ALGEBRA 2

v 0.9.9.2 del 25/06/2021

Disclaimer, copyright, ringraziamenti e change.log

Queste dispense sono rivolte agli studenti del corso di Algebra 2 del CdL in Matematica dell'Università di Pisa, e costituiscono la prima parte di un testo, Esercizi di Algebra 2, di Patrizia Gianni ed Enrico Sbarra, ancora in preparazione.

In questa parte sono contenuti i risultati teorici, essenziali per lo svolgimento degli esercizi, ed alcuni problemi che riteniamo di fondamentale importanza per la comprensione degli argomenti trattati.

Vogliamo ringraziare Carlo Traverso per il suo importante contributo nella scelta degli argomenti e dell'impostazione del corso di Algebra 2. Vogliamo altresí ringraziare Andrea Bandini per la sua generosa collaborazione e i suoi validi suggerimenti.

Patrizia Gianni, Enrico Sbarra

Pisa, 25/05/2019

Copyright

change.log

1. Versione 0.9.9.2 del 20210630: Abbiamo corretto alcuni typos e gli errori emersi durante lo svolgimento del corso; abbiamo tolto la dimostrazione di **T.**131, che era un imbroglio :-) Abbiamo aggiunto una piccola appendice sulla forma di Jordan.
2. Versione 0.9.9.1 del 20200604: Abbiamo corretto alcuni typos e gli errori emersi durante lo svolgimento del corso.
3. Versione 0.9.9 del 20200225: Abbiamo aggiunto gli esercizi Vero o Falso.
4. Versione 0.9.8 del 20200224: Abbiamo aggiunto gli esercizi sui moduli noetheriani e decomposizione primaria.
5. Versione 0.9.7 del 20200214: Abbiamo aggiunto gli esercizi sulla localizzazione e ampliato la Sezione 6.5; corretto un errore nell'Esempio 6.1.
6. Versione 0.9.6 del 20191210: Abbiamo aggiunto gli esercizi sul prodotto tensoriale.
7. Versione 0.9.5 del 20191129: Abbiamo aggiunto gli esercizi sui moduli su PID e la forma di Smith. Abbiamo aggiunto le Osservazioni 4.10 e 4.11.
8. Versione 0.9.4 del 20191119: Abbiamo aggiunto la prima parte degli esercizi sui moduli.
9. Versione 0.9.3 del 20191105: Abbiamo aggiunto gli esercizi su anello di polinomi, basi di Gröbner, risultante, varietà.
10. Versione 0.9.2 del 20190725: Abbiamo aggiunto gli esercizi su anelli e ideali, e inserito gli altri esercizi a cui si fa esplicitamente riferimento nella teoria in un capitolo a parte, con le relative soluzioni; inserito l'enunciato e la dimostrazione del teorema di Berlekamp. Corretto un errore nell'osservazione 4.6, punto 2., e un errore nella dimostrazione di **T.**108. Corretti alcuni typos. Inserito un'osservazione sul calcolo del quoziente di ideali nell'anello dei polinomi e il test di appartenenza al radicale in fondo alla sezione 2.2.5. Spellcheck. Altri link sono diventati cliccabili.
11. Versione 0.9 del 20190525: Prima versione. Contiene essenzialmente la parte di teoria che si svolge nel corso di Algebra 2, insieme con alcuni esercizi teorici ed alcuni complementi. Lo studente potrà trovare gran parte del materiale trattato nei seguenti testi: [AM], capitoli 1, 2, 3, 4, 6, 7, 8; [CLS], capitoli 1, 2, 3 4; [AL], capitoli 1 e 2, fino alla sezione 2.5. Abbiamo cercato di completare questa prima parte in tempo per renderla fruibile agli studenti che hanno seguito il corso quest'anno; vi sono pertanto ancora alcuni dettagli da sistemare, ad esempio i riferimenti ad alcuni esercizi che non compaiono - ma

si tratta di esercizi assegnati a lezione - ed è possibile che siano presenti imprecisioni o errori; per questo preghiamo di segnalare eventuali correzioni e commenti a enrico punto sbarra chiocciola unipi punto it specificando il numero di versione, la data, il numero della pagina e il numero della riga. Questa versione sarà sostituita da versioni rivedute e completate, sarà cura dello studente controllare quale sia l'ultima versione disponibile! Anche per questo motivo, nel rispetto dell'ambiente, vi chiediamo di stampare il meno possibile!

Indice

Parte I

Teoria

1

Anelli

In questo capitolo introdurremo le nozioni base per lo studio della teoria generale degli anelli commutativi con identità. Nel secondo capitolo ci soffermeremo sugli anelli dei polinomi che forniscono al contempo una interessante fonte di esempi e una importante motivazione geometrica per lo studio dell'algebra commutativa, come si capirà meglio dallo studio delle varietà algebriche affini, che affronteremo nel terzo capitolo.

1.1 Anelli e ideali

In questa sezione ricorderemo le definizioni principali e le prime proprietà degli anelli commutativi con identità e dei loro elementi; introdurremo gli omomorfismi di anelli e i teoremi di omomorfismo, gli ideali e le operazioni comunemente definite su essi. È utile tenere presente che molte definizioni e proprietà degli anelli commutativi sono state introdotte e studiate pensando agli esempi fondamentali di $\mathbb{Z}$ e dell'anello dei polinomi $K[x]$ a coefficienti in un campo K, dotati delle usuali operazioni di somma e prodotto. Ad esempio, si pensi alla definizione e le proprietà dei domini a fattorizzazione unica, cf. Sezione 1.6.

Un *anello* $(A, +, \cdot)$ è un gruppo abeliano $(A, +)$ dotato di un'operazione prodotto $A \times A \longrightarrow A$, $(a, b) \longrightarrow ab$, tale che per ogni $a, b, c \in A$ valgono

i) $(ab)c = a(bc)$;

ii) $(a + b)c = ac + bc$;

iii) $a(b + c) = ab + ac$.

Un anello è *commutativo* se il prodotto è commutativo. Un anello si dice *unitario* o *con identità* se esiste un elemento neutro del prodotto, indicato con 1 o 1_A; se tale elemento esiste è facile verificare che esso è unico.

Esempio 1.1. Sia n un intero positivo e K un campo. Gli insiemi $\mathbb{Z}$, $\mathbb{Z}/(n)$, $K[x]$, $K[x_1, \ldots, x_n]$ e $K[x_n \colon n \in \mathbb{N}]$, con le operazioni di somma e prodotto usuali, sono anelli commutativi con identità. L'insieme $M_n(K)$ delle matrici quadrate di ordine n a coefficienti in K è un anello con identità, non commutativo se $n > 1$, il gruppo $n\mathbb{Z}$ è un anello commutativo senza identità.

Osserviamo che si può avere $1 = 0$, ma in questo caso $A = 0$, poiché, per ogni $a \in A$, si ha $a = 1 \cdot a = 0 \cdot a = 0$.
Nel seguito considereremo sempre anelli commutativi con identità, diversi da 0, a meno che non venga specificato il contrario.
Un sottoinsieme $B \subseteq A$ si dice *sottoanello* di A se B è un sottogruppo del gruppo additivo di A, è chiuso rispetto al prodotto di A e $1_B = 1_A$. È immediato verificare che l'intersezione di una qualsiasi famiglia $\{B_i\}_{i \in I}$ di sottoanelli di A è un sottoanello.

Alcuni elementi speciali di un anello A

- $a \in A$ si dice **invertibile** se esiste $b \in A$ tale che $ab = 1$.
  Denotiamo l'insieme degli elementi invertibili di A con A^*.
- $a \in A$ si dice **divisore di zero** o *zero divisore* se esiste un elemento $b \in A$, $b \neq 0$, tale che $ab = 0$.
  Denotiamo l'insieme dei divisori di zero di A con $\mathcal{D}(A)$.
- $a \in A$ si dice **nilpotente** se esiste $n \in \mathbb{N}$, tale che $a^n = 0$.
  Denotiamo l'insieme degli elementi nilpotenti di A con $\mathcal{N}(A)$.
- $a \in A$ si dice **idempotente** se $a^2 = a$.

Osserviamo che, dalle definizioni, si ha subito che $\mathcal{N}(A) \subseteq \mathcal{D}(A)$.

Un anello per cui ogni elemento non nullo è invertibile, i.e. $A^* = A \setminus \{0\}$, si dice *campo*.
Se $\mathcal{D}(A) = \{0\}$ allora l'anello A si dice *dominio di integrità* o più semplicemente *dominio*.

L'insieme $\mathcal{N}(A)$ si chiama il *nilradicale* di A. Un anello tale che $\mathcal{N}(A) = (0)$ si dice *ridotto*.
Un anello A si dice *booleano* se tutti i suoi elementi sono idempotenti.

