Università degli Studi Roma Tre
Dipartimento di Matematica e Fisica

Algebra commutativa

- MAT/02 AL410 -

Raffaele Di Donna
Matricola: 523997

Indice

Algebra commutativa (Matematica, Roma Tre) Oct 6, 2020

Lezione 7

Raffaele Di Donna

La somma diretta esterna e il prodotto diretto di moduli. Somma diretta interna di sottomoduli. Sistemi di generatori e basi. Moduli finitamente generati e moduli liberi.

1 Moduli

Nel seguito supporremo sempre che A sia un anello commutativo e unitario e che $\mathbb{K}$ sia un campo. In ambo i casi assumeremo che $1 \neq 0$, cioè che A e $\mathbb{K}$ siano non banali. Useremo la notazione del simbolo di Kronecker cioè, dato un insieme J, per ogni $i, j \in J$ definiamo:

$$\delta_{ij} := \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

Per ogni intero $n \geq 1$, denoteremo quindi I_n la matrice identità di ordine n, cioè la matrice quadrata (δ_{ij}) di ordine n.

1.1 Operazioni sui sottomoduli

Ricordiamo, innanzitutto, la seguente definizione.

Definizione 1.1. Siano N e P due sottomoduli di un A-modulo M. Il modulo N *diviso* P è definito come:

$$(N : P) := \{a \in A \colon aP \subseteq N\}$$

In particolare, si dice *annullatore di* M e si denota $\mathrm{Ann}(M)$ il modulo $\{0\}$ diviso M, cioè:

$$\mathrm{Ann}(M) = \{a \in A \colon aM = 0\}$$

Un A-modulo M si dice *fedele* se $\mathrm{Ann}(M) = 0$.

Ricordiamo che, come immediata conseguenza della definizione, il modulo N diviso P e, di conseguenza, l'annullatore di M sono ideali di A.

Lemma 1.2. *Sia M un A-modulo e sia I un ideale di A tale che $I \subseteq \mathrm{Ann}(M)$. Allora M è un A/I-modulo rispetto al prodotto esterno:*

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

Dimostrazione. Basta semplicemente osservare che $IM = \{0\}$ per l'ipotesi che $I \subseteq \mathrm{Ann}(M)$ e ricordare che M/IM è un A/I-modulo rispetto al prodotto esterno:

$$(a + I)(m + IM) = am + IM$$ □

Lemma 1.3. *Sia M un A-modulo. Allora M è un $A/\mathrm{Ann}(M)$-modulo fedele.*

Dimostrazione. Sappiamo, per il lemma 1.2, che M è un $A/\mathrm{Ann}(M)$-modulo, per cui bisogna solo mostrare che è fedele. Sia dunque $a + \mathrm{Ann}(M)$ un elemento dell'annullatore di M pensato come $A/\mathrm{Ann}(M)$-modulo. Per definizione di annullatore si ha $(a + \mathrm{Ann}(M))M = 0$, cioè $aM + \mathrm{Ann}(M)M = 0$, o equivalentemente $aM = 0$. Ma allora $a \in \mathrm{Ann}(M)$ e quindi $a + \mathrm{Ann}(M) = \mathrm{Ann}(M)$. Questo dimostra che l'annullatore di M pensato come $A/\mathrm{Ann}(M)$-modulo è banale e dunque la dimostrazione è conclusa. □

Prima di enunciare il risultato che segue si tenga a mente che, se I è un ideale di A, allora A/I acquista una struttura di A-modulo con il prodotto esterno:

$$a(x+I) = ax + I$$

Osservazione 1.4. Sia I un ideale di A. Allora l'annullatore di A/I pensato come A-modulo è I.

Dimostrazione. Osserviamo innanzitutto che, dati $x \in I$ e $a + I \in A/I$, per definizione di prodotto esterno sul modulo quoziente si ha $x(a+I) = xa + I$. D'altra parte abbiamo che $xa \in I$, perché I è un ideale di A. Ma allora $x(a+I) = I$, cioè x appartiene all'annullatore di A/I pensato come A-modulo. Sia invece $x \in A$ tale che, per ogni $a + I \in A/I$, valga $x(a+I) = I$, cioè $xa + I = I$. Allora, prendendo $a := 1$, troviamo che $x \in I$ in quanto $x + I = I$ e dunque la dimostrazione è conclusa. □

1.2 Somma diretta e prodotto diretto

Definizione 1.5. Sia A un anello e sia $\{M_j\}_{j\in J}$ una famiglia di A-moduli. Si dice *prodotto diretto* (*esterno*) *della famiglia* $\{M_j\}_{j\in J}$ il seguente insieme, che acquisisce una struttura di A-modulo con le usuali operazioni di somma e prodotto componente per componente:

$$\prod_{j\in J} M_j := \{(x_j)_{j\in J} \colon x_j \in M_j \text{ per ogni } j \in J\}$$

Se nella descrizione di questo insieme richiediamo anche che x_j sia non nullo per al più un numero finito di indici $j \in J$, parleremo di *somma diretta* (*esterna*) *della famiglia* $\{M_j\}_{j\in J}$ e useremo la notazione $\bigoplus_{j\in J} M_j$.

Osservazione 1.6. Se l'insieme J degli indici è finito, allora $\prod_{j\in J} M_j = \bigoplus_{j\in J} M_j$.

Adesso vogliamo adottare un altro punto di vista: consideriamo un A-modulo M e una famiglia $\{M_j\}_{j\in J}$ di sottomoduli di M. Allora è facile verificare che la seguente applicazione è un omomorfismo di A-moduli:

$$\begin{aligned} \phi \colon \bigoplus_{j\in J} M_j &\longrightarrow M \\ (x_j)_{j\in J} &\longmapsto \sum_{j\in J} x_j \end{aligned}$$

Si noti, in particolare, che ϕ è ben definita perché $x_j \in M_j \subseteq M$ per ogni $j \in J$ e $x_j \neq 0$ per al più un numero finito di indici $j \in J$. Per costruzione, l'immagine di ϕ è il sottomodulo $\sum_{j\in J} M_j$ di M. Sia l'immagine che il nucleo di ϕ sono, a priori, non banali. È dunque giustificata la seguente definizione.

Definizione 1.7. Sia M un A-modulo e sia $\{M_j\}_{j\in J}$ una famiglia di sottomoduli di M. Se l'applicazione ϕ definita sopra è un isomorfismo di A-moduli, diremo che M è *somma diretta interna della famiglia* $\{M_j\}_{j\in J}$.

Le osservazioni che seguono mettono in evidenza delle analogie con la nozione di somma diretta per gli spazi vettoriali.

Osservazione 1.8. Dalla definizione di isomorfismo discende che M è somma diretta interna della famiglia $\{M_j\}_{j\in J}$ se e solo se, per ogni $m \in M$, esiste un'unica scelta di elementi $x_j \in M_j$, al variare dell'indice $j \in J$, tale che $m = \sum_{j\in J} x_j$.

Osservazione 1.9. Vale che M è somma diretta interna della famiglia $\{M_j\}_{j\in J}$ se e solo se $M = \sum_{j\in J} M_j$ e, per ogni $i \in J$, si ha:

$$M_i \cap \sum_{j\in J, j\neq i} M_j = \{0\} \tag{1}$$

Dimostrazione. Innanzitutto, è evidente che $M = \sum_{j\in J} M_j$ se e solo se, per ogni $m \in M$, esiste almeno una scelta di elementi $x_j \in M_j$, al variare dell'indice $j \in J$, tale che $m = \sum_{j\in J} x_j$. Per l'osservazione 1.8 basterà dimostrare che una tale scelta è unica se e solo se è verificata la condizione (1) per ogni $i \in J$. Supponiamo che

una tale scelta sia unica e fissiamo $m \in M_i \cap \sum_{j\in J, j\neq i} M_j$. In particolare possiamo scegliere, per ogni $j \in J$ con $j \neq i$, un elemento $y_j \in M_j$ in maniera tale che valga $m = \sum_{j\in J, j\neq i} y_j$. Per ogni $j \in J$, definiamo adesso:

$$x_j := \begin{cases} y_j & \text{se } j \neq i \\ m & \text{se } j = i \end{cases}$$

Per costruzione, abbiamo che $0 = \sum_{j\in J} x_j$ ma, ovviamente, vale anche $0 = \sum_{j\in J} 0$. Per unicità, abbiamo in particolare $m = 0$.

Viceversa, supponiamo che valga (1) per ogni $i \in J$ e fissiamo, per ogni $j \in J$, degli elementi $x_j, y_j \in M_j$. Per qualsiasi $i \in J$ valgono allora le seguenti implicazioni:

$$\begin{aligned} &\sum_{j\in J} x_j = \sum_{j\in J} y_j \\ \implies\ & x_i + \sum_{j\in J, j\neq i} x_j = y_i + \sum_{j\in J, j\neq i} y_j \\ \implies\ & x_i - y_i = \sum_{j\in J, j\neq i} (y_j - x_j) \end{aligned}$$

Ne segue che $x_i - y_i$ è sia un elemento di M_i che di $\sum_{j\in J, j\neq i} M_j$ e allora dalle ipotesi segue che è nullo, cioè che $x_i = y_i$. □

Esempio 1.10. Come conseguenza del teorema cinese del resto[1], si ha che $\mathbb{Z}_6$ è somma diretta di $\mathbb{Z}_2$ e $\mathbb{Z}_3$. Similmente, si può esprimere $\mathbb{Z}_{12}$ come somma diretta di $\mathbb{Z}_4$ e $\mathbb{Z}_3$, ma non di $\mathbb{Z}_2$ e $\mathbb{Z}_6$. In effetti, possiamo osservare che $\mathbb{Z}_2$ è isomorfo al sottogruppo di $\mathbb{Z}_{12}$ generato dalla classe di 6, che denotiamo $(\bar{6})$, mentre $\mathbb{Z}_6$ è isomorfo a $(\bar{2})$ e si ha che $(\bar{2}) \cap (\bar{6}) = (\bar{6}) \neq (\bar{0})$. Dall'osservazione 1.9 discende quindi che $\mathbb{Z}_{12}$ non è somma diretta interna di $(\bar{2})$ e $(\bar{6})$.

1.3 Moduli finitamente generati

Definizione 1.11. Sia M un A-modulo e sia $S \subseteq M$ un insieme non vuoto. Si definisce come il *sottomodulo di M generato da S* l'insieme:

$$\langle S \rangle := \left\{ \sum_{j=1}^{k} a_j x_j : a_j \in A,\, x_j \in S,\, k \geq 1 \text{ intero} \right\}$$

Se $\langle S \rangle = M$, diremo anche che S è un *sistema di generatori per M*. Se inoltre $S = \{m_1, m_2, \ldots, m_n\}$ allora, per semplicità, scriveremo $\langle S \rangle = \langle m_1, m_2, \ldots, m_n \rangle$.

Osservazione 1.12. Si dimostra assai facilmente che $\langle S \rangle$ è il più piccolo sottomodulo di M che contiene S.

Definizione 1.13. Un A-modulo si dice *finitamente generato* se ammette un sistema di generatori finito.

Esempio 1.14. L'anello dei polinomi $A[X_1, X_2, \ldots, X_n]$ è un A-modulo *non* finitamente generato. Infatti, se S fosse un sistema di generatori finito per $A[X_1, X_2, \ldots, X_n]$, potremmo considerare un intero positivo M che sia il grado massimo dei polinomi in S e avremmo un assurdo in quanto $X_1^{M+1} \notin \langle S \rangle$.

A proposito dell'esempio precedente vale la pena anticipare che, quando parleremo di $\mathbb{K}$-algebre, l'anello dei polinomi $\mathbb{K}[X_1, X_2, \ldots, X_n]$ sarà finitamente generato come $\mathbb{K}$-algebra. Cambiando dunque la struttura algebrica soggiacente, la proprietà di essere finitamente generato non viene preservata.

[1] Si veda anche la proposizione 4.11 nelle dispense del corso AL210.

Definizione 1.15. Sia M un A-modulo. Un sottoinsieme non vuoto $\{m_j\}_{j\in J}$ di M è detto una *base di* M se la seguente applicazione è un isomorfismo di A-moduli:

$$\begin{aligned}\phi\colon \bigoplus_{j\in J} A &\longrightarrow M\\ (x_j)_{j\in J} &\longmapsto \sum_{j\in J} x_j m_j\end{aligned}$$

Un A-modulo M si dice *libero* se ammette una base.

La definizione precedente è ben posta perché, per definizione di somma diretta esterna, si ha $x_j \neq 0$ per al più un numero finito di indici $j \in J$ e dunque ϕ è un'applicazione ben definita.

Osservazione 1.16. Si vede facilmente che ϕ è sempre un omomorfismo di A-moduli. Inoltre, dalle definizioni discende facilmente che $\{m_j\}_{j\in J}$ è un sistema di generatori per M se e solo se l'omomorfismo ϕ è suriettivo.

Esempio 1.17. È facile verificare che $A^n := \bigoplus_{j=1}^n A$ è un A-modulo libero e finitamente generato. Infatti, una sua base è $\{(1,0,0,\dots,0,0),(0,1,0,\dots,0,0),\dots,(0,0,0,\dots,0,1)\}$.

Esempio 1.18. L'anello dei polinomi $A[X]$ è un A-modulo libero, ma *non* è finitamente generato. Infatti, una sua base è $\{X^n\colon n \geq 0 \text{ intero}\}$ e abbiamo già visto, nell'esempio 1.14, che $A[X]$ non può ammettere una base finita.

Tuttavia, emerge qui una differenza significativa tra moduli e spazi vettoriali: diversamente dagli spazi vettoriali, non tutti i moduli non banali hanno una base. Ricordiamo infatti il seguente risultato di algebra lineare.

Osservazione 1.19. Sia V uno spazio vettoriale non nullo su $\mathbb{K}$. Allora V ammette una base.

Dimostrazione. Osserviamo, innanzitutto, che una base di V è un sottoinsieme linearmente indipendente[2] massimale di V. Se infatti B è una base di V e S è un sottoinsieme linearmente indipendente di V contenente B, allora $S = B$ perché, se fosse $S \neq B$, potrei esprimere un vettore in $S\setminus B$ come combinazione lineare degli elementi di B. Viceversa, qualsiasi sottoinsieme linearmente indipendente massimale $M \subseteq V$ è una base di V perché, se così non fosse, allora esisterebbe un vettore $v \in V$ che non si può esprimere come combinazione lineare degli elementi di M. Ma allora $M \cup \{v\}$ sarebbe un sottoinsieme linearmente indipendente di V che contiene strettamente M e dunque avremmo un assurdo.

Dobbiamo allora mostrare l'esistenza di un sottoinsieme linearmente indipendente massimale di V. Per farlo, ci serviremo del lemma di Zorn. Sia dunque $\mathcal{X}$ la famiglia di tutti gli insiemi linearmente indipendenti di V ordinata rispetto all'inclusione e sia $\mathcal{C}$ una catena di $\mathcal{X}$, cioè una sottofamiglia totalmente ordinata di $\mathcal{X}$. Asserisco allora che $F := \bigcup_{S\in\mathcal{C}} S$ è un maggiorante per $\mathcal{C}$. Per costruzione, vale che $S \subseteq F$ per ogni $S \in \mathcal{C}$. Dobbiamo soltanto dimostrare che F è un sottoinsieme linearmente indipendente di V. Consideriamo allora dei vettori $v_1, v_2, \dots, v_n \in F$. Per definizione di F e di catena, possiamo individuare un sottoinsieme $S \in \mathcal{C}$ che contiene $v_1, v_2, \dots, v_n$. Poiché S è linearmente indipendente, ogni combinazione lineare a coefficienti in $\mathbb{K}$ non tutti nulli di $v_1, v_2, \dots, v_n$ è non nulla e allora F è linearmente indipendente. Avendo mostrato che F è un maggiorante per $\mathcal{C}$, il lemma di Zorn permette di concludere la dimostrazione. □

D'altra parte, per i moduli abbiamo questo risultato.

Osservazione 1.20. Sia $I \subseteq A$ un ideale non nullo. Allora A/I è un A-modulo non libero.

Dimostrazione. Sarà sufficiente osservare che un qualunque omomorfismo di A-moduli $\phi\colon \bigoplus_{j\in J} A \to A/I$ non è iniettivo e quindi non è un isomorfismo. Per ipotesi, possiamo scegliere un elemento $x \in I$ non nullo. Fissiamo $i \in J$ e, tenendo a mente la notazione del simbolo di Kronecker, consideriamo l'elemento $(\delta_{ij})_{j\in J}$. Servendoci del fatto che ϕ è un omomorfismo e dell'osservazione 1.4 arriviamo facilmente alla conclusione:

$$\phi(x(\delta_{ij})_{j\in J}) = x\phi((\delta_{ij})_{j\in J}) = I = \phi((0)_{j\in J})$$ □

[2] Un sottoinsieme $S \subseteq V$ è detto *linearmente indipendente* se, per ogni $v_1, v_2, \dots, v_n \in S$ e per ogni $k_1, k_2, \dots, k_n \in \mathbb{K}$, la condizione $k_1v_1 + k_2v_2 + \cdots + k_nv_n = 0$ implica $k_j = 0$ per ogni $j = 1, 2, \dots, n$. D'altra parte, una *base di* V è un sistema di generatori per V linearmente indipendente.

È fondamentale specificare che stiamo considerando A/I come un A-modulo e non come un A/I-modulo. Infatti, come caso particolare dell'esempio 1.17, ma anche come banale conseguenza della definizione, A/I è un A/I-modulo libero e una sua base come A/I-modulo è $\{1+I\}$.

Esempio 1.21. Dall'osservazione precedente segue, in particolare, che $\mathbb{Z}_n$ è uno $\mathbb{Z}$-modulo non libero per ogni intero $n \geq 1$.

Osservazione 1.22. Sia $I \subseteq A$ un ideale. Allora I è un A-modulo libero se e solo se I si può esprimere come l'ideale principale generato da un non divisore dello zero di A.

Dimostrazione. Supponiamo, in un primo momento, che $I = (a)$ con a non divisore dello zero di A. Allora la seguente applicazione è un isomorfismo di A-moduli:

$$\begin{aligned} \phi\colon A &\longrightarrow I \\ x &\longmapsto xa \end{aligned} \tag{2}$$

Infatti è ben definita per definizione di ideale, iniettiva perché a non è un divisore dello zero di A e suriettiva perché $I = (a)$. Si verifica assai facilmente che ϕ è un omomorfismo di A-moduli. E allora I è un A-modulo libero perché, per definizione, una sua base è $\{a\}$.

Viceversa, assumiamo che I sia un A-modulo libero e consideriamo una sua base $\{m_j\}_{j\in J}$. Supponiamo per assurdo che in J vi siano almeno due indici i e k distinti e definiamo, per ogni $j \in J$:

$$x_j := \begin{cases} 0 & \text{se } j \neq i, j \neq k \\ m_k & \text{se } j = i \\ -m_i & \text{se } j = k \end{cases}$$

Allora abbiamo un assurdo perché l'applicazione ϕ della definizione 1.15 non è iniettiva, contro l'ipotesi che $\{m_j\}_{j\in J}$ sia una base di I:

$$\phi((x_j)_{j\in J}) = m_k m_i - m_i m_k = 0 = \phi((0)_{j\in J})$$

Ne deduciamo che ogni base di I è costituita da un unico elemento. Data ora una base $\{a\}$ di I, l'isomorfismo ϕ della definizione 1.15 assume la forma (2). Ma allora concludiamo che $I = (a)$ perché ϕ è suriettiva, mentre a non è un divisore dello zero di A perché ϕ è iniettiva. □

Algebra commutativa (Matematica, Roma Tre) Oct 8, 2020

Lezione 8

Raffaele Di Donna

Tutte le basi di un modulo libero hanno la stessa cardinalità. Esercizi.

Ricordiamo innanzitutto la seguente definizione.

Definizione 1.15. Sia M un A-modulo. Un sottoinsieme non vuoto $\{m_j\}_{j\in J}$ di M è detto una *base di* M se la seguente applicazione è un isomorfismo di A-moduli:

$$\begin{aligned}\phi\colon \bigoplus_{j\in J} A &\longrightarrow M\\ (x_j)_{j\in J} &\longmapsto \sum_{j\in J} x_j m_j\end{aligned}$$

Un A-modulo M si dice *libero* se ammette una base.

Avevamo osservato che, se ϕ è solo suriettiva, allora l'insieme $\{m_j\}_{j\in J}$ è un sistema di generatori per M. Adesso vogliamo capire quali delle proprietà vere per gli spazi vettoriali continuano a essere valide nel caso dei moduli liberi. Vediamo innanzitutto il seguente risultato.

Proposizione 1.23. *Sia M un A-modulo libero. Allora le basi di M hanno tutte la stessa cardinalità.*

Dimostrazione. Sia I un ideale massimale di A. Un tale ideale sicuramente esiste per il teorema di esistenza degli ideali massimali. Sappiamo che A/I è un campo e dunque M/IM non è solo un A/I-modulo, ma anche un A/I-spazio vettoriale. Sia adesso $\pi\colon M \to M/IM$ la mappa quoziente. Basterà dimostrare che π manda una qualsiasi base di M come A-modulo in una base di M/IM come A/I-spazio vettoriale per poi applicare il risultato noto dell'algebra lineare, cioè sfruttare il fatto che le basi di uno spazio vettoriale hanno tutte la stessa cardinalità.

Sia allora $\{m_j\}_{j\in J}$ una base di M. Osserviamo che $\{m_j + IM\}_{j\in J}$ è banalmente un sistema di generatori per M/IM e dunque, per l'osservazione 1.16, l'omomorfismo di A-moduli seguente è suriettivo:

$$\begin{aligned}\phi\colon \bigoplus_{j\in J} A/I &\longrightarrow M/IM\\ (a_j + I)_{j\in J} &\longmapsto \sum_{j\in J} a_j m_j + IM\end{aligned}$$

Se dimostriamo che è iniettivo, allora ϕ sarà anche un isomorfismo e di conseguenza $\{m_j + IM\}_{j\in J}$ sarà una base di M/IM, che è quanto vogliamo mostrare. Supponiamo che esistano degli elementi $a_1, a_2, \dots, a_n \in A$ e degli indici $j_1, j_2, \dots, j_n \in J$ tali che:

$$\sum_{k=1}^{n} a_k m_{j_k} + IM = IM$$

Per concludere, mostreremo che le classi laterali $a_1 + I, a_2 + I, \dots, a_n + I$ sono tutte banali, cioè che $a_k \in I$ per ogni $k = 1, 2, \dots, n$. Osserviamo innanzitutto che:

$$\sum_{k=1}^{n} a_k m_{j_k} \in IM$$

Per definizione di base e di ideale prodotto esiste allora un sottoinsieme $\{b_j\}_{j\in J}$ di elementi di I, con $b_j \neq 0$ per al più un numero finito di indici $j \in J$, tale che:

$$\sum_{k=1}^{n} a_k m_{j_k} = \sum_{j\in J} b_j m_j$$

Equivalentemente, abbiamo che:

$$\sum_{k=1}^{n} (a_k - b_{j_k}) m_{j_k} - \sum_{j\in J\setminus\{j_1,j_2,\dots,j_n\}} b_j m_j = 0$$

Dal fatto che $\{m_j\}_{j\in J}$ è una base di M segue allora che $a_k = b_{j_k}$ per ogni $k = 1, 2, \dots, n$. In particolare, vale che $a_k \in I$ per ogni $k = 1, 2, \dots, n$ e questo, per quanto si era già osservato, conclude la dimostrazione. □

È dunque ben posta la seguente definizione.

Definizione 1.24. Sia M un A-modulo libero. La cardinalità di una base di M viene detta il *rango di* M.

Come abbiamo già osservato nella dimostrazione della proposizione 1.23, ogni sistema di generatori per un A-modulo libero M viene mandato in un sistema di generatori per M/IM come A/I-spazio vettoriale. Il risultato che segue è dunque una conseguenza immediata del fatto analogo per l'algebra lineare.

Proposizione 1.25. *Sia M un A-modulo libero. Allora i sistemi di generatori di M hanno tutti cardinalità maggiore o uguale al rango di M.*

Facciamo ora una semplice considerazione.

Osservazione 1.26. Sia M un A-modulo. Allora M è un A-modulo libero se e solo se è isomorfo a una somma diretta di copie di A.

Dimostrazione. L'implicazione diretta segue banalmente dalla definizione di A-modulo libero. Viceversa, se esiste un isomorfismo di A-moduli $\phi\colon \bigoplus_{j\in J} A_j \to M$ allora, per qualunque indice $i \in J$, possiamo definire:

$$m_i := \phi((\delta_{ij})_{j\in J})$$

Ma dalla definizione di omomorfismo di A-moduli segue che, per ogni elemento $(a_j)_{j\in J}$ della somma diretta:

$$\phi((a_j)_{j\in J}) = \phi\Big(\sum_{i\in J} a_i(\delta_{ij})_{j\in J}\Big) = \sum_{i\in J} a_i \phi((\delta_{ij})_{j\in J}) = \sum_{i\in J} a_i m_i$$

Con questo è dimostrato che $\{m_i\}_{i\in J}$ è una base di M e concludiamo allora che M è un A-modulo libero. □

Diamo adesso la seguente caratterizzazione degli A-moduli finitamente generati.

Proposizione 1.27. *Un A-modulo M è finitamente generato se e solo se è isomorfo a un quoziente di A^n per qualche intero $n \geq 1$.*

Dimostrazione. Se M è finitamente generato, cioè se ammette un sistema di generatori $\{m_1, m_2, \dots, m_n\}$, allora l'omomorfismo $\phi\colon A^n \to M$ della definizione 1.15 è suriettivo e dunque $M \simeq A^n/\operatorname{Ker}\phi$ per il primo teorema di isomorfismo. Viceversa, se esistono un intero $n \geq 1$, un sottomodulo N di A^n e un isomorfismo di A-moduli $\psi\colon A^n/N \to M$, allora l'applicazione $\phi\colon A^n \to M$ ottenuta componendo la mappa di passaggio al quoziente $\pi\colon A^n \to A^n/N$ con $\psi\colon A^n/N \to M$ è un omomorfismo di A-moduli suriettivo. Ripetendo allora l'argomento già visto nella dimostrazione precedente, si costruisce un sistema di generatori finito per M. □

Esercizio 1.28. Dimostrare che $\mathbb{Q}$ non è uno $\mathbb{Z}$-modulo finitamente generato né libero.

Svolgimento. Ragioniamo per assurdo con entrambe le asserzioni.

- Se $\mathbb{Q}$ fosse uno $\mathbb{Z}$-modulo finitamente generato, allora esisterebbero $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in \mathbb{Z}$ con $b_1, b_2, \ldots, b_n \neq 0$ tali che $\mathbb{Q} = \langle a_1/b_1, a_2/b_2, \ldots, a_n/b_n \rangle$. Ma se consideriamo un numero primo p che non divide $b_1, b_2, \ldots, b_n$, allora $1/p \notin \langle a_1/b_1, a_2/b_2, \ldots, a_n/b_n \rangle$ pur essendo $1/p \in \mathbb{Q}$ e questo è assurdo.

- Se $\mathbb{Q}$ fosse uno $\mathbb{Z}$-modulo libero, potremmo considerare una base B di $\mathbb{Q}$ come $\mathbb{Z}$-modulo. Poiché $\mathbb{Q}$ non è uno $\mathbb{Z}$-modulo finitamente generato, esisterebbero sicuramente almeno due elementi distinti $a_1/b_1, a_2/b_2 \in B$. Per avere un assurdo, basta osservare che gli interi $x_1 := a_2 b_1$ e $x_2 := -a_1 b_2$ sono non entrambi nulli e che:
$$x_1 \frac{a_1}{b_1} + x_2 \frac{a_2}{b_2} = 0$$
Perciò la mappa ϕ della definizione 1.15 non è iniettiva, cioè B non è una base di $\mathbb{Q}$ come $\mathbb{Z}$-modulo.

Esercizio 1.29. Sia A un dominio a ideali principali e siano I e J due ideali di A.

(i) Dimostrare che $\sqrt{I+J} = \sqrt{I} + \sqrt{J}$.

(ii) Dimostrare che tale uguaglianza è in generale falsa se A non è un dominio a ideali principali.

Svolgimento.

(i) Poiché per ipotesi A è un dominio a ideali principali, esistono due elementi $a, b \in A$ tali che $I = (a)$ e $J = (b)$. Un dominio a ideali principali è in particolare un dominio a fattorizzazione unica, perciò possiamo considerare, per opportuni $u, v \in A$ invertibili, $p_1, p_2, \ldots, p_k \in A$ irriducibili a due a due non associati, $d_1, d_2, \ldots, d_k, e_1, e_2, \ldots, e_k \geq 0$ interi, delle fattorizzazioni:
$$a = u p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$$
$$b = v p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$
Ricordiamo che, in un dominio a fattorizzazione unica, il massimo comune divisore di due elementi esiste sempre e che, se definiamo $f_i := \min\{d_i, e_i\}$ per ogni $i = 1, 2, \ldots, k$, allora[3]:
$$\mathrm{MCD}(a, b) = p_1^{f_1} p_2^{f_2} \ldots p_k^{f_k}$$
Definiamo ora $d_i' := \min\{d_i, 1\}$, $e_i' := \min\{e_i, 1\}$, $f_i' := \min\{f_i, 1\}$ per ogni $i = 1, 2, \ldots, k$ e notiamo che gli interi così definiti possono essere uguali solo a 0 o a 1. Per una proprietà degli ideali radicali, sappiamo che:
$$\sqrt{I} = (p_1^{d_1'} p_2^{d_2'} \cdots p_k^{d_k'})$$
$$\sqrt{J} = (q_1^{e_1'} q_2^{e_2'} \cdots q_k^{e_k'})$$
Ricordando che $(a) + (b) = (\mathrm{MCD}(a, b))$, abbiamo anche:
$$\sqrt{I+J} = (p_1^{f_1'} p_2^{f_2'} \cdots p_k^{f_k'})$$
Adesso però osserviamo che, per ogni $i = 1, 2, \ldots, k$, si ha:
$$\min\{d_i', e_i'\} = \min\{\min\{d_i, e_i\}, 1\} = \min\{f_i, 1\} = f_i'$$
Ne deduciamo che il massimo comune divisore tra i generatori di $\sqrt{I}$ e $\sqrt{J}$ coincide con il generatore dell'ideale $\sqrt{I+J}$ e questo ci permette di concludere che:
$$\sqrt{I} + \sqrt{J} = \sqrt{I+J}$$

[3] Per una giustificazione di questo fatto si rimanda alla dimostrazione del punto (iv) della proposizione 9.3 delle dispense del corso AL210.

