Possiamo ora concludere che $m = n$ e che $B \cong M_n(K)$. □

Osservazione 2.9. Il teorema di Burnside permette di dimostrare che $\mathrm{End}(V)$, con V K-spazio vettoriale, è un'algebra semplice in un altro modo rispetto a quanto dimostrato nell'esempio 2.5. Se u, v sono due elementi non nulli di V, allora esiste $T \in \mathrm{End}(V)$ tale che $Tv = u$ (per esempio prendiamo $f \in V^*, f : V \to K$ tale che $f(v) = 1$ e definiamo $Tx := f(x)u$ per ogni $x \in V$). Allora $\mathrm{End}(V)v = V$. Consideriamo $B \subseteq \mathrm{End}(V), B \neq 0$ ideale

destro e sinistro, $v \in V, v \neq 0$ e $Bv \subseteq V$. Allora poichè B è ideale destro $Bv = B\text{End}(V)v = BV \neq 0$ e poichè è anche ideale sinistro $B = \text{End}(V)B$ e quindi BV è invariante per End$V$ (ovvero $\text{End}(V)BV = BV$). Così vale anche che $V \subseteq Bv$, allora $Bv = BV = V$ per ogni $v \in V, v \neq 0$ e quindi V è un B-modulo semplice. Per il teorema di Burnside $B = \text{End}(V)$ e quindi $\text{End}(V)$ è un algebra semplice.

2.3 Teorema di Wedderburn-Artin

Sfruttando i risultati precedenti possiamo ora dimostrare il Teorema di Wedderburn-Artin relativo alla rappresentazione di algebre semplici.

Teorema 2.10 (di Wedderburn-Artin)**.** *Sia A una K-algebra con unità semplice di dimensione finita. Allora esiste un K-spazio vettoriale V di dimensione finita tale che $A \cong End(V)$.*

Dimostrazione. Definiamo la rappresentazione sinistra regolare di A:

$$\begin{aligned} \lambda : A &\rightarrow \text{End}(A) \\ x &\mapsto \lambda_x(y) := xy. \end{aligned}$$

Scegliamo $V \subset A$ ideale sinistro di dimensione minima e definiamo:

$$\begin{aligned} \tilde{\lambda} : A &\rightarrow \text{End}(V) \\ x &\mapsto \tilde{\lambda}_x(y) := xy \end{aligned}$$

dove $\tilde{\lambda}_x = \lambda_x|_V$. $\tilde{\lambda}$ è una rappresentazione irriducibile di A su V, allora per il teorema di Burnside $\tilde{\lambda}(A) = \text{End}(V)$ e per il lemma di Schur (sia A sia $\text{End}(V)$ sono algebre semplici) $A \cong \text{End}(V)$ come algebra. □

Definizione 2.11. Una K-algebra A è detta *semisemplice* se è somma diretta di algebre semplici.

Teorema 2.12 (classificazione delle algebre semisemplici)**.** *Sia A una K-algebra. A è semisemplice se e solo se è somma diretta di algebre di matrici.*

Dimostrazione. Se A è somma diretta di algebre di matrici allora per l'osservazione 2.9 e per la definizione 2.11 A è semisemplice.
Viceversa, se A è semisemplice, allora $A \cong \bigoplus_{\lambda \in L} A^\lambda$, dove A^λ sono algebre semplici e L è un insieme finito. Allora per il teorema 2.3 esistono V^λ, K-spazi vettoriali di dimensione finita, tali che $A^\lambda \cong \mathrm{End}(V^\lambda)$ e quindi

$$A \cong \bigoplus_{\lambda \in L} \mathrm{End}(V^\lambda).$$

□

Questo teorema permette di classificare completamente le algebre semisemplici su di un campo K.

Bibliografia

[1] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1969.

[2] R. Goodman, N. R. Wallach, *Representations and Invariants of the Classical Groups*, Cambridge University Press, 1998.

[3] T. W. Hungerford, *Algebra*, Springer, 1974.

[4] S. Lang, *Algebra*, Springer, 2002.

[5] I. R. Shafarevich, *Basic Notions of Algebra*, Springer, 2005.

Ringraziamenti

Un ringraziamento alla Prof. Fioresi che mi ha seguito in questo lavoro dedicandomi il suo tempo e mi ha consigliato anche per le scelte future.
Grazie alla mia famiglia che mi sostiene e aiuta sempre, anche ascoltandomi quando prima di un esame giro per casa raccontando teoremi assurdi e incomprensibili; grazie a Silvia che sopporta una sorella matematica e alla Robi per tutte le giornate a Pesaro e le serate in gelateria!
Grazie alle amiche di Sangio: Miki con cui spesso ci siamo trovate a elaborare strane teorie assolutamente applicabili alla vita quotidiana :) , la mia "alleata" Vale, perchè in due i punti di vista si difendono meglio, e Marzia per l'allegria che mi ha saputo donare.
Grazie ai miei matematici, ai bolognesi e alle pesaresi e dintorni. In particolare ringrazio la Lucy per il sostegno reciproco che ci siamo date durante le lezioni, in vista degli esami e non solo e per tutte le uscite fatte, e la Samy per tutte le chiacchiere, le confessioni, i racconti e le dediche sui quaderni. Grazie per avermi fatto passare tre anni indimenticabili, per tutti i momenti felici e per l'aiuto dato nei momenti difficili.
Un ultimo ringraziamento anche alla danza e alle persone con cui condivido questa passione, perchè libera da ogni pensiero, mi rilassa se sono nervosa, mi carica la sera prima di una giornata impegnativa, perchè insegna che se fai parte di un gruppo anche se sei in disparte e sembrano tutte più brave di te devi dare comunque il meglio, altrimenti il gruppo intero ne risente. Poi entrare in un teatro e pensare "io ho ballato su quel palco" è una sensazione bellissima.