Esempio 1.2. Consideriamo $A = \mathbb{Z}/(12)$, allora $A^* = \{m \in A\colon \gcd(m, 12) = 1\}$, $\mathcal{D}(A) = \{m \in A\colon \gcd(m, 12) \neq 1\}$, $\mathcal{N}(A) = \{0, 6\}$ e gli idempotenti sono $\{0, 1, 4, 9\}$. Notiamo che $\mathcal{N}(A) \subset \mathcal{D}(A)$, $\mathcal{D}(A) \cap A^* = \emptyset$ e $A = A^* \sqcup \mathcal{D}(A)$.

Ricordiamo infine che, se $A \neq 0$, vale sempre che $\mathcal{D}(A) \cap A^* = \emptyset$.

T. 1. Sia A un anello finito; allora $A = A^* \sqcup \mathcal{D}(A)$.

Dimostrazione T. 1 Proviamo che se $a \notin \mathcal{D}(A)$ allora $a \in A^*$. Consideriamo la mappa di moltiplicazione per a, $m_a : A \longrightarrow A$ data da $m_a(b) = ab$. La mappa m_a è iniettiva, dal momento che se $m_a(b) = m_a(c)$ allora $a(b - c) = 0$ e quindi $b - c = 0$ dato che $a \notin \mathcal{D}(A)$. Dal momento che A è finito, m_a è anche surgettiva e quindi esiste $a' \in A$ tale che $1 = m_a(a') = aa'$, cioè $a \in A^*$.

In particolare, un dominio finito è un campo.

Un sottoinsieme non vuoto $I \subseteq A$ è un *ideale* di A se

i) $(I, +)$ è un sottogruppo di A, ossia $0 \in I$ e se $a, b \in I$ allora $a - b \in I$;
ii) per ogni $a \in A$ e per ogni $i \in I$, $ai \in I$.

Un ideale si dice *proprio* se è un sottoinsieme proprio di A.
Segue dalla definizione che un ideale è proprio se e solo se $1 \notin I$, cioè se e solo se $A^* \cap I = \emptyset$.

Siano A un anello e $S \subset A$ un sottoinsieme non vuoto; allora l'insieme

$$\left\{ \sum_{i=1}^{n} a_i s_i \colon a_i \in A, s_i \in S \right\}$$

costituito da tutte le combinazioni lineari finite di elementi di S a coefficienti in A è un ideale, che denotiamo con (S) e chiamiamo l'*ideale generato* da S; è il più piccolo ideale di A che contiene S. Gli elementi di S si chiamano *generatori* di (S). Se esistono un numero finito di elementi $s_1, \ldots, s_n$ che

generano un ideale I, allora I si dice *finitamente generato*. Se in particolare $S = \{s\}$ allora l'ideale $(\{s\})$, che denotiamo semplicemente con (s), si dice *principale*.
Un anello A si dice *ad ideali principali*, abbreviato *PIR*, se ogni suo ideale è principale. Quando A è un dominio, diremo che A è un *dominio ad ideali principali*, abbreviato *PID*.

Ogni anello contiene sempre gli ideali (0) e $(1) = A$, ma non solo, come mostra il seguente risultato, che discende dal Lemma di Zorn.

Sia $(\Sigma, \leq)$ un *poset*, ovvero un insieme non vuoto e parzialmente ordinato con una relazione d'ordine riflessiva, transitiva, antisimmetrica $\leq$. Una *catena* di Σ è un sottoinsieme totalmente ordinato di Σ.

Lemma di Zorn

Sia $(\Sigma, \leq)$ un poset tale che ogni catena è superiormente limitata in Σ; allora esistono elementi di Σ massimali rispetto a $\leq$.

T. 2. Sia $A \neq 0$ un anello.

1. A possiede almeno un ideale $\mathfrak{m}$ massimale rispetto all'inclusione.
2. Dato I ideale proprio di A, esiste un ideale massimale $\mathfrak{m} \supseteq I$.
3. Ogni elemento non invertibile di A è contenuto in un ideale massimale.

Dimostrazione T. 2 1. Usiamo il Lemma di Zorn. Consideriamo l'insieme degli ideali propri di A

$$\Sigma = \{I \subsetneq A \colon I \text{ ideale di } A\}$$

ordinato tramite $\subseteq$. Allora, $\Sigma \neq \emptyset$ dato che $(0) \in \Sigma$. Consideriamo una catena $\mathcal{C} = \{I_1 \subseteq I_2 \subseteq \dots I_h \subseteq \dots : h \in H\}$ di elementi di Σ e proviamo che $I = \bigcup_{h \in H} I_h$ è un maggiorante per $\mathcal{C}$. L'insieme I è un ideale di A: infatti se $a, b \in I$, esistono i, j tali che $a \in I_i$ e $b \in I_j$; dato che $\mathcal{C}$ è totalmente ordinato, senza perdita di generalità sia $I_i \subseteq I_j$. Allora, $a, b \in I_j$ e dunque $a + b \in I_j \subset I$. Analogamente, se $c \in A$ e $a \in I$ allora $a \in I_j$ per qualche j e quindi $ca \in I_j \subset I$. Inoltre, $I \subsetneq A$ dato che $1 \notin I_i$ per ogni i. Possiamo

allora concludere che ogni catena ammette un maggiorante in Σ e quindi, per il Lemma di Zorn, esistono elementi massimali in Σ, ossia ideali massimali in A.

2. Possiamo ripetere la dimostrazione del punto precedente considerando l'insieme $\Sigma_I = \{J \subsetneq A \colon J \text{ ideale di } A,\ I \subseteq J\}$.

3. Se $a \in A$ non è un elemento invertibile, allora $(a) \neq (1)$ è un ideale proprio, per cui basta applicare il punto precedente.

Operazioni fra ideali

- **Intersezione.** Data una famiglia qualunque $\{I_h\}_{h\in H}$ di ideali di A, l'intersezione $\bigcap_{h\in H} I_h$ è un ideale di A.

- **Somma.** Data una famiglia qualunque $\{I_h\}_{h\in H}$ di ideali di A, l'ideale generato dall'insieme $\bigcup_{h\in H} I_h$ si chiama *ideale somma* degli ideali I_h. Esso viene denotato con $\sum_{h\in H} I_h$.

  In particolare, se $I, J \subset A$ sono ideali di A, si ha

$$I + J = \{i + j \colon i \in I, j \in J\}.$$

- **Prodotto.** Data una famiglia finita $I_1, \ldots, I_k$ di ideali di A, l'ideale generato da tutti i prodotti $i_1 \cdots i_k$, con $i_j \in I_j$, si chiama *ideale prodotto* di $I_1, \ldots, I_k$. Esso viene denotato con $\prod_{i=1}^{k} I_i$.

  In particolare, si possono considerare le potenze I^n, $n \in \mathbb{N}$.

- **Quoziente e annullatore.** Dati I e J ideali di A, si definisce *quoziente di I per J* l'insieme $I \colon J = \{a \in A \colon aJ \subseteq I\}$.

  In particolare, se $I = 0$ allora il quoziente $0 : J$ si chiama l'*annullatore* di J e si indica anche con $\operatorname{Ann}_A J$ o semplicemente $\operatorname{Ann} J$.

- **Radicale di un ideale.** Sia I un ideale di A. Definiamo il *radicale* di I, indicato con $\sqrt{I}$, come l'insieme $\{a \in A \colon a^n \in I \text{ per qualche } n \in \mathbb{N}\}$.

Osserviamo che $I \supseteq I^2 \supseteq I^3 \supseteq \cdots \supseteq I^h \supseteq \cdots$. Inoltre è possibile che $I = I^2$, per esempio $(\overline{2}) = (\overline{4})$ in $\mathbb{Z}/(6)$.

T. 3. Siano I, J ideali di un anello A; allora il quoziente $I : J$ e il radicale $\sqrt{I}$ sono ideali.

***Dimostrazione T.** 3* Siano $a, b \in I : J$; allora per ogni $j \in J$ si ha $aj, bj \in I$ e, dato che I è un ideale, si ha $(a+b)j = aj + bj \in I$, ossia $a+b \in I : J$. Analogamente, se $aj \in I$ per ogni $j \in J$ allora, per ogni $c \in A$, si ha che $c(aj) \in I$ e quindi $ca \in I : J$. Infine $0 \in I : J$.

È ovvio che $\sqrt{A} = A$, quindi supponiamo $I \subsetneq A$ in modo che $a^n \in I$ implichi $n > 0$. È chiaro che $0 \in \sqrt{I}$. Se $a \in \sqrt{I}$, allora esiste $n \in \mathbb{N}$ tale che $a^n \in I$ e quindi per ogni $c \in A$ si ha $(ca)^n \in I$ ossia $ca \in \sqrt{I}$. Siano ora $a, b \in \sqrt{I}$; allora esistono $n, m \in \mathbb{N}$ tali che $a^n, b^m \in I$. Consideriamo $(a+b)^{n+m-1} = \sum_{k=0}^{n+m-1} \binom{n+m-1}{k} a^k b^{n+m-1-k} = b^m \sum_{k=0}^{n-1} \binom{n+m-1}{k} a^k b^{n-1-k} + a^n \sum_{k=n}^{n+m-1} \binom{n+m-1}{k} a^{k-n} b^{n+m-1-k}$. Osserviamo che sia il primo che il secondo addendo appartengono ad I, da cui $(a+b)^{n+m-1} \in I$, ossia $a+b \in \sqrt{I}$.