(ii) Consideriamo $A := \mathbb{K}[X, Y]$, che non è un dominio a ideali principali[4]. Sappiamo che, in generale:

$$\sqrt{\sqrt{I} + \sqrt{J}} = \sqrt{I + J}$$

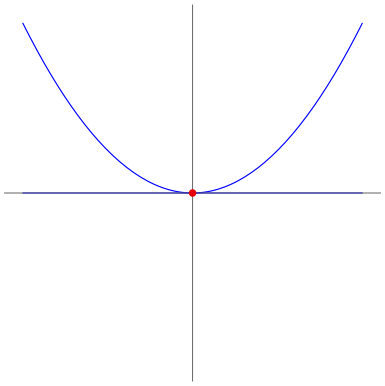
Per questo motivo, basterà esibire due ideali I e J di A tali che $\sqrt{I} + \sqrt{J}$ non sia un ideale radicale. In particolare, sarà sufficiente trovare due ideali radicali I e J di A tali che $I + J$ non sia un ideale radicale. Prendiamo allora $I := (Y)$, $J := (Y - X^2)$. Poiché Y e $Y - X^2$ sono polinomi irriducibili e A è un dominio a fattorizzazione unica, gli ideali da essi generati sono primi, quindi sono radicali. D'altra parte:

$$\sqrt{I + J} = \sqrt{(Y, Y - X^2)} = \sqrt{(Y, X^2)} = \sqrt{(Y) + (X^2)} = \sqrt{(Y) + (X)} = \sqrt{(X, Y)} = (X, Y)$$

Nell'ultima uguaglianza abbiamo usato il fatto che (X, Y) è un ideale massimale, dunque radicale, di A, in quanto ideale del punto $(0, 0)$. Concludiamo allora che $I + J$ non è un ideale radicale.

Geometricamente, l'idea del controesempio che abbiamo esibito nel punto (ii) dell'esercizio 1.29 è di scegliere I e J come ideali di due insiemi algebrici del piano affine $\mathbb{A}^2(\mathbb{K})$ e cioè, rispettivamente:

- La parabola di equazione $Y = X^2$.
- L'asse $Y = 0$.



L'ideale $I + J$ corrisponde perciò all'origine, ma questa viene "contata due volte" dato che è un punto di tangenza. Questa anomalia suggerisce che $I + J$ non è un ideale radicale. Si noti invece che l'ideale (X, Y) è un ideale radicale e corrisponde all'origine "contata una sola volta".

Esercizio 1.30. Dimostrare che nell'anello $\mathbb{K}[X, Y, Z]$ si ha:

$$\sqrt{(XY, YZ + XZ)} = (XY, YZ, XZ)$$

Svolgimento. Definiamo per semplicità $I := (XY, YZ + XZ)$, $J := (XY, YZ, XZ)$. Dobbiamo dimostrare che $\sqrt{I} = J$. Innanzitutto, osserviamo che un polinomio di $\mathbb{K}[X, Y, Z]$ appartiene a J se e solo se in ogni suo monomio compaiono almeno due delle tre variabili X, Y e Z. Ma, per qualsiasi polinomio $f \in \mathbb{K}[X, Y, Z]$ e per ogni intero $n \geq 1$, questa condizione viene soddisfatta da f se e solo se è soddisfatta da f^n, ovvero $f \in J$ se e solo se $f^n \in J$. In effetti, l'implicazione diretta è ovvia, ma vale anche il viceversa per contronominale perché per esempio, se in f appare il monomio X, allora in f^n comparirà X^n. Perciò J è un ideale radicale. Fatta questa premessa, dimostriamo che $\sqrt{I} = J$ per doppia inclusione.

($\subseteq$) Ovviamente $I \subseteq J$ e quindi $\sqrt{I} \subseteq \sqrt{J} = J$.

($\supseteq$) Basta osservare che i generatori di J appartengono tutti a $\sqrt{I}$. Innanzitutto, vale che $XY \in I \subseteq \sqrt{I}$. Ora:

$$\begin{aligned} Y^2Z = Y(YZ + XZ) - Z(XY) \in I \\ \implies Y^2Z^2 \in I \\ \implies YZ \in \sqrt{I} \end{aligned} \qquad \begin{aligned} X^2Z = X(YZ + XZ) - Z(XY) \in I \\ \implies X^2Z^2 \in I \\ \implies XZ \in \sqrt{I} \end{aligned}$$

Osservazione 1.31. Se si assume che $\mathbb{K}$ sia un campo algebricamente chiuso, si può risolvere geometricamente l'esercizio 1.30 sfruttando il teorema degli zeri di Hilbert, che dimostreremo in seguito e che, nel nostro caso, fornisce una corrispondenza biunivoca:

$$\begin{aligned} \{\text{Ideali radicali di } \mathbb{K}[X, Y, Z]\} &\longleftrightarrow \{\text{Sottoinsiemi algebrici di } \mathbb{A}^3(\mathbb{K})\} \\ I &\longmapsto \mathcal{V}(I) \\ \mathcal{I}(X) &\longmapsfrom X \end{aligned}$$

[4] Un ideale non principale di $\mathbb{K}[X, Y]$ è l'ideale (X, Y). Questo è stato dimostrato nell'esempio 10.2 delle dispense del corso AL210.

In particolare, se I è un ideale radicale di $\mathbb{K}[X, Y, Z]$, allora $\mathcal{I}(\mathcal{V}(I)) = I$. Per risolvere l'esercizio precedente sarebbe dunque bastato osservare che J è un ideale radicale e che $\mathcal{V}(\sqrt{I}) = \mathcal{V}(J)$. Si può vedere facilmente[5] che $\mathcal{V}(\sqrt{I}) = \mathcal{V}(I)$ e quindi, oltre al fatto che J è un ideale radicale, si deve solo verificare che $\mathcal{V}(I) = \mathcal{V}(J)$, cioè che i due seguenti sistemi di equazioni hanno lo stesso insieme di soluzioni:

$$\begin{cases} XY = 0 \\ XZ + YZ = 0 \end{cases} \qquad \begin{cases} XY = 0 \\ YZ = 0 \\ XZ = 0 \end{cases}$$

[5] La dimostrazione viene trattata negli appunti nel corso GE410.

Algebra commutativa (Matematica, Roma Tre) Oct 13, 2020

Lezione 9

Raffaele Di Donna

Esercizi su anelli e ideali.

Esercizio 1.32. Nell'anello di polinomi $\mathbb{R}[X,Y]$ si considerino:

$$f = 1 + X^2$$
$$g = Y^2(X + X^3) + (Y-1)X^2 + Y + 2$$

Stabilire se l'ideale $I = (f,g)$ è primo o massimale.

Svolgimento. Osserviamo che:

$$\begin{aligned} g &= XY^2(1+X^2) + (Y-1)X^2 + Y + 2 \\ &= XY^2(1+X^2) + Y(1+X^2) - X^2 + 2 \\ &= XY^2(1+X^2) + Y(1+X^2) - (1+X^2) + 3 \\ &= (XY^2 + Y - 1)(1+X^2) + 3 \end{aligned}$$

Ne deduciamo che $I = (f,3)$, ma 3 è un elemento invertibile di $\mathbb{R}[X,Y]$ e dunque $I = \mathbb{R}[X,Y]$ che non è un ideale primo né massimale.

Esercizio 1.33. Sia A un anello (commutativo e unitario) e sia I un ideale proprio di A. Dimostrare che le seguenti condizioni sono equivalenti.

(a) Vale che I è un ideale primo di A.

(b) Presi due ideali qualsiasi J e L di A, se $JL \subseteq I$, allora $J \subseteq I$ oppure $L \subseteq I$.

Svolgimento. Mostriamo le due implicazioni. Per l'implicazione (a) $\implies$ (b) mostreremo la contronominale.

($\Downarrow$) Siano J e L due ideali di A tali che $J \nsubseteq I$ e $L \nsubseteq I$. Allora esistono degli elementi $x \in J \setminus I, y \in L \setminus I$. In particolare, si ha $x, y \notin I$ e quindi, per il punto (a), anche $xy \notin I$. D'altra parte, per definizione di ideale prodotto, sappiamo che $xy \in JL$ e dunque $JL \nsubseteq I$.

($\Uparrow$) Siano $x, y \in A$ tali che $xy \in I$. Definiamo $J := (x)$, $L := (y)$. Allora $(xy) = JL$ in virtù dell'ipotesi che A sia un anello commutativo e unitario[6]. Ma allora $JL \subseteq I$ e quindi, per il punto (b), possiamo concludere che $J \subseteq I$ oppure $L \subseteq I$, cioè che $x \in I$ oppure $y \in I$.

Esercizio 1.34. Sia A un anello. Dimostrare che un polinomio di $A[X]$ è nilpotente se e solo se tutti i suoi coefficienti sono nilpotenti.

Svolgimento. Sia $f \in A[X]$ un polinomio. Assumiamo $f = a_0 + a_1X + \cdots + a_nX^n$ con $a_0, a_1, \ldots, a_n \in A$ e dimostriamo le due implicazioni. Ricordiamo anche che il nilradicale di un anello, che è l'insieme di tutti i suoi elementi nilpotenti, è un ideale, perciò la somma di nilpotenti e il prodotto per un elemento nilpotente sono a loro volta nilpotenti. Dimostriamo ora le due implicazioni.

($\Leftarrow$) Se $a_0, a_1, \ldots, a_n \in A$ sono nilpotenti, allora $a_0, a_1X, \ldots, a_nX^n \in A[X]$ sono nilpotenti e dunque f è nilpotente in quanto somma di elementi nilpotenti.

[6] Questo passaggio viene giustificato in maniera dettagliata nella dimostrazione del punto (iii) della proposizione 7.5 delle dispense del corso AL210. Nell'esempio 7.6 delle stesse dispense si vede anche che l'ipotesi di lavorare con anelli commutativi è irrinunciabile. Al contrario, l'ipotesi che A sia un anello unitario può essere indebolita richiedendo che valga invece $A^2 = A$.

($\Rightarrow$) Procediamo per induzione sull'intero $n \geq 0$. La base di induzione, vale a dire il caso $n = 0$, è banale. Nel passo induttivo supponiamo che $n \geq 1$ e che, se un polinomio di grado $n-1$ è nilpotente, allora sono nilpotenti tutti i suoi coefficienti. Se f è nilpotente, allora $f^k = 0$ per un qualche intero $k \geq 1$. Osserviamo però che il coefficiente direttore di f^k, cioè il coefficiente del termine di grado massimo di f^k, è a_n^k e quindi, per il principio di identità dei polinomi, abbiamo $a_n^k = 0$, cioè a_n è nilpotente. In particolare, il monomio $a_n X^n$ è nilpotente e quindi $f - a_n X^n$ è un polinomio nilpotente di grado $n-1$. Per ipotesi induttiva, otteniamo allora che tutti i suoi coefficienti, cioè $a_0, a_1, \ldots, a_{n-1}$, sono nilpotenti. Concludiamo allora che tutti i coefficienti di f sono nilpotenti.

Esercizio 1.35.

(i) Dimostrare che la contrazione di un ideale primo è un ideale primo.

(ii) Provare con un esempio che l'estensione di un ideale primo non è necessariamente un ideale primo.

(iii) Provare con un esempio che la contrazione di un ideale massimale non è sempre un ideale massimale.

(iv) Dare un'interpretazione geometrica del punto (i) precedente.

Svolgimento.

(i) Sia $f\colon A \to B$ un omomorfismo di anelli e sia J un ideale primo di B. Dimostriamo che $J^{\mathrm{c}} = f^{-1}(J)$ è un ideale primo di A. Siano dunque $x, y \in A$ tali che $xy \in J^{\mathrm{c}}$. Allora $f(xy) \in J$, cioè $f(x)f(y) \in J$. Ma J è un ideale primo di B, quindi $f(x) \in J$ oppure $f(y) \in J$. Dunque abbiamo che $x \in J^{\mathrm{c}}$ oppure $y \in J^{\mathrm{c}}$.

(ii) Consideriamo l'omomorfismo di anelli $\mathrm{ev}_0\colon \mathbb{R}[X] \to \mathbb{R}$ definito da $\mathrm{ev}_0(f) := f(0)$. Allora (X^2+1) è un ideale primo la cui estensione è tutto $\mathbb{R}$ in quanto contiene l'elemento $1 = \mathrm{ev}_0(X^2+1)$ e sappiamo che $\mathbb{R}$ non può essere un ideale primo in quanto non è nemmeno un ideale proprio.

Un altro esempio è dato dal considerare la mappa inclusione $i\colon \mathbb{Z} \to \mathbb{Q}$ e l'ideale principale (p) con p numero primo. Sappiamo che in $\mathbb{Z}$ tale ideale è primo, ma la sua estensione tramite i è tutto $\mathbb{Q}$ in quanto p è invertibile in $\mathbb{Q}$.

(iii) Consideriamo nuovamente la mappa inclusione $i\colon \mathbb{Z} \to \mathbb{Q}$. Basta osservare che l'ideale banale (0) è massimale in $\mathbb{Q}$ ma non in $\mathbb{Z}$ perché $\mathbb{Q} \simeq \mathbb{Q}/\{0\}$ è un campo mentre $\mathbb{Z} \simeq \mathbb{Z}/\{0\}$ non lo è.

(iv) Sia $g\colon X \to Y$ un morfismo di insiemi algebrici e sia $g^*\colon \mathcal{A}(Y) \to \mathcal{A}(X)$ l'omomorfismo indotto da g sui rispettivi anelli delle funzioni polinomiali, cioè la mappa data da $g^*(h + \mathcal{I}(Y)) := h \circ g + \mathcal{I}(X)$. Abbiamo visto che, se Z è un sottoinsieme algebrico di X, allora:

$$\mathcal{I}_{g(Z)/Y} = (g^*)^{-1}(\mathcal{I}_{Z/X}) = (\mathcal{I}_{Z/X})^{\mathrm{c}}$$

Inoltre, è noto che Z è irriducibile se e solo se $\mathcal{I}_{Z/X}$ è un ideale primo. Ma per il punto (i) precedente, se $\mathcal{I}_{Z/X}$ è un ideale primo, lo è anche la sua contrazione $\mathcal{I}_{g(Z)/Y}$ e in particolare $g(Z)$ è irriducibile. Ne deduciamo che l'interpretazione geometrica è la seguente: l'immagine tramite un morfismo di un insieme algebrico irriducibile è ancora irriducibile.

Osservazione 1.36. Una conferma della proprietà geometrica individuata nello svolgimento del punto (iv) dell'esercizio 1.35 è data dal fatto che:

(1) I morfismi di insiemi algebrici sono applicazioni continue[7].

[7] Per una dimostrazione di questo fatto rimandiamo all'osservazione 2.9 delle dispense del corso GE410.

(2) L'immagine di un insieme irriducibile tramite una mappa continua è ancora un insieme irriducibile. Se infatti $g\colon X \to Y$ è un'applicazione continua tra spazi topologici e Z è un sottoinsieme di X tale che $f(Z)$ sia riducibile, allora esistono due chiusi propri Y_1 e Y_2 di $f(Z)$ tali che:

$$\begin{aligned} & f(Z) = Y_1 \cup Y_2 \\ \implies & f^{-1}(f(Z)) = f^{-1}(Y_1) \cup f^{-1}(Y_2) \\ \implies & Z = (f^{-1}(Y_1) \cap Z) \cup (f^{-1}(Y_2) \cap Z) \end{aligned}$$

Poiché si assume che g sia continua, la preimmagine di un chiuso di Y tramite g è un chiuso di X e dunque $f^{-1}(Y_1) \cap Z$ e $f^{-1}(Y_2) \cap Z$ sono chiusi di Z. Inoltre, sono chiusi propri perché per esempio:

$$\begin{aligned} & f^{-1}(Y_1) \cap Z = Z \\ \implies & Z \subseteq f^{-1}(Y_1) \\ \implies & f(Z) \subseteq f(f^{-1}(Y_1)) \subseteq Y_1 \\ \implies & f(Z) = Y_1 \end{aligned}$$

L'ultima implicazione contraddice il fatto che Y_1 sia un chiuso proprio di $f(Z)$. Si ottiene perciò che Z è riducibile.

Prima di svolgere l'ultimo esercizio di questa lezione, generalizziamo il seguente risultato, già noto per gli interi[8].

Osservazione 1.37 (Identità di Bezout per domini euclidei). Sia A un dominio euclideo con funzione euclidea $\delta\colon A\setminus\{0\} \to \mathbb{N}$. Allora, per ogni $a, b \in A$, esistono $x, y \in A$ tali che si abbia l'identità $ax + by = \mathrm{MCD}(a, b)$.

Dimostrazione. Osserviamo innanzitutto che, se a e b sono entrambi nulli, allora il risultato è banale perché per definizione $\mathrm{MCD}(0, 0) = 0$. Supponiamo perciò, senza perdita di generalità, che $b \neq 0$. Definiamo ora:

$$S := \{x \in A\colon x \neq 0,\ x = ax + by \text{ per certi } x, y \in A\}$$

Prendendo $x := 0$ e $y := 1$ si vede che $b \in S$, perciò S è un insieme non vuoto. In particolare, si ha che $\delta(S)$ è un sottoinsieme non vuoto di $\mathbb{N}$ e dunque ammette minimo per il principio del buon ordinamento. Sia allora $d \in S$ un elemento tale che $\delta(d)$ sia il minimo di $\delta(S)$. Dimostreremo che $d = \mathrm{MCD}(a, b)$. Innanzitutto, per definizione di S, sappiamo che $d \neq 0$ e che esistono $x, y \in A$ tali che $d = ax + by$. Per definizione di funzione euclidea esistono $q, r \in A$, con $r = 0$ oppure $r \neq 0$ e $\delta(r) < \delta(d)$, tali che $x = qd + r$. In particolare, vale che:

$$r = x - qd = x - q(ax + by) = (1 - qa)x + (qb)y$$

Se fosse $r \neq 0$ e $\delta(r) < \delta(d)$, allora $r \in S$ e avremmo una contraddizione con la minimalità di $\delta(d)$. Dunque $r = 0$, cioè $d \mid x$. In modo simile si ottiene che $d \mid y$. Sia ora $d' \in A$ tale che $d' \mid x$ e $d' \mid y$. Allora $d' \mid d$ perché d' divide qualsiasi combinazione lineare di x e y. Con questo otteniamo che $d = \mathrm{MCD}(a, b)$ e quindi abbiamo concluso. □

Ci serviremo, inoltre, del seguente fatto.

Osservazione 1.38. Sia A un dominio a fattorizzazione unica e sia K il campo dei quozienti di A. Valgono le due seguenti affermazioni.

(a) Dato un polinomio non nullo $f \in K[X]$, esiste $\alpha \in K$ con $\alpha \neq 0$ tale che $\alpha f \in A[X]$ e tale che αf sia un polinomio primitivo, cioè con coefficienti coprimi.

(b) Dati $f, g \in A[X]$ con f polinomio primitivo, vale che f divide g in $A[X]$ se e solo se f divide g in $K[X]$.

[8] Prima di proseguire si ricordi che, per il teorema 9.2 delle dispense del corso AL210, un dominio euclideo è in particolare un dominio a fattorizzazione unica perciò, in un dominio euclideo, il massimo comune divisore tra due elementi esiste sempre.

Dimostrazione.

(a) Per ipotesi possiamo scrivere, per opportuni $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_n \in A$ con $b_1, b_2, \ldots, b_n \neq 0$:

$$f(X) = \sum_{i=0}^{n} \frac{a_i}{b_i} X^i$$

Chiaramente, se definiamo $b := b_0 b_1 \cdots b_n$, allora $bf \in A[X]$. Scriviamo adesso $bf = cf_0$ con $c \in A$ e $f_0 \in A[X]$ polinomio primitivo. Dato che per ipotesi f è un polinomio non nullo, si deve avere $c \neq 0$. Definendo dunque $\alpha := b/c$, otteniamo che $\alpha f = f_0$, quindi $\alpha f \in A[X]$ ed è un polinomio primitivo.

(b) L'implicazione diretta è ovvia, perciò dimostriamo il viceversa. Possiamo escludere il caso banale in cui g è il polinomio nullo e scrivere quindi $g = cg_0$ con $c \in A$, $c \neq 0$ e $g_0 \in A[X]$ polinomio primitivo. Dato che per ipotesi f divide g in $K[X]$ e $c \neq 0$, si ha anche che f divide g_0 in $K[X]$, cioè $g_0 = fh$ per un opportuno polinomio $h \in K[X]$. Per il punto (a) precedente, possiamo trovare $\alpha \in K$, con $\alpha \neq 0$, tale che, se poniamo $h_0 := \alpha h$, allora $h_0 \in A[X]$ e h_0 è un polinomio primitivo. Osserviamo ora che:

$$\alpha g_0 = \alpha f h = f h_0$$

Per il lemma di Gauss[9] sappiamo che fh_0 è un polinomio primitivo in quanto prodotto di polinomi primitivi. Dunque g_0 e fh_0 sono entrambi polinomi primitivi. Inoltre sono associati in $K[X]$, perché $\alpha \neq 0$ è invertibile in $K[X]$. Sappiamo allora che g_0 e fh_0 sono associati anche in $A[X]$. Con questo si ha, in particolare, che fh_0 divide g_0 in $A[X]$ e quindi possiamo concludere che f divide g_0 in $A[X]$ per transitività. □

Esercizio 1.39. Sia A un dominio a ideali principali. Dimostrare che gli ideali primi non nulli di $A[X]$ sono tutti e soli di una delle seguenti forme:

(i) $I = (p)$ con $p \in A$ elemento primo.

(ii) $I = (f(X))$ con $f(X) \in A[X]$ polinomio irriducibile.

(iii) $I = (p, f(X))$ con $p \in A$ elemento primo e $f(X) \in A[X]$ polinomio tale che $\bar{f}(X) \in A/(p)[X]$ sia un polinomio irriducibile, dove abbiamo indicato con $\bar{f}(X)$ il polinomio ottenuto da $f(X)$ riducendo i suoi coefficienti modulo (p).

Dimostrare inoltre che gli ideali della forma (iii) sono anche ideali massimali di $A[X]$.

Svolgimento. Per semplicità, indicheremo le classi laterali con la notazione della barretta in alto. Dobbiamo in primo luogo dimostrare che tutti gli ideali con una delle forme indicate nel testo dell'esercizio sono primi.

(i) Osserviamo che l'ideale (p) è il nucleo del seguente omomorfismo suriettivo di anelli:

$$\begin{aligned} A[X] &\longrightarrow A/(p)[X] \\ f(X) = \sum_{i=0}^{n} a_i X^i &\longmapsto \bar{f}(X) = \sum_{i=0}^{n} \bar{a}_i X^i \end{aligned}$$

Allora, per il primo teorema di isomorfismo, abbiamo che:

$$A[X]/(p) \simeq A/(p)[X] \tag{3}$$

Ora, poiché per ipotesi A è un dominio a ideali principali, l'ideale (p) è massimale in A e quindi $A/(p)$ è un campo. Ne deduciamo che $A/(p)[X]$ è un dominio a ideali principali[10] e dunque, in particolare, è un dominio di integrità. Per l'isomorfismo trovato prima, anche $A[X]/(p)$ è un dominio di integrità, perciò possiamo concludere che (p) è un ideale primo di $A[X]$.

[9] Ci si riferisce al lemma 10.1 delle dispense del corso AL210. Tra poco useremo anche il lemma 10.2 delle stesse dispense.
[10] In questo passaggio stiamo applicando il punto (i) del teorema 9.2 e il corollario 10.2 visti nelle dispense del corso AL210.

(ii) Sappiamo che A è un dominio a ideali principali e quindi, in particolare, un dominio a fattorizzazione unica[11]. Di conseguenza, anche l'anello di polinomi $A[X]$ è un dominio a fattorizzazione unica e ciò garantisce che, se $f(X) \in A[X]$ è un polinomio irriducibile, allora $(f(X))$ è un ideale primo di $A[X]$.

(iii) Per il terzo teorema di isomorfismo, abbiamo che:

$$A[X]/(p, f(X)) \simeq \big(A[X]/(p)\big)/\big((p, f(X))/(p)\big)$$

Osserviamo ora che gli elementi di $(p, f(X))/(p)$ sono tutti e soli della forma seguente, per opportuni $g(X), h(X) \in A[X]$:

$$\bar{g}(X)\bar{p} + \bar{h}(X)\bar{f}(X) = \bar{h}(X)\bar{f}(X)$$

Perciò vale chiaramente che:

$$(p, f(X))/(p) = (\bar{f}(X))$$

In virtù di questo fatto e dell'isomorfismo (3) precedente, otteniamo allora che:

$$A[X]/(p, f(X)) \simeq A/(p)[X]/(\bar{f}(X))$$

Ricordiamo adesso che, per quanto detto prima, l'anello di polinomi $A/(p)[X]$ è un dominio a ideali principali e quindi, dato che per ipotesi il polinomio $\bar{f}(X) \in A/(p)[X]$ è irriducibile, l'ideale $(\bar{f}(X))$ è massimale in $A/(p)[X]$. In particolare, l'anello quoziente $A/(p)[X]/(\bar{f}(X))$ è un campo e allora, per l'isomorfismo appena trovato, anche $A[X]/(p, f(X))$ è un campo. Questo dimostra che $(p, f(X))$ è un ideale massimale, quindi primo, di $A[X]$.

A questo punto, per poter concludere l'esercizio, dobbiamo solo far vedere che ogni ideale primo non nullo di $A[X]$ è di una delle tre forme indicate. Sia dunque I un ideale primo non nullo di $A[X]$. Si verifica facilmente che $I \cap A$ è un ideale primo di A. Poiché per ipotesi A è un dominio a ideali principali, abbiamo che $I \cap A = 0$ oppure $I \cap A = (p)$ con $p \in A$ elemento primo. Distinguiamo i due casi.

- Supponiamo che $I \cap A = (p)$ con $p \in A$ elemento primo. Si osservi che $p \in I$, perciò I contiene (p). Si presti attenzione al fatto che qui (p) denota l'ideale generato da p in tutto $A[X]$ e non solo in A. Ora, per il teorema di corrispondenza, la composizione π tra l'isomorfismo (3) e la mappa quoziente $A[X] \to A[X]/(p)$ induce una corrispondenza biunivoca:

$$\{\text{Ideali primi di } A[X] \text{ contenenti } (p)\} \longleftrightarrow \{\text{Ideali primi di } A/(p)[X]\}$$

Sappiamo, in particolare, che $\pi(I)$ è un ideale primo di $A/(p)[X]$. Avevamo visto che $A/(p)[X]$ è un dominio a ideali principali, perciò $\pi(I) = 0$ oppure $\pi(I) = (\bar{f}(X))$ con $\bar{f}(X) \in A/(p)[X]$ polinomio primo, quindi irriducibile. Osserviamo che:

$$\pi\big((p, f(X))\big) = (\bar{f}(X))$$

Questo si verifica facilmente per doppia inclusione. Da una parte, infatti, vale che $\bar{f}(X) = \pi(f(X))$, mentre per ogni $g(X), h(X) \in A[X]$ si ha:

$$\pi(g(X)p + h(X)f(X)) = \bar{h}(X)\bar{f}(X) \in (\bar{f}(X))$$

Dunque, per la biunivocità della corrispondenza, si ha che $I = (p, f(X))$ se e solo se $\pi(I) = (\bar{f}(X))$ con $\bar{f}(X) \in A/(p)[X]$ polinomio irriducibile, mentre $I = (p)$ se e solo se $\pi(I) = 0$.

- Supponiamo che $I \cap A = 0$. Questo significa che I non contiene polinomi costanti non nulli perciò, se consideriamo un polinomio $f(X) \in I$ non nullo e di grado minimo, il suo grado sarà sicuramente maggiore o uguale di 1. Inoltre, possiamo supporre che $f(X)$ sia un polinomio primitivo, ovvero con

[11] Con riferimento alle dispense del corso AL210, questo passaggio è garantito dal punto (ii) del teorema 9.2, mentre quello successivo è giustificato dal teorema 10.2.

coefficienti coprimi. Questo perché, se $f(X)$ non è primitivo allora, per un certo $c \in A$ e per qualche polinomio primitivo $f_0(X) \in A[X]$, possiamo scrivere:

$$f(X) = cf_0(X)$$

Sappiamo però che I è un ideale primo di $A[X]$ e dunque, siccome $c \notin I$, dobbiamo avere $f_0(X) \in I$. Inoltre, vale che $f_0(X)$ è un polinomio non costante dello stesso grado di $f(X)$, cioè di grado minimo e positivo. Infatti, poiché per ipotesi A è un dominio integrale, possiamo usare la formula del grado[12]:

$$\deg(f(X)) = \deg(c) + \deg(f_0(X)) = \deg(f_0(X))$$

Supponiamo allora che $f(X)$ sia un polinomio primitivo. Adesso il nostro obiettivo è dimostrare che $I = (f(X))$. Per farlo, consideriamo un polinomio $g(X) \in I$ e dimostriamo che $f(X)$ divide $g(X)$. Sia K il campo dei quozienti di A. Allora $K[X]$ è un dominio euclideo e dunque in $K[X]$ il massimo comune divisore tra due elementi esiste sempre. In particolare, possiamo definire:

$$h(X) := \mathrm{MCD}(f(X), g(X))$$

Adesso, per l'osservazione 1.37, esistono due polinomi $p(X), q(X) \in K[X]$ tali che si abbia l'identità:

$$h(X) = p(X)f(X) + q(X)g(X)$$

Si presti attenzione al fatto che, in generale, si ha $p(X), q(X) \notin A[X]$, perciò *non* si può concludere dalla definizione di ideale che $h(X) \in I$. Moltiplicando però i due membri dell'equazione precedente per un'opportuna costante $\alpha \in A$, con $\alpha \neq 0$, che di fatto può essere scelta come il massimo comune denominatore dei coefficienti di $p(X)$ e $q(X)$, possiamo affermare che $\alpha h(X) \in I$. Osserviamo ora che, siccome $h(X)$ divide $f(X)$ in $K[X]$, esiste un polinomio $u(X) \in K[X]$ tale che valga l'identità:

$$f(X) = h(X)u(X)$$

Per la formula che grado, che possiamo applicare perché K è un campo, quindi un dominio integrale e per la minimalità del grado di $f(X)$ tra tutti quelli dei polinomi in I, otteniamo che:

$$\begin{aligned} \deg(f(X)) &= \deg(h(X)) + \deg(u(X)) \\ &= \deg(\alpha h(X)) + \deg(u(X)) \\ &\geq \deg(f(X)) + \deg(u(X)) \end{aligned}$$

Dunque $u(X)$ è una costante $u \in K$. Inoltre vale che $u \neq 0$, altrimenti si avrebbe una contraddizione col fatto che $f(X)$ è un polinomio non nullo. E allora u è invertibile in K, perciò $f(X)$ divide $h(X)$ in $K[X]$. Per transitività, si ha che $f(X)$ divide anche $g(X)$ in $K[X]$ e quindi $f(X)$ divide $g(X)$ in $A[X]$ per il punto (b) dell'osservazione 1.38.