In particolare l'insieme degli elementi nilpotenti di un anello, $\mathcal{N}(A) = \sqrt{(0)}$ è un ideale. Osserviamo che invece $\mathcal{D}(A)$ in generale non è un ideale. Per esempio, se consideriamo $\overline{2}, \overline{3} \in \mathbb{Z}/(6)$, si ha $\overline{2}, \overline{3} \in \mathcal{D}(\mathbb{Z}/(6))$ ma $\overline{2} + \overline{3} = \overline{5} \in (\mathbb{Z}/(6))^*$.

Segue immediatamente dalle definizioni che, se I, J sono ideali di un anello A, allora $IJ \subseteq I \cap J$. In generale questa inclusione è propria ma

$$I + J = (1) \Longrightarrow IJ = I \cap J.$$

Infatti, in questo caso, dal momento che esistono $i \in I$ e $j \in J$ tali che $i + j = 1$, per ogni elemento $a \in I \cap J$ vale $a = 1 \cdot a = (i+j)a = ia + ja \in IJ$.

Se gli ideali I e J sono tali che $I + J = (1)$ diremo che I e J sono *comassimali* o *coprimi*.

T. 4. Siano $I_1, \ldots, I_n$ ideali di A tali che $I_i + I_j = (1)$ per ogni $i \neq j$; allora $\bigcap_{i=1}^n I_i = \prod_{i=1}^n I_i$.

***Dimostrazione T.** 4* Per induzione sul numero degli ideali n. Abbiamo già verificato il caso $n = 2$. Supponiamo dunque che $I = \bigcap_{i=1}^{n-1} I_i = \prod_{i=1}^{n-1} I_i$. Dato che $I_n + I_j = (1)$ per ogni $j < n$, esistono elementi $a_j \in I_n$ e $b_j \in I_j$ tali che $a_j + b_j = 1$. Quindi $1 = \prod_{j=1}^{n-1}(a_j + b_j) = a + b_1 \cdots b_{n-1} \in I_n + I$. Allora, $\prod_{i=1}^n I_i = \prod_{i=1}^{n-1} I_i \cdot I_n = I I_n = I \cap I_n = \bigcap_{i=1}^n I_i$.

Valgono anche le seguenti relazioni:

T. 5. Siano I, J, H ideali di un anello A; allora

1. $(I+J)H = IH + JH$;
2. $(I+J)(I \cap J) \subseteq IJ$;
3. $I \cap (J+H) \supseteq (I \cap J) + (I \cap H)$;
4. [Legge modulare] se $I \supseteq J$ oppure $I \supseteq H$, allora

$$I \cap (J+H) = (I \cap J) + (I \cap H).$$

Dimostrazione T. *5* Ricordiamo che la somma di due ideali $I + J$ è per definizione il più piccolo ideale che contiene I e J.

1. È ovvio che $(I+J)H \subseteq IH+JH$; dato che $IH \subseteq (I+J)H$ e $JH \subseteq (I+J)H$ si ha anche $IH + JH \subseteq (I+J)H$.

2. Da 1 segue che $(I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ + IJ = IJ$.

3. Dal momento che $J, H \subseteq J + H$ si ha che $I \cap J, I \cap H \subseteq I \cap (J+H)$ e quindi $(I \cap J) + (I \cap H) \subseteq I \cap (J+H)$.

4. Per il punto precedente basta dimostrare che se $I \supseteq J$ allora $I \cap (J+H) \subseteq J + (I \cap H)$: possiamo scrivere $i \in I \cap (J+H)$ come $i = j+h$, con $i \in I$, $j \in J$ e $h \in H$. Avremo allora che $h = i - j \in I \cap H$, e dunque $i = j + h \in J + I \cap H$.

Osservazione 1.3. Un'altra relazione utile è

$$I + JH \subseteq (I+J) \cap (I+H).$$

L'uguaglianza non vale in generale: basta prendere $A = \mathbb{Z}$, $I = (2^2)$ e $J = H = (2)$. In alternativa si consideri $A = K[x, y]$, con K campo, $I = (x+y)$, $J = (x)$ e $H = (y)$; questo fornisce un controesempio anche per l'uguaglianza in **T.**5.3, infatti

$$I \cap (J+H) = I \cap (x, y) = I \text{ e } (I \cap J) + (I \cap H) = (x^2 + xy) + (xy + y^2) \neq I\,.$$

È possibile trovare un controesempio all'uguaglianza nel punto 3 con $A = \mathbb{Z}$?

Proprietà del radicale

T. 6. Siano A un anello e I, J, H ideali di A:

1. se $I \subseteq J$, allora $\sqrt{I} \subseteq \sqrt{J}$;
2. $I \subseteq \sqrt{I}$ e $\sqrt{\sqrt{I}} = \sqrt{I}$;
3. $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$;
4. $\sqrt{I^n} = \sqrt{I}$ per ogni intero positivo n;
5. $\sqrt{I} = (1)$ se e solo se $I = (1)$;
6. $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$;
7. $\sqrt{I + JH} = \sqrt{I + J} \cap \sqrt{I + H}$.

Dimostrazione T. *6* 1, 2 e 4 seguono immediatamente dalla definizione.
3. Proviamo che $\sqrt{IJ} \subseteq \sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J} \subseteq \sqrt{IJ}$. Dato che $IJ \subseteq I \cap J$, la prima inclusione segue dal punto 1 e la seconda è di verifica immediata. Infine, dato $a \in \sqrt{I} \cap \sqrt{J}$, avremo che, per qualche m, n, $a^m \in I$ e $a^n \in J$, e dunque $a^{m+n} = a^m a^n \in IJ$, e abbiamo concluso.
5. $1 = 1^n \in I$ se e solo se $1 \in \sqrt{I}$.
6. Certamente $I + J \subseteq \sqrt{I} + \sqrt{J}$ e l' inclusione "$\subseteq$" segue da 1.

Per l'altra inclusione, se $a \in \sqrt{\sqrt{I} + \sqrt{J}}$, allora esistono $i \in \sqrt{I}$ e $j \in \sqrt{J}$ tali che $a^t = i + j$, per qualche t. Se inoltre $n, m \in \mathbb{N}$ sono tali che $i^n \in I$ e $j^m \in J$, allora

$$a^{t(n+m-1)} = \sum_{k=0}^{n-1} \binom{n+m-1}{k} i^k j^{m+n-1-k} + \sum_{k=n}^{n+m-1} \binom{n+m-1}{k} i^k j^{n+m-1-k}$$

sta in $I + J$; dunque $a \in \sqrt{I + J}$.
7. L'inclusione "$\subseteq$" segue da $I + JH \subseteq (I + J) \cap (I + H)$ e da 3.

Per l'altra inclusione, sia $a \in \sqrt{I + J} \cap \sqrt{I + H}$; allora $a^n = i_1 + j$ e $a^m = i_2 + h$ per qualche $n, m \in \mathbb{N}$, $i_1, i_2 \in I$, $j \in J$ e $h \in H$. Dunque $a^{n+m} = i_1 i_2 + i_1 h + i_2 j + jh \in I + JH$ e $a \in \sqrt{I + JH}$.

Ideali speciali /I

Siano A un anello e $I \subset A$ un ideale proprio; allora I si dice

- **massimale**, se non esiste un ideale proprio di A che contiene I strettamente;
- **primo**, se vale $ab \in I \Longrightarrow a \in I$ oppure $b \in I$;
- **radicale**, se $I = \sqrt{I}$;
- **primario**, se vale $ab \in I \Longrightarrow a \in I$ oppure $b \in \sqrt{I}$;
- **irriducibile**, se vale $I = I_1 \cap I_2 \Longrightarrow I = I_1$ oppure $I = I_2$.

Denotiamo l'insieme degli ideali primi e degli ideali massimali di un anello A con $\operatorname{Spec} A$ e $\operatorname{Max} A$ rispettivamente.

Il seguente risultato sarà più volte utile nel seguito.

T. 7. Sia I un ideale proprio di A:

1. se I è primario, allora $\sqrt{I}$ è primo;
2. se $\sqrt{I} = \mathfrak{m}$ è massimale, allora I è primario.

Dimostrazione T. *7* 1. Sia $ab \in \sqrt{I}$; allora esiste $m \in \mathbb{N}$ tale che $(ab)^m \in I$. Dal momento che I è primario si ha allora che o $a^m \in I$ oppure esiste $n \in \mathbb{N}$ tale che $b^{mn} \in I$, ossia $a \in \sqrt{I}$ oppure $b \in \sqrt{I}$.
2. Proviamo che, se $ab \in I$ e $b \notin \mathfrak{m}$, allora $a \in I$. Dato che $\mathfrak{m}$ è un ideale massimale, $(b) + \mathfrak{m} = (1)$, quindi esistono $c \in A$ e $m \in \mathfrak{m}$ tali che $1 = cb + m$. Sia ora $n \geq 1$ un intero tale che $m^n \in I$; allora avremo anche che $1 = 1^n = (cb + m)^n \in (b) + I$. Moltiplicando per a, otteniamo che $a \in (ab) + I \subseteq I$, come volevamo.

Dato un anello A introduciamo il concetto di dimensione per misurarne la "grandezza".

Dimensione di Krull

Sia A un anello. Chiamiamo *dimensione di Krull* di A la quantità

$$\sup\{k\colon \text{ esiste } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_k, \text{ con } \mathfrak{p}_i \in \operatorname{Spec} A\},$$

che denotiamo con $\dim A$.

Dalla definizione discende immediatamente che se A è un campo allora $\dim A = 0$ e se A è un PID ma non un campo allora $\dim A = 1$, cf. **E.**56. Inoltre, se $A = K[x_1, \ldots, x_n]$, usando la catena $(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \ldots \subsetneq (x_1, \ldots, x_n)$, deduciamo subito che $\dim A \geq n$, mentre è più complesso dimostrare che $\dim A = n$, ma non tratteremo qui lo studio della teoria della dimensione. Diciamo che un ideale I in un anello A è *zero dimensionale* se $\dim A/I = 0$.

1.2 Omomorfismi e quozienti

Dato un anello A, un qualsiasi ideale I di A è un sottogruppo normale di A e si può dunque considerare il gruppo quoziente A/I. Dato un elemento $a \in A$, denotiamo con $\overline{a}$ la classe di resto di a modulo I, i.e. $a + I$; si ha dunque che $\overline{a} = \overline{b}$ se e solo se $a - b \in I$. Dotiamo A/I di una struttura di anello ponendo $\overline{a} + \overline{b} = \overline{a + b}$ e $\overline{a}\overline{b} = \overline{ab}$. L'anello A/I si chiama l'*anello quoziente* di A modulo I.

T. 8. La moltiplicazione in A/I sopra descritta è ben definita.

Dimostrazione T. *8* Bisogna provare che se $\overline{a} = \overline{c}$, $\overline{b} = \overline{d}$ in A/I allora $\overline{ab} = \overline{cd}$, ovvero che se $a - c$, $b - d \in I$, allora $ab - cd \in I$. L'elemento $ab - cd = ab - ad - cd + ad = a(b - d) + d(a - c)$ sta in I, poiché entrambi i suoi addendi sono elementi di I.

Siano A e B anelli. Un'applicazione $f : A \longrightarrow B$ è un *omomorfismo* di anelli se vale che, per ogni $a, b \in A$,
i) $f(a + b) = f(a) + f(b)$;
ii) $f(ab) = f(a)f(b)$;
iii) $f(1_A) = 1_B$.

Osservazione 1.4. $f = 0$ non è un omomorfismo di anelli, a meno che $B = 0$.

Dato un omomorfismo di anelli f, ricordiamo che *il nucleo* di f è definito come $\operatorname{Ker} f = \{a \in A \colon f(a) = 0\} = f^{-1}((0))$, *l'immagine* di f è l'insieme $\operatorname{Im} f = \{b \in B \colon b = f(a) \text{ per qualche } a \in A\} = f(A)$.

Dalla definizione di omomorfismo di anelli segue immediatamente che

1. $\operatorname{Ker} f$ è un ideale di A;
2. $\operatorname{Im} f$ è un sottoanello di B.

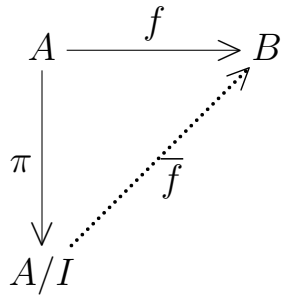
Più in generale, è utile tenere a mente che, dato $f : A \longrightarrow B$ un omomorfismo di anelli e I, J ideali di A e B rispettivamente,

1. $f^{-1}(J)$ è un ideale di A;
2. se f è surgettivo, $f(I)$ è un ideale di B,

cf. Sezione 1.4.

Un omomorfismo bigettivo di anelli è detto *isomorfismo* di anelli. Se esiste un isomorfismo $f : A \longrightarrow B$, allora A e B si dicono *isomorfi* e si scrive $A \simeq B$. Osserviamo che la composizione di omomorfismi è un omomorfismo e che l'inverso di un isomorfismo è un isomorfismo, quindi $\simeq$ definisce una relazione di equivalenza fra anelli.

Sia $f \colon A \longrightarrow B$ un omomorfismo di anelli e sia $I \subset A$ un ideale di A. Se $I \subseteq \operatorname{Ker} f$ allora f induce un unico omomorfismo $\overline{f} \colon A/I \longrightarrow B$ tale che il seguente diagramma commuti



dove la mappa $\pi \colon A \longrightarrow A/I$ è l'omomorfismo definito da $a \mapsto \overline{a}$, ovvero la *proiezione canonica* di A su A/I; essa è chiaramente surgettiva.

È chiaro che, affinché il diagramma commuti, $\overline{f}$ deve essere definita come $\overline{f}(\overline{a}) = \overline{f(a)}$; questa è una buona definizione. Infatti, se $\overline{a} = \overline{b}$ allora $a - b \in$

$I \subseteq \operatorname{Ker} f$; quindi $0 = f(a-b) = f(a) - f(b)$, da cui segue che $\overline{f}(\overline{a}) = \overline{f}(\overline{b})$. Inoltre, che $\overline{f}$ sia un omomorfismo segue immediatamente dal fatto che f lo è.

Teoremi di omomorfismo di anelli.

T. 9. Siano A e B anelli.

I Un omomorfismo $f : A \longrightarrow B$ induce un isomorfismo

$$A/\operatorname{Ker}(f) \simeq \operatorname{Im} f.$$

II Siano $I, J \subset A$ ideali e sia $I \subset J$; allora J/I è un ideale di A/I e

$$(A/I)/(J/I) \simeq A/J.$$

III Sia $I \subset A$ un ideale e sia $B \subset A$ un sottoanello; allora

a) $B + I = \{b + i \colon b \in B, i \in I\} \subset A$ è un sottoanello;

b) I è un ideale di $B + I$;

c) $I \cap B$ è un ideale di B.

Infine,

$$B + I/I \simeq B/(B \cap I).$$

Dimostrazione T. 9 **I**. Per dimostrare il primo teorema, in virtù della precedente discussione, basta dapprima restringere il codominio di f a $\operatorname{Im} f$, rendendola surgettiva; la funzione indotta $\overline{f} \colon A/\operatorname{Ker} f \longrightarrow \operatorname{Im} f$ risulterà essere un omomorfismo iniettivo e surgettivo per costruzione.

II. Consideriamo elementi $\overline{j_1}, \overline{j_2} \in J/I = \{\overline{j} \ : \ j \in J\}$ e $\overline{a} \in A/I$; avremo allora che $\overline{j_1} + \overline{j_2} = \overline{j_1 + j_2}$, con $j_1 + j_2 \in J$ e che $\overline{a}\overline{j_1} = \overline{aj_1}$, con $aj_1 \in J$. Quindi J/I è un ideale di A/I ed ha pertanto senso considerare l'anello quoziente.

Consideriamo ora la mappa $\pi \colon A/I \longrightarrow A/J$, ove $\overline{a} \mapsto \overline{\overline{a}}$. Essa è ben definita: se $\overline{a} = \overline{b}$ allora $a - b \in I \subseteq J$, e pertanto $\overline{\overline{a}} = \overline{\overline{b}}$. Chiaramente, π è un omomorfismo surgettivo e $J/I \subseteq \operatorname{Ker} \pi$. Sia allora $\overline{a} \in \operatorname{Ker} \pi$, cioè $0 = \pi(\overline{a}) =$

$\overline{\overline{a}}$; questo vuol dire che $a \in J$ e dunque $J/I = \operatorname{Ker}\pi$. La tesi ora segue dal primo teorema di omomorfismo.

III. a), b), c) sono semplici verifiche, necessarie affinché l'ultimo isomorfismo abbia senso. Consideriamo la mappa $f\colon B \xrightarrow{i} B+I \xrightarrow{\pi} B+I/I$, definita come composizione della mappa di inclusione di B in $B+I$ e la proiezione sul quoziente. In quanto tale, è un omomorfismo, che risulta essere surgettivo: ogni elemento $\overline{b+i}$ è immagine di $b \in B$. Inoltre, se $b \in B$ è tale che $\overline{b} = 0$, avremo che $b \in I$, e dunque $b \in B \cap I$. Il nucleo di f è $B \cap I$, da cui segue la tesi per il primo teorema di omomorfismo.

T. 10. Vi è una corrispondenza biunivoca fra gli ideali di A che contengono I e gli ideali di A/I; inoltre, in questa corrispondenza, gli ideali primi corrispondono ad ideali primi e gli ideali massimali ad ideali massimali.