Con questo abbiamo mostrato che $I = (f(X))$. Per concludere l'esercizio, basta osservare che $f(X)$ è un polinomio irriducibile in $A[X]$. Poiché sappiamo, per la discussione precedente, che $f(X)$ è un polinomio primitivo e non costante, sarà sufficiente[13] mostrare che $f(X)$ è un polinomio irriducibile in $K[X]$. Siano dunque $p(X), q(X) \in K[X]$ polinomi tali che:

$$f(X) = p(X)q(X)$$

Moltiplicando $p(X)$ e $q(X)$ per delle costanti opportune $\alpha, \beta \in A$, con $\alpha, \beta \neq 0$, che possono essere scelte come i massimi comuni denominatori dei rispettivi coefficienti, abbiamo le condizioni seguenti:

$$\alpha p(X) \in A[X]\,, \quad \beta q(X) \in A[X]$$

[12] Si rimanda a tal proposito all'osservazione 10.4 delle dispense del corso AL210.
[13] Questo è garantito dal lemma 10.3 delle dispense del corso AL210.

Possiamo perciò sfruttare il fatto che I è un ideale primo di $A[X]$. Sappiamo infatti che $\alpha\beta f(X) \in I$ e dunque vale $\alpha p(X) \in I$ oppure $\beta q(X) \in I$. Senza perdita di generalità, assumiamo che $\alpha p(X) \in I$. Allora, ricordando che $I = (f(X))$, esiste un polinomio $h(X) \in A[X]$ tale che si abbia l'uguaglianza:

$$\alpha p(X) = f(X)h(X)$$

In particolare:

$$\begin{aligned} &\alpha\beta f(X) = \beta f(X)h(X)q(X) \\ &\implies \alpha = h(X)q(X) \\ &\implies q(X) \text{ è invertibile in } K[X] \end{aligned}$$

Algebra commutativa (Matematica, Roma Tre) Oct 15, 2020

Lezione 10

Raffaele Di Donna

Generalizzazione del Teorema di Cayley-Hamilton. Lemma di Nakayama e suoi corollari.

In generale, i moduli liberi finitamente generati si comportano come gli spazi vettoriali. Infatti, si hanno le seguenti proprietà:

(1) Dato un A-modulo libero finitamente generato M di rango n, la scelta di una base per M equivale a dare un isomorfismo di A-moduli tra M e A^n.

(2) Dati due A-moduli liberi finitamente generati M e N, di rango m e n rispettivamente, abbiamo che:

$$\mathrm{Hom}_A(M,N) \simeq \mathrm{Hom}_A(A^m, A^n) \simeq \mathrm{Mat}(A, m \times n)$$

Abbiamo qui introdotto le due notazioni:

- $\mathrm{Hom}_A(M,N)$, per indicare l'insieme degli omomorfismi di A-moduli da M in N.
- $\mathrm{Mat}(A, m \times n)$, per indicare l'insieme delle matrici a coefficienti in A con m righe e n colonne.

Questi insiemi acquistano una naturale struttura di A-modulo con le operazioni usuali di somma e prodotto per uno scalare. Poniamo anche $\mathrm{End}_A(M) := \mathrm{Hom}_A(M,M)$. Chiameremo *endomorfismi di M* gli elementi di $\mathrm{End}_A(M)$.

(3) Data una matrice $C \in \mathrm{Mat}(A, n \times n)$, possiamo definire il suo determinante $\det C$ e questo soddisfa le proprietà note. In particolare, vale che C è invertibile se e solo se $\det C$ è invertibile in A.

Vediamo ora un risultato preliminare.

Lemma 1.40. *Sia A un anello. Allora esiste una corrispondenza biiettiva:*

$$\{A[X]\text{-}moduli\} \longleftrightarrow \{(M,\varphi)\colon M \text{ è un } A\text{-modulo, } \varphi \in \mathrm{End}_A(M)\}$$

Dimostrazione. Un $A[X]$-modulo M è anche un A-modulo e possiamo considerare un endomorfismo su M:

$$\begin{aligned} \varphi\colon M &\longrightarrow M \\ m &\longmapsto Xm \end{aligned}$$

Viceversa, sia M un A-modulo e sia $\varphi \in \mathrm{End}_A(M)$. Diamo a M una struttura di $A[X]$-modulo definendo il prodotto esterno nel modo seguente:

$$\Big(\sum_{i=0}^{n} a_i X^i\Big) m := \sum_{i=0}^{n} a_i \varphi^i(m)$$

Abbiamo qui usato le notazioni:

$$\varphi^i := \underbrace{\varphi \circ \varphi \circ \cdots \circ \varphi}_{i \text{ volte}}, \quad \varphi^0 := \mathrm{id}_M$$

A questo punto è facile verificare che, con queste definizioni, abbiamo stabilito la corrispondenza biunivoca voluta. □

Ricordiamo poi la seguente nozione di algebra lineare.

Definizione 1.41. Sia $C \in \mathrm{Mat}(A, n \times n), C = (c_{ij})$ una matrice. Per ogni $i, j = 0, 1, \ldots, n$, introduciamo la notazione $C(1 \ldots \hat{i} \ldots n \mid 1 \ldots \hat{j} \ldots n)$ per indicare la sottomatrice quadrata di ordine $n-1$ di C ottenuta cancellando la i-esima riga e la j esima colonna di C. Definiamo allora il *cofattore* (o *complemento algebrico*) dell'elemento c_{ij} di C come:

$$C_{ij} := (-1)^{i+j} \det C(1 \ldots \hat{i} \ldots n \mid 1 \ldots \hat{j} \ldots n)$$

La matrice quadrata di ordine n che ha C_{ji} per elemento di posto ij, al variare degli indici $i, j = 1, 2, \ldots, n$, è detta la *matrice aggiunta di* C e si denota $\mathrm{Adj}(C)$.

Esercizio 1.42. Sia $C \in \mathrm{Mat}(A, n \times n)$ una matrice. Allora si ha che $\mathrm{Adj}(C)C = (\det C)I_n = C\,\mathrm{Adj}(C)$.

Svolgimento. Ci limitiamo a dimostrare la prima identità, poiché la seconda si dimostra in modo analogo. Supponiamo che $C = (c_{ij})$ e facciamo vedere che le matrici $\mathrm{Adj}(C)C$ e $(\det C)I_n$ sono costituite dagli stessi elementi. Fissiamo dunque due indici $i, j \in \{1, 2, \ldots, n\}$. Se $i = j$, allora basta sviluppare il determinante di C lungo la riga i applicando la formula di Laplace:

$$\det C = \sum_{k=1}^{n} c_{ki} C_{ki}$$

Se invece $i \neq j$, consideriamo la matrice $C' = (c'_{ij})$ ottenuta da C per sostituzione della colonna i di C con la colonna j di C. Allora vale che $\det C' = 0$, perché C' ha due colonne uguali. D'altra parte, sviluppando il determinante di C' lungo la colonna i con la formula di Laplace, si ottiene:

$$0 = \sum_{k=0}^{n} c'_{ki} C'_{ki} = \sum_{k=0}^{n} c_{kj} C_{ki}$$

Proposizione 1.43. *Siano M un A-modulo finitamente generato, $\varphi \in \mathrm{End}_A(M)$ e sia I un ideale di A tale che valga $\varphi(M) \subseteq IM$. Allora esistono un intero $n \geq 1$ e degli elementi $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in I$ tali che si abbia:*

$$\varphi^n + \alpha_{n-1}\varphi^{n-1} + \cdots + \alpha_1 \varphi + \alpha_0 \mathrm{id}_M = 0$$

Dimostrazione. Sappiamo per ipotesi che M ammette un sistema di generatori $\{m_1, m_2, \ldots, m_n\}$. Inoltre, essendo $\varphi(M) \subseteq IM$, vale che, per ogni $i = 1, 2, \ldots, n$, esistono degli elementi $a_{i1}, a_{i2}, \ldots, a_{in} \in I$ tali che:

$$\varphi(m_i) = \sum_{j=1}^{n} a_{ij} m_j$$

Equivalentemente, per ogni $i = 1, 2, \ldots, n$, abbiamo che:

$$\sum_{j=1}^{n} (\delta_{ij}\varphi - a_{ij}\mathrm{id}_M)(m_j) = 0$$

Per il lemma 1.40, possiamo considerare M come un $A[X]$-modulo definendo il prodotto esterno come segue:

$$\Big(\sum_{i=1}^{n} \alpha_i X^i\Big) m := \sum_{i=1}^{n} \alpha_i \varphi^i(m)$$

Definendo la matrice quadrata $C := (\delta_{ij} X - a_{ij})$ di ordine n e il vettore colonna $m := (m_1, m_2, \ldots, m_n)$, la relazione che abbiamo trovato prima si scrive come $Cm = 0$. Ora, se moltiplichiamo a sinistra per la matrice aggiunta di C, per l'esercizio 1.42 otteniamo la condizione $(\det C)m_j = 0$ per ogni $j = 1, 2, \ldots, n$. Adesso, scrivendo esplicitamente il determinante di C, si ottiene un polinomio monico in X di grado n a coefficienti in I, questo perché gli elementi a_{ij} erano stati scelti nell'ideale I di A. Per opportuni $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in I$ troviamo allora, per ogni $j = 1, 2, \ldots, m$, la condizione:

$$0 = (\det C)m_j = (X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_1 X + \alpha_0)m_j$$

Equivalentemente, per come è definito il prodotto esterno di M come $A[X]$-modulo, per $j = 1, 2, \dots, n$ si ha:

$$(\varphi^n + \alpha_{n-1}\varphi^{n-1} + \cdots + \alpha_1\varphi + \alpha_0)(m_j) = 0$$

Ricordando infine che l'insieme $\{m_1, m_2, \dots, m_n\}$ è un sistema di generatori per M, otteniamo la tesi. □

Il risultato precedente generalizza il seguente fatto di algebra lineare.

Osservazione 1.44 (Teorema di Cayley-Hamilton). Sia V un $\mathbb{K}$-spazio vettoriale di dimensione finita. Allora ogni endomorfismo di V è una radice del proprio polinomio caratteristico.

Dimostrazione. Sia φ un endomorfismo di V fissato. Dato che un $\mathbb{K}$-spazio vettoriale di dimensione finita è un $\mathbb{K}$-modulo finitamente generato, possiamo ripetere passo passo la dimostrazione della proposizione 1.43, considerando però come sistema finito di generatori per V una base $B = \{v_1, v_2, \dots, v_n\}$ e definendo $I := \mathbb{K}$. Osserviamo ora che, posto $a'_{ij} := a_{ji}$ per ogni $i, j = 1, 2, \dots, n$, la matrice $M_B(\varphi) := (a'_{ij})$ è la matrice che rappresenta l'endomorfismo φ nella base B. Ne deduciamo che la matrice $C := (\delta_{ij}X - a_{ij})$ è la trasposta della matrice $XI_n - M_B(\varphi)$. Ma allora, poiché il determinante di una matrice coincide con il determinante della matrice trasposta, otteniamo che φ è una radice del polinomio $\det C = \det(XI_n - M_B(\varphi))$, ossia una radice del proprio polinomio caratteristico. □

Lemma 1.45 (di Nakayama)**.** *Sia M un A-modulo finitamente generato e sia I un ideale di A tale che valga $IM = M$. Allora esiste un elemento $a \in A$ tale che $1 - a \in I$ e $aM = 0$. Se inoltre $I \subseteq \mathrm{Jac}(A)$, vale $M = 0$.*

Osservazione 1.46. In particolare, l'elemento $1 - a \in I$ che compare nell'enunciato del lemma di Nakayama agisce come l'identità sugli elementi di M, ossia soddisfa la condizione $(1 - a)m = m$ per qualsiasi $m \in M$.

Dimostrazione (Lemma di Nakayama). Poiché per ipotesi vale l'inclusione non banale $M \subseteq IM$, possiamo applicare la proposizione 1.43 prendendo $\varphi := \mathrm{id}_M$ e dunque esistono $\alpha_0, \alpha_1, \dots, \alpha_{n-1} \in I$ tali che si abbia:

$$(1 + \alpha_{n-1} + \cdots + \alpha_1 + \alpha_0)\mathrm{id}_M = 0$$

Definiamo allora:

$$a := 1 + \alpha_{n-1} + \cdots + \alpha_1 + \alpha_0$$

Per costruzione, tale elemento $a \in A$ è tale che $1 - a \in I$ e $aM = 0$. Ora, se assumiamo anche che $I \subseteq \mathrm{Jac}(A)$ allora, per un risultato precedente, l'elemento $a = 1 - (1 - a)$ è invertibile in A e dunque possiamo scrivere:

$$M = a^{-1}aM = a^{-1}0 = 0$$ □

Vediamo ora qualche conseguenza di questo importante risultato.

Corollario 1.47. *Sia M un A-modulo finitamente generato e sia $\varphi \in \mathrm{End}_A(M)$. Se φ è un endomorfismo suriettivo di M, allora φ è un isomorfismo.*

Dimostrazione. Per il lemma 1.40, possiamo attribuire a M una struttura di $A[X]$-modulo in maniera tale che $Xm = \varphi(m)$. In particolare, se consideriamo l'ideale $I := (X)$ di $A[X]$, abbiamo la condizione $IM = M$. Inoltre, un A-modulo finitamente generato è ovviamente un $A[X]$-modulo finitamente generato e possiamo allora applicare il lemma di Nakayama, dal quale deduciamo l'esistenza di un polinomio $p(X) \in A[X]$ tale che $1 - p(X) \in I$ e $p(X)M = 0$. Siccome $I = (X)$, il polinomio $q(X) := 1 - p(X)$ è privo di termine noto e quindi, per un certo intero $n \geq 1$ e per opportuni $a_1, a_2, \dots, a_n \in A$, possiamo esprimere $q(X)$ come segue:

$$q(X) = \sum_{i=1}^{n} a_i X^i$$

Dall'osservazione 1.46 e dalla definizione del prodotto esterno di M come $A[X]$-modulo segue allora che, per ogni $m \in M$, si ha:

$$m = q(X)m = \Big(\sum_{i=1}^{n} a_i X^i\Big)m = \sum_{i=1}^{n} a_i \varphi^i(m)$$

In particolare, se $m \in \mathrm{Ker}\,\varphi$, allora $m = 0$ e questo dimostra che φ è iniettiva, dunque un isomorfismo. □

Corollario 1.48. *Siano M un A-modulo finitamente generato, N un sottomodulo di M e sia $I \subseteq \mathrm{Jac}(A)$ un ideale di A. Se $IM + N = M$, allora $M = N$.*

Dimostrazione. In primo luogo, mostriamo che $I(M/N) = (IM + N)/N$. Si procede per doppia inclusione:

($\subseteq$) Un elemento di $I(M/N)$ si esprime, per un qualche intero $k \geq 1$ e per opportuni $x_1, x_2, \ldots, x_k \in I$, $m_1, m_2, \ldots, m_k \in M$, nel modo seguente:

$$\sum_{i=1}^{k} x_i(m_i + N)$$

Adesso, sfruttando le definizioni di prodotto esterno e somma nel modulo quoziente M/N, vediamo che è anche un elemento di $(IM)/N$, quindi di $(IM + N)/N$:

$$\sum_{i=1}^{k} x_i(m_i + N) = \sum_{i=1}^{k} (x_i m_i + N) = \Big(\sum_{i=1}^{k} x_i m_i\Big) + N$$

($\supseteq$) Un elemento di $(IM + N)/N$ si scrive, per qualche intero $k \geq 1$ e per opportuni $x_1, x_2, \ldots, x_k \in I$, $m_1, m_2, \ldots, m_k \in M$, $n \in N$, nel modo seguente:

$$\Big(\sum_{i=1}^{k} x_i m_i + n\Big) + N$$

Ora, utilizzando il fatto che $n \in N$ assieme alle definizioni di somma e prodotto esterno nel modulo quoziente M/N, otteniamo che è anche un elemento di $I(M/N)$:

$$\Big(\sum_{i=1}^{k} x_i m_i + n\Big) + N = \Big(\sum_{i=1}^{k} x_i m_i\Big) + N = \sum_{i=1}^{k} (x_i m_i + N) = \sum_{i=1}^{k} x_i(m_i + N)$$

Ricordiamo adesso che, per ipotesi, si ha $IM + N = M$ e dunque $I(M/N) = M/N$. Osserviamo inoltre che, se M è un A-modulo finitamente generato, allora M/N è ovviamente un A-modulo finitamente generato e quindi si può applicare il lemma di Nakayama, dal quale segue che $M/N = 0$ perché per ipotesi $I \subseteq \mathrm{Jac}(A)$. Equivalentemente, abbiamo che $M = N$, cioè la tesi. □

Nella dimostrazione della proposizione 1.23 avevamo osservato che, se M è un A-modulo libero e se I è un ideale massimale di A, allora la mappa di passaggio al quoziente $\pi\colon M \to M/IM$ manda ogni base di M come A-modulo in una base di M/IM come A/I-spazio vettoriale. Il risultato che segue ci dice che, se M è un A-modulo finitamente generato (non necessariamente libero) con A anello locale e se un sottoinsieme di M viene mandato tramite π in una base di M/IM, allora quel sottoinsieme è un insieme di generatori per M.

Corollario 1.49. *Siano A un anello locale, $\mathfrak{m}$ il suo ideale massimale e sia $\mathbb{K} = A/\mathfrak{m}$ il suo campo residuo. Siano inoltre M un A-modulo finitamente generato, $\pi\colon M \to M/\mathfrak{m}M$ la mappa quoziente, $\{m_1, m_2, \ldots, m_n\}$ un sottoinsieme di M tale che $\{\pi(m_1), \pi(m_2), \ldots, \pi(m_n)\}$ sia una base di $M/\mathfrak{m}M$ come $\mathbb{K}$-spazio vettoriale. Allora $\{m_1, m_2, \ldots, m_n\}$ è un sistema di generatori per M.*

Dimostrazione. Definiamo $N := \langle m_1, m_2, \ldots, m_n \rangle$. Dalle ipotesi segue immediatamente che, se $i\colon N \to M$ è la mappa inclusione, allora la seguente composizione di applicazioni è suriettiva:

$$\pi \circ i\colon N \longrightarrow M \longrightarrow M/\mathfrak{m}M$$

Perciò, per ogni $m \in M$, esiste $n \in N$ tale che $m + \mathfrak{m}M = n + \mathfrak{m}M$, dunque $m - n = x$ per un opportuno elemento $x \in \mathfrak{m}M$ e in particolare $m \in \mathfrak{m}M + N$. Otteniamo allora che $\mathfrak{m}M + N = M$ e quindi, osservando che $\mathfrak{m} = \mathrm{Jac}(A)$, possiamo concludere, per il corollario 1.48, che $M = N$. □

Algebra commutativa (Matematica, Roma Tre) Oct 16, 2020

Lezione 11

Raffaele Di Donna

Successioni esatte e successioni esatte corte, lemma del serpente.

2 Successioni esatte

Definizione 2.1. Consideriamo una successione di A-moduli e omomorfismi di A-moduli:

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \longrightarrow \cdots$$

Una tale successione si dice *esatta in* M_i se $\operatorname{Ker} f_i = \operatorname{Im} f_{i-1}$ e viene detta *esatta* se è esatta in ciascun M_i.

Vediamo alcuni casi particolari della definizione:

(1) Una successione $0 \longrightarrow M \xrightarrow{\varphi} N$ è esatta se e solo se φ è un omomorfismo iniettivo di A-moduli.

(2) Una successione $M \xrightarrow{\psi} N \longrightarrow 0$ è esatta se e solo se ψ è un omomorfismo suriettivo di A-moduli.

(3) Una successione $0 \longrightarrow M \longrightarrow 0$ è esatta se e solo se $M = 0$.

(4) Una successione $0 \longrightarrow M \xrightarrow{\varphi} N \longrightarrow 0$ è esatta se e solo se φ è un isomorfismo di A-moduli.

(5) Una successione $0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$ è esatta se e solo se φ è un omomorfismo iniettivo di A-moduli, ψ è un omomorfismo suriettivo di A-moduli e vale $\operatorname{Ker} \psi = \operatorname{Im} \varphi$. Una successione esatta di questo tipo prende il nome di *successione esatta corta*.

Vediamo adesso alcuni esempi significativi di successioni esatte corte:

(A) Sia $f\colon M \to N$ un omomorfismo di A-moduli e sia $\bar{f}\colon M \to \operatorname{Im} f$ definito da $\bar{f}(m) := f(m)$. Allora, se consideriamo la mappa inclusione $i\colon \operatorname{Ker} f \to M$, abbiamo la seguente successione esatta corta:

$$0 \longrightarrow \operatorname{Ker} f \xhookrightarrow{i} M \xrightarrow{\bar{f}} \operatorname{Im} f \longrightarrow 0$$

(B) Sia M un A-modulo e sia N un sottomodulo di M. Consideriamo la mappa inclusione $i\colon N \to M$ e l'applicazione canonica di passaggio al quoziente $\pi\colon M \to M/N$. Si ha una successione esatta corta:

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

In particolare, se M e N sono due A-moduli qualsiasi e $f\colon M \to N$ è un omomorfismo di A-moduli allora, ricordando che $\operatorname{Coker} f = N/\operatorname{Im} f$, possiamo considerare la mappa inclusione $i\colon \operatorname{Im} f \to N$ e la mappa quoziente $\pi\colon N \to \operatorname{Coker} f$ e perciò abbiamo una successione esatta corta:

$$0 \longrightarrow \operatorname{Im} f \xhookrightarrow{i} N \xrightarrow{\pi} \operatorname{Coker} f \longrightarrow 0$$

Osservazione 2.2. Consideriamo una successione esatta:

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \longrightarrow \cdots$$

Dal punto (A) segue che possiamo ridurla a successioni esatte corte del tipo:

$$0 \longrightarrow \operatorname{Ker} f_i = \operatorname{Im} f_{i-1} \xhookrightarrow{} M_i \xrightarrow{} \operatorname{Ker} f_{i+1} = \operatorname{Im} f_i \longrightarrow 0$$

Questo spiega l'importanza delle successioni esatte corte.

Vediamo adesso un risultato fondamentale in algebra omologica.

Lemma 2.3 (Snake Lemma)**.** *Consideriamo un diagramma commutativo di omomorfismi di A-moduli:*

$$\begin{array}{ccccccccc} & & M & \xrightarrow{\varphi} & N & \xrightarrow{\psi} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & M' & \xrightarrow{\varphi'} & N' & \xrightarrow{\psi'} & P' & & \end{array}$$

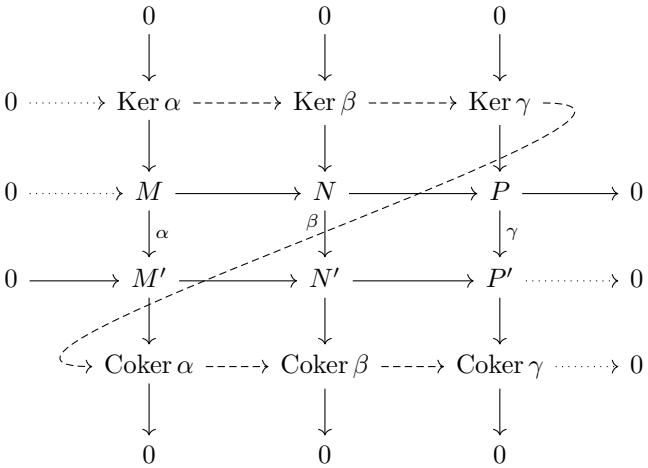
Supponiamo che le due righe del diagramma siano successioni esatte. Allora abbiamo una successione esatta:

$$\operatorname{Ker}\alpha \longrightarrow \operatorname{Ker}\beta \longrightarrow \operatorname{Ker}\gamma \longrightarrow \operatorname{Coker}\alpha \longrightarrow \operatorname{Coker}\beta \longrightarrow \operatorname{Coker}\gamma$$

Inoltre:

- *Se φ è un omomorfismo iniettivo, allora lo è anche la prima mappa della successione esatta trovata.*
- *Se ψ' è un omomorfismo suriettivo, allora lo è anche l'ultima mappa della successione esatta sopra.*

Prima di passare alla dimostrazione, vediamo che l'asserto dello Snake Lemma si esprime graficamente nel modo seguente. Completando gli omomorfismi di A-moduli verticali α, β e γ a successioni esatte corte come abbiamo fatto nell'esempio (B) precedente, si ottengono le frecce continue nel diagramma che segue:



Lo Snake Lemma garantisce l'esistenza della successione esatta indicata sopra con delle frecce tratteggiate. In particolare, il nome attribuito a questo risultato allude all'omomorfismo, probabilmente inaspettato, da $\operatorname{Ker}\gamma$ in $\operatorname{Coker}\alpha$. Le frecce punteggiate rappresentano poi le due asserzioni aggiuntive dello Snake Lemma: il diagramma si può leggere senza le frecce punteggiate, oppure omettendo quelle sulla sinistra o sulla destra.

Dimostrazione. Innanzitutto, costruiamo gli omomorfismi di A-moduli della successione:

$$\operatorname{Ker}\alpha \xrightarrow{\tilde{\varphi}} \operatorname{Ker}\beta \xrightarrow{\tilde{\psi}} \operatorname{Ker}\gamma \xrightarrow{\delta} \operatorname{Coker}\alpha \xrightarrow{\tilde{\varphi}'} \operatorname{Coker}\beta \xrightarrow{\tilde{\psi}'} \operatorname{Coker}\gamma$$

(a) *Le prime due mappe.* Definiamo $\tilde{\varphi}\colon \operatorname{Ker}\alpha \to \operatorname{Ker}\beta$ come l'omomorfismo di A-moduli ottenuto per restrizione di φ a $\operatorname{Ker}\alpha$, cioè definito da $\tilde{\varphi}(m) := \varphi(m)$. Si noti che la sua immagine è effettivamente contenuta in $\operatorname{Ker}\beta$ perché, dato un elemento $m \in \operatorname{Ker}\alpha$, per la commutatività del diagramma dato si ha:

$$\beta(\varphi(m)) = \varphi'(\alpha(m)) = 0$$

Allo stesso modo, si definisce $\tilde{\psi}\colon \operatorname{Ker}\beta \to \operatorname{Ker}\gamma$ come la restrizione di ψ a $\operatorname{Ker}\beta$.

(b) *Le ultime due mappe.* La mappa $\tilde{\varphi}'\colon \operatorname{Coker}\alpha \to \operatorname{Coker}\beta$ è indotta da φ per passaggio al quoziente, secondo il seguente diagramma:

$$\begin{array}{ccc} M' & \xrightarrow{\varphi} & N' \\ \downarrow & & \downarrow \\ \operatorname{Coker}\alpha & \xrightarrow{\tilde{\varphi}'} & \operatorname{Coker}\beta \end{array}$$

Precisamente, l'applicazione $\tilde{\varphi}'\colon \operatorname{Coker}\alpha \to \operatorname{Coker}\beta$ è definita da $\tilde{\varphi}'(m' + \operatorname{Im}\alpha) := \varphi'(m') + \operatorname{Im}\beta$. Tale definizione non dipende dalla scelta del rappresentante della classe laterale $m' + \operatorname{Im}\alpha$ in virtù dell'inclusione $\varphi'(\operatorname{Im}\alpha) \subseteq \operatorname{Im}\beta$, la quale è garantita dalla commutatività del diagramma. In effetti, per ogni $m \in M$, si ha:

$$\varphi'(\alpha(m)) = \beta(\varphi(m))$$

Similmente si definisce $\tilde{\psi}'\colon \operatorname{Coker}\beta \to \operatorname{Coker}\gamma$ ed è facile verificare che questi sono omomorfismi di A-moduli.

(c) *La mappa centrale δ.* L'esistenza di questa applicazione è la parte fondamentale di questo risultato. L'idea per la costruzione è schematizzata nel diagramma in basso: si prende un elemento nella fibra tramite ψ, poi l'immagine tramite β e infine di nuovo un elemento nella controimmagine tramite φ'.

$$\begin{array}{ccccccccc} & & M & \xrightarrow{\varphi} & N & \xrightarrow{\psi} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & M' & \xrightarrow[\varphi']{} & N' & \xrightarrow[\psi']{} & P' & & \end{array}$$

Più precisamente, fissiamo $p \in \operatorname{Ker}\gamma \subseteq P$. Poiché ψ è suriettiva, esiste un elemento $n \in N$ tale che $\psi(n) = p$. Sia ora $n' := \beta(n)$. Allora $n' \in \operatorname{Ker}\psi'$ perché, per la commutatività del diagramma, si ha:

$$\psi'(n') = \psi'(\beta(n)) = \gamma(\psi(n)) = \gamma(p) = 0$$

Ma $\operatorname{Ker}\psi' = \operatorname{Im}\varphi'$, perciò esiste $m' \in M'$ tale che $\varphi'(m') = n'$. Poniamo allora $\delta(p) := m' + \operatorname{Im}\alpha$. Dobbiamo accertarci che questa definizione sia indipendente dalla scelta delle due immagini inverse. Notiamo, a tal proposito, che la scelta di m' è univocamente determinata dal fatto che φ' è iniettivo. Supponiamo adesso di scegliere un elemento $\tilde{n} \in N$, eventualmente diverso da n, tale che $\psi(\tilde{n}) = p$ e poniamo $\tilde{n}' := \beta(\tilde{n})$. Come prima, si ha che $n' \in \operatorname{Ker}\psi' = \operatorname{Im}\varphi'$ e dunque esiste un unico elemento $\tilde{m}' \in M'$ tale che $\varphi'(\tilde{m}') = \tilde{n}'$. Dobbiamo dimostrare che $m' - \tilde{m}' \in \operatorname{Im}\alpha$. Notiamo allora che vale:

$$\begin{aligned} &\psi(\tilde{n} - n) = 0 \\ &\implies \tilde{n} - n \in \operatorname{Ker}\psi = \operatorname{Im}\varphi \\ &\implies \exists\, m \in M\colon \tilde{n} - n = \varphi(m) \end{aligned}$$

Per la commutatività del diagramma, ne segue che:

$$\varphi'(\tilde{m}' - m') = \tilde{n}' - n' = \beta(\tilde{n} - n) = \beta(\varphi(m)) = \varphi'(\alpha(m))$$

Dunque $\tilde{m}' - m' = \alpha(m)$ in quanto φ' è iniettivo. Abbiamo così ottenuto che m' e $\tilde{m}'$ definiscono la stessa classe laterale in $\operatorname{Coker}\alpha$ e perciò la mappa $\delta\colon \operatorname{Ker}\gamma \to \operatorname{Coker}\alpha$ è ben definita. Inoltre è facile verificare che δ è un omomorfismo di A-moduli. Infatti, basta ripercorrere la costruzione di δ e usare il fatto che ψ, β e φ' sono omomorfismi.