Dimostrazione T. 10 Sia J un ideale di A che contiene I; dato che la proiezione è surgettiva, $\pi(J)$ è un ideale di A/I. Viceversa, dato un ideale H in A/I, la sua controimmagine è un ideale di A; esso contiene I poiché $\pi(I) = 0 \subset H$. Che la corrispondenza sia $1:1$ sugli ideali massimali discende subito dalla definizione di ideale massimale. La controimmagine di un ideale primo è sempre un ideale primo, cf. **T.**17.7. Per il viceversa, supponiamo che $\mathfrak{p}$ sia un ideale primo di A che contiene I, e sia $\overline{ab} \in \pi(\mathfrak{p})$. Allora esiste $c \in \mathfrak{p}$ tale che $\overline{c} = \overline{ab}$, da cui segue che $c - ab \in I \subseteq \mathfrak{p}$, quindi $ab \in \mathfrak{p}$, e la tesi segue dalla primalità di $\mathfrak{p}$.

Come conseguenza dei teoremi di omomorfismo otteniamo le seguenti caratterizzazioni delle proprietà degli ideali in termini dell'anello quoziente.

Ideali speciali /II

T. 11. Sia I un ideale di un anello A; allora

1. I è proprio se e solo se $A/I \neq 0$;
2. I è massimale se e solo se A/I è un campo;
3. I è primo se e solo se A/I è un dominio;
4. I è radicale se e solo se A/I è un anello ridotto;

5. I è primario se e solo se $\mathcal{N}(A/I) = \mathcal{D}(A/I)$;
6. I massimale $\Longrightarrow$ I primo;
7. I primo $\Longrightarrow$ I radicale;
8. I primo $\Longrightarrow$ I primario.

Dimostrazione T. *11* 1. L'anello quoziente A/I è non banale se e solo se $\overline{1} \neq \overline{0}$ in A/I se e solo se $1 \notin I$, cioè esattamente quando I è proprio.

2. A/I è un campo se e solo se gli unici suoi ideali sono 0 e 1. Per la corrispondenza biunivoca tra gli ideali di A/I e gli ideali di A che contengono I, ciò vuol dire che gli unici ideali che contengono I sono A e I stesso, i.e. I è massimale.

3. A/I è un dominio se e solo se, per ogni coppia di elementi $\overline{a}, \overline{b} \neq \overline{0}$ di A/I, il prodotto $\overline{ab} \neq \overline{0}$. Quindi A/I è un dominio se e solo se, per ogni coppia di elementi $a, b \in A \setminus I$ si ha che $ab \notin I$, ovvero quando I è un ideale primo di A.

4. A/I è un anello ridotto se e solo se $\mathcal{N}(A/I) = 0$, i.e. se vale che $\overline{a}^k = \overline{0}$ implica $\overline{a} = \overline{0}$. Quindi A/I è ridotto se e solo se vale che $a^k \in I$ implica $a \in I$, cioè se e solo se $\sqrt{I} \subseteq I$, ovvero se e solo se I è radicale.

5. Sia $\mathcal{D}(A/I) \subseteq \mathcal{N}(A/I)$ e dimostriamo che I è un ideale primario di A. Dobbiamo mostrare che se $a, b \in$ sono tali che $a \notin I$ e $ab \in I$ allora $b^n \in I$ per qualche intero n. Infatti, in A/I, $\overline{0} \neq \overline{a}$ e $\overline{a}\overline{b} = \overline{0}$ implicano $\overline{b} \in \mathcal{D}(A/I) \subseteq \mathcal{N}(A/I)$, cioè $\overline{b}^n = \overline{b^n} = \overline{0}$ per qualche n e $b \in \sqrt{I}$.

Il viceversa si ottiene invertendo le implicazioni.

6. Se A/I è un campo allora A/I è un dominio.

7. Se A/I è un dominio allora $\mathcal{N}(A/I) \subseteq \mathcal{D}(A/I) = 0$; in questo caso allora A/I è ridotto e la conclusione segue dal punto 4.

8. Dato che $\mathcal{N}(A/I) = \mathcal{D}(A/I) = 0$, la tesi segue applicando il punto 5.

Gli ideali primi soddisfano le seguenti importanti proprietà rispetto all'intersezione e all'unione di ideali; ricordiamo che quest'ultima in generale non è un ideale!

T. 12. 1. [Lemma di scansamento] Siano $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideali primi e sia I un ideale tale che $I \subseteq \bigcup_{j=1}^n \mathfrak{p}_j$; allora esiste j_0 tale che $I \subseteq \mathfrak{p}_{j_0}$.
2. Siano $I_1, \ldots, I_n$ ideali e sia $\mathfrak{p}$ un ideale primo tale che $\bigcap_{j=1}^n I_j \subseteq \mathfrak{p}$; allora esiste j_0 tale che $I_{j_0} \subseteq \mathfrak{p}$. Inoltre, se $\bigcap_{j=1}^n I_j = \mathfrak{p}$ allora esiste j_0 tale che $I_{j_0} = \mathfrak{p}$.

Dimostrazione T. 12 1. Proviamo, per induzione su n, che se $I \not\subseteq \mathfrak{p}_j$ per ogni $1 \leq j \leq n$ allora $I \not\subseteq \cup_{j=1}^n \mathfrak{p}_j$, ovvero dimostriamo che se I "scansa" tutti i primi allora I "scansa" anche la loro unione. Certamente l'affermazione è vera se $n = 1$.
Se $n > 1$ e l'affermazione è vera per $n-1$, allora, considerando tutti i possibili sottoinsiemi di $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ costituiti da $n-1$ elementi, otteniamo che per ogni i esiste un elemento $a_i \in I$ tale che $a_i \notin \bigcup_{j=1, j\neq i}^n \mathfrak{p}_j$. Se per almeno uno di questi elementi si ha $a_i \notin \mathfrak{p}_i$ allora $I \not\subseteq \cup_{j=1}^n \mathfrak{p}_j$. In caso contrario, si ha che $a_i \in \mathfrak{p}_i$ per ogni i e quindi l'elemento $b = \sum_{i=1}^n \prod_{j=1, j\neq i}^n a_j \in I$ ma $b \notin \mathfrak{p}_i$ per ogni i perché tutti i suoi addendi tranne uno sono in $\mathfrak{p}_i$, da cui segue che $I \not\subseteq \cup_{j=1}^n \mathfrak{p}_j$.
2. Dimostriamo per assurdo e supponiamo che $\mathfrak{p} \not\supseteq I_i$ per ogni i. In questo caso allora per ogni i esiste almeno un elemento $a_i \in I_i \setminus \mathfrak{p}$, quindi si ha $\prod_{i=1}^n a_i \in \bigcap_{j=1}^n I_j$ e $\prod_{i=1}^n a_i \notin \mathfrak{p}$, dal momento che $\mathfrak{p}$ è un ideale primo. Quindi $\mathfrak{p} \not\supseteq \bigcap_{j=1}^n I_j$.
Infine se $\bigcap_{j=1}^n I_j = \mathfrak{p}$ allora esiste j_0 tale che $\mathfrak{p} = \bigcap_{j=1}^n I_j \subseteq I_{j_0} \subseteq \mathfrak{p}$, da cui $\mathfrak{p} = I_{j_0}$.

Come corollario, otteniamo il seguente risultato.

T. 13. Ogni ideale primo è irriducibile.

Dimostrazione T. 13 Siano $I \subset A$ un ideale primo e $I = J \cap K$ una decomposizione di I; allora $I = J$ oppure $I = K$ per **T.**12.2, ovvero la decomposizione è banale, cioè la tesi.

1.3 Il nilradicale e il radicale di Jacobson. Anelli locali

Abbiamo osservato che dalle definizioni discende che $\sqrt{(0)} = \mathcal{N}(A)$. Per costruzione, l'anello $A/\mathcal{N}(A)$ è ridotto: se $\overline{a}^k = \overline{0}$, vuol dire che a^k è nilpotente, quindi a lo è, e dunque $\overline{a} = 0$. Vale inoltre la seguente proposizione.

T. 14. [Caratterizzazione del radicale di un ideale]

1.
$$\mathcal{N}(A) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}.$$

2. Sia $I \subset A$ un ideale; allora
$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \supseteq I}} \mathfrak{p}.$$

Dimostrazione T. *14* 1. Verifichiamo dapprima che un elemento nilpotente a appartiene ad ogni ideale primo di A: se $a^n = 0$ per qualche $n \in \mathbb{N}$, avremo che $a^n \in \mathfrak{p}$ per ogni primo $\mathfrak{p}$, da cui discende che $a \in \mathfrak{p}$ per ogni $\mathfrak{p}$. Il viceversa è un'altra applicazione del Lemma di Zorn. Dimostriamo che se $a \notin \mathcal{N}(A)$, allora esiste un primo $\mathfrak{p}$ tale che $a \notin \mathfrak{p}$. A tal scopo, consideriamo la famiglia $\Sigma = \{J \subset A \colon a^n \notin J \text{ per ogni } n \in \mathbb{N}\}$, ordinata tramite "$\subseteq$". Essa non è vuota poiché $(0) \in \Sigma$, dato che per ipotesi a non è nilpotente. È facile verificare che l'unione degli ideali in una catena di Σ è un elemento di Σ. Vogliamo mostrare che un elemento massimale I di Σ, che esiste per il lemma di Zorn, è un ideale primo; dato che non contiene a è l'ideale primo cercato. Supponiamo allora che esistano elementi $x, y \notin I$ tali che $xy \in I$; allora l'ideale $I : x$ contiene propriamente I e dunque, per la massimalità di I, non è un elemento di Σ; ne segue che esiste un intero n tale che $a^n \in I : x$. Pertanto $I \subsetneq (I, x) \subseteq I : a^n \notin \Sigma$, ed esiste un intero m tale che $a^m \in I : a^n$, cosicché $a^{n+m} \in I$, che è la contraddizione cercata.

2. Basta considerare l'anello A/I. Il suo nilradicale corrisponde in A proprio a $\sqrt{I}$, e si decompone come intersezione dei primi di A/I per il punto precedente. A questo punto la conclusione segue dalla corrispondenza 1:1 tra i primi di A/I e i primi di A che contengono I, cf. **T.**10.

Quanto visto sopra caratterizza il nilradicale di un anello A come intersezione di tutti gli ideali primi di A.

Il *radicale di Jacobson* di un anello A, denotato con $\mathcal{J}(A)$, è invece l'ideale definito come intersezione di tutti gli ideali massimali di A. Dalla definizione segue dunque subito che

$$\mathcal{N}(A) \subseteq \mathcal{J}(A).$$

Gli elementi del radicale di Jacobson di un anello sono caratterizzati dalla seguente fondamentale proprietà.

T. 15. [Caratterizzazione del radicale di Jacobson] Sia A un anello,

$$a \in \mathcal{J}(A) \quad \text{se e solo se} \quad 1 - ab \in A^* \ \text{ per ogni } \ b \in A.$$

Dimostrazione T. 15 Sia $a \in A$, $a \notin \mathcal{J}(A)$; allora esiste un ideale massimale $\mathfrak{m}$ tale che $a \notin \mathfrak{m}$ e $(a, \mathfrak{m}) = (1)$. Quindi esiste $b \in A$, tale che l'elemento $1 - ab \in \mathfrak{m}$ non è invertibile.
Viceversa, sia $a \in \mathcal{J}(A)$ e supponiamo che esista $b \in A$ per cui $1 - ab$ non sia invertibile. Allora $1 - ab \in \mathfrak{m}$, per qualche ideale massimale $\mathfrak{m}$, con $ab \in \mathfrak{m}$. Da ciò segue che $1 \in \mathfrak{m}$, che è assurdo.

Un anello si dice *locale* se ha un unico ideale massimale $\mathfrak{m}$. Il campo $K = A/\mathfrak{m}$ si chiama il *campo residuo* di A; in questo caso si usano le notazioni $(A, \mathfrak{m})$ oppure $(A, \mathfrak{m}, K)$. Un anello con un numero finito di ideali massimali si dice *semilocale*.
Ci sono numerosi esempi di anelli locali: i campi, l'anello delle serie formali in una variabile, $\mathbb{Z}/(p^n)$, con $p \in \mathbb{Z}$ primo. La proprietà che li definisce, i.e. avere un solo ideale massimale, sebbene non contribuisca a capire come sono fatti tutti gli altri ideali primi dell'anello, li rende più semplici da studiare.

T. 16. [Caratterizzazione degli anelli locali]

1. Se esiste un ideale $\mathfrak{m} \subset A$ tale che $A \setminus \mathfrak{m} \subseteq A^*$ allora A è locale con ideale massimale $\mathfrak{m}$.
2. Se $\mathfrak{m} \subset A$ è un ideale massimale tale che per ogni $a \in \mathfrak{m}$ si ha $1 + a \in A^*$ allora A è locale, con ideale massimale $\mathfrak{m}$.

***Dimostrazione T.** 16* 1. Per ogni ideale proprio $I \subsetneq A$ si ha che $I \subseteq A \setminus A^*$ e quindi $I \subseteq \mathfrak{m}$ che allora è l'unico ideale massimale di A.

2. Se proviamo che ogni elemento $a \notin \mathfrak{m}$ è invertibile, la tesi segue dal punto precedente. Se $a \notin \mathfrak{m}$, dal momento che $\mathfrak{m}$ è massimale si ha $(a, \mathfrak{m}) = (1)$, ossia esistono $b \in A$, $m \in \mathfrak{m}$ tali che $ba + m = 1$ e quindi $ba = 1 - m$, che è invertibile per ipotesi; da ciò segue che $a \in A^*$.

1.4 Ideali estesi e contratti

Abbiamo già visto la corrispondenza fra gli ideali di un anello A e di un suo quoziente rispetto ad un ideale I considerando l'omomorfismo di proiezione $\pi : A \longrightarrow A/I$. Più in generale se A e B sono due anelli e $f\colon A \longrightarrow B$ un omomorfismo vogliamo studiare la corrispondenza fra gli ideali di A e quelli di B determinata dall'omomorfismo f.
Se $I \subset A$ è un ideale, in generale l'immagine $f(I)$ non è un ideale di B; definiamo *ideale esteso* rispetto a f di I l'ideale generato dall'immagine $f(I)$ e lo denotiamo con I^e.

Invece, se $J \subset B$ allora $f^{-1}(J) = \{a \in A\colon f(a) \in J\}$ è sempre un ideale di A che contiene $\operatorname{Ker} f$. Chiamiamo questo ideale *ideale contratto* di J rispetto a f e lo denotiamo con J^c.

Le operazioni di estensione e contrazione di un ideale soddisfano le seguenti relazioni.

Ideali estesi e contratti

T. 17. Siano $I, I_1, I_2 \subseteq A$ e $J, J_1, J_2 \subseteq B$ ideali.

1. $I_1 \subseteq I_2 \implies I_1^e \subseteq I_2^e$;
2. $J_1 \subseteq J_2 \implies J_1^c \subseteq J_2^c$;
3. $I \subseteq I^{ec}$, ma il contenimento può essere stretto;
4. $J^{ce} \subseteq J$, ma il contenimento può essere stretto;
5. $I^{ece} = I^e$;
6. $J^{cec} = J^c$;

7. J primo $\Longrightarrow$ J^c primo;
8. J primario $\Longrightarrow$ J^c primario;
9. J radicale $\Longrightarrow$ J^c radicale.
10. In generale 7, 8 e 9 non valgono per gli ideali estesi.

***Dimostrazione T.** 17* I punti 1 e 2 seguono immediatamente dalle definizioni.

3. Se $a \in I$, allora $f(a) \in f(I) \subseteq I^e$ e quindi $a \in I^{ec}$. Se si considera l'immersione $\mathbb{Z} \longrightarrow \mathbb{Q}$, $I = (n)$, $n \neq 0, 1$, allora $I^{ec} = \mathbb{Z} \supsetneq I$.

4. Si ha $J^{ce} = (f(J^c))$ e, dato che $f(J^c) \subseteq J$ per definizione, abbiamo che $(f(J^c)) \subseteq J$. Pertanto $J^{ce} \subseteq J$. Se si considera l'immersione $K \longrightarrow K[x]$, e $J = (x)$ allora $J^{ce} = (0) \subsetneq J$.

5. Per i punti 3 e 1, $I \subseteq I^{ec}$ implica $I^e \subseteq I^{ece}$.
Per l'altra inclusione, si ha che $I^{ec} = f^{-1}(I^e)$ e quindi $f(I^{ec}) = f(f^{-1}(I^e)) \subseteq I^e$, da cui $I^{ece} \subseteq I^e$.

6. Per i punti 4 e 2, $J^{ce} \subseteq J$ implica $J^{cec} \subseteq J^c$.
Per l'altra inclusione, si ha che $f(J^c) \subseteq J^{ce}$; quindi $J^c \subseteq J^{cec}$.

7. Se $ab \in J^c$ allora $f(a)f(b) = f(ab) \in J$; dato che J è primo, $f(a) \in J$ oppure $f(b) \in J$ e quindi $a \in J^c$ oppure $b \in J^c$.

8. Se $ab \in J^c$ allora $f(a)f(b) = f(ab) \in J$; dato che J è primario, $f(a) \in J$ oppure $f(b^n) = f(b)^n \in J$ e quindi $a \in J^c$ oppure $b^n \in J^c$.

9. Se $a \in \sqrt{J^c}$ allora $f(a)^n = f(a^n) \in J$ per qualche n; quindi $f(a) \in \sqrt{J} = J$ e $a \in J^c$; ciò mostra che J^c è radicale.

10. L'immersione $\mathbb{Z} \longrightarrow \mathbb{Q}$ e un ideale primo non nullo (p) di $\mathbb{Z}$ forniscono un controesempio alle affermazioni 7 e 8. Per la 9 si consideri l'immersione $\mathbb{Z} \longrightarrow \mathbb{Z}[i]$ con $(2)^e = (1+i)^2$.