Ora, per dimostrare l'esattezza della successione, la tecnica da seguire è la stessa che abbiamo utilizzato per la costruzione dell'omomorfismo δ sopra: seguire gli elementi nel diagramma commutativo, una cosiddetta "caccia al diagramma". Per questo motivo, probabilmente il resto della dimostrazione non sarà interessante, ma lo tratteremo comunque per completezza.

- *Esattezza in* $\operatorname{Ker}\beta$. Sarà sufficiente mostrare, per doppia inclusione, che $\varphi(\operatorname{Ker}\alpha) = \operatorname{Ker}\psi \cap \operatorname{Ker}\beta$.

  ($\subseteq$) Per l'esattezza della prima riga del diagramma commutativo dato, abbiamo che $\operatorname{Ker}\psi = \operatorname{Im}\varphi$. Adesso l'inclusione $\varphi(\operatorname{Ker}\alpha) \subseteq \operatorname{Im}\varphi$ è banale e già sappiamo che $\varphi(\operatorname{Ker}\alpha) \subseteq \operatorname{Ker}\beta$ per quanto avevamo osservato nel punto (a) precedente.

  ($\supseteq$) Fissiamo un elemento $m' \in \operatorname{Ker}\psi \cap \operatorname{Ker}\beta = \operatorname{Im}\varphi \cap \operatorname{Ker}\beta$. In particolare, per qualche $m \in M$ si ha $m' = \varphi(m)$. Basta mostrare che $m \in \operatorname{Ker}\alpha$. Osserviamo allora che, per la commutatività del diagramma dato:
  $$0 = \beta(m') = \beta(\varphi(m)) = \varphi'(\alpha(m))$$
  Dunque, per iniettività di φ', otteniamo che $\alpha(m) = 0$.

- *Esattezza in* $\operatorname{Ker}\gamma$. Dimostriamo, di nuovo per doppia inclusione, che $\psi(\operatorname{Ker}\beta) = \operatorname{Ker}\delta$.

  ($\subseteq$) Sia $n \in \operatorname{Ker}\beta$ un elemento fissato e sia $p := \psi(n)$. Dobbiamo dimostrare che $\delta(p) = 0 + \operatorname{Im}\alpha$. Ma questa è una conseguenza della costruzione di δ: siccome $n' := \beta(n) = 0$ e φ' è iniettiva, se $m' \in M'$ è tale che $\varphi'(m') = n' = 0$, allora $m' = 0$.

  ($\supseteq$) Fissiamo $p \in \operatorname{Ker}\delta$. Riprendiamo di nuovo la costruzione di δ: esiste $n \in N$ tale che $p = \psi(n)$ e, posto $n' := \beta(n)$, esiste $m' \in M'$ tale che $\varphi'(m') = n'$. Adesso, se scegliamo $p \in \operatorname{Ker}\delta$, allora $m' \in \operatorname{Im}\alpha$, cioè esiste un elemento $m \in M$ tale che $m' = \alpha(m)$. Ora, per la commutatività del diagramma:
  $$\beta(n) = n' = \varphi'(m') = \varphi'(\alpha(m)) = \beta(\varphi(m))$$
  Dunque $n - \varphi(m) \in \operatorname{Ker}\beta$. A questo punto, usando il fatto che $\operatorname{Ker}\psi = \operatorname{Im}\varphi$, basta osservare che:
  $$\psi(n - \varphi(m)) = \psi(n) - \psi(\varphi(m)) = \psi(n) = p$$

- *Esattezza in* $\operatorname{Coker}\alpha$. Facciamo vedere, ancora per doppia inclusione, che $\operatorname{Im}\delta = \operatorname{Ker}\tilde{\varphi}'$.

  ($\subseteq$) Fissiamo $m' + \operatorname{Im}\alpha \in \operatorname{Im}\delta$. Allora $m' + \operatorname{Im}\alpha = \delta(p)$ per un qualche $p \in \operatorname{Ker}\gamma$ e, come sempre, dobbiamo riprendere la costruzione di δ: sappiamo che esiste $n \in N$ tale che $p = \psi(n)$ e che, se definiamo $n' := \beta(n)$, allora esiste un elemento $\tilde{m}' \in M'$ tale che $\varphi'(\tilde{m}') = n'$. Otteniamo così che $m' + \operatorname{Im}\alpha = \tilde{m}' + \operatorname{Im}\alpha$ e quindi, utilizzando il fatto che $n' \in \operatorname{Im}\beta$, si trova la condizione:
  $$\tilde{\varphi}'(m' + \operatorname{Im}\alpha) = \tilde{\varphi}'(\tilde{m}' + \operatorname{Im}\alpha) = n' + \operatorname{Im}\beta = 0 + \operatorname{Im}\beta$$

  ($\supseteq$) Sia fissato $m' + \operatorname{Im}\alpha \in \operatorname{Ker}\tilde{\varphi}'$. Allora $n' := \varphi'(m') \in \operatorname{Im}\beta$ e dunque esiste un elemento $n \in N$ tale che $n' = \beta(n)$. Osserviamo che, posto $p := \psi(n)$, per costruzione di δ possiamo concludere che $m' + \operatorname{Im}\alpha = \delta(p)$ se prima però dimostriamo che $p \in \operatorname{Ker}\gamma$. Per farlo, usiamo l'ipotesi di commutatività del diagramma e il fatto che $\operatorname{Ker}\psi' = \operatorname{Im}\varphi'$:
  $$\gamma(p) = \gamma(\psi(n)) = \psi'(\beta(n)) = \psi'(n') = \psi'(\varphi'(m')) = 0$$

- *Esattezza in* $\operatorname{Coker}\beta$. Sempre per doppio contenimento, dobbiamo dimostrare che $\operatorname{Im}\tilde{\varphi}' = \operatorname{Ker}\tilde{\psi}'$.

  ($\subseteq$) Se $n' + \operatorname{Im}\beta \in \operatorname{Im}\tilde{\varphi}'$, allora $n' + \operatorname{Im}\beta = \tilde{\varphi}'(m' + \operatorname{Im}\alpha)$ per qualche $m' \in M'$. Perciò, usando l'esattezza della seconda riga del diagramma in N', cioè il fatto che $\operatorname{Ker}\psi' = \operatorname{Im}\varphi'$, si ottiene:
  $$\begin{aligned}\tilde{\psi}'(n' + \operatorname{Im}\beta) &= \tilde{\psi}'(\tilde{\varphi}'(m' + \operatorname{Im}\alpha)) \\ &= \tilde{\psi}'(\varphi'(m') + \operatorname{Im}\beta) \\ &= \psi'(\varphi'(m')) + \operatorname{Im}\gamma = 0 + \operatorname{Im}\gamma\end{aligned}$$

($\supseteq$) Consideriamo un elemento $n' + \operatorname{Im}\beta \in \operatorname{Ker}\tilde{\psi}'$. Allora $\psi'(n') \in \operatorname{Im}\gamma$, ossia $\psi'(n') = \gamma(p)$ per qualche $p \in P$. Ma siccome ψ è suriettiva, possiamo scegliere $n \in N$ tale che $p = \psi(n)$ e allora, usando la commutatività del diagramma dato:

$$\begin{aligned} &\psi'(n' - \beta(n)) = \gamma(p) - \gamma(\psi(n)) = 0 \\ &\implies n' - \beta(n) \in \operatorname{Ker}\psi' = \operatorname{Im}\varphi' \\ &\implies \exists\, m' \in M' \colon n' - \beta(n) = \varphi'(m') \\ &\implies \tilde{\varphi}'(m' + \operatorname{Im}\alpha) = n' + \operatorname{Im}\beta \end{aligned}$$

Giustifichiamo infine le due asserzioni aggiuntive del lemma.

- *Iniettività di $\tilde{\varphi}$.* Poiché $\tilde{\varphi}$ è semplicemente una restrizione di φ, è evidente che $\tilde{\varphi}$ è iniettiva se φ lo è.
- *Suriettività di $\tilde{\psi}$.* Se ψ è suriettiva allora, per qualunque $p' \in P'$, esiste un elemento $n' \in N'$ tale che $\psi'(n') = p'$ e dunque $\tilde{\psi}'(n' + \operatorname{Im}\beta) = p' + \operatorname{Im}\gamma$. □

Osservazione 2.4. Sia $0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$ una successione esatta corta. Ci chiediamo se è possibile ricavare uno dei tre moduli conoscendo altri elementi della successione.

- Se sono noti M, N e $\varphi \colon M \to N$, allora per la suriettività di ψ, per il primo teorema di isomorfismo e per l'esattezza in N abbiamo che:

$$P = \operatorname{Im}\psi \simeq N/\operatorname{Ker}\psi = N/\operatorname{Im}\varphi$$

- Analogamente, se conosciamo N, P e $\psi \colon N \to P$, allora per l'iniettività di φ, per il primo teorema di isomorfismo e per l'esattezza in N si ha:

$$M = M/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi = \operatorname{Ker}\psi$$

La domanda più interessante è se possiamo determinare il modulo centrale N conoscendo M e P, ma nessun omomorfismo. I due esempi successivi mostrano che in generale questo non è possibile.

Esempio 2.5. Siano M e P due A-moduli. Consideriamo la mappa inclusione $\varphi \colon M \to M \oplus P$ definita da $\varphi(m) := (m, 0)$ e la proiezione canonica $\psi \colon M \oplus P \to P$ definita ponendo $\psi(m, p) := p$. Allora la seguente è una successione esatta corta:

$$0 \longrightarrow M \xhookrightarrow{\varphi} M \oplus P \xrightarrow{\psi} P \longrightarrow 0$$

Esempio 2.6. Sia p un numero primo. Consideriamo $\mathbb{Z}_p$ e $\mathbb{Z}_{p^2}$ come $\mathbb{Z}$-moduli, cioè come gruppi additivi. Siano $i \colon \mathbb{Z}_p \to \mathbb{Z}_{p^2}$ e $\pi \colon \mathbb{Z}_{p^2} \to \mathbb{Z}_p$ i due omomorfismi di gruppi definiti ponendo $i(\bar{x}) := \bar{p}\bar{x}$ e $\pi(\bar{x}) := \bar{x}$. Si ha allora una successione esatta corta[14]:

$$0 \longrightarrow \mathbb{Z}_p \xhookrightarrow{i} \mathbb{Z}_{p^2} \xrightarrow{\pi} \mathbb{Z}_p \longrightarrow 0$$

Adesso, se nell'esempio 2.5 prendiamo $M := P := \mathbb{Z}_p$, abbiamo anche la seguente successione esatta corta:

$$0 \longrightarrow \mathbb{Z}_p \xhookrightarrow{\varphi} \mathbb{Z}_p \oplus \mathbb{Z}_p \xrightarrow{\psi} \mathbb{Z}_p \longrightarrow 0$$

Tuttavia $\mathbb{Z}_p \oplus \mathbb{Z}_p$ non è isomorfo a $\mathbb{Z}_{p^2}$ perché non è un gruppo ciclico[15]. Questo dimostra che, in generale, il modulo centrale di una successione esatta corta non è univocamente determinato dagli altri due moduli.

[14] Questo fatto è dimostrato dettagliatamente nell'esempio 4.16 delle dispense del corso AL210.

[15] Ovviamente $\mathbb{Z}_{p^2}$ è invece un gruppo ciclico e quindi, per l'osservazione 1.18 delle dispense del corso AL210, i due gruppi non possono essere isomorfi. Per dimostrare che $\mathbb{Z}_p \oplus \mathbb{Z}_p$ non è un gruppo ciclico si può ragionare per assurdo utilizzando il fatto che $(\bar{0}, \bar{1}), (\bar{1}, \bar{1}) \in \mathbb{Z}_p \oplus \mathbb{Z}_p$ e ricordando che $\mathbb{Z}_p$ è un dominio di integrità.

Corollario 2.7. *Consideriamo un diagramma commutativo di omomorfismi di A-moduli:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\varphi} & N & \xrightarrow{\psi} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & M' & \xrightarrow{\varphi'} & N' & \xrightarrow{\psi'} & P' & \longrightarrow & 0 \end{array}$$

Supponiamo che le due righe del diagramma siano successioni esatte corte. Se due delle mappe α, β e γ sono isomorfismi di A-moduli, allora lo è anche la terza.

Dimostrazione. Per lo Snake Lemma, abbiamo una successione esatta:

$$0 \longrightarrow \operatorname{Ker}\alpha \longrightarrow \operatorname{Ker}\beta \longrightarrow \operatorname{Ker}\gamma \longrightarrow \operatorname{Coker}\alpha \longrightarrow \operatorname{Coker}\beta \longrightarrow \operatorname{Coker}\gamma \longrightarrow 0$$

Ora, se assumiamo per esempio che α e γ siano isomorfismi di A-moduli, allora $\operatorname{Ker}\alpha = \operatorname{Ker}\gamma = \operatorname{Coker}\alpha = \operatorname{Coker}\gamma = 0$ e la successione esatta diventa:

$$0 \longrightarrow 0 \longrightarrow \operatorname{Ker}\beta \longrightarrow 0 \longrightarrow 0 \longrightarrow \operatorname{Coker}\beta \longrightarrow 0 \longrightarrow 0$$

Quindi, per il caso particolare (3) visto a inizio lezione, dobbiamo avere $\operatorname{Ker}\beta = \operatorname{Coker}\beta = 0$, cioè anche β deve essere un isomorfismo. □

Algebra commutativa (Matematica, Roma Tre) Oct 20, 2020

Lezione 12

Raffaele Di Donna

Successioni esatte spezzanti. Prodotto tensoriale di moduli: definizione mediante la proprietà universale, dimostrazione esistenza e unicità.

Nella scorsa lezione abbiamo dimostrato il seguente risultato.

Corollario 2.7. *Consideriamo un diagramma commutativo di omomorfismi di A-moduli:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\varphi} & N & \xrightarrow{\psi} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & M' & \xrightarrow{\varphi'} & N' & \xrightarrow{\psi'} & P' & \longrightarrow & 0 \end{array}$$

Supponiamo che le due righe del diagramma siano successioni esatte corte. Se due delle mappe α, β e γ sono isomorfismi di A-moduli, allora lo è anche la terza.

Ricordiamo anche che, dati due A-moduli M e P, se consideriamo la mappa inclusione $i_M \colon M \to M \oplus P$ definita ponendo $i_M(m) := (m, 0)$ e la proiezione sulla seconda componente $\pi_P \colon M \oplus P \to P$, cioè la mappa definita da $\pi_P(m, p) := p$, allora la seguente è una successione esatta corta:

$$0 \longrightarrow M \xhookrightarrow{i_M} M \oplus P \xrightarrow{\pi_P} P \longrightarrow 0$$

Adesso vorremmo capire come fare per riconoscere le successioni esatte di questo tipo. Abbiamo il seguente risultato.

Proposizione 2.8. *Sia $0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$ una successione esatta corta. Allora le affermazioni che seguono sono equivalenti.*

(a) *Esiste un isomorfismo di A-moduli $f \colon N \to M \oplus P$ tale che sia commutativo il seguente diagramma di omomorfismi:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\varphi} & N & \xrightarrow{\psi} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_M} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}_P} & & \\ 0 & \longrightarrow & M & \xrightarrow{i_M} & M \oplus P & \xrightarrow{\pi_P} & P & \longrightarrow & 0 \end{array}$$

(b) *Esiste un omomorfismo di A-moduli $\alpha \colon N \to M$ tale che $\alpha \circ \varphi = \mathrm{id}_M$, cioè α è un'inversa a sinistra di φ.*

(c) *Esiste un omomorfismo di A-moduli $\beta \colon P \to N$ tale che $\psi \circ \beta = \mathrm{id}_P$, ovvero β è un'inversa a destra di ψ.*

Dimostrazione. Dimostriamo prima che (a) implica (b) e (c), per poi giustificare le implicazioni (b) $\Longrightarrow$ (a) e (c) $\Longrightarrow$ (a).

($\Downarrow_b$) Consideriamo la proiezione $\pi_M \colon M \oplus P \to M$ sulla prima componente, vale a dire l'omomorfismo di A-moduli dato da $\pi_M(m, p) := m$. Allora è del tutto evidente che π_M sia un'inversa a destra di i_M e inoltre, definendo $\alpha := \pi_M \circ f$, per la commutatività del diagramma dato nel punto (a) abbiamo:

$$\begin{aligned} \alpha \circ \varphi &= (\pi_M \circ f) \circ (\varphi \circ \mathrm{id}_M) \\ &= (\pi_M \circ f) \circ (f^{-1} \circ i_M) \\ &= \pi_M \circ i_M = \mathrm{id}_M \end{aligned}$$

($\Downarrow_c$) Questa implicazione si dimostra esattamente come la precedente. Infatti, basta porre $\beta := f^{-1} \circ i_P$, dove $i_P \colon P \to M \oplus P$ è la mappa inclusione definita da $i_P(p) := (0, p)$ e utilizzare la commutatività del diagramma.

($\Uparrow_b$) Sia $(\alpha, \psi) \colon N \to M \oplus P$ l'omomorfismo di A-moduli definito da $(\alpha, \psi)(n) := (\alpha(n), \psi(n))$. Allora è facile verificare che il seguente diagramma di omomorfismi è commutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\varphi} & N & \xrightarrow{\psi} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_M} & & \downarrow{\scriptstyle (\alpha,\psi)} & & \downarrow{\scriptstyle \mathrm{id}_P} & & \\ 0 & \longrightarrow & M & \xrightarrow{i_M} & M \oplus P & \xrightarrow{\pi_P} & P & \longrightarrow & 0 \end{array}$$

Per il corollario 2.7, possiamo concludere che (α, ψ) è un isomorfismo di A-moduli.

($\Uparrow_c$) Sia $(\varphi + \beta) \colon M \oplus P \to N$ l'applicazione definita da $(\varphi + \beta)(m, p) := \varphi(m) + \beta(p)$, che ovviamente è un omomorfismo di A-moduli. Si dimostra facilmente che il seguente diagramma di omomorfismi è commutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i_M} & M \oplus P & \xrightarrow{\pi_P} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_M} & & \downarrow{\scriptstyle (\varphi+\beta)} & & \downarrow{\scriptstyle \mathrm{id}_P} & & \\ 0 & \longrightarrow & M & \xrightarrow{\varphi} & N & \xrightarrow{\psi} & P & \longrightarrow & 0 \end{array}$$

Perciò, applicando il corollario 2.7, otteniamo che $(\varphi + \beta)$ è un isomorfismo di A-moduli. □

Definizione 2.9. Si dice che una successione esatta corta $0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$ *spezza* (oppure che *splitta*) se soddisfa una delle tre condizioni equivalenti della proposizione 2.8.

Non tutte le successioni esatte corte spezzano, come mostra il seguente esempio.

Esempio 2.10. Siano $i \colon \mathbb{Z}_p \to \mathbb{Z}_{p^2}$ e $\pi \colon \mathbb{Z}_{p^2} \to \mathbb{Z}_p$ gli omomorfismi di gruppi definiti ponendo $i(\bar{x}) := \bar{p}\bar{x}$ e $\pi(\bar{x}) := \bar{x}$. Allora questi omomorfismi definiscono una successione esatta corta che non spezza:

$$0 \longrightarrow \mathbb{Z}_p \xhookrightarrow{i} \mathbb{Z}_{p^2} \xrightarrow{\pi} \mathbb{Z}_p \longrightarrow 0$$

Nell'esempio 2.6 abbiamo infatti osservato che $\mathbb{Z}_{p^2}$ non è isomorfo a $\mathbb{Z}_p \oplus \mathbb{Z}_p$ e dunque non può mai valere il punto (a) della proposizione 2.8.

Vediamo infine cosa succede se consideriamo $\mathbb{K}$-spazi vettoriali anziché A-moduli qualsiasi.

Osservazione 2.11. Siano U, V, W tre $\mathbb{K}$-spazi vettoriali e sia $0 \longrightarrow U \xrightarrow{\varphi} V \xrightarrow{\psi} W \longrightarrow 0$ una successione esatta corta. Allora questa spezza sempre. Sia infatti $\{w_j\}_{j \in J}$ una base di W. Dato che ψ è suriettiva, per ogni $j \in J$ esiste un elemento $v_j \in V$ tale che $\psi(v_j) = w_j$. Possiamo allora definire $\beta \colon W \to V$ come l'unica applicazione lineare tale che $\beta(w_j) = v_j$ per ogni $j \in J$. Si verifica facilmente che la composizione $\psi \circ \beta$ fissa ogni elemento della base $\{w_j\}_{j \in J}$ e dunque $\psi \circ \beta = \mathrm{id}_W$, cioè β è un'inversa a destra di ψ. Si noti che β non è in generale l'inversa bilatera di ψ perché non è unica. La definizione di β dipende infatti dalla scelta degli elementi $v_j \in V$ al variare di $j \in J$ e questi non sono univocamente determinati perché ψ non è, in generale, un omomorfismo iniettivo.

3 Prodotto tensoriale

Definizione 3.1. Siano M, N, P tre A-moduli. Un'applicazione $f \colon M \times N \to P$ si dice A-*bilineare* se:

(1) Per ogni $m \in M$, la mappa $f(m, -) \colon N \to P$ definita da $f(m, -)(n) := f(m, n)$ è un omomorfismo di A-moduli.

(2) Per ogni $n \in N$, la mappa $f(-, n) \colon M \to P$ definita da $f(-, n)(m) := f(m, n)$ è un omomorfismo di A-moduli.

Inoltre, un omomorfismo di A-moduli è anche detto un'applicazione *A-lineare*.

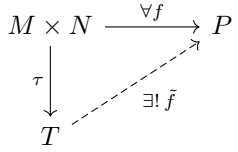
Osservazione 3.2. È importante notare che la nozione di applicazione A-bilineare non coincide, in generale, con quella di omomorfismo di A-moduli. Siano infatti M, N, P tre A-moduli e si consideri un'applicazione $f\colon M \times N \to P$. Siano inoltre $m \in M$, $n \in N$, $a \in A$ degli elementi fissati.

- Se f è un'applicazione A-bilineare, allora $af(m,n) = f(am,n) = f(m,an)$.
- Se f è un omomorfismo di A-moduli, allora $af(m,n) = f(a(m,n)) = f(am,an)$.

Definizione 3.3. Siano M e N due A-moduli. Una coppia (T,τ) dove T è un A-modulo e $\tau\colon M \times N \to T$ è un'applicazione A-bilineare si dice un *prodotto tensoriale di M e N rispetto ad A* se è soddisfatta la seguente proprietà universale:

$$\forall\, A\text{-modulo } P\,,\ \forall\, f\colon M \times N \to P \text{ applicazione } A\text{-bilineare}$$
$$\exists!\, \tilde{f}\colon T \to P \text{ omomorfismo di } A\text{-moduli tale che } \tilde{f} \circ \tau = f$$

In altre parole, ogni applicazione A-bilineare definita su $M \times N$ fattorizza in modo unico tramite τ. Questo fatto si può esprimere, equivalentemente, affermando che, per ogni A-modulo P, il seguente diagramma di omomorfismi è commutativo:



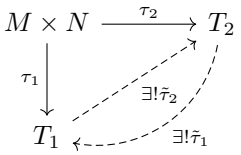
Osservazione 3.4. Un modo equivalente di definire un prodotto tensoriale di due A-moduli M e N è quello di richiedere che, per ogni A-modulo P, ci sia una corrispondenza biunivoca

$$\begin{array}{ccc} \{\text{Applicazioni } A\text{-bilineari da } M \times N \text{ in } P\} & \longleftrightarrow & \{\text{Omomorfismi di } A\text{-moduli da } T \text{ in } P\} \\ f & \longmapsto & \tilde{f} \\ g \circ \tau & \longmapsto & g \end{array}$$

Il prossimo risultato garantisce che una tale coppia (T,τ) è "unica a meno di isomorfismo" nel senso che andremo a precisare. E allora, nel seguito, non si parlerà più di *un* prodotto tensoriale di due A-moduli, bensì *del* prodotto tensoriale.

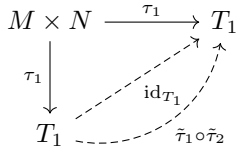
Teorema 3.5 (Unicità del prodotto tensoriale)**.** *Siano M e N due A-moduli. Se (T_1,τ_1) e (T_2,τ_2) sono due prodotti tensoriali di M e N rispetto ad A, allora esiste un unico isomorfismo di A-moduli $\varphi\colon T_1 \to T_2$ tale che $\tau_2 = \varphi \circ \tau_1$.*

Dimostrazione. Per definizione di prodotto tensoriale, l'applicazione $\tau_2\colon M \times N \to T_2$ è A-bilineare, perciò possiamo applicare la proprietà universale di (T_1,τ_1) prendendo $P := T_2$ e $f := \tau_2$. Otteniamo dunque che esiste un unico omomorfismo di A-moduli $\tilde{\tau}_2\colon T_1 \to T_2$ tale che $\tilde{\tau}_2 \circ \tau_1 = \tau_2$. Allo stesso modo, scambiando i ruoli dei prodotti tensoriali, abbiamo un unico omomorfismo di A-moduli $\tilde{\tau}_1\colon T_2 \to T_1$ tale che $\tilde{\tau}_1 \circ \tau_2 = \tau_1$. La situazione è descritta dal seguente diagramma di omomorfismi:



Per concludere la dimostrazione, basta far vedere che $\tilde{\tau}_1$ e $\tilde{\tau}_2$ sono l'una l'inversa dell'altra e definire $\varphi := \tilde{\tau}_2$. Applichiamo di nuovo la proprietà universale di (T_1,τ_1), stavolta scegliendo $P := T_1$ e $f := \tau_1$. Osserviamo

che, da una parte, abbiamo $\tilde{\tau}_1 \circ \tilde{\tau}_2 \circ \tau_1 = \tilde{\tau}_1 \circ \tau_2 = \tau_1$, ma al tempo stesso $\mathrm{id}_{T_1} \circ \tau_1 = \tau_1$, perciò $\tilde{\tau}_1 \circ \tilde{\tau}_2$ e id_{T_1} fanno entrambe commutare il seguente diagramma di omomorfismi:



Per l'unicità asserita dalla proprietà universale di (T_1, τ_1) si ottiene quindi che $\tilde{\tau}_1 \circ \tilde{\tau}_2 = \mathrm{id}_{T_1}$. Analogamente, sfruttando il fatto che $\tilde{\tau}_2 \circ \tilde{\tau}_1 \circ \tau_2 = \tilde{\tau}_2 \circ \tau_1 = \tau_2$ e applicando la proprietà universale di (T_2, τ_2), si dimostra che $\tilde{\tau}_2 \circ \tilde{\tau}_1 = \mathrm{id}_{T_2}$ e dunque la dimostrazione è conclusa. □

Ora invece dimostreremo che il prodotto tensoriale di due A-moduli esiste sempre. Per farlo, ne daremo una costruzione esplicita.