Nel caso di omomorfismi surgettivi, come ad esempio la proiezione $\pi : A \longrightarrow A/I$, questa corrispondenza soddisfa la seguente proprietà.

T. 18. Siano A e B anelli e sia $f : A \longrightarrow B$ un omomorfismo surgettivo. Se $\operatorname{Ker} f \subseteq I \subset A$ e $J \subset B$ sono ideali vale:

1. l'immagine $f(I)$ è un ideale di B e quindi $I^e = f(I)$.

2. $I = I^{ec}$ e $J = J^{ce}$. Quindi le operazioni di estensione e contrazione stabiliscono corrispondenze biunivoche, una l'inversa dell'altra, fra gli ideali di A che contengono $\operatorname{Ker} f$ e gli ideali di B.
3. Rispetto a tale corrispondenza, i massimali corrispondono ai massimali, i primi ai primi, i primari ai primari e i radicali ai radicali.

Dimostrazione T. *18* 1. Ovviamente $f(I) \subseteq I^e$. Sia dunque $b \in I^e = (f(I))$. Allora $b = \sum_j b_j f(i_j)$ con $b_j \in B$ e $i_j \in I$. Dal momento che f è surgettiva per ogni b_j esiste $a_j \in A$ tale che $b_j = f(a_j)$ e quindi $b = \sum_j b_j f(i_j) = \sum_j f(a_j)f(i_j) = \sum_j f(a_j i_j) = f(\sum_j a_j i_j) \in f(I)$

Alternativamente si può dimostrare direttamente che $f(I)$ è un ideale di B.

2. Abbiamo che $I^{ec} = f^{-1}(I^e)$, ma essendo f surgettiva si ha che $I^e = f(I)$ e quindi se $a \in I^{ec}$ allora $f(a) = f(b)$, per qualche $b \in I$, da cui $a - b \in \operatorname{Ker} f \subseteq I$ e allora $a \in I$. Sempre dalla surgettività di f segue che $J^{ce} = f(J^c) = f(f^{-1}(J)) = J$.

3. Tutte le affermazioni seguono dal fatto che se f è surgettiva e $I \subset A$ contiene $\operatorname{Ker} f$ allora $A/I \simeq B/I^e$, mentre se J è un ideale di B allora $A/J^c \simeq B/J$.

1.5 Teorema cinese del resto e applicazioni

Siano $A_1, \ldots, A_n$ anelli. È possibile definire sul prodotto cartesiano $A = \prod_{i=1}^{n} A_i = A_1 \times A_2 \times \cdots \times A_n$ una struttura di anello ponendo $a + b = (a_1 + b_1, \ldots, a_n + b_n)$ e $ab = (a_1 b_1, \ldots, a_n b_n)$, per ogni $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in A$, ovvero definendo somma e prodotto componente per componente usando la somma e il prodotto definiti sui singoli A_i. Ovviamente avremo che $0_A = (0_{A_1}, \ldots, 0_{A_n})$ e $1_A = (1_{A_1}, \ldots, 1_{A_n})$. Chiamiamo tale anello la *somma diretta* di $A_1, \ldots, A_n$.
Tale anello non può mai essere un dominio se $n > 1$; inoltre esistono in A elementi idempotenti non banali.

T. 19. Un anello A è isomorfo ad una somma diretta $A_1 \times \cdots \times A_n$ se e solo se esistono n elementi idempotenti $e_1, \ldots, e_n \in A$ *ortogonali*, i.e. tali che $e_i e_j = 0$ se $i \neq j$, e tali che $\sum_i e_i = 1_A$.

Dimostrazione T. 19 Sia $f\colon A \xrightarrow{\simeq} \prod_{i=1}^{n} A_i$ un isomorfismo di anelli; gli elementi $e_i = f^{-1}(0, \ldots, 0, 1_{A_i}, 0, \ldots, 0)$ sono idempotenti ortogonali tali che $\sum_i e_i = 1$.

Viceversa, consideriamo gli anelli commutativi $A_i = e_i A$, la cui identità è e_i, e definiamo $f\colon A \longrightarrow \prod_{i=1}^{n} A_i$, ponendo $f(a) = (e_1 a, \ldots, e_n a)$. Si verifica che f è un omomorfismo di anelli. Proviamo che è un isomorfismo. È iniettivo, infatti se $f(a) = f(b)$ allora per ogni i si ha $e_i a = e_i b$ da cui segue che $a = a \cdot 1 = a \sum_i e_i = \sum_i e_i a = \sum_i e_i b = b \sum_i e_i = b$. È anche surgettivo: sia $(e_1 a_1, \ldots, e_n a_n) \in \prod_{i=1}^{n} A_i$. L'elemento $a = e_1 a_1 + \ldots + e_n a_n \in A$ è tale che $f(a) = (e_1 a_1, \ldots, e_n a_n)$.

Un caso in cui un anello si spezza come somma diretta di anelli è quando esistono in A ideali comassimali, come illustrato dai seguenti risultati.

Teorema cinese del resto

T. 20. Siano $I_1, \ldots, I_n \subset A$ ideali tali che $I_i + I_j = (1)$ se $i \neq j$; allora per ogni $a_1, \ldots, a_n \in A$ esiste $a \in A$ tale che $a \equiv a_i \mod I_i$ per ogni i.

Dimostrazione T. 20 Per ipotesi, per ogni $i \neq j$ esistono elementi $\gamma_i^{(j)} \in I_i$ tali che $\gamma_i^{(j)} + \gamma_j^{(i)} = 1$. Definiamo, per ogni i, $L_i = \prod_{j \neq i} \gamma_j^{(i)}$, allora $L_i \equiv 0 \mod I_j$ se $j \neq i$, e $L_i = \prod_{i \neq j} (1 - \gamma_i^{(j)}) \equiv 1 \mod I_i$. Avremo allora che l'elemento $a = \sum_i a_i L_i \in A$ soddisfa le condizioni richieste.

T. 21. Siano $I_1, \ldots, I_n \subset A$ ideali di A e sia $f\colon A \longrightarrow \prod_{i=1}^{n} A/I_i$ l'omomorfismo definito da $f(a) = (\overline{a}_1, \ldots, \overline{a}_n)$, ove $a_i \equiv a \mod I_i$. Valgono i seguenti fatti:

1. f è surgettivo se e solo se $I_i + I_j = (1)$ per ogni $i \neq j$;

2. f è iniettivo se e solo se $\bigcap_{i=1}^{n} I_i = 0$.

Dimostrazione T. 21 1. Se gli ideali in questione sono a due a due comassimali, da **T.**20 segue che f è surgettivo. Viceversa, se f è surgettivo, per ogni i possiamo scegliere elementi $a_i \in A$ tali che $f(a_i) = (0, \dots, 0, 1, 0, \dots, 0)$, ove l'1 è in posizione i-esima; in questo modo, avremo che $a_i \equiv 1 \mod I_i$ e $a_i \equiv 0 \mod I_j$ per ogni $j \neq i$. Allora, per ogni $j \neq i$, $1 = (1 - a_i) + a_i \in I_i + I_j$, come volevamo.
2. Il nucleo di f è chiaramente dato da $\bigcap_{i=1}^{n} I_i$.

In conclusione, se in A esistono ideali I_i, con $i = 1, \dots, n$, che sono a due a due comassimali e tali che $\prod_{i=1}^{n} I_i = 0$, per **T.**4 e **T.**21 avremo che $f\colon A \xrightarrow{\simeq} \prod_{i=1}^{n} A/I_i$ è un isomorfismo.

I due fatti seguenti sono rilevanti applicazioni del teorema cinese del resto.

T. 22. [Interpolazione di Lagrange] Siano $\alpha_1, \dots, \alpha_n \in K$ campo qualsiasi, tali che $\alpha_i \neq \alpha_j$ se $i \neq j$ e $\beta_1, \dots, \beta_n \in K$; allora esiste un polinomio $f(x) \in K[x]$ di grado n tale che $f(\alpha_i) = \beta_i$ per ogni i. Tale f è dato da

$$f = \sum_{i=1}^{n} \beta_i \prod_{\substack{j=1,\dots,n \\ j \neq i}} \frac{(x - \alpha_j)}{(\alpha_i - \alpha_j)}.$$

Dimostrazione T. 22 Chiamiamo $I_i = (x - \alpha_i)$ per ogni $i = 1, \dots, n$. Costruire un polinomio $f(x)$ tale che $f(\alpha_i) = \beta_i$ per ogni i, equivale a cercare un elemento $f(x) \in K[x]$ tale che $f(x) \equiv \beta_i \mod I_i$ per ogni i. Nell'anello euclideo $K[x]$ gli ideali I_i e I_j sono massimali e dunque comassimali se $i \neq j$. È facile verificare che con $c_i^{(j)} := \frac{1}{\alpha_j - \alpha_i}$ si ottiene $c_i^{(j)}(x - \alpha_i) + c_j^{(i)}(x - \alpha_j) = 1$. Quindi se definiamo $L_i = \prod_{j \neq i} \frac{(x - \alpha_j)}{(\alpha_i - \alpha_j)}$, si ha $L_i \equiv 0 \mod I_j$ se $j \neq i$ e $L_i \equiv 1 \mod I_i$. Allora il polinomio cercato è dato da

$$f = \sum_{i=1}^{n} \beta_i L_i = \sum_{i=1}^{n} \beta_i \prod_{\substack{j=1,\dots,n \\ j \neq i}} \frac{(x - \alpha_j)}{(\alpha_i - \alpha_j)}.$$