Teorema 3.6 (Esistenza del prodotto tensoriale)**.** *Siano M e N due A-moduli. Allora il prodotto tensoriale di M e N rispetto ad A esiste.*

Dimostrazione. Sia F la somma diretta di copie di A indicizzata dagli elementi di $M \times N$, cioè:

$$F := \bigoplus_{(m,n) \in M \times N} A$$

Sappiamo allora che F è un A-modulo. Se introduciamo la seguente notazione per gli elementi di F, vediamo che F è costituito da combinazioni lineari formali a coefficienti in A di elementi di $M \times N$:

$$\sum_{(m,n) \in M \times N} a(m,n) := \{a_{(m,n)}\}_{(m,n) \in M \times N}$$

Si osservi che, per definizione di somma diretta, i termini sommati sono non nulli per al più un numero finito di indici $(m,n) \in M \times N$ e dunque F è costituito, più precisamente, dalle combinazioni lineari formali *finite* a coefficienti in A di elementi di $M \times N$, cioè:

$$F = \Big\{ \sum_{i=1}^{k} a_i(m_i, n_i) \colon k \geq 1 \text{ intero}, a_i \in A, (m_i, n_i) \in M \times N \text{ per ogni } i = 1, 2, \ldots, k \Big\}$$

Osserviamo che, per definizione, le coppie $(m,n) \in M \times N$ sono tutte "indipendenti" in F. Per esempio, dati $a \in A, m \in M, n \in N$, le combinazioni lineari $a(m,n), 1(am,n), 1(m,an)$ sono, in generale, elementi diversi di F. Per costruire il prodotto tensoriale vogliamo perciò imporre determinate relazioni tra gli elementi di F che facciano diventare bilineari le combinazioni lineari formali. In particolare, vogliamo identificare le tre combinazioni lineari menzionate prima. Definiamo allora:

$$G := \left\langle \begin{array}{ll} 1(m+m',n) - 1(m,n) - 1(m',n), & 1(am,n) - a(m,n), \\ 1(m,n+n') - 1(m,n) - 1(m,n'), & 1(m,an) - a(m,n) \end{array} \;\middle|\; a \in A, m, m' \in M, n, n' \in N \right\rangle$$

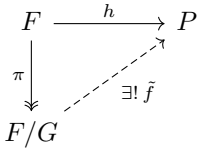
Poniamo $T := F/G$ e indichiamo con una barretta in alto la classe laterale rispetto a G di un elemento di F. Sia $\tau \colon M \times N \to T$ l'applicazione definita da $\tau(m,n) := \overline{1(m,n)}$. Allora τ è per costruzione un'applicazione A-bilineare. Infatti, per come è stato definito G abbiamo che, per esempio, per ogni $m, m' \in M, n \in N$, vale:

$$\tau(m+m',n) = \overline{1(m+m',n)} = \overline{1(m,n)} + \overline{1(m',n)} = \tau(m,n) + \tau(m',n)$$

A questo punto dobbiamo solo verificare che (T, τ) soddisfa la proprietà universale del prodotto tensoriale. Sia dunque P un A-modulo e sia $f \colon M \times N \to P$ un'applicazione A-bilineare. Consideriamo l'omomorfismo di A-moduli ausiliario $h \colon F \to P$ definito da:

$$h\Big(\sum_{i=1}^{k} a_i(m_i, n_i) \Big) := \sum_{i=1}^{k} a_i f(m_i, n_i)$$

Dal fatto che f è A-bilineare discende che $h(G) = 0$, cioè che $G \subseteq \operatorname{Ker} h$. Si può allora applicare la proprietà universale dei quozienti grazie alla quale abbiamo che, se $\pi\colon F \to F/G$ è la mappa quoziente, esiste un'unico omomorfismo di A-moduli $\tilde{f}\colon F/G \to P$ tale che $\tilde{f} \circ \pi = h$, ovvero tale che sia commutativo il diagramma di omomorfismi seguente[16]:



Inoltre, tale omomorfismo è definito da:

$$\tilde{f}\Big(\sum_{i=1}^{k} a_i\overline{(m_i, n_i)}\Big) := h\Big(\sum_{i=1}^{k} a_i(m_i, n_i)\Big) = \sum_{i=1}^{k} a_i f(m_i, n_i)$$

In particolare, otteniamo che $\tilde{f} \circ \tau = f$. Infine si verifica facilmente che, se $g\colon F/G \to P$ è un omomorfismo di A-moduli tale che $g \circ \tau = f$, allora $g = \tilde{f}$. Possiamo dunque concludere che (T, τ) è il prodotto tensoriale di M e N rispetto ad A. □

Definizione 3.7. Siano M e N due A-moduli. Sia inoltre (T, τ) il prodotto tensoriale di M e N rispetto ad A. Indichiamo T con la notazione $M \otimes_A N$ o più semplicemente con $M \otimes N$, se non vi è ambiguità. Inoltre, per ogni coppia $(m, n) \in M \times N$, chiamiamo *prodotto tensoriale di m e n* l'elemento $\tau(m, n)$, che denotiamo $m \otimes n$. Infine, chiamiamo *tensori* tutti gli elementi di $M \otimes_A N$ e diciamo che quelli della forma $m \otimes n$ sono *tensori puri* (o *semplici*).

Nel seguito, con un piccolo abuso di linguaggio, useremo l'espressione "prodotto tensoriale" per indicare anche la sola componente T della coppia (T, τ).

Osservazione 3.8. Nella dimostrazione del teorema di esistenza del prodotto tensoriale si vede che in generale non tutti i tensori in $M \otimes_A N$ sono puri. Ciò che vale sempre, invece, è che i tensori puri generano $M \otimes_A N$ come A-modulo. Questo perché ogni elemento di $M \otimes_A N$ è una combinazione lineare finita a coefficienti in A di tensori puri, cioè si scrive, per qualche intero $k \geq 1$ e per certi $a_1, a_2, \ldots, a_k \in A$, $m_1, m_2, \ldots, m_k \in M$, $n_1, n_2, \ldots, n_k \in N$, nel modo seguente:

$$\sum_{i=1}^{k} a_i(m_i \otimes n_i)$$

Si osservi però che questi generatori non sono "indipendenti" perché sono legati dalle relazioni che abbiamo imposto quando nella dimostrazione siamo passati al modulo quoziente rispetto al sottomodulo G. Vi sono dunque, in generale, molti modi diversi di esprimere un tensore come combinazione lineare di tensori puri e anche stabilire se due tali combinazioni lineari definiscono lo stesso tensore non è banale.

[16] Tale proprietà universale è stata dimostrata nel corso AL210 per la teoria dei gruppi, ma la dimostrazione per la teoria dei moduli è essenzialmente identica.

Lezione 13

Raffaele Di Donna

Isomorfismi canonici. Esempi di prodotti tensoriali.

Con i teoremi di esistenza e unicità del prodotto tensoriale visti nella scorsa lezione abbiamo dimostrato che, dati due A-moduli M e N, esiste sempre una coppia (T, τ), unica a meno di isomorfismo, tale che T sia un A-modulo, $\tau\colon M \times N \to T$ sia un'applicazione A-bilineare e tale che qualsiasi applicazione A-bilineare definita su $M \times N$ fattorizzi in modo unico tramite τ, nel senso che abbiamo specificato in modo più preciso nella definizione 3.3.

Ricordiamo che T si denota con $M \otimes_A N$ e che i tensori puri formano un sistema di generatori per T come A-modulo, in quanto ogni elemento di T è una combinazione lineare finita a coefficienti in A di tensori puri. Ora però facciamo alcune considerazioni.

Osservazione 3.9. Dalla costruzione esplicita vista nella dimostrazione del teorema di esistenza del prodotto tensoriale discendono immediatamente le seguenti proprietà:

(1) $(m + m') \otimes n = (m \otimes n) + (m' \otimes n)$ per ogni $m, m' \in M$, $n \in N$.

(2) $m \otimes (n + n') = (m \otimes n) + (m \otimes n')$ per ogni $m \in M$, $n, n' \in N$.

(3) $a(m \otimes n) = (am) \otimes n = m \otimes (an)$ per ogni $a \in A$, $m \in M$, $n \in N$.

Inoltre, l'applicazione $\tau\colon M \times N \to M \otimes_A N$ è quella definita dalla relazione $\tau(m, n) := m \otimes n$ ed è chiaro che le tre condizioni precedenti sono del tutto equivalenti a richiedere che τ sia un'applicazione A-bilineare.

Osserviamo che, in particolare, non vi è ambiguità nello scrivere $am \otimes n$ per indicare, indifferentemente, uno dei tre tensori della proprietà (3) precedente. Adesso vediamo alcune conseguenze dell'osservazione 3.9.

Osservazione 3.10. Prendendo $a := 0$ nella proprietà (3) precedente si ottiene che, per ogni $m \in M$, $n \in N$:

$$m \otimes 0 = 0 \otimes n = 0$$

Osservazione 3.11. Dalla proprietà (3) precedente segue che, inglobando tutti gli scalari nella prima o nella seconda componente dei tensori puri, ogni elemento di $M \otimes_A N$ si può scrivere come *somma* finita di tensori puri, cioè si può esprimere, per un qualche intero $k \geq 1$ e per certi $m_1, m_2, \ldots, m_k \in M$, $n_1, n_2, \ldots, n_k \in N$, nel modo seguente:

$$m_1 \otimes n_1 + m_2 \otimes n_2 + \cdots + m_k \otimes n_k$$

Riprendendo però quanto avevamo già accennato nell'osservazione 3.8, tale scrittura non è in generale unica, come suggeriscono le proprietà (1) e (2) precedenti. In generale, dunque, i tensori puri non formano una base di $M \otimes_A N$, cioè $M \otimes_A N$ non è un A-modulo libero.

Osservazione 3.12. Dalle proprietà menzionate nell'osservazione 3.9 segue anche che, se $\{m_i\}_{i \in I}$ e $\{n_j\}_{j \in J}$ sono sistemi di generatori per M e N rispettivamente, allora $\{m_i \otimes n_j\}_{i \in I, j \in J}$ è un sistema di generatori per il prodotto tensoriale $M \otimes_A N$. In particolare, se M e N sono finitamente generati, allora lo è anche $M \otimes_A N$.

Le due nozioni di applicazione A-bilineare e di prodotto tensoriale si generalizzano in modo naturale per coinvolgere non più due, bensì un qualsiasi numero finito di A-moduli, come viene meglio precisato nelle due definizioni che seguono.

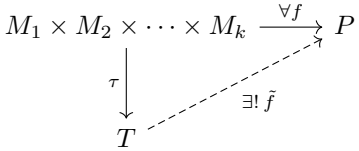
Definizione 3.13. Siano $M_1, M_2, \ldots, M_k, P$ degli A-moduli. Una mappa $f\colon M_1 \times M_2 \times \cdots \times M_k \to P$ si dice un'applicazione A-*multilineare* se è A-lineare in ogni variabile, cioè se, per ogni $i = 1, 2, \ldots, k$ e per ogni scelta di elementi $m_1, m_2, \ldots, m_{i-1}, m_{i+1}, \ldots, m_k \in M$, la seguente mappa è un omomorfismo di A-moduli:

$$\begin{aligned} M_i &\longrightarrow P \\ m_i &\longmapsto f(m_1, m_2, \ldots, m_{i-1}, m_i, m_{i+1}, \ldots, m_k) \end{aligned}$$

Definizione 3.14. Siano $M_1, M_2, \dots, M_k$ degli A-moduli. Una coppia (T, τ) nella quale T è un A-modulo e $\tau\colon M_1 \times M_2 \times \cdots \times M_k \to T$ è una mappa A-multilineare si dice un *prodotto tensoriale di* $M_1, M_2, \dots, M_k$ *rispetto ad* A se è soddisfatta la seguente proprietà universale:

$$\forall\, A\text{-modulo } P\,,\ \forall\, f\colon M_1 \times M_2 \times \cdots \times M_k \to P \text{ applicazione } A\text{-multilineare}$$
$$\exists!\, \tilde{f}\colon T \to P \text{ omomorfismo di } A\text{-moduli tale che } \tilde{f} \circ \tau = f$$

In altre parole, ogni applicazione A-multilineare definita su $M_1 \times M_2 \times \cdots \times M_k$ fattorizza in modo unico tramite τ. Questo fatto si può esprimere, equivalentemente, dicendo che, per ogni A-modulo P, il seguente diagramma di omomorfismi è commutativo:



Adattando le dimostrazioni dei teoremi di esistenza e unicità del prodotto tensoriale di due A-moduli si trovano gli stessi risultati per il prodotto tensoriale di un qualsiasi numero finito di A-moduli. In particolare, valgono osservazioni analoghe a quelle fatte all'inizio di questa lezione e possiamo anche fornire le seguenti notazioni.

Definizione 3.15. Siano $M_1, M_2, \dots, M_k$ degli A-moduli, (T, τ) il prodotto tensoriale di $M_1, M_2, \dots, M_k$ rispetto ad A. Indichiamo T con la notazione $M_1 \otimes_A M_2 \otimes_A \cdots \otimes_A M_k$ o anche con $M_1 \otimes M_2 \otimes \cdots \otimes M_k$, se non vi è ambiguità. Inoltre, per ogni tupla $(m_1, m_2, \dots, m_k) \in M_1 \times M_2 \times \cdots \times M_k$, chiamiamo *prodotto tensoriale di* $m_1, m_2, \dots, m_k$ l'elemento $\tau(m_1, m_2, \dots, m_k)$, che sarà denotato $m_1 \otimes m_2 \otimes \cdots \otimes m_k$. Infine, chiamiamo *tensori* gli elementi di $M_1 \otimes_A M_2 \otimes_A \cdots \otimes_A M_k$ e chiameremo *tensori puri* (o *semplici*) quelli della forma $m_1 \otimes m_2 \otimes \cdots \otimes m_k$.

Prima di fornire degli esempi espliciti di prodotti tensoriali, dimostriamo prima alcune semplici proprietà che renderanno più facile lo studio degli esempi.

Proposizione 3.16 (Isomorfismi canonici)**.** *Siano M, N, P tre A-moduli. Allora vi sono degli isomorfismi:*

(i) $M \otimes_A N \simeq N \otimes_A M$.

(ii) $(M \otimes_A N) \otimes_A P \simeq M \otimes_A N \otimes_A P \simeq M \otimes_A (N \otimes_A P)$.

(iii) $(M \oplus N) \otimes_A P \simeq (M \otimes_A P) \oplus (N \otimes_A P)$.

(iv) $A \otimes_A M \simeq M$.

Inoltre, i suddetti isomorfismi sono tali che, per ogni $a \in A$, $m \in M$, $n \in N$, $p \in P$, valga, rispettivamente:

(a) $m \otimes n \mapsto n \otimes m$.

(b) $(m \otimes n) \otimes p \mapsto m \otimes n \otimes p \mapsto m \otimes (n \otimes p)$.

(c) $(m, n) \otimes p \mapsto (m \otimes p, n \otimes p)$.

(d) $a \otimes m \mapsto am$.

Dimostrazione. La strategia da seguire sarà la stessa in tutti e quattro i casi: costruire degli omomorfismi di A-moduli tra i prodotti tensoriali applicando la proprietà universale a opportune applicazioni A-bilineari o A-multilineari e osservare che le mappe costruite sono le une le inverse delle altre.

(i) Sia $f\colon M \times N \to N \otimes_A M$ la mappa definita da $f(m,n) := n \otimes m$. Per l'osservazione 3.9, si tratta di un'applicazione A-bilineare. Applichiamo allora la proprietà universale del prodotto tensoriale, da cui segue l'esistenza di un omomorfismo di A-moduli $\tilde{f}\colon M \otimes_A N \to N \otimes_A M$ tale che, per ogni $m \in M$, $n \in N$, si abbia:

$$\tilde{f}(m \otimes n) = n \otimes m$$

Con un procedimento analogo, si costruisce un omomorfismo di A-moduli $\tilde{h}\colon N \otimes_A M \to M \otimes_A N$ tale che, per ogni $m \in M$, $n \in N$, si abbia:

$$\tilde{h}(n \otimes m) = m \otimes n$$

A questo punto basta osservare che l'applicazione composta $\tilde{h} \circ \tilde{f}$ fissa i tensori puri di $M \otimes_A N$, ma siccome questi generano $M \otimes_A N$ e $\tilde{h} \circ \tilde{f}$ è un omomorfismo, si deve avere che:

$$\tilde{h} \circ \tilde{f} = \mathrm{id}_{M \otimes_A N}$$

Analogamente si trova che $\tilde{f} \circ \tilde{h} = \mathrm{id}_{N \otimes_A M}$.

(ii) Sia $p \in P$ un elemento fissato e sia $f_p\colon M \times N \to M \otimes_A N \otimes_A P$ l'applicazione A-bilineare definita da $f_p(m,n) := m \otimes n \otimes p$. Applicando la proprietà universale del prodotto tensoriale, otteniamo un omomorfismo di A-moduli $\tilde{f}_p\colon M \otimes_A N \to M \otimes_A N \otimes_A P$ tale che, per ogni $m \in M$, $n \in N$, valga:

$$\tilde{f}_p(m \otimes n) = m \otimes n \otimes p$$

Si consideri ora l'unica applicazione A-bilineare $f\colon (M \otimes_A N) \times P \to M \otimes_A N \otimes_A P$ tale che, per ogni $m \in M$, $n \in N$, $p \in P$, valga $f(m \otimes n, p) = \tilde{f}_p(m \otimes n)$. Allora, per la proprietà universale del prodotto tensoriale, abbiamo un omomorfismo di A-moduli $\tilde{f}\colon (M \otimes_A N) \otimes_A P \to M \otimes_A N \otimes_A P$ tale che, per ogni $m \in M$, $n \in N$, $p \in P$, si abbia:

$$\tilde{f}((m \otimes n) \otimes p) = m \otimes n \otimes p$$

Adesso si consideri l'applicazione A-multilineare $g\colon M \times N \times P \to (M \otimes_A N) \otimes_A P$ definita dalla condizione $g(m,n,p) := (m \otimes n) \otimes p$. Di nuovo per la proprietà universale del prodotto tensoriale, tale applicazione induce un omomorfismo di A-moduli $\tilde{g}\colon M \otimes_A N \otimes_A P \to (M \otimes_A N) \otimes_A P$ tale che, per ogni $m \in M$, $n \in N$, $p \in P$, valga:

$$\tilde{g}(m \otimes n \otimes p) = (m \otimes n) \otimes p$$

A questo punto, come abbiamo già fatto nella dimostrazione del punto (i) precedente, si vede assai facilmente che $\tilde{f}$ e $\tilde{g}$ sono l'una l'inversa dell'altra perché le loro composizioni fissano tutti i tensori puri. Per dimostrare l'altro isomorfismo basta seguire un procedimento del tutto analogo.

(iii) Consideriamo l'applicazione A-bilineare $f\colon (M \oplus N) \times P \to (M \otimes_A P) \oplus (N \otimes_A P)$ definita dalla condizione $f((m,n),p) := (m \otimes p, n \otimes p)$. Per la proprietà universale del prodotto tensoriale, esiste un omomorfismo di A-moduli $\tilde{f}\colon (M \oplus N) \otimes_A P \to (M \otimes_A P) \oplus (N \otimes_A P)$ tale che, per qualsiasi $m \in M$, $n \in N$, $p \in P$, si abbia:

$$\tilde{f}((m,n) \otimes p) = (m \otimes p, n \otimes p)$$

Sia ora $\varphi\colon M \times P \to (M \oplus N) \otimes_A P$ l'applicazione A-bilineare data da $\varphi(m,p) := (m,0) \otimes p$. Essa induce un omomorfismo di A-moduli $\tilde{\varphi}\colon M \otimes_A P \to (M \oplus N) \otimes_A P$ tale che, per qualsiasi $m \in M$, $p \in P$, valga:

$$\tilde{\varphi}(m \otimes p) = (m,0) \otimes p$$

Analogamente possiamo costruire un omomorfismo di A-moduli $\tilde{\psi}\colon N \otimes_A P \to (M \oplus N) \otimes_A P$ tale che, per ogni $n \in N$, $p \in P$, si abbia:

$$\tilde{\psi}(n \otimes p) = (0,n) \otimes p$$

Sia adesso $\tilde{g}\colon (M \otimes_A P) \oplus (N \otimes_A P) \to (M \oplus N) \otimes_A P$ l'unico omomorfismo di A-moduli tale che, per ogni $m \in M$, $n \in N$, $p, q \in P$, si abbia:

$$\tilde{g}(m \otimes p, n \otimes q) = \tilde{\varphi}(m \otimes p) + \tilde{\psi}(n \otimes q) = (m, 0) \otimes p + (0, n) \otimes q$$

Osserviamo che $\tilde{g}$ è ben definita sui tensori in virtù del fatto che lo sono $\tilde{\varphi}$ e $\tilde{\psi}$. Per esempio, per ogni $m, m' \in M$, $n \in N$, $p, q \in P$, abbiamo che:

$$\tilde{g}((m + m') \otimes p, n \otimes q) = \tilde{g}(m \otimes p + m' \otimes p, n \otimes q)$$

Si vede facilmente che $\tilde{f}$ e $\tilde{g}$ sono l'una l'inversa dell'altra sfruttando il fatto che le loro composizioni fissano tutti i tensori puri.

(iv) Sia $f\colon A \times M \to M$ la mappa definita da $f(a, m) := am$. Allora f è un'applicazione A-bilineare per definizione di A-modulo. Per la proprietà universale del prodotto tensoriale, esiste un omomorfismo di A-moduli $\tilde{f}\colon A \otimes_A M \to M$ tale che, per ogni $a \in A$, $m \in M$, si abbia:

$$\tilde{f}(a \otimes m) = am$$

Consideriamo poi l'omomorfismo di A-moduli $\tilde{g}\colon M \to A \otimes_A M$ definito da $\tilde{g}(m) := 1 \otimes m$. Allora è facile verificare che $\tilde{f}$ e $\tilde{g}$ sono l'una l'inversa dell'altra usando ancora una volta il fatto che le loro composizioni fissano i tensori puri. □

Osservazione 3.17. Siano M e N due A-moduli liberi finitamente generati. Notiamo che M e N hanno rango finito per la proposizione 1.25. Se dunque k e h sono i ranghi di M e N rispettivamente, si ha che $M \simeq A^k$ mentre $N \simeq A^h$. Adesso, per gli isomorfismi canonici (iii) e (iv) forniti dalla proposizione 3.16, abbiamo che:

$$\begin{aligned} M \otimes_A N \simeq (\underbrace{A \oplus A \oplus \cdots \oplus A}_{k \text{ volte}}) \otimes_A A^h &\simeq (A \otimes_A A^h) \oplus (A \otimes_A A^h) \oplus \cdots \oplus (A \otimes_A A^h) \\ &\simeq A^h \oplus A^h \oplus \cdots \oplus A^h \simeq A^{kh} \end{aligned}$$

Abbiamo perciò ottenuto che $M \otimes_A N$ è un A-modulo libero, finitamente generato, con rango kh. Se inoltre consideriamo una base $\{m_i\}_{1 \le i \le k}$ di M e una base $\{n_j\}_{1 \le j \le h}$ di N, allora $\{m_i \otimes n_j\}_{1 \le i \le k, 1 \le j \le h}$ è una base di $M \otimes_A N$. Questo segue in modo naturale dalla costruzione degli isomorfismi canonici, che abbiamo visto nella dimostrazione della proposizione 3.16. Per definizione di base, abbiamo infatti i seguenti isomorfismi:

$$\begin{aligned} \phi_M\colon A^k &\longrightarrow M & \qquad \phi_N\colon A^h &\longrightarrow N \\ (x_1, x_2, \ldots, x_k) &\longmapsto \sum_{i=1}^{k} x_i m_i & \qquad (y_1, y_2, \ldots, y_h) &\longmapsto \sum_{j=1}^{h} y_j n_j \end{aligned}$$

Facciamo vedere che l'isomorfismo $\phi\colon A^{kh} \to M \otimes_A N$ ottenuto componendo gli isomorfismi come indicato implicitamente sopra è tale che:

$$\phi(a_{11}, a_{12}, \ldots, a_{1h}, a_{21}, a_{22}, \ldots, a_{2h}, \ldots, a_{k1}, a_{k2}, \ldots, a_{kh}) = \sum_{i=1}^{k} \sum_{j=1}^{h} a_{ij}(m_i \otimes n_j)$$

Poiché sappiamo già che ϕ è un omomorfismo di A-moduli è sufficiente mostrare che, per ogni $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, h$, l'uguaglianza sopra vale nel caso particolare in cui poniamo:

$$a_{rs} := \begin{cases} 1 & \text{se } r = i,\ s = j \\ 0 & \text{altrimenti} \end{cases}$$

Per fare questo, dobbiamo semplicemente ripercorrere gli isomorfismi canonici:

$$\begin{aligned}
&(a_{11}, a_{12}, \dots, a_{1h}, a_{21}, a_{22}, \dots, a_{2h}, \dots, a_{k1}, a_{k2}, \dots, a_{kh}) \\
&\longmapsto ((a_{11}, a_{12}, \dots, a_{1h}), (a_{21}, a_{22}, \dots, a_{2h}), \dots, (a_{k1}, a_{k2}, \dots, a_{kh})) \\
&\longmapsto (1 \otimes (a_{11}, a_{12}, \dots, a_{1h}), 1 \otimes (a_{21}, a_{22}, \dots, a_{2h}), \dots, 1 \otimes (a_{k1}, a_{k2}, \dots, a_{kh})) \\
&\longmapsto (1, 0, \dots, 0) \otimes (a_{11}, \dots, a_{1h}) + (0, 1, \dots, 0) \otimes (a_{21}, \dots, a_{2h}) + \cdots + (0, 0, \dots, 1) \otimes (a_{k1}, \dots, a_{kh}) \\
&\longmapsto m_i \otimes n_j
\end{aligned}$$

Per giustificare l'ultimo passaggio notiamo che tutte le tuple $(a_{r1}, a_{r2}, \dots, a_{rh})$ con $r \neq i$ sono nulle, mentre la tupla $(a_{i1}, a_{i2}, \dots, a_{ih})$ ha tutte le entrate nulle con l'eccezione della componente j-esima, che è 1. Perciò:

$$\begin{aligned}
&(1, 0, \dots, 0) \otimes (a_{11}, \dots, a_{1h}) + (0, 1, \dots, 0) \otimes (a_{21}, \dots, a_{2h}) + \cdots + (0, 0, \dots, 1) \otimes (a_{k1}, \dots, a_{kh}) \\
&= (0, 0, \dots, \underset{\substack{\uparrow \\ \text{posizione } i}}{1}, 0, \dots, 0) \otimes (0, 0, \dots, \underset{\substack{\uparrow \\ \text{posizione } j}}{1}, 0, \dots, 0)
\end{aligned}$$

Alla fine otteniamo il tensore puro $m_i \otimes n_j$ in quanto l'ultimo omomorfismo che definisce ϕ è indotto dagli isomorfismi ϕ_M e ϕ_N.

Si noti che, chiaramente, quanto abbiamo appena osservato vale anche nel caso più particolare in cui M e N sono $\mathbb{K}$-spazi vettoriali di dimensione finita.

Osservazione 3.18. Siano I e J due ideali coprimi di un anello A. Allora $A/I \oplus_A A/J = 0$. Infatti, se I e J sono coprimi, esistono due elementi $x \in I$, $y \in J$ tali che $x + y = 1$ e perciò, per ogni $a, b \in A$, abbiamo che:

$$\overline{a} \otimes \overline{b} = (x + y)(\overline{a} \otimes \overline{b}) = \overline{xa} \otimes \overline{b} + \overline{a} \otimes \overline{yb} = 0$$

Qui, allo scopo di semplificare la notazione, per indicare le classi laterali abbiamo adottato la notazione della barretta in alto. L'ultimo passaggio è giustificato dal fatto che $xa \in I$ mentre $yb \in J$. Avendo così ottenuto che i tensori puri di $A/I \oplus_A A/J$ sono tutti nulli, possiamo concludere che $A/I \oplus_A A/J = 0$ perché i tensori puri generano il prodotto tensoriale.

Esempio 3.19. Siano $m, n \geq 2$ interi coprimi. Sappiamo allora che gli ideali $m\mathbb{Z}$ e $n\mathbb{Z}$ di $\mathbb{Z}$ sono coprimi e dunque, per l'osservazione 3.18, abbiamo che $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n = 0$.

Esempio 3.20. Siano $m, n \geq 2$ interi. Calcoliamo $n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_m$. Sfruttando il fatto che la moltiplicazione per l'intero n è un isomorfismo tra $\mathbb{Z}$ e $n\mathbb{Z}$ e applicando l'isomorfismo canonico (iv) della proposizione 3.16, si ha:

$$n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_m \simeq \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_m \simeq \mathbb{Z}_m$$

Inoltre, per ogni $a, b \in \mathbb{Z}$, la composizione di tali isomorfismi manda il tensore puro $(na) \otimes b$ nella classe $\overline{ab}$.

Esempio 3.21. Calcoliamo in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2$ il tensore puro:

$$2 \otimes \overline{1} = 1 \otimes \overline{2} = 0$$

Tuttavia, se adesso consideriamo $2 \otimes \overline{1}$ come elemento di $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2$, il calcolo che abbiamo fatto non è valido in quanto $1 \notin 2\mathbb{Z}$. Ci chiediamo allora se sia ancora vero che $2 \otimes \overline{1} = 0$ in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2$. La risposta è negativa perché, come abbiamo visto nell'esempio 3.20 precedente, esiste un isomorfismo da $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2$ in $\mathbb{Z}_2$ e questo manda l'elemento $2 \otimes \overline{1}$ in $\overline{1}$, perciò dobbiamo avere $2 \otimes \overline{1} \neq 0$ in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2$.

La morale dell'esempio 3.21 è che, quando scriviamo dei tensori $m \otimes n$, dobbiamo fare sempre attenzione al prodotto tensoriale che stiamo considerando: se $n \in N$ e $m \in M'$ con M' sottomodulo di M, può accadere che il tensore puro $m \otimes n$ sia nullo nel prodotto tensoriale $M \otimes_A N$ ma al contempo non nullo in $M' \otimes_A N$.

Esercizio 3.22. Dimostrare che $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}$.

Svolgimento. Osserviamo innanzitutto che, per ogni $a, b, c, d \in \mathbb{Z}$ con $b, d \neq 0$, in $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ valgono le seguenti identità:

$$\frac{a}{b} \otimes \frac{c}{d} = \frac{ad}{bd} \otimes \frac{c}{d} = \frac{a}{bd} \otimes \frac{cd}{d} = \frac{a}{bd} \otimes c = \frac{ac}{bd} \otimes 1$$

In altre parole, ogni tensore puro si può esprimere nella forma $\alpha \otimes 1$ per un qualche $\alpha \in \mathbb{Q}$. Inoltre, quanto osservato ci suggerisce di considerare l'applicazione A-bilineare $f \colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ data da $f(\alpha, \beta) := \alpha\beta$. Per la proprietà universale del prodotto tensoriale, questa induce un omomorfismo di $\mathbb{Z}$-moduli $\tilde{f} \colon \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Q}$ tale che, per ogni $\alpha, \beta \in \mathbb{Q}$, si abbia:

$$\tilde{f}(\alpha \otimes \beta) = \alpha\beta$$

Per concludere, basta dimostrare che $\tilde{f}$ è un isomorfismo di $\mathbb{Z}$-moduli, cioè che è un omomorfismo iniettivo e suriettivo. Chiaramente $\tilde{f}$ è suriettivo, perché possiamo scrivere $\alpha = \alpha \cdot 1$ per ogni $\alpha \in \mathbb{Q}$. Ora, per mostrare che $\tilde{f}$ è anche iniettivo, osserviamo prima che, per ogni $\alpha, \beta \in \mathbb{Q}$, si ha:

$$\alpha \otimes 1 + \beta \otimes 1 = (\alpha + \beta) \otimes 1$$

Poiché abbiamo visto che ogni tensore puro è del tipo $\alpha \otimes 1$ per qualche $\alpha \in \mathbb{Q}$ e, per l'osservazione 3.11, ogni tensore si può esprimere come una somma finita di tensori puri, dalla relazione precedente segue che tutti i tensori di $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ sono della forma $\alpha \otimes 1$ per un qualche $\alpha \in \mathbb{Q}$. Per concludere che $\tilde{f}$ è una mappa iniettiva, basta perciò osservare che, per qualsiasi $\alpha \in \mathbb{Q}$, se $\tilde{f}(\alpha \otimes 1) = 0$, allora $\alpha = 0$ e quindi $\alpha \otimes 1 = 0$, cioè si ha che $\operatorname{Ker} \tilde{f} = 0$.

Algebra commutativa (Matematica, Roma Tre) Oct 23, 2020

Lezione 14

Raffaele Di Donna

Algebre e prodotti tensoriali di algebre.

3.1 Algebre

Sia $f\colon A \to B$ un omomorfismo di anelli. Allora B acquista una struttura di A-modulo rispetto al prodotto esterno che definiamo tramite il prodotto in B ponendo, per ogni $a \in A$, $b \in B$:

$$a \cdot b := f(a) \cdot b$$

Inoltre, per ogni $a \in A$, $b_1, b_2 \in B$, abbiamo che:

$$a(b_1 \cdot b_2) = (ab_1) \cdot b_2 = b_1 \cdot (ab_2)$$

In altre parole, il prodotto in B è un'applicazione A-bilineare. Queste considerazioni giustificano la seguente definizione.

Definizione 3.23. Un anello B dotato di una struttura di A-modulo rispetto alla quale il prodotto in B è un'applicazione A-bilineare viene detto una *A-algebra*.

Osservazione 3.24. Una A-algebra B è univocamente determinata da un omomorfismo di anelli $f\colon A \to B$. Infatti, si è già visto che un tale omomorfismo induce su B una struttura di A-algebra. Viceversa, se B è una A-algebra, allora possiamo definire un omomorfismo di anelli $f\colon A \to B$ ponendo $f(a) := a \cdot 1$ ed è evidente che questo omomorfismo induce su B la stessa struttura di A-algebra che si aveva in partenza. D'altra parte, se un omomorfismo di anelli $f\colon A \to B$ induce su B una struttura di A-algebra allora, per ogni $a \in A$, si avrà necessariamente $f(a) = a \cdot 1$.

Esempio 3.25. L'esempio più significativo di A-algebra è senza alcun dubbio quello fornito dall'anello di polinomi $A[X_1, X_2, \dots, X_n]$, a cui possiamo attribuire la struttura di A-algebra indotta dall'omomorfismo naturale che immerge gli elementi di A in $A[X_1, X_2, \dots, X_n]$ come polinomi costanti. Allo stesso modo, dato un qualsiasi ideale I di $A[X_1, X_2, \dots, X_n]$, l'anello quoziente $A[X_1, X_2, \dots, X_n]/I$ possiede una struttura di A-algebra.

Osservazione 3.26. Sia A un anello non nullo. Allora le tre seguenti condizioni sono equivalenti:

(i) Vale che A è un campo.

(ii) Gli unici ideali di A sono 0 e A.

(iii) Ogni omomorfismo da A in un anello non nullo B è iniettivo.

Dimostrazione. Facciamo vedere che (i) $\overset{1}{\Longrightarrow}$ (ii) $\overset{2}{\Longrightarrow}$ (iii) $\overset{3}{\Longrightarrow}$ (i).

(1) Basta osservare che, se I è un ideale non nullo di A, allora I contiene un elemento $x \neq 0$. Ma A è un campo, perciò x è invertibile e dunque $I = A$.

(2) Sia B un anello non nullo e sia $f\colon A \to B$ un omomorfismo di anelli. Allora $\operatorname{Ker} f$ è un ideale di A ed è diverso da A in quanto $f(1) = 1 \neq 0$. Per ipotesi si ha allora $\operatorname{Ker} f = 0$, ossia f è un omomorfismo iniettivo.

(3) Fissiamo un elemento $x \in A$ non invertibile e mostriamo che $x = 0$. Innanzitutto, si ha che $(x) \neq A$ e dunque $A/(x)$ è un anello non nullo. Sappiamo allora, per ipotesi, che mappa canonica di passaggio al quoziente $\pi\colon A \to A/(x)$ è un omomorfismo di anelli iniettivo. D'altra parte, sappiamo anche che $\operatorname{Ker}\pi = (x)$, perciò $x = 0$. □

Osservazione 3.27. Sia $\mathbb{K}$ un campo. Per l'osservazione 3.26 precedente, ogni omomorfismo da $\mathbb{K}$ in un anello non nullo B è iniettivo, perciò $\mathbb{K}$ può essere identificato in modo canonico con la sua immagine in B. Dunque una $\mathbb{K}$-algebra è un anello che contiene $\mathbb{K}$ come sottoanello.

Esempio 3.28. Come caso particolare dell'osservazione 3.27, possiamo affermare che $\mathbb{C}$ è una $\mathbb{R}$-algebra.

Osservazione 3.29. Sia A un anello. Allora esiste un unico omomorfismo di anelli $f\colon \mathbb{Z} \to A$. Infatti, si deve avere $f(1) = 1$ e di conseguenza $f(n) = n \cdot 1$ per ogni $n \in \mathbb{Z}$. Ne segue che ogni anello ha un'unica struttura di $\mathbb{Z}$-algebra.

Definizione 3.30. Siano B e C due A-algebre. Un omomorfismo di anelli $h\colon B \to C$ che sia al contempo un omomorfismo di A-moduli viene detto un *omomorfismo di A-algebre*.

Diamo ora una semplice caratterizzazione della nozione appena definita.

Osservazione 3.31. Siano B e C due A-algebre e sia $h\colon B \to C$ un omomorfismo di anelli. Siano $f\colon A \to B$ e $g\colon A \to C$ gli omomorfismi di anelli che inducono su B e su C le rispettive strutture di A-algebra. Allora h è un omomorfismo di A-algebre se e solo se $g = h \circ f$, cioè se e solo se il seguente diagramma di omomorfismi è commutativo:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow^{g} & \downarrow{\scriptstyle h} \\ & & C \end{array}$$

Infatti, abbiamo che h è un omomorfismo di A-algebre se e solo se valgono le seguenti condizioni equivalenti:

$$\begin{aligned} & h(a \cdot b) = a \cdot h(b) && \text{per ogni } a \in A,\, b \in B \\ \iff\ & h(f(a) \cdot b) = g(a) \cdot h(b) && \text{per ogni } a \in A,\, b \in B \\ \iff\ & h(f(a)) \cdot h(b) = g(a) \cdot h(b) && \text{per ogni } a \in A,\, b \in B \\ \iff\ & h(f(a)) = g(a) && \text{per ogni } a \in A \end{aligned}$$

L'ultima equivalenza è giustificata dal fatto che, per l'implicazione diretta, possiamo prendere $b = 1$, mentre per il viceversa basta moltiplicare a destra per $h(b)$.

Esempio 3.32. Sia $f\colon X \to Y$ un morfismo di insiemi algebrici con $X \subseteq \mathbb{A}^n(\mathbb{K})$ e $Y \subseteq \mathbb{A}^m(\mathbb{K})$. Sappiamo che questo induce una mappa:

$$\begin{aligned} f^*\colon \mathcal{A}(Y) &\longrightarrow \mathcal{A}(X) \\ [g] &\longmapsto [g \circ f] \end{aligned}$$

Abbiamo indicato le classi laterali con delle parentesi quadre per semplicità. Allora f^* è un omomorfismo di $\mathbb{K}$-algebre. Infatti, è facile vedere che si tratta di un omomorfismo di anelli. Ricordiamo poi che, per quanto abbiamo osservato nell'esempio 3.25, gli omomorfismi di anelli che inducono su $\mathcal{A}(Y)$ e su $\mathcal{A}(X)$ le rispettive strutture di $\mathbb{K}$-algebra sono quelli che mappano gli elementi di $\mathbb{K}$ nei corrispondenti polinomi costanti. Per l'osservazione 3.31 possiamo allora affermare che f^* è un omomorfismo di $\mathbb{K}$-algebre perché manda la classe laterale di un qualunque polinomio costante in $\mathcal{A}(Y)$ nella classe laterale del medesimo polinomio costante in $\mathcal{A}(X)$.

Definizione 3.33. Una A-algebra B si dice:

(1) *finita*, se B è un A-modulo finitamente generato.

(2) *finitamente generata*, se esistono degli elementi $b_1, b_2, \dots, b_n \in B$ tali che ogni elemento di B possa esprimersi come un polinomio in $b_1, b_2, \dots, b_n$ a coefficienti in A o, equivalentemente, se esistono un intero $n \geq 0$ e un omomorfismo suriettivo di A-algebre dall'anello di polinomi $A[X_1, X_2, \dots, X_n]$ in B. In tal caso, si scriverà $B = A[b_1, b_2, \dots, b_n]$.

Dimostriamo che le condizioni date nel punto (2) della definizione 3.33 sono effettivamente equivalenti.

($\Rightarrow$) Sia $f\colon A[X_1, X_2, \dots, X_n] \to B$ l'applicazione definita da $f(p(X_1, X_2, \dots, X_n)) := p(b_1, b_2, \dots, b_n)$. Si tratta ovviamente di un omomorfismo di anelli, ma è anche un omomorfismo di A-algebre. Questo perché, per l'esempio 3.25, l'omomorfismo di anelli che induce su $A[X_1, X_2, \dots, X_n]$ una struttura di A-algebra è quello che manda un elemento $a \in A$ nel polinomio costante p di valore a, il quale viene mandato da f nell'elemento $a = a \cdot 1$ di B. Ma $a \cdot 1$ è anche l'immagine di a tramite l'omomorfismo di anelli che induce su B la struttura di A-algebra data e dunque, per l'osservazione 3.31, possiamo concludere che f è un omomorfismo di A-algebre. Inoltre, si tratta di un omomorfismo suriettivo in quanto stiamo supponendo che ogni elemento di B possa esprimersi come polinomio in $b_1, b_2, \dots, b_n$ a coefficienti in A.

($\Leftarrow$) Per ipotesi, esistono un intero $n \geq 0$ e una mappa $f\colon A[X_1, X_2, \dots, X_n] \to B$ che è un omomorfismo suriettivo di A-algebre. Basta definire $b_i := f(X_i)$ per ogni $i = 1, 2, \dots, n$. Sia infatti $b \in B$ fissato. Poiché f è suriettivo, esiste un polinomio in $A[X_1, X_2, \dots, X_n]$ la cui immagine tramite f è b. Tale polinomio, per opportuni $a_{i_1, i_2, \dots, i_n} \in A$ non nulli per al più un numero finito di tuple $(i_1, i_2, \dots, i_n)$ di interi non negativi, avrà la forma:

$$\sum_{i_1, i_2, \dots, i_n \in \mathbb{N}} a_{i_1, i_2, \dots, i_n} X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$$

Dunque, grazie all'ipotesi che f sia un omomorfismo di A-algebre, otteniamo che b si esprime come polinomio in $b_1, b_2, \dots, b_n$ a coefficienti in A:

$$b = \sum_{i_1, i_2, \dots, i_n \in \mathbb{N}} a_{i_1, i_2, \dots, i_n} b_1^{i_1} b_2^{i_2} \dots b_n^{i_n}$$

Osservazione 3.34. La nozione di A-algebra finita è più forte di quella di A-algebra finitamente generata nel senso che, se B è una A-algebra finita, allora è finitamente generata. Questo perché, se $\{b_1, b_2, \dots, b_n\}$ è un sistema di generatori per B come A-modulo, allora ogni elemento di B si esprime come combinazione lineare degli elementi $b_1, b_2, \dots, b_n$ a coefficienti in A, ossia come polinomio di grado 1 in $b_1, b_2, \dots, b_n$ a coefficienti in A.

Riprendendo quanto avevamo anticipato nella lezione 7, facciamo vedere con un esempio che la nozione di A-algebra finita e quella di A-algebra finitamente generata non coincidono, cioè che non tutte le A-algebre finitamente generate sono finite.

Esempio 3.35. L'anello di polinomi $\mathbb{K}[X_1, X_2, \dots, X_n]$ è banalmente una $\mathbb{K}$-algebra finitamente generata, ma non è finita. Questo perché nell'esempio 1.14 avevamo dimostrato che $\mathbb{K}[X_1, X_2, \dots, X_n]$ non può essere finitamente generato come $\mathbb{K}$-modulo.

Esempio 3.36. L'anello dei numeri complessi $\mathbb{C}$ è una $\mathbb{R}$-algebra finita, mentre l'anello degli interi di Gauss $\mathbb{Z}[i]$ è una $\mathbb{Z}$-algebra finita. Infatti, l'insieme $\{1, i\}$ è un sistema finito di generatori sia per $\mathbb{C}$ come $\mathbb{R}$-modulo, sia per $\mathbb{Z}[i]$ come $\mathbb{Z}$-modulo.

3.2 Prodotto tensoriale di algebre

Siano B e C due A-algebre. Dal momento che B e C sono in particolare due A-moduli, possiamo considerarne il prodotto tensoriale $B \otimes_A C$, che per definizione è un A-modulo. Adesso è naturale chiedersi se sia possibile attribuire a $B \otimes_A C$ una struttura di A-algebra partendo da quelle già note su B e su C. In questa sezione vediamo che la risposta è affermativa.

Consideriamo la seguente applicazione:

$$\begin{aligned} B \times C \times B \times C &\longrightarrow B \otimes_A C \\ (b, c, b', c') &\longmapsto bb' \otimes cc' \end{aligned}$$

Si tratta di un'applicazione A-multilineare in virtù del fatto che, per definizione di A-algebra, il prodotto in B e il prodotto in C sono applicazioni A-bilineari. Per la proprietà universale del prodotto tensoriale esiste un omomorfismo di A-moduli $\alpha\colon B \otimes_A C \otimes_A B \otimes_A C \to B \otimes_A C$ tale che, per ogni $b, b' \in B$, $c, c' \in C$, valga:

$$\alpha(b \otimes c \otimes b' \otimes c') = bb' \otimes cc'$$

Si consideri inoltre l'isomorfismo canonico $\varphi\colon (B \otimes_A C) \otimes_A (B \otimes_A C) \to B \otimes_A C \otimes_A B \otimes_A C$ tale che, per ogni $b, b' \in B$, $c, c' \in C$, si abbia:

$$\varphi((b \otimes c) \otimes (b' \otimes c')) = b \otimes c \otimes b' \otimes c'$$

Infine, consideriamo la mappa A-bilineare $\tau\colon (B \otimes_A C) \times (B \otimes_A C) \to (B \otimes_A C) \otimes_A (B \otimes_A C)$ data dalla definizione di prodotto tensoriale la quale, per ogni $b, b' \in B$, $c, c' \in C$, soddisfa:

$$\tau(b \otimes c, b' \otimes c') = (b \otimes c) \otimes (b' \otimes c')$$

Allora la composizione $\alpha \circ \varphi \circ \tau$ definisce un'operazione binaria $\cdot$ su $B \otimes_A C$ che è A-bilineare e tale che, per ogni $b, b' \in B$, $c, c' \in C$, si abbia la condizione:

$$(b \otimes c) \cdot (b' \otimes c') = bb' \otimes cc'$$

In generale, scelti $b_1, b_2, \ldots, b_n, b'_1, b'_2, \ldots, b'_m \in B$, $c_1, c_2, \ldots, c_n, c'_1, c'_2, \ldots, c'_m \in C$, per A-bilinearità si ha:

$$\Big(\sum_{i=1}^{n} b_i \otimes c_i\Big) \cdot \Big(\sum_{j=1}^{m} b'_j \otimes c'_j\Big) = \sum_{i=1}^{n}\sum_{j=1}^{m} (b_i b'_j \otimes c_i c'_j)$$

Abbiamo così attribuito al prodotto tensoriale $B \otimes_A C$ una struttura di A-algebra.

Osservazione 3.37. Ci chiediamo quale sia l'omomorfismo di anelli $h\colon A \to B \otimes_A C$ che induce su $B \otimes_A C$ la struttura di A-algebra appena definita e quale relazione vi sia tra tale omomorfismo e gli omomorfismi di anelli $f\colon A \to B$, $g\colon A \to C$ che inducono su B e su C le rispettive strutture di A-algebra. Innanzitutto, si noti che l'elemento neutro per il prodotto in $B \otimes_A C$ è il tensore $1 \otimes 1$. Sappiamo allora che $h(a) = a(1 \otimes 1)$ per ogni $a \in A$. Quindi, per ogni $a \in A$, abbiamo che:

$$h(a) = f(a) \otimes 1 = 1 \otimes g(a)$$

Esempio 3.38. Sia A un anello. Vogliamo dimostrare che $A[X, Y] \simeq A[X] \otimes_A A[Y]$ come A-algebre, ossia che gli anelli di polinomi in più variabili si possono pensare come prodotti tensoriali di anelli di polinomi in una variabile. Per farlo, consideriamo innanzitutto la seguente mappa:

$$\begin{aligned} A[X] \times A[Y] &\longrightarrow A[X, Y] \\ (f, g) &\longmapsto fg \end{aligned}$$

Si tratta di un'applicazione A-bilineare perciò, per la proprietà universale del prodotto tensoriale, abbiamo un omomorfismo di A-moduli $\varphi\colon A[X] \otimes_A A[Y] \to A[X, Y]$ tale che, per ogni $f \in A[X]$, $g \in A[Y]$, si abbia:

$$\varphi(f \otimes g) = fg$$

Vogliamo ora costruire l'inversa di φ. Si consideri perciò la mappa $\psi\colon A[X, Y] \to A[X] \otimes_A A[Y]$ definita da:

$$\psi\Big(\sum_{i,j \in \mathbb{N}} a_{ij} X^i Y^j\Big) := \sum_{i,j \in \mathbb{N}} a_{ij} (X^i \otimes Y^j)$$

Si verifica facilmente che ψ è un omomorfismo di A-moduli. Ora, siccome $\{X^iY^j : i, j \in \mathbb{N}\}$ è un sistema di generatori per $A[X, Y]$ come A-modulo e $\{X^i \otimes Y^j : i, j \in \mathbb{N}\}$ è un sistema di generatori per $A[X] \otimes_A A[Y]$ come A-modulo, per far vedere che φ e ψ sono l'una l'inversa dell'altra basta osservare che, per ogni $i, j \in \mathbb{N}$:

$$(\psi \circ \varphi)(X^i \otimes Y^j) = X^i \otimes Y^j$$
$$(\varphi \circ \psi)(X^iY^j) = X^iY^j$$

Con questo abbiamo dimostrato che φ è un isomorfismo di A-moduli. Per concludere che è un isomorfismo di A-algebre, basta mostrare che è un omomorfismo di anelli. Ma questo è vero perché i tensori puri generano il prodotto tensoriale e, per ogni $f, f' \in A[X]$, $g, g' \in A[Y]$, si ha:

$$\varphi((f \otimes g) \cdot (f' \otimes g')) = \varphi(ff' \otimes gg') = ff'gg' = \varphi(f \otimes g)\varphi(f' \otimes g')$$

Algebra commutativa (Matematica, Roma Tre) Oct 27, 2020

Lezione 15

Raffaele Di Donna

Motivazioni per il concetto di localizzazione. Parti moltiplicative, anelli di frazioni, proprietà universale della localizzazione.

4 Localizzazione

La localizzazione è uno strumento molto potente in algebra commutativa perché permette spesso di ridurre le domande sugli anelli e sui moduli a una serie di problemi "locali" più facili da studiare. Può essere motivata sia da un punto di vista algebrico che da un punto di vista geometrico.

(a) *Motivazione algebrica.* Sia A un anello che non è un campo. L'idea algebrica della localizzazione è quella di rendere invertibili più elementi non nulli di A introducendo le frazioni, allo stesso modo in cui si passa dall'anello degli interi $\mathbb{Z}$ a quello dei numeri razionali $\mathbb{Q}$.

Studiamo in modo più preciso questo caso particolare. Sia dunque $S := \mathbb{Z}\setminus\{0\}$ l'insieme di tutti gli interi che vorremmo rendere invertibili. Definiamo una relazione di equivalenza su $\mathbb{Z}\times S$ ponendo $(a,s)\sim(a',s')$ se $as'-a's=0$. Dobbiamo verificare che si tratta effettivamente di una relazione di equivalenza. Le proprietà riflessiva e simmetrica sono del tutto banali, mentre la proprietà transitiva è più delicata, perciò la verifichiamo esplicitamente. Dati $a,a',a''\in\mathbb{Z}$, $s,s',s''\in S$, osserviamo che:

$$\begin{aligned} & as'-a's=0,\ a's''-a''s'=0 \\ \implies & s''(as'-a's)+s(a's''-a''s')=0 \\ \implies & s'(as''-a''s)=0 \\ \implies & as''-a''s=0 \end{aligned}$$

Nell'ultimo passaggio abbiamo usato il fatto che $\mathbb{Z}$ è un dominio di integrità e che $s'\neq 0$. La classe di equivalenza di una coppia $(a,s)\in\mathbb{Z}\times S$ si denota:

$$\frac{a}{s}$$

L'insieme quoziente viene invece indicato con $\mathbb{Q}$. Sappiamo che $\mathbb{Q}$ acquista una struttura di anello, o meglio di campo, rispetto alle due operazioni seguenti[17]:

$$\frac{a}{s}+\frac{a'}{s'}:=\frac{as'+a's}{ss'}\,,\qquad \frac{a}{s}\cdot\frac{a'}{s'}:=\frac{aa'}{ss'}$$

(b) *Motivazione geometrica.* Sia $X\subseteq\mathbb{A}^n(\mathbb{K})$ un insieme algebrico e sia $A:=\mathcal{A}(X)$, cioè A è l'anello delle funzioni polinomiali su X. Il nostro obiettivo è considerare quozienti di funzioni polinomiali, ovvero funzioni razionali su X. Osserviamo che, date due funzioni polinomiali $f,g\in A$, la seguente funzione non è in generale ben definita:

$$\begin{aligned} X &\longrightarrow \mathbb{K} \\ x &\longmapsto \frac{f(x)}{g(x)} \end{aligned}$$

[17] Bisognerebbe mostrare che tali operazioni sono ben definite, ma lo faremo nel seguito in un contesto più generale. Per la dimostrazione del fatto che $\mathbb{Q}$ è un campo, si rimanda invece alla proposizione 8.2 delle dispense del corso AL210, che fornisce un risultato più generale.

Questo perché il denominatore g potrebbe annullarsi su qualche punto di X. Se consideriamo però funzioni su sottoinsiemi di X opportuni, allora tali frazioni possono essere ben definite. L'esempio più importante dal punto di vista della localizzazione è il seguente: per un punto fissato $a \in X$, sia S l'insieme di tutte le funzioni polinomiali su X che non si annullano in a, cioè:

$$S := \{g \in A \colon g(a) \neq 0\}$$

Allora la funzione f/g con $f \in A$ e $g \in S$ è ben definita in a e dunque in un intorno di a, rispetto alla topologia indotta su X dalla topologia di Zariski, sufficientemente piccolo. Questo perché $a \notin \mathcal{V}(g)$, quindi a appartiene al complementare di $\mathcal{V}(g)$ in $\mathbb{A}^n(\mathbb{K})$, cioè a un aperto di $\mathbb{A}^n(\mathbb{K})$, la cui intersezione con X è un aperto di X. Parleremo perciò di "funzioni locali" in a. In effetti, è questa interpretazione geometrica ad aver dato origine al nome "localizzazione" per indicare il procedimento di costruzione di frazioni che discuteremo nel seguito.

Introduciamo adesso tali frazioni con un approccio rigoroso. Come prima, l'anello A sarà quello di partenza, mentre S sarà il sottoinsieme degli elementi di A che vogliamo rendere invertibili. Possiamo già osservare che una delle condizioni da richiedere su S è che sia chiuso rispetto alla moltiplicazione, perché altrimenti le due formule per l'addizione e il prodotto di frazioni non avrebbero senso. Si ha, in effetti, la seguente definizione.

Definizione 4.1. Sia A un anello. Un sottoinsieme S di A viene detto una *parte moltiplicativa di A* quando:

(1) Vale che $1 \in S$.

(2) L'insieme S è chiuso rispetto alla moltiplicazione, cioè $ab \in S$ per ogni $a, b \in S$.

Proposizione 4.2. *Sia S una parte moltiplicativa di A. Valgono allora le due seguenti proprietà:*

(i) *La relazione su $A \times S$ definita ponendo $(a, s) \sim (a', s')$ se esiste un elemento $u \in S$ tale che si abbia $u(as' - a's) = 0$ è una relazione di equivalenza.*

(ii) *Indichiamo la classe di equivalenza di una coppia $(a, s) \in A \times S$ con la notazione:*

$$\frac{a}{s}$$

Allora l'insieme quoziente, che denotiamo $S^{-1}A$, è un anello rispetto alle due operazioni che seguono:

$$\frac{a}{s} + \frac{a'}{s'} := \frac{as' + a's}{ss'}, \qquad \frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}$$

Definizione 4.3. Sia S una parte moltiplicativa di A. L'anello $S^{-1}A$ prende il nome di *anello delle frazioni di A rispetto a S*.

La principale differenza tra la nozione appena introdotta e quella già nota di campo dei quozienti è che, in generale, l'anello delle frazioni non è un campo. Prima di vedere la dimostrazione della proposizione 4.2, facciamo perciò la seguente considerazione.

Osservazione 4.4. Nell'anello $S^{-1}A$ abbiamo invertito ogni elemento di S. Infatti, per ogni $s \in S$, l'inverso di s è, come ci aspettiamo, l'elemento $1/s$. Non è detto però che gli elementi di A non nulli e non appartenenti a S siano invertibili in $S^{-1}A$ e quindi $S^{-1}A$ non è, in generale, un campo. Inoltre, alla luce di quanto appena osservato, può apparire strano il fatto che, nella definizione 4.1, non si escluda che $0 \in S$. In effetti, se $0 \in S$, allora ogni coppia $(a, s) \in A \times S$ è in relazione con $(0, 1)$ prendendo $u := 0$ e di conseguenza $S^{-1}A$ è l'anello banale. Non è dunque interessante considerare parti moltiplicative che contengono 0.

Dimostrazione (Proposizione 4.2).

(i) Le proprietà riflessiva e simmetrica sono ovvie, perciò dimostriamo che la relazione data è transitiva. Siano dunque $a, a', a'' \in A$, $s, s', s'' \in S$ degli elementi prefissati tali che, per certi $u, v \in S$, si abbia:

$$u(as' - a's) = 0\,,\ v(a's'' - a''s') = 0$$

Moltiplicando la prima equazione per vs'', la seconda per us e sommandole, otteniamo:

$$\begin{aligned} &uvs''(as' - a's) + uvs(a's'' - a''s') = 0 \\ \implies\ &uvs'(as'' - a''s) = 0 \end{aligned}$$

Usando il fatto che S è chiuso rispetto alla moltiplicazione, possiamo affermare che $uvs' \in S$ e quindi concludiamo che la relazione data è transitiva.

(ii) Dimostreremo soltanto che le due operazioni date sono ben definite, omettendo la facile verifica del fatto che queste conferiscono a $S^{-1}A$ una struttura di anello[18]. Consideriamo perciò degli elementi $a, a', a'' \in A$, $s, s', s'' \in S$ e facciamo vedere che:

$$\frac{a}{s} = \frac{a''}{s''} \implies \frac{as' + a's}{ss'} = \frac{a''s' + a's''}{s''s'}\,,\ \frac{aa'}{ss'} = \frac{a''a'}{s''s'}$$

Poiché supponiamo sempre che A sia un anello commutativo, scambiando i ruoli di a e a', di s e s', si troverà anche la condizione:

$$\frac{a'}{s'} = \frac{a''}{s''} \implies \frac{as' + a's}{ss'} = \frac{as'' + a''s}{ss''}\,,\ \frac{aa'}{ss'} = \frac{aa''}{ss''}$$

Per ipotesi, sappiamo dunque che esiste un elemento $u \in S$ tale che:

$$u(as'' - a''s) = 0$$

In particolare, abbiamo che:

$$\begin{aligned} u(aa's''s' - a''a'ss') &= ua's'(as'' - a''s) = 0 \\ u((as' + a's)s''s' - (a''s' + a's'')ss') &= u(s')^2(as'' - a''s) = 0 \end{aligned}$$

□

Potrebbe apparire sorprendente che la relazione di equivalenza data nel punto (i) della proposizione 4.2 non sia definita dalla condizione $as' - a's = 0$, bensì da $u(as' - a's) = 0$ per un certo $u \in S$. Diamo perciò una motivazione per l'introduzione dell'elemento $u \in S$. Come prima, possiamo adottare un punto di vista algebrico oppure geometrico.

(a) *Motivazione algebrica.* Senza l'elemento $u \in S$, la relazione non sarebbe transitiva. Questo perché, se prendiamo $u := v := 1$ nella dimostrazione precedente, allora possiamo concludere soltanto che:

$$s'(as'' - a''s) = 0$$

Nel caso particolare visto a inizio lezione per fornire una motivazione algebrica della localizzazione si considerava l'anello degli interi $\mathbb{Z}$, che è un dominio di integrità e questo ha permesso di semplificare l'elemento $s' \in S$, ma nel caso generale non è detto che tale $s' \in S$ non sia un divisore dello zero di A.

(b) *Motivazione geometrica.* Sia $X := \mathcal{V}(X_1X_2)$ in $\mathbb{A}^2(\mathbb{R})$, cioè X è l'unione dei due assi cartesiani come nella figura di seguito. Con un argomento simile a quello visto nello svolgimento dell'esercizio 1.30 si vede facilmente che (X_1X_2) è un ideale radicale di $\mathbb{R}[X_1, X_2]$ e dunque, per il teorema degli zeri di Hilbert, l'anello delle funzioni polinomiali su X è dato da $A := \mathbb{R}[X_1, X_2]/(X_1X_2)$. Osserviamo che le due funzioni $(x_1, x_2) \mapsto x_2$ e $(x_1, x_2) \mapsto 0$ coincidono in un intorno del punto $a := (1, 0)$, in quanto

[18] La dimostrazione è identica a quella usata per dimostrare che il campo dei quozienti è un anello, perciò rimandiamo alla proposizione 8.2 delle dispense del corso AL210.

coincidono nel complementare di $\mathcal{V}(X_1)$ in X, il quale è un aperto di X. Vorremmo perciò che queste funzioni definiscano una stessa funzione locale in a, cioè uno stesso elemento di $S^{-1}A$, dove poniamo:

$$S := \{g \in A \colon g(a) \neq 0\}$$

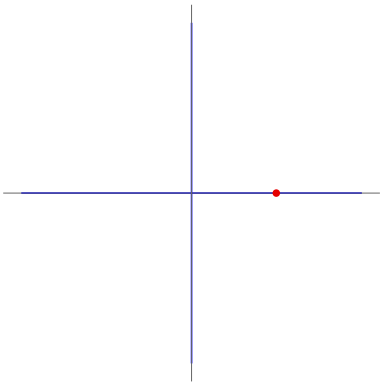
Senza l'elemento $u \in S$, questo sarebbe falso, perché $x_2 \cdot 1 - 0 \cdot 1 = x_2 \neq 0$ in A e di conseguenza in $S^{-1}A$ avremmo che:

$$\frac{x_2}{1} \neq \frac{0}{1}$$

Tuttavia, se possiamo scegliere $u := x_1 \in S$, allora otteniamo che $x_1(x_2 \cdot 1 - 0 \cdot 1) = x_1 x_2 = 0$ in A e dunque in $S^{-1}A$ vale che:

$$\frac{x_2}{1} = \frac{0}{1}$$

Nell'osservazione 4.4 abbiamo implicitamente identificato S con un sottoinsieme di $S^{-1}A$, considerando uguali gli elementi s e $s/1$. Adesso vogliamo rendere più preciso questo fatto con la seguente osservazione.



Osservazione 4.5. Sia $\varphi \colon A \to S^{-1}A$ la mappa definita dalla relazione:

$$\varphi(a) := \frac{a}{1}$$

Si verifica facilmente che φ è un omomorfismo di anelli.

Ci si aspetta che tale omomorfismo sia iniettivo come accade per la costruzione del campo dei quozienti[19], ma questo in generale non è vero per gli anelli di frazioni. Abbiamo infatti il seguente risultato.

Lemma 4.6. *L'omomorfismo φ è iniettivo se e solo se S non contiene divisori dello zero di A.*

Dimostrazione. Verifichiamo che valgono le due implicazioni.

($\Rightarrow$) Facciamo vedere che vale la contronominale. Se esiste un elemento $u \in S$ che è un divisore dello zero di A, allora $ua = 0$ per qualche $a \in A$ con $a \neq 0$. E di conseguenza φ non è iniettivo, perché vale che:

$$\varphi(a) = \frac{a}{1} = \frac{0}{1} = \varphi(0)$$

($\Leftarrow$) Fissiamo un elemento $a \in \operatorname{Ker} \varphi$. Per definizione, si ha allora $\varphi(a) = 0$, cioè:

$$\frac{a}{1} = \frac{0}{1}$$

Esiste quindi un elemento $u \in S$ tale che $ua = 0$ e, dato che per ipotesi S non contiene divisori dello zero di A, otteniamo $a = 0$. □

Possiamo ora riformulare l'osservazione 4.4 in modo più preciso come segue.

Osservazione 4.7. L'immagine tramite φ di S, cioè $\varphi(S)$, contiene solo elementi invertibili di $S^{-1}A$. Questo perché, per ogni $s \in S$, si ha:

$$\frac{1}{s} \cdot \frac{s}{1} = 1$$

Osservazione 4.8. A questo punto è chiaro che la nozione di anello delle frazioni generalizza quella di campo dei quozienti, che ritroviamo nel caso particolare in cui A è un dominio di integrità e scegliamo $S := A \setminus \{0\}$.

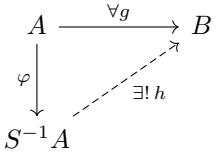
Vediamo infine che l'anello delle frazioni possiede una proprietà universale.

[19] Per maggiori dettagli, rimandiamo alla proposizione 8.3 delle dispense del corso AL210. Qui vediamo che il punto (i) non vale per gli anelli di frazioni e nel seguito generalizziamo la proprietà universale espressa dal punto (ii) dello stesso risultato.

Proposizione 4.9. *Sia S una parte moltiplicativa di A. Allora $S^{-1}A$ ha la seguente proprietà universale:*

$$\forall\, g\colon A \to B \text{ omomorfismo di anelli tale che } g(s) \text{ sia invertibile in } B \text{ per ogni } s \in S$$
$$\exists!\, h\colon S^{-1}A \to B \text{ omomorfismo di anelli tale che } g = h \circ \varphi$$

In altre parole, ogni omomorfismo di anelli definito su A fattorizza in modo unico tramite φ. Questo fatto si può esprimere, in modo equivalente, affermando che il seguente diagramma di omomorfismi è commutativo:



Dimostrazione. Dimostriamo prima l'unicità di un tale omomorfismo di anelli $h\colon S^{-1}A \to B$. Innanzitutto, dalla commutatività del diagramma segue che, per ogni $a \in A$, vale:

$$h\Big(\frac{a}{1}\Big) = h(\varphi(a)) = g(a)$$

D'altra parte, poiché si assume che h sia un omomorfismo di anelli, per ogni $a \in A$, $s \in S$, si ha la condizione:

$$h\Big(\frac{a}{s}\Big) = h\Big(\frac{a}{1} \cdot \frac{1}{s}\Big) = h\Big(\frac{a}{1}\Big) h\Big(\frac{s}{1}\Big)^{-1}$$

E allora h è univocamente determinato da g, tramite la relazione seguente:

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

Questo dimostra che h è unico e ci suggerisce anche come mostrarne l'esistenza. Definiamo infatti h a partire da g, tramite la condizione precedente. Dobbiamo far vedere che questa definizione non dipende dalla scelta di un rappresentante della frazione. Siano dunque $a, a' \in A$, $s, s' \in S$ tali che $u(as' - a's) = 0$ per un certo $u \in S$. Allora, applicando g a primo e secondo membro di tale identità, per le assunzioni fatte su g si ha che:

$$\begin{aligned} & g(u)(g(a)g(s') - g(a')g(s)) = 0 \\ \implies\ & g(a)g(s') - g(a')g(s) = 0 \\ \implies\ & g(a)g(s)^{-1} = g(a')g(s')^{-1} \end{aligned}$$

Questo dimostra che h è un'applicazione ben definita. Ora è facile verificare che h è un omomorfismo di anelli. Inoltre, tale omomorfismo rende commutativo il diagramma dato perché, per ogni $a \in A$, valgono le identità:

$$h(\varphi(a)) = h\Big(\frac{a}{1}\Big) = g(a)g(1)^{-1} = g(a)$$ □

Lezione 16

Raffaele Di Donna

Esempi di localizzazioni. Comportamento degli ideali rispetto alla localizzazione.

Vediamo adesso alcuni esempi di parti moltiplicative, quindi di anelli delle frazioni, di un dato anello A.

Esempio 4.10. Possiamo innanzitutto considerare la parte moltiplicativa banale $S = \{1\}$, quindi l'anello delle frazioni $S^{-1}A \simeq A$. In effetti, l'omomorfismo φ dell'osservazione 4.5 è, anche in virtù del lemma 4.6, un isomorfismo di anelli.

L'esempio seguente rende più preciso quanto già detto nell'osservazione 4.8.

Esempio 4.11. Sia S l'insieme degli elementi di A che non sono divisori dello zero. Abbiamo allora che S è una parte moltiplicativa di A perché 1 non è un divisore dello zero e, se $a, b \in A$ non sono divisori dello zero, nemmeno il loro prodotto ab lo è. Infatti, per ogni $c \in A$, si ha:

$$\begin{aligned} &(ab)c = 0 \\ \implies\ &a(bc) = 0 \\ \implies\ &bc = 0 \\ \implies\ &c = 0 \end{aligned}$$

Particolarmente significativo è il caso in cui A è un dominio di integrità e quindi $S = A\setminus\{0\}$. Infatti, l'anello delle frazioni $S^{-1}A$ diventa un campo, detto il *campo dei quozienti di* A, perché ogni suo elemento non nullo a/s è invertibile con inverso s/a. Il campo dei quozienti di A si denota Quot A.

Se inoltre T è una parte moltiplicativa di A e $0 \notin T$, allora $T^{-1}A$ si identifica in maniera naturale con un sottoanello di Quot A. Infatti, la mappa $f\colon T^{-1}A \to$ Quot A definita come segue è un omomorfismo iniettivo di anelli:

$$f\left(\frac{a}{t}\right) := \frac{a}{t}$$

Per dimostrarlo, bisogna innanzitutto osservare che è una mappa ben definita. Questo è vero per due motivi:

(1) Poiché $0 \notin T$, si ha $T \subseteq A\setminus\{0\}$ e quindi le frazioni a/t con $a \in A, t \in T$ sono ben definite in Quot A.

(2) Dati $a, a' \in A, t, t' \in T$ tali che $u(at' - a't) = 0$ per qualche $u \in T$, abbiamo anche $u \in A\setminus\{0\}$ grazie all'inclusione $T \subseteq A\setminus\{0\}$. Questo garantisce che f non dipende dalla scelta dei rappresentanti delle frazioni. In altre parole, se due frazioni sono uguali in $T^{-1}A$, allora esse coincidono anche in Quot A.

A questo punto si verifica facilmente che f è un omomorfismo di anelli. Facciamo vedere, piuttosto, che f è un'applicazione iniettiva. Consideriamo perciò degli elementi $a, a' \in A, t, t' \in T$ tali che in Quot A si abbia:

$$\frac{a}{t} = \frac{a'}{t'}$$

Allora $at' - a't = 0$ e dunque, siccome $1 \in T$ per definizione di parte moltiplicativa, le frazioni considerate sono uguali anche in $T^{-1}A$.

Esempio 4.12. Sia $a \in A$ un elemento fissato. Allora l'insieme $S := \{a^n\colon n \geq 0 \text{ intero}\}$ è chiaramente una parte moltiplicativa di A. In questo caso, l'anello $S^{-1}A$ si denota A_a e viene detto la *localizzazione di* A *in* a.

Esempio 4.13. Sia P un ideale primo di A. Osserviamo che l'insieme $S := A\setminus P$ è una parte moltiplicativa di A. Per definizione di ideale primo sappiamo infatti che, se $a, b \in A$ sono tali che $a \notin P$ e $b \notin P$, allora anche $ab \notin P$. Inoltre, gli ideali primi di A sono ideali propri e quindi $1 \notin P$. L'anello $S^{-1}A$ si indica, in questo caso, con la notazione A_P e viene detto la *localizzazione di* A *nell'ideale primo* P.

Vediamo ora alcuni esempi concreti di localizzazioni di anelli in un elemento o in un ideale primo.

Esempio 4.14 (Localizzazioni di $\mathbb{Z}$)**.** Consideriamo l'anello degli interi $\mathbb{Z}$. Sappiamo che $\mathbb{Z}$ è un dominio di integrità, perciò il campo dei quozienti di $\mathbb{Z}$ esiste e inoltre $\operatorname{Quot}\mathbb{Z} = \mathbb{Q}$ perché la costruzione del campo dei quozienti generalizza quella di $\mathbb{Q}$ a partire da $\mathbb{Z}$. Fissato invece $n \in \mathbb{Z}$, la localizzazione di $\mathbb{Z}$ in n è descritta da:

$$\mathbb{Z}_n = \left\{ \frac{a}{n^k} \colon a \in \mathbb{Z},\ k \geq 0 \text{ intero} \right\}$$

Dato invece un numero primo p, la localizzazione di $\mathbb{Z}$ nell'ideale primo (p) è descritta dal seguente insieme[20]:

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \colon a, b \in \mathbb{Z},\ p \text{ non divide } b \right\}$$

Per quanto si era osservato nell'esempio 4.11 questi sono entrambi, a meno di isomorfismo, sottoanelli di $\mathbb{Q}$. Si noti che qui $\mathbb{Z}_n$ non indica l'anello degli interi modulo n e quindi, per non creare confusione, da qui in poi per tale anello useremo preferibilmente la notazione $\mathbb{Z}/n\mathbb{Z}$.

Adesso vedremo che, nel caso dell'anello dei polinomi a coefficienti in un campo algebricamente chiuso, la localizzazione in un ideale primo è l'anello delle funzioni razionali definite in "quasi tutti i punti" dell'insieme degli zeri dell'ideale primo.

Esempio 4.15. Sia $\mathbb{K}$ un campo algebricamente chiuso e sia $A := \mathbb{K}[X_1, X_2, \ldots, X_n]$. La localizzazione di A in un ideale primo P sarà descritta da:

$$A_P = \left\{ \frac{f}{g} \colon f, g \in A,\ g \notin P \right\}$$

Sia inoltre $X := \mathcal{V}(P)$. Mostriamo che A_P è l'anello delle funzioni razionali definite su un aperto denso di X. Da una parte, dati $f, g \in A$, è chiaro che:

$$\begin{aligned} & g \in P \\ & \implies g \in \mathcal{I}(X) \\ & \implies g(x) = 0 \text{ per ogni } x \in X \end{aligned}$$

Dunque la funzione razionale f/g non può essere definita su nessun aperto denso di X perché non è definita in alcun punto di X. Viceversa, supponiamo che $g \notin P$. Ci serviremo del teorema degli zeri di Hilbert, il quale garantisce che $\mathcal{I}(X) = P$. Abbiamo perciò:

$$\begin{aligned} & g \notin P \\ & \implies P \subsetneq P + (g) \\ & \implies X \cap \mathcal{V}(g) \subsetneq X \end{aligned}$$

Poiché l'inclusione è stretta, la funzione razionale f/g è definita su un aperto non vuoto di X. Ma sappiamo che, se P è un ideale primo di A, allora X è irriducibile e, in particolare, ogni aperto non vuoto di X è denso[21]. Concludiamo perciò che f/g è definita su un aperto denso di X.

L'esempio che segue riprende l'esempio visto nella scorsa lezione quando abbiamo dato una motivazione geometrica della localizzazione.

Esempio 4.16. Sia $X \subseteq \mathbb{A}^n(\mathbb{K})$ un insieme algebrico e sia $A := \mathcal{A}(X)$. Sia inoltre $a \in X$ un punto fissato e sia $\mathfrak{m} := \mathcal{I}_{a/X}$. Sappiamo allora che $\mathfrak{m}$ è un ideale massimale di A e in particolare un ideale primo. Possiamo perciò considerare la localizzazione di A nell'ideale primo $\mathfrak{m}$. Essa è descritta dal seguente insieme:

$$A_{\mathfrak{m}} = \left\{ \frac{f}{g} \colon f, g \in A,\ g(a) \neq 0 \right\}$$

[20] Gli ideali primi di $\mathbb{Z}$ sono gli ideali principali generati da numeri primi. Ricordiamo infatti che l'anello $\mathbb{Z}$ è un dominio a ideali principali e che un elemento di un anello è primo se e solo se l'ideale principale da questo generato è un ideale primo.

[21] Questa proprietà è stata dimostrata negli appunti del corso GE410.

Per quanto abbiamo già osservato all'inizio della lezione precedente, quando abbiamo dato una motivazione della localizzazione da un punto di vista geometrico, l'anello $A_{\mathfrak{m}}$ è costituito dalle funzioni locali in a, ossia dalle funzioni razionali definite in a e dunque in un intorno sufficientemente piccolo di a.

Adesso che abbiamo esaminato diversi esempi, torniamo a studiare le proprietà degli anelli delle frazioni. Ci chiediamo, innanzitutto, come si comportano gli ideali rispetto alla localizzazione. La risposta è data dal seguente risultato. Nel seguito considereremo contrazioni ed estensioni di ideali mediante l'omomorfismo di anelli $\varphi\colon A \to S^{-1}A$ definito da:

$$\varphi(a) := \frac{a}{1}$$

Proposizione 4.17. *Sia S una parte moltiplicativa di A. Valgono allora le seguenti affermazioni.*

(i) *Per ogni ideale I di A, si ha:*

$$I^{\mathrm{e}} = \left\{ \frac{a}{s} \colon a \in I, s \in S \right\}$$

(ii) *Per ogni ideale J di $S^{-1}A$, si ha $(J^{\mathrm{c}})^{\mathrm{e}} = J$.*

(iii) *Esiste una corrispondenza biunivoca:*

$$\begin{array}{rcl} \{\textit{Ideali primi di } A \textit{ che non intersecano } S\} & \longleftrightarrow & \{\textit{Ideali primi di } S^{-1}A\} \\ I & \longmapsto & I^{\mathrm{e}} \\ J^{\mathrm{c}} & \longmapsfrom & J \end{array}$$

Dimostrazione.

(i) Basta dimostrare le due inclusioni.

($\subseteq$) Ricordiamo che I^{e} è per definizione il più piccolo ideale di $S^{-1}A$ che contiene $\varphi(I)$. Basta perciò osservare che l'insieme delle frazioni a/s con $a \in I$, $s \in S$ è un ideale di $S^{-1}A$ contenente $\varphi(I)$.

($\supseteq$) Siano $a \in I$, $s \in S$ degli elementi fissati. Allora:

$$\frac{a}{1} = \varphi(a) \in \varphi(I) \subseteq I^{\mathrm{e}}$$

Poiché I^{e} è un ideale di $S^{-1}A$, ne segue che:

$$\frac{a}{s} = \frac{1}{s} \cdot \frac{a}{1} \in I^{\mathrm{e}}$$

(ii) Procediamo di nuovo per doppio contenimento.

($\subseteq$) Questa inclusione vale anche sotto l'ipotesi che φ sia un omomorfismo di anelli qualsiasi e segue facilmente dalla definizione di estensione. Sappiamo infatti che J è un ideale e inoltre vale che:

$$\varphi(J^{\mathrm{c}}) = \varphi(\varphi^{-1}(J)) \subseteq J$$

($\supseteq$) Sia $a/s \in J$ un elemento fissato. Poiché supponiamo che J sia un ideale di $S^{-1}A$, abbiamo che:

$$\varphi(a) = \frac{a}{1} = \frac{a}{s} \cdot \frac{s}{1} \in J$$

Ma allora $a \in J^{\mathrm{c}}$ per definizione di contrazione e dunque $a/s \in (J^{\mathrm{c}})^{\mathrm{e}}$ per il punto (i) precedente.

(iii) Dobbiamo innanzitutto mostrare che le mappe indicate nell'enunciato sono ben definite, nel senso che le loro immagini sono contenute nei rispettivi codomini.

($\hookleftarrow$) Consideriamo un ideale primo J di $S^{-1}A$ e facciamo vedere che J^{c} è un ideale primo di A tale che $J^{\mathrm{c}} \cap S = \varnothing$. Già sappiamo, grazie al punto (i) dell'esercizio 1.35, che J^{c} è un ideale primo di A. Dimostriamo l'altra asserzione passando alla contronominale, ovvero supponiamo che esista un elemento $s \in J^{\mathrm{c}} \cap S$ e facciamo vedere che in tal caso J non è un ideale primo di $S^{-1}A$. Basta osservare che, da una parte, si ha $\varphi(s) \in J$ per definizione di contrazione, ma al contempo $\varphi(s)$ è un elemento invertibile di $S^{-1}A$ per l'osservazione 4.7 e quindi $J = S^{-1}A$ perché J è un ideale. Ma allora J non può essere un ideale primo di $S^{-1}A$, perché non è nemmeno un ideale proprio.

($\hookrightarrow$) Sia I un ideale primo di A tale che $I \cap S = \varnothing$. Dobbiamo far vedere che I^{e} è un ideale primo di $S^{-1}A$. Questo non è un fatto immediato come nel caso della contrazione perché sappiamo, per il punto (ii) dell'esercizio 1.35, che l'estensione di un ideale primo non è, in generale, un ideale primo. Siano dunque $a/s, b/t \in S^{-1}A$ tali che $ab/st \in I^{\mathrm{e}}$. Per il punto (i) precedente, esistono $c \in I$, $r \in S$ tali che:

$$\frac{ab}{st} = \frac{c}{r}$$

Esiste allora un elemento $u \in S$ tale che $u(abr - cst) = 0$ e in particolare $uabr = ucst \in I$. Ora, usando il fatto che I è un ideale primo di A e che $I \cap S = \varnothing$, otteniamo le implicazioni seguenti:

$$\begin{aligned} & u, r \in S \\ \implies\ & u, r \notin I \\ \implies\ & ur \notin I \\ \implies\ & ab \in I \\ \implies\ & a \in I \text{ oppure } b \in I \end{aligned}$$

Otteniamo perciò, per il punto (i) precedente, che $a/s \in I^{\mathrm{e}}$ oppure che $b/t \in I^{\mathrm{e}}$. Dobbiamo ora osservare che I^{e} è un ideale proprio di $S^{-1}A$. Lo facciamo vedere passando alla contronominale, cioè assumiamo che $I^{\mathrm{e}} = S^{-1}A$ e dimostriamo che $I \cap S$ è non vuoto. Per ipotesi, sappiamo in particolare che $1 \in I^{\mathrm{e}}$ e quindi, per il punto (i) precedente, esistono $a \in I$, $s \in S$ tali che valga:

$$\frac{1}{1} = \frac{a}{s}$$

Abbiamo allora $u(s - a) = 0$ per un opportuno $u \in S$ e in particolare $us = ua \in I$. Ma $us \in S$ perché S è una parte moltiplicativa, perciò $us \in I \cap S$. Concludiamo quindi che I^{e} è un ideale primo di $S^{-1}A$.

Ora dobbiamo soltanto mostrare che la corrispondenza è biunivoca. Per il punto (ii) precedente, già sappiamo che $(J^{\mathrm{c}})^{\mathrm{e}} = J$ per ogni ideale J di $S^{-1}A$, perciò basta mostrare che $(I^{\mathrm{e}})^{\mathrm{c}} = I$ per un fissato ideale primo I di A che non intersechi S. Per farlo, dimostriamo di nuovo un doppio contenimento.

($\supseteq$) Questa inclusione vale sotto l'ipotesi più generale che φ sia un omomorfismo di anelli qualsiasi e non usa il fatto che I sia un ideale primo di A, né che $I \cap S = \varnothing$. In effetti, basta osservare che:

$$(I^{\mathrm{e}})^{\mathrm{c}} = \varphi^{-1}(I^{\mathrm{e}}) \supseteq \varphi^{-1}(\varphi(I)) \supseteq I$$

($\subseteq$) Se fissiamo un elemento $a \in (I^{\mathrm{e}})^{\mathrm{c}}$, allora innanzitutto $\varphi(a) \in I^{\mathrm{e}}$ per definizione di contrazione. Equivalentemente, per il punto (i) precedente, sappiamo che esistono $b \in I$, $s \in S$ tali che valga:

$$\frac{a}{1} = \frac{b}{s}$$

Esiste allora un elemento $u \in S$ tale che $u(as - b) = 0$ e in particolare $uas = ub \in I$. Usando ora l'ipotesi che I sia un ideale primo di A e che $I \cap S = \varnothing$, otteniamo le seguenti implicazioni:

$$\begin{aligned} & u, s \in S \\ \implies\ & u, s \notin I \\ \implies\ & us \notin I \\ \implies\ & a \in I \end{aligned}$$

□

Osservazione 4.18. La corrispondenza biunivoca individuata al punto (iii) della proposizione 4.17 preserva le inclusioni. Se infatti I_1 e I_2 sono ideali di A con $I_1 \subseteq I_2$, allora si ha ovviamente $\varphi(I_1) \subseteq \varphi(I_2)$ e quindi, per definizione di estensione, abbiamo anche l'inclusione $I_1^{\mathrm{e}} \subseteq I_2^{\mathrm{e}}$. D'altra parte, se J_1 e J_2 sono ideali di $S^{-1}A$ con $J_1 \subseteq J_2$, allora $J_1^{\mathrm{c}} \subseteq J_2^{\mathrm{c}}$ banalmente, per definizione di contrazione. Per restrizione, si ha in particolare una corrispondenza biunivoca tra gli ideali primi di A che sono massimali tra quelli che non intersecano S, da non confondere con gli ideali massimali di A che non intersecano S, e gli ideali massimali di $S^{-1}A$.

Vediamo infine alcune conseguenze della proposizione 4.17.

Corollario 4.19. *Sia P un ideale primo di A. Allora esiste una corrispondenza biunivoca:*

$$\begin{array}{rcl} \{\textit{Ideali primi di } A \textit{ contenuti in } P\} & \longleftrightarrow & \{\textit{Ideali primi di } A_P\} \\ I & \longmapsto & I^{\mathrm{e}} \\ J^{\mathrm{c}} & \longmapsfrom & J \end{array}$$

Dimostrazione. Ricordiamo che $A_P = S^{-1}A$ dove $S := A \setminus P$ e osserviamo che, per ogni $I \subseteq A$, si ha $I \subseteq P$ se e solo se vale $I \cap S = \varnothing$. L'asserto è dunque un caso particolare del punto (iii) della proposizione 4.17. □

Osservazione 4.20. Sia P un ideale primo di A e sia $\pi\colon A \to A/P$ la mappa quoziente. È naturale confrontare il risultato che abbiamo appena ottenuto dal corollario 4.19 con la già nota corrispondenza biunivoca indotta da π:

$$\begin{array}{rcl} \{\text{Ideali primi di } A \text{ contenenti } P\} & \longleftrightarrow & \{\text{Ideali primi di } A/P\} \\ I & \longmapsto & \pi(I) \\ \pi^{-1}(J) & \longmapsfrom & J \end{array}$$

Corollario 4.21. *Sia P un ideale primo di A. Allora A_P è un anello locale il cui unico ideale massimale è P^{e}.*

Dimostrazione. Osserviamo che P è l'unico ideale primo di A massimale tra quelli contenuti in P. Dunque, per l'osservazione 4.18 e per il corollario 4.19, si può concludere che P^{e} è l'unico ideale massimale di A_P. □

Diamo anche una dimostrazione alternativa del risultato precedente.

Dimostrazione. Poiché P è un ideale primo di A contenuto in P, per il corollario 4.19 sappiamo che P^{e} è un ideale primo di A_P, quindi un ideale proprio. Per un risultato precedente, la conclusione segue dal fatto che qualunque elemento di $A_P \setminus P^{\mathrm{e}}$ è invertibile in A_P. Poniamo infatti $S := A \setminus P$. Allora, per il punto (i) della proposizione 4.17, un elemento di $A_P \setminus P^{\mathrm{e}}$ si può sempre scrivere come una frazione del tipo a/s con $a, s \notin P$, ovvero con $a, s \in S$. In particolare, possiamo considerare la frazione $s/a \in S^{-1}A$, che è l'inversa di a/s. □

Algebra commutativa (Matematica, Roma Tre) Nov 3, 2020

Lezione 18

Raffaele Di Donna

Esattezza del prodotto tensoriale.

4.1 Proprietà di esattezza del prodotto tensoriale

Lo scopo di questa sezione sarà capire come si comporta il prodotto tensoriale rispetto alle successioni esatte. Per farlo, dovremo prima studiare il comportamento del funtore $\mathrm{Hom}_A(-, N)$, dove N è un A-modulo fissato.

Osservazione 4.22. Sia N un A-modulo e sia $f\colon M \to M'$ un omomorfismo di A-moduli. Si vede facilmente che la seguente applicazione, associata a f mediante il funtore $\mathrm{Hom}_A(-, N)$, è un omomorfismo di A-moduli:

$$\begin{aligned} f^*\colon \mathrm{Hom}_A(M', N) &\longrightarrow \mathrm{Hom}_A(M, N) \\ g &\longmapsto g \circ f \end{aligned}$$

Nel linguaggio delle categorie, l'osservazione precedente si esprime dicendo che $\mathrm{Hom}_A(-, N)$ è un funtore controvariante. Il risultato che vedremo adesso ci dice invece che $\mathrm{Hom}_A(-, N)$ è un funtore esatto a sinistra.

Proposizione 4.23. *Consideriamo una successione $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$ di A-moduli e omomorfismi di A-moduli. Tale successione è esatta se e solo se, per qualsiasi A-modulo N, è esatta la seguente successione:*

$$0 \longrightarrow \mathrm{Hom}_A(M_3, N) \xrightarrow{f_2^*} \mathrm{Hom}_A(M_2, N) \xrightarrow{f_1^*} \mathrm{Hom}_A(M_1, N)$$

Dimostrazione. Dimostriamo le due implicazioni.

($\Leftarrow$) Sarà sufficiente dimostrare che la prima successione è esatta in M_2 e che f_2 è una mappa suriettiva.

- *Suriettività di f_2.* Per ipotesi, l'omomorfismo f_2^* è iniettivo per qualsiasi scelta di un A-modulo N. Poniamo allora $N := \mathrm{Coker}\, f_2$ e consideriamo la mappa quoziente $\pi\colon M_3 \to N$. Si noti che:

  $$f_2^*(\pi) = \pi \circ f_2 = 0$$

  Poiché f_2^* è iniettivo dobbiamo avere $\pi = 0$, ma questo implica che $\mathrm{Im}\, f_2 = M_3$ in quanto π è un omomorfismo suriettivo.

- *Esattezza in M_2.* Dobbiamo mostrare che $\mathrm{Ker}\, f_2 = \mathrm{Im}\, f_1$. Ragioniamo per doppia inclusione.

  ($\supseteq$) Poiché per ipotesi, per ogni A-modulo N, la seconda successione è esatta in $\mathrm{Hom}_A(M_2, N)$, per qualunque omomorfismo di A-moduli $g\colon M_3 \to N$ si ha:

  $$0 = f_1^*(f_2^*(g)) = f_1^*(g \circ f_2) = g \circ f_2 \circ f_1$$

  Scegliendo adesso $N := M_3$ e $g := \mathrm{id}_N$, otteniamo che $f_2 \circ f_1 = 0$, cioè che $\mathrm{Im}\, f_1 \subseteq \mathrm{Ker}\, f_2$.

  ($\subseteq$) Poniamo $N := \mathrm{Coker}\, f_1$ e consideriamo la mappa quoziente $\pi\colon M_2 \to N$. Allora abbiamo:

  $$\begin{aligned} & f_1^*(\pi) = \pi \circ f_1 = 0 \\ \implies & \pi \in \mathrm{Ker}\, f_1^* = \mathrm{Im}\, f_2^* \\ \implies & \exists\, g \in \mathrm{Hom}_A(M_3, N)\colon \pi = f_2^*(g) = g \circ f_2 \\ \implies & \mathrm{Ker}\, f_2 \subseteq \mathrm{Ker}\, \pi = \mathrm{Im}\, f_1 \end{aligned}$$

($\Rightarrow$) Bisogna mostrare che, fissato un A-modulo N, la seconda successione è esatta in $\mathrm{Hom}_A(M_2, N)$ e f_2^* è una mappa iniettiva.

- *Iniettività di f_2^*.* Sia $g \in \mathrm{Ker}\, f_2^*$ un omomorfismo di A-moduli fissato. Allora:

$$0 = f_2^*(g) = g \circ f_2$$

  Per ipotesi, sappiamo che f_2 è un omomorfismo suriettivo, perciò $\mathrm{Ker}\, g \supseteq \mathrm{Im}\, f_2 = M_3$ e quindi dobbiamo avere $g = 0$.

- *Esattezza in* $\mathrm{Hom}_A(M_2, N)$. Dimostriamo che $\mathrm{Ker}\, f_1^* = \mathrm{Im}\, f_2^*$. Procediamo ancora per doppia inclusione.

  ($\supseteq$) Dall'ipotesi che la prima successione sia esatta in M_2 segue che, per qualsiasi omomorfismo di A-moduli $g\colon M_3 \to N$, vale:

$$f_1^*(f_2^*(g)) = f_1^*(g \circ f_2) = g \circ f_2 \circ f_1 = 0$$

  Otteniamo perciò che $f_1^* \circ f_2^* = 0$, cioè che $\mathrm{Im}\, f_2^* \subseteq \mathrm{Ker}\, f_1^*$.

  ($\subseteq$) Sia $h \in \mathrm{Ker}\, f_1^*$ un omomorfismo di A-moduli. Allora abbiamo:

$$0 = f_1^*(h) = h \circ f_1$$

  Ne deduciamo che $\mathrm{Ker}\, h \supseteq \mathrm{Im}\, f_1 = \mathrm{Ker}\, f_2$. Si consideri adesso l'applicazione $g\colon M_3 \to N$ definita ponendo $g(x) := h(y)$ quando $y \in f_2^{-1}(x)$. Dobbiamo osservare che la definizione di g è ben posta. Ciò è vero perché, per ogni $y, y' \in M_2$, si hanno le seguenti implicazioni:

$$\begin{aligned} & f_2(y) = f_2(y') \\ \implies\ & y - y' \in \mathrm{Ker}\, f_2 \subseteq \mathrm{Ker}\, h \\ \implies\ & h(y) = h(y') \end{aligned}$$

  Inoltre, è facile verificare che g è un omomorfismo di A-moduli. Adesso basta osservare che:

$$\begin{aligned} & f_2^*(g)(y) = g(f_2(y)) = h(y) \text{ per ogni } y \in M_2 \\ \implies\ & f_2^*(g) = h \\ \implies\ & h \in \mathrm{Im}\, f_2^* \end{aligned}$$

□

Vediamo adesso con un controesempio che, se $0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$ è una successione esatta corta, allora non è detto che sia esatta corta anche la successione:

$$0 \longrightarrow \mathrm{Hom}_A(M_3, N) \xrightarrow{f_2^*} \mathrm{Hom}_A(M_2, N) \xrightarrow{f_1^*} \mathrm{Hom}_A(M_1, N) \longrightarrow 0$$

Questo perché se $f_1\colon M_1 \to M_2$ è un omomorfismo di A-moduli iniettivo allora, in generale, non è suriettivo l'omomorfismo di A-moduli f_1^* e, se $\pi\colon M_2 \to \mathrm{Coker}\, f_1$ è la mappa quoziente allora, per il primo teorema di isomorfismo, la seguente è una successione esatta corta:

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{\pi} \mathrm{Coker}\, f_1 \longrightarrow 0$$

Nella teoria delle categorie diciamo che il funtore $\mathrm{Hom}_A(-, N)$ non è esatto a destra e dunque non è esatto.

Esempio 4.24. Consideriamo $M_1 := M_2 := \mathbb{Z}$ come $\mathbb{Z}$-moduli, cioè come gruppi abeliani e l'omomorfismo di gruppi $f\colon \mathbb{Z} \to \mathbb{Z}$ definito ponendo $f(a) := na$ con $n \geq 2$ intero fissato. Scegliamo $N := \mathbb{Z}/n\mathbb{Z}$ e notiamo che, per qualunque omomorfismo di gruppi $g\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ e per ogni $a \in \mathbb{Z}$, abbiamo la condizione seguente:

$$f^*(g)(a) = g(f(a)) = g(na) = ng(a) = 0$$

Dunque f^* è l'applicazione nulla e non è un omomorfismo suriettivo perché $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}$ non è il gruppo nullo.

In maniera analoga, possiamo dimostrare che $\mathrm{Hom}_A(M, -)$, dove M è un A-modulo fissato, è un funtore covariante esatto a sinistra.

Osservazione 4.25. Sia M un A-modulo e sia $f\colon N \to N'$ un omomorfismo di A-moduli. Si vede facilmente che la seguente applicazione, associata a f mediante il funtore $\mathrm{Hom}_A(M, -)$, è un omomorfismo di A-moduli:

$$\begin{aligned} \bar{f}\colon \mathrm{Hom}_A(M, N) &\longrightarrow \mathrm{Hom}_A(M, N') \\ g &\longmapsto f \circ g \end{aligned}$$

Esercizio 4.26. Data una successione $0 \longrightarrow N_1 \xrightarrow{f_1} N_2 \xrightarrow{f_2} N_3$ di A-moduli e omomorfismi di A-moduli, abbiamo che tale successione è esatta se e solo se, per qualsiasi A-modulo M, è esatta la seguente successione:

$$0 \longrightarrow \mathrm{Hom}_A(M, N_1) \xrightarrow{\bar{f}_1} \mathrm{Hom}_A(M, N_2) \xrightarrow{\bar{f}_2} \mathrm{Hom}_A(M, N_3)$$

Svolgimento. Dimostriamo le due implicazioni.

($\Leftarrow$) Sarà sufficiente mostrare che la prima successione è esatta in N_2 e che f_1 è un'applicazione iniettiva.

- *Iniettività di f_1.* Sappiamo per ipotesi che f_1^* è iniettivo per qualsiasi scelta di un A-modulo N. Poniamo allora $M := \mathrm{Ker}\, f_1$ e consideriamo la mappa inclusione $i\colon M \to N_1$. Osserviamo che:

  $$f_1^*(i) = f_1 \circ i = 0$$

  Poiché f_1^* è iniettivo si deve avere $i = 0$, ma i è la mappa inclusione e quindi $\mathrm{Ker}\, f_1 = \mathrm{Im}\, i = 0$.
- *Esattezza in N_2.* Dobbiamo dimostrare che $\mathrm{Ker}\, f_2 = \mathrm{Im}\, f_1$. Ragioniamo per doppia inclusione.

  ($\supseteq$) Poiché per ipotesi, per ogni A-modulo M, la seconda successione è esatta in $\mathrm{Hom}_A(M, N_2)$, per qualunque omomorfismo di A-moduli $g\colon M \to N_1$ si ha:

  $$0 = \bar{f}_2(\bar{f}_1(g)) = \bar{f}_2(f_1 \circ g) = f_2 \circ f_1 \circ g$$

  Scegliendo adesso $M := N_1$ e $g := \mathrm{id}_M$, si ottiene che $f_2 \circ f_1 = 0$, cioè che $\mathrm{Im}\, f_1 \subseteq \mathrm{Ker}\, f_2$.

  ($\subseteq$) Definiamo $M := \mathrm{Ker}\, f_2$ e consideriamo la mappa inclusione $i\colon M \to N_2$. Allora abbiamo:

  $$\begin{aligned} &\bar{f}_2(i) = f_2 \circ i = 0 \\ &\implies i \in \mathrm{Ker}\, \bar{f}_2 = \mathrm{Im}\, \bar{f}_1 \\ &\implies \exists\, g \in \mathrm{Hom}_A(M, N_1)\colon i = \bar{f}_1(g) = f_1 \circ g \\ &\implies \mathrm{Ker}\, f_2 = \mathrm{Im}\, i \subseteq \mathrm{Im}\, f_1 \end{aligned}$$

($\Rightarrow$) Bisogna mostrare che, fissato un A-modulo M, la seconda successione è esatta in $\mathrm{Hom}_A(M, N_2)$ e $\bar{f}_1$ è una mappa iniettiva.

- *Iniettività di $\bar{f}_1$.* Sia $g \in \mathrm{Ker}\, \bar{f}_1$ un omomorfismo di A-moduli. Allora:

  $$0 = \bar{f}_1(g) = f_1 \circ g$$

  Stiamo supponendo che f_1 sia un omomorfismo iniettivo, perciò $\mathrm{Im}\, g \subseteq \mathrm{Ker}\, f_1 = 0$ e dunque si deve avere $g = 0$.
- *Esattezza in $\mathrm{Hom}_A(M_2, N)$.* Dimostriamo che $\mathrm{Ker}\, \bar{f}_2 = \mathrm{Im}\, \bar{f}_1$. Procediamo ancora per doppia inclusione.

  ($\supseteq$) Dall'ipotesi che la prima successione sia esatta in N_2 segue che, per qualsiasi omomorfismo di A-moduli $g\colon M \to N_1$, si ha:

  $$\bar{f}_2(\bar{f}_1(g)) = \bar{f}_2(f_1 \circ g) = f_2 \circ f_1 \circ g = 0$$

  Otteniamo perciò che $\bar{f}_2 \circ \bar{f}_1 = 0$, cioè che $\mathrm{Im}\, \bar{f}_1 \subseteq \mathrm{Ker}\, \bar{f}_2$.

($\subseteq$) Sia $h \in \operatorname{Ker} \bar{f}_2$ un omomorfismo di A-moduli fissato. Allora:

$$0 = \bar{f}_2(h) = f_2 \circ h$$

Ne deduciamo che $\operatorname{Im} h \subseteq \operatorname{Ker} f_2 = \operatorname{Im} f_1$. Si può perciò considerare la mappa $g\colon M \to N_1$ definita ponendo $g(x) := y$ quando $f_1(y) = h(x)$. Bisogna osservare che tale applicazione è ben posta perché un tale elemento y esiste grazie all'inclusione $\operatorname{Im} h \subseteq \operatorname{Im} f_1$ ed è unico per l'iniettività di f_1. Si vede facilmente che g è un omomorfismo di A-moduli. A questo punto basta osservare che:

$$\begin{aligned} &\bar{f}_1(g)(x) = f_1(g(x)) = h(x) \text{ per ogni } x \in M \\ &\implies \bar{f}_1(g) = h \\ &\implies h \in \operatorname{Im} \bar{f}_1 \end{aligned}$$

Possiamo vedere con un controesempio che, se $0 \longrightarrow N_1 \xrightarrow{f_1} N_2 \xrightarrow{f_2} N_3 \longrightarrow 0$ è una successione esatta corta, allora non è detto che sia esatta corta anche la successione:

$$0 \longrightarrow \operatorname{Hom}_A(M, N_1) \xrightarrow{\bar{f}_1} \operatorname{Hom}_A(M, N_2) \xrightarrow{\bar{f}_2} \operatorname{Hom}_A(M, N_3) \longrightarrow 0$$

Questo perché se $f_2\colon N_2 \to N_3$ è un omomorfismo di A-moduli suriettivo allora, in generale, non è suriettivo l'omomorfismo di A-moduli $\bar{f}_2$ e inoltre, se $i\colon \operatorname{Ker} f_2 \to N_2$ è la mappa inclusione allora, per il primo teorema di isomorfismo, la seguente è una successione esatta corta:

$$0 \longrightarrow \operatorname{Ker} f_2 \xrightarrow{i} N_2 \xrightarrow{f_2} N_3 \longrightarrow 0$$

Dunque, nel linguaggio delle categorie, anche il funtore $\operatorname{Hom}_A(M, -)$ non è esatto a destra e, in particolare, non è esatto.

Esempio 4.27. Consideriamo $N_1 := \mathbb{Z}$, $N_2 := \mathbb{Z}/n\mathbb{Z}$ come $\mathbb{Z}$-moduli, ossia come gruppi abeliani e fissiamo un omomorfismo di gruppi $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ qualsiasi, come per esempio la mappa quoziente. Sia $M := \mathbb{Z}/n\mathbb{Z}$. Si noti che $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$ è il gruppo nullo perché, se $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ è un omomorfismo di gruppi allora, per ogni $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$:

$$nf(\bar{a}) = f(n\bar{a}) = f(\bar{0}) = 0$$

Poiché $\mathbb{Z}$ è un dominio di integrità, dobbiamo avere $f(\bar{a}) = 0$. D'altra parte, il gruppo $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ è chiaramente non nullo perché contiene, per esempio, l'omomorfismo identità. Concludiamo perciò che $\bar{\pi}$ non è un omomorfismo suriettivo.

A questo punto vogliamo sfruttare l'esattezza a sinistra di $\operatorname{Hom}_A(-, N)$ per studiare il comportamento del funtore $- \otimes_A N$ rispetto alle successioni esatte, dove N è ancora un A-modulo fissato. Ci serviremo però del seguente risultato intermedio.

Lemma 4.28. *Siano M, N e P tre A-moduli. Allora esiste un isomorfismo canonico:*

$$\operatorname{Hom}_A(M \otimes_A N, P) \simeq \operatorname{Hom}_A(M, \operatorname{Hom}_A(N, P))$$

Dimostrazione. Definiamo innanzitutto una mappa $\varphi\colon \operatorname{Hom}_A(M \otimes_A N, P) \to \operatorname{Hom}_A(M, \operatorname{Hom}_A(N, P))$ in modo tale che φ risulti essere un omomorfismo di A-moduli. Sia dunque $\alpha\colon M \otimes_A N \to P$ un omomorfismo di A-moduli. Allora, per ogni $m \in M$, l'applicazione $\alpha(m \otimes -)\colon N \to P$ data da $\alpha(m \otimes -)(n) := \alpha(m \otimes n)$ è un omomorfismo di A-moduli in virtù del fatto che lo è α e che il prodotto tensoriale è A-bilineare. Possiamo ora considerare la mappa $\varphi(\alpha)\colon M \to \operatorname{Hom}_A(N, P)$ definita ponendo:

$$\varphi(\alpha)(m) := \alpha(m \otimes -)$$

Osserviamo che $\varphi(\alpha)$ è un'applicazione ben definita perché, per quanto detto prima, la mappa $\varphi(\alpha)(m)$ è un omomorfismo di A-moduli per ogni $m \in M$. Inoltre, è facile vedere che $\varphi(\alpha)$ è un omomorfismo di A-moduli,

perciò $\varphi\colon \alpha \mapsto \varphi(\alpha)$ è un'applicazione ben definita. Altrettanto facilmente si vede che φ è un omomorfismo di A-moduli.

Ora bisogna costruire un'applicazione $\psi\colon \mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P)) \to \mathrm{Hom}_A(M \otimes_A N, P)$ in modo tale che ψ sia l'inversa di φ. Sia allora $\beta\colon M \to \mathrm{Hom}_A(N,P)$ un omomorfismo di A-moduli. Si può considerare la seguente mappa:

$$\begin{aligned} M \times N &\longrightarrow P \\ (m,n) &\longmapsto \beta(m)(n) \end{aligned}$$

Si tratta di un'applicazione A-bilineare e quindi, per la proprietà universale del prodotto tensoriale, induce un omomorfismo di A-moduli $\psi(\beta)\colon M \otimes_A N \to P$ tale che, per ogni $m \in M$, $n \in N$, si abbia la condizione:

$$\psi(\beta)(m \otimes n) = \beta(m)(n)$$

Dunque la mappa $\psi\colon \beta \mapsto \psi(\beta)$ è ben definita. A questo punto, tenendo a mente che i tensori puri generano il prodotto tensoriale, è facile vedere che φ e ψ sono l'una l'inversa dell'altra e dunque abbiamo l'isomorfismo cercato. □

Prima di passare al risultato principale di questa sezione, ci sarà utile la seguente costruzione.

Osservazione 4.29. Siano $f\colon M \to N$ e $g\colon M' \to N'$ omomorfismi di A-moduli. Si consideri l'applicazione:

$$\begin{aligned} M \times M' &\longrightarrow N \otimes_A N' \\ (m,m') &\longmapsto f(m) \otimes g(m') \end{aligned}$$

Si tratta di una mappa A-bilineare e dunque essa induce, per la proprietà universale del prodotto tensoriale, un unico omomorfismo di A-moduli $f \otimes g\colon M \otimes_A M' \to N \otimes_A N'$ tale che, per qualsiasi $m \in M$, $m' \in M'$, si abbia:

$$(f \otimes g)(m \otimes m') = f(m) \otimes g(m')$$

Dobbiamo però giustificare l'utilizzo della notazione $f \otimes g$ che, per la definizione 3.7, dovrebbe indicare non un elemento di $\mathrm{Hom}_A(M \otimes_A M', N \otimes_A N')$, bensì un tensore puro di $\mathrm{Hom}_A(M,N) \otimes_A \mathrm{Hom}_A(M',N')$. In effetti si vede facilmente, sfruttando la proprietà universale del prodotto tensoriale, che esiste un isomorfismo naturale:

$$\mathrm{Hom}_A(M,N) \otimes_A \mathrm{Hom}_A(M',N') \simeq \mathrm{Hom}_A(M \otimes_A M', N \otimes_A N')$$

Questo isomorfismo manda un tensore puro $f \otimes g$ nell'omomorfismo di A-moduli ottenuto con la costruzione precedente, che perciò indichiamo con la stessa notazione.

Arriviamo finalmente al risultato che avevamo anticipato il quale, nel linguaggio delle categorie, afferma che $- \otimes_A N$ è un funtore covariante esatto a destra per ogni A-modulo N. Per semplicità, qui indicheremo con id l'applicazione identità su N.

Teorema 4.30. *Si consideri una successione esatta $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$ di A-moduli e omomorfismi di A-moduli. Allora, per qualsiasi A-modulo N, è esatta anche la seguente successione:*

$$M_1 \otimes_A N \xrightarrow{f_1 \otimes \mathrm{id}} M_2 \otimes_A N \xrightarrow{f_2 \otimes \mathrm{id}} M_3 \otimes_A N \longrightarrow 0$$

Dimostrazione. Siano N e P due A-moduli fissati. Per la proposizione 4.23, è esatta la seguente successione:

$$0 \longrightarrow \mathrm{Hom}_A(M_3, \mathrm{Hom}_A(N,P)) \xrightarrow{f_2^*} \mathrm{Hom}_A(M_2, \mathrm{Hom}_A(N,P)) \xrightarrow{f_1^*} \mathrm{Hom}_A(M_1, \mathrm{Hom}_A(N,P))$$

Adesso, per $i = 1,2,3$, sia $\varphi_i\colon \mathrm{Hom}_A(M_i \otimes_A N, P) \to \mathrm{Hom}_A(M_i, \mathrm{Hom}_A(N,P))$ l'isomorfismo che abbiamo costruito nella dimostrazione del lemma 4.28 e sia ψ_i l'applicazione inversa di φ_i. Allora abbiamo il seguente diagramma:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_A(M_3, \mathrm{Hom}_A(N,P)) & \xrightarrow{f_2^*} & \mathrm{Hom}_A(M_2, \mathrm{Hom}_A(N,P)) & \xrightarrow{f_1^*} & \mathrm{Hom}_A(M_1, \mathrm{Hom}_A(N,P)) \\ & & \downarrow{\scriptstyle \psi_3} \uparrow{\scriptstyle \varphi_3} & & \downarrow{\scriptstyle \psi_2} \uparrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \psi_1} \\ & & \mathrm{Hom}_A(M_3 \otimes_A N, P) & & \mathrm{Hom}_A(M_2 \otimes_A N, P) & & \mathrm{Hom}_A(M_1 \otimes_A N, P) \end{array}$$

Componendo le mappe del diagramma, otteniamo una successione di A-moduli e omomorfismi di A-moduli:

$$0 \longrightarrow \mathrm{Hom}_A(M_3 \otimes_A N, P) \longrightarrow \mathrm{Hom}_A(M_2 \otimes_A N, P) \longrightarrow \mathrm{Hom}_A(M_1 \otimes_A N, P)$$

Osserviamo che tale successione è esatta. Da una parte, infatti, è chiaro che $\psi_2 \circ f_2^* \circ \varphi_3$ sia un'applicazione iniettiva in quanto composizione di omomorfismi iniettivi. Inoltre, si vede facilmente che vale la condizione:

$$\mathrm{Ker}\, \psi_1 \circ f_1^* \circ \varphi_2 = \mathrm{Im}\, \psi_2 \circ f_2^* \circ \varphi_3$$

A questo punto, poiché P è un A-modulo qualsiasi, applicando di nuovo la proposizione 4.23 otteniamo una successione esatta:

$$M_1 \otimes_A N \longrightarrow M_2 \otimes_A N \longrightarrow M_3 \otimes_A N \longrightarrow 0$$

Per concludere che gli omomorfismi di questa successione sono proprio quelli indicati nell'enunciato, basterà dimostrare che:

$$(f_1 \otimes \mathrm{id})^* = \psi_1 \circ f_1^* \circ \varphi_2\,, \quad (f_2 \otimes \mathrm{id})^* = \psi_2 \circ f_2^* \circ \varphi_3$$

Verificheremo solo la prima identità, in quanto la seconda si dimostra esattamente allo stesso modo. Per farlo sarà sufficiente dimostrare che, fissato un omomorfismo di A-moduli $\alpha\colon M_2 \otimes_A N \to P$, si ha la condizione:

$$\alpha \circ (f_1 \otimes \mathrm{id}) = \psi_1(\varphi_2(\alpha) \circ f_1)$$

Poiché i tensori puri generano il prodotto tensoriale basta osservare che, per ogni $m \in M_2$, $n \in N$, abbiamo:

$$\psi_1(\varphi_2(\alpha) \circ f_1)(m \otimes n) = \varphi_2(\alpha)(f_1(m))(n) = \alpha(f_1(m) \otimes n) = \alpha((f_1 \otimes \mathrm{id})(m \otimes n)) \qquad \square$$

Adesso vedremo con un controesempio che, se $0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$ è una successione esatta corta, allora non è detto che sia esatta corta anche la successione:

$$0 \longrightarrow M_1 \otimes_A N \xrightarrow{f_1 \otimes \mathrm{id}} M_2 \otimes_A N \xrightarrow{f_2 \otimes \mathrm{id}} M_3 \otimes_A N \longrightarrow 0$$

In effetti, se $f_1\colon M_1 \to M_2$ è un omomorfismo di A-moduli iniettivo allora $f_1 \otimes \mathrm{id}$ non è, in generale, iniettivo. Nel linguaggio delle categorie si dice perciò che il funtore $- \otimes_A N$ non è esatto a sinistra e, in particolare, non è esatto.

Esempio 4.31. Consideriamo $M_1 := M_2 := \mathbb{Z}$ come $\mathbb{Z}$-moduli, ossia come gruppi abeliani e l'omomorfismo iniettivo di gruppi $f\colon \mathbb{Z} \to \mathbb{Z}$ definito da $f(a) := 2a$. Scegliamo inoltre $N := \mathbb{Z}/2\mathbb{Z}$. Osserviamo che, per ogni $m \in \mathbb{Z}$, $\bar{n} \in \mathbb{Z}/2\mathbb{Z}$, si ha:

$$(f \otimes \mathrm{id})(m \otimes \bar{n}) = 2m \otimes \bar{n} = m \otimes 2\bar{n} = m \otimes \bar{0} = 0$$

Ricordando che i tensori puri generano il prodotto tensoriale, otteniamo dunque che $f \otimes \mathrm{id}$ è l'omomorfismo nullo. Concludiamo allora che $f \otimes \mathrm{id}$ non è iniettivo perché il suo dominio di definizione, cioè $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \simeq \mathbb{Z}_2$, non è il gruppo nullo.

Definizione 4.32. Un A-modulo N si dice *piatto* se, data una successione $0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$ di A-moduli e omomorfismi di A-moduli che sia esatta corta, anche la successione che segue è esatta corta:

$$0 \longrightarrow M_1 \otimes_A N \xrightarrow{f_1 \otimes \mathrm{id}} M_2 \otimes_A N \xrightarrow{f_2 \otimes \mathrm{id}} M_3 \otimes_A N \longrightarrow 0$$

Equivalentemente, diciamo che N è un A-modulo piatto se, preso un omomorfismo iniettivo di A-moduli f, anche $f \otimes \mathrm{id}$ è iniettivo. Nella teoria delle categorie, queste due condizioni equivalenti si esprimono dicendo che il funtore $- \otimes_A N$ è esatto a sinistra e quindi esatto.

Dall'esempio 4.31 deduciamo in particolare che $\mathbb{Z}/2\mathbb{Z}$ non è uno $\mathbb{Z}$-modulo piatto.

Osservazione 4.33. Gli A-moduli liberi finitamente generati sono piatti. Consideriamo infatti un A-modulo libero finitamente generato N. Per la proposizione 1.25, un tale A-modulo ha rango finito e dunque esiste un isomorfismo $\phi\colon A^k \to N$ per un qualche intero $k \geq 1$. Sia adesso $f\colon M_1 \to M_2$ un omomorfismo iniettivo di A-moduli. Notiamo che, per $i = 1, 2$, grazie alla proposizione 3.16 abbiamo i seguenti isomorfismi canonici:

$$M_i \otimes_A A^k \simeq (\underbrace{A \oplus A \oplus \cdots \oplus A}_{k \text{ volte}}) \otimes_A M_i \simeq (A \otimes_A M_i) \oplus (A \otimes_A M_i) \oplus \cdots \oplus (A \otimes_A M_i) \simeq M_i^k$$

Sia ψ la composizione di questi isomorfismi e sia $(f, f, \ldots, f)\colon M_1^k \to M_2^k$ l'applicazione che agisce come f su ciascuna componente, cioè la mappa definita da:

$$(f, f, \ldots, f)(m_1, m_2, \ldots, m_k) := (f(m_1), f(m_2), \ldots, f(m_k))$$

Si tratta ovviamente di un omomorfismo iniettivo di A-moduli. Si consideri adesso il seguente diagramma:

$$\begin{array}{ccc}
M_1 \otimes_A N & \xrightarrow{f \otimes \mathrm{id}} & M_2 \otimes_A N \\
{\scriptstyle \mathrm{id}_{M_1} \otimes \phi^{-1}} \downarrow & & \uparrow {\scriptstyle \mathrm{id}_{M_2} \otimes \phi} \\
M_1 \otimes_A A^k & & M_2 \otimes_A A^k \\
{\scriptstyle \psi} \downarrow & & \uparrow {\scriptstyle \psi^{-1}} \\
M_1^k & \xrightarrow{(f, f, \ldots, f)} & M_2^k
\end{array}$$

Se dimostriamo che questo diagramma è commutativo, possiamo concludere che $f \otimes \mathrm{id}$ è iniettivo in quanto composizione di omomorfismi iniettivi. Come al solito, possiamo limitarci a considerare i tensori puri, perché questi generano il prodotto tensoriale. Siano perciò $m \in M_1$, $n \in N$ elementi fissati. Per la suriettività di ϕ, esistono $a_1, a_2, \ldots, a_k \in A$ tali che $n = \phi(a_1, a_2, \ldots, a_k)$. Ripercorriamo ora gli isomorfismi del diagramma:

$$\begin{aligned}
& m \otimes n \\
& \longmapsto m \otimes (a_1, a_2, \ldots, a_k) \\
& \longmapsto (a_1, a_2, \ldots, a_k) \otimes m \\
& \longmapsto (a_1 \otimes m, a_2 \otimes m, \ldots, a_k \otimes m) \\
& \longmapsto (a_1 m, a_2 m, \ldots, a_k m) \\
& \longmapsto (a_1 f(m), a_2 f(m), \ldots, a_k f(m)) \\
& \longmapsto (a_1 \otimes f(m), a_2 \otimes f(m), \ldots, a_k \otimes f(m)) \\
& \longmapsto (a_1, a_2, \ldots, a_k) \otimes f(m) \\
& \longmapsto f(m) \otimes (a_1, a_2, \ldots, a_k) \\
& \longmapsto f(m) \otimes n
\end{aligned}$$

Vediamo infine una conseguenza del teorema precedente.

Corollario 4.34. *Sia I un ideale di A e sia M un A-modulo. Allora $M/IM \simeq M \otimes_A A/I$.*

Dimostrazione. Sappiamo che, se $i\colon I \to A$ è la mappa inclusione e $\pi\colon A \to A/I$ è la mappa quoziente, allora abbiamo una successione esatta corta:

$$0 \longrightarrow I \xrightarrow{i} A \xrightarrow{\pi} A/I \longrightarrow 0$$

Sia inoltre $\mathrm{id}\colon M \to M$ l'applicazione identità. Allora, per il teorema 4.30, è esatta la seguente successione:

$$0 \longrightarrow I \otimes_A M \xrightarrow{i \otimes \mathrm{id}} A \otimes_A M \xrightarrow{\pi \otimes \mathrm{id}} A/I \otimes_A M \longrightarrow 0$$

Si considerino adesso gli isomorfismi canonici $\varphi\colon A \otimes_A M \to M$ e $\psi\colon A/I \otimes_A M \to M \otimes_A A/I$ individuati nella proposizione 3.16. Possiamo allora costruire un diagramma di omomorfismi di A-moduli come segue:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I \otimes_A M & \xrightarrow{i\otimes\mathrm{id}} & A \otimes_A M & \xrightarrow{\pi\otimes\mathrm{id}} & A/I \otimes_A M & \longrightarrow & 0 \\ & & & & \varphi\downarrow\uparrow\varphi^{-1} & & \psi\downarrow & & \\ & & & & M & & M \otimes_A A/I & & \end{array}$$

Proprio come accade nella dimostrazione del teorema 4.30, componendo le mappe del diagramma si ottiene una successione esatta:

$$0 \longrightarrow I \otimes_A M \xrightarrow{f} M \xrightarrow{g} M \otimes_A A/I \longrightarrow 0$$

Per il primo teorema di isomorfismo e per l'esattezza della successione, si ha:

$$M \otimes_A A/I = \operatorname{Im} g \simeq M/\operatorname{Ker} g = M/\operatorname{Im} f$$

Per concludere, sarà sufficiente notare che $\operatorname{Im} f = IM$. Questo discende immediatamente dalla definizione di IM, dal fatto che f è un omomorfismo di A-moduli e dalla relazione seguente, vera per ogni $x \in I, m \in M$:

$$f(x \otimes m) = \varphi((i \otimes \mathrm{id})(x \otimes m)) = \varphi(x \otimes m) = xm \qquad \square$$