T. 23. [Berlekamp] Siano $A = \mathbb{Z}/(p)[x]$, $f \in A$ un polinomio monico libero da quadrati. Siano inoltre $B = A/(f)$ e $\varphi_p : B \longrightarrow B$ l'endomorfismo di Frobenius dato da $\varphi_p(\overline{g}) = \overline{g}^p$. Allora

1. $\mathrm{Ker}(\varphi_p - \mathrm{id}_B) \simeq (\mathbb{Z}/(p))^n$ dove n è il numero di fattori irriducibili di f;
2. per ogni $\bar{g} \in \mathrm{Ker}(\varphi_p - \mathrm{id}_B)$ si ha $f(x) = \prod_{a \in \mathbb{Z}/(p)} \gcd(f(x), g(x) - a)$, dove $g(x) \in A$ è un qualsiasi rappresentante di $\overline{g}$.

***Dimostrazione* T. 23** Sia $f(x) = \prod_{i=1}^{n} f_i(x)$ con $f_i(x) \in \mathbb{Z}/(p)[x]$ irriducibili e distinti. Ricordiamo che $B = A/(f)$ è uno spazio vettoriale di dimensione finita su $\mathbb{Z}/(p)$ e che φ_p è un endomorfismo. Per **T.**21, esiste un isomorfismo $F : B \longrightarrow \prod_{i=1}^{n} A/(f_i)$, dove gli $A/(f_i)$ sono campi finiti che contengono $\mathbb{Z}/(p)$ per ogni i.

1. Sia $\overline{g} \in \mathrm{Ker}(\varphi_p - \mathrm{id}_B)$ e scriviamo $F(\overline{g}) = (\overline{g}_1, \ldots, \overline{g}_n)$, dove $\overline{g}_i \equiv \overline{g} \mod (f_i)$ per ogni i; allora si ha $\overline{g}_i^p = \overline{g}_i$ in $A/(f_i)$. Le uniche radici di $y^p - y$ in $A/(f_i)$ sono gli elementi di $\mathbb{Z}/(p)$, dunque $\overline{g} \in \mathrm{Ker}(\varphi_p - \mathrm{id}_B)$ se e solo se $\overline{g}_i \in \mathbb{Z}/(p)$ per ogni i, i.e. se e solo se $F(\overline{g}) \in (\mathbb{Z}/(p))^n$. Dato che F è un isomorfismo si ha $\mathrm{Ker}(\varphi_p - \mathrm{id}_B) \simeq (\mathbb{Z}/(p))^n$.

2. Sia ancora $\overline{g} \in \mathrm{Ker}(\varphi_p - \mathrm{id}_B)$ e sia g un suo rappresentante in A. Sia $F(\overline{g}) = (a_1, \ldots, a_n) \in (\mathbb{Z}/(p))^n$. Allora per ogni $a \in \mathbb{Z}/(p)$ si ha che $f_i \mid (g - a)$ se e solo se la i-esima coordinata di $F(\overline{g - a}) = F(\overline{g}) - F(a) = (a_1 - a, \ldots, a_n - a)$ è nulla, cioè se e solo se $a_i = a$. Quindi

$$\gcd(f, g - a) = \prod_{\substack{i=1,\ldots,n \\ a_i = a}} f_i$$

e la formula finale segue immediatamente.

1.6 Fattorizzazione in domini commutativi: PID e UFD.

In questa sezione analizziamo il problema della divisione e della fattorizzazione in un dominio A, dove vale la legge di cancellazione, cf. **E.**2. Ricordiamo che un dominio è PID se tutti i suoi ideali sono principali.

Dati $a, b \in A$, diciamo che a *divide* b, e scriviamo $a \mid b$, se esiste $c \in A$ tale che $b = ca$; in questo caso diciamo che a è un *divisore* di b e che b è un *multiplo* di a. In questo modo i divisori di 1 sono proprio gli elementi di A^*. Osserviamo che se a è un divisore di b e b è un divisore di c, allora a è un divisore di c. Due elementi $a, b \in A$ sono *associati* se esiste $u \in A^*$ tale che $b = ua$. Si verifica facilmente che essere associati definisce una relazione di equivalenza $\mathcal{R}$ su A.
Da qui alla fine di questa sezione assumeremo che A sia un dominio. Osserviamo allora che se $b = ac$, c è univocamente determinato da a e b; se $a, c \notin A^*$, diciamo che a (e c) è un *divisore proprio* di b. Inoltre a e b sono associati esattamente quando $a \mid b$ e $b \mid a$. Diciamo che un elemento $a \notin A^*$ è *primo* se per ogni $b, c \in A$ si ha che $a \mid bc$ se e solo se $a \mid b$ oppure $a \mid c$. Un elemento $a \notin A^*$ si dice *irriducibile* se $a = bc \Longrightarrow b \in A^*$ oppure $c \in A^*$; equivalentemente se ogni divisore di a è associato ad a, o ancora se a non ha divisori propri.
Questi concetti possono essere facilmente espressi in termini di proprietà degli ideali principali generati dagli elementi di A, come mostrato in quanto segue.

Siano $a, b \in A$; allora

1. a è un'unità se e solo se $(a) = (1)$;
2. a e b sono associati se e solo se $(a) = (b)$;
3. a divide b se e solo se $(b) \subseteq (a)$;
4. a è un divisore proprio di b se e solo se $(b) \subsetneq (a) \subsetneq (1)$;
5. a è primo se e solo se (a) è un ideale primo.

Infatti, per ogni $a \in A$, $(a) \subseteq (1)$; l'elemento a è invertibile se e solo se esiste b invertibile in A tale che $ab = 1$, che mostra che $(1) \subseteq (a)$. Inoltre a e b sono associati se e solo se esiste $c \in A^*$ tale che $ac = b$ e $a = bc^{-1}$, e questo è equivalente a $(b) \subseteq (a)$ e $(a) \subseteq (b)$. L'elemento a è un divisore di b se e solo se esiste $c \in A$ tale che $ac = b$, da cui discende che $(b) \subseteq (a)$. Se poi a è un divisore proprio di $b \neq 0$, non può essere che $(a) = (b)$. Infatti in tal caso avremmo che $b = ac = bdc$ per qualche $c, d \in A$. Allora, visto che A è un dominio, $b(1 - dc) = 0$ implicherebbe che c è invertibile, che è contro

l'ipotesi. Visto che anche (a) non è invertibile, avremo $(b) \subsetneq (a) \subsetneq (1)$. Sia infine $a \notin A^*$. La condizione $\big(a \mid bc$ se e solo se $a \mid b$ oppure $a \mid c\big)$, per quanto visto al punto 3 è equivalente a $\big((bc) \subseteq (a)$ se e solo se $(b) \subseteq (a)$ oppure $(c) \subseteq (a)\big)$, che a sua volta è equivalente alla condizione $\big(bc \in (a)$ se e solo se $b \in (a)$ oppure $c \in (a)\big)$, che vuol dire appunto che (a) è primo.

T. 24. In un dominio A,

1. se $a \in A \setminus \{0\}$ è primo, allora a è irriducibile;
2. se A è PID e $a \in A$ è irriducibile, allora a è primo.

Dimostrazione T. 24 1. Supponiamo che a non sia irriducibile; allora esistono $b, c \notin A^*$ tali che $a = bc$. Ora, né b né c sono elementi di (a): consideriamo ad esempio il caso $b = ab_1$, per qualche $b_1 \in A$. Allora $a = bc = ab_1c$, da cui segue che c è invertibile, che non è possibile. Abbiamo pertanto trovato $b, c \notin (a)$ tali che $bc \in (a)$, che è contro l'ipotesi.

2. Supponiamo che (a) non sia primo. Esistono dunque $b, c \in A \setminus (a)$ tali che $bc \in (a)$. Allora $(a) \subsetneq (a, b) = (d)$, per qualche d, visto che A è PID. Avremo allora che $a = da_1$, con $a_1 \notin A^*$, altrimenti $b \in (d) = (a)$. Se mostriamo che $d \notin A^*$ abbiamo concluso, perché da ciò discende che a ha una fattorizzazione propria da_1, che è assurdo. Se fosse $d \in A^*$, cioè $(1) = (d) = (a, b)$, esisterebbero $\alpha, \beta \in A$ tali che $1 = \alpha a + \beta b$, da cui seguirebbe che $c = c \cdot 1 \in (a) + (bc) \subseteq (a)$, che non è possibile.

Esempio 1.5. Gli ideali primi non nulli, che sono anche massimali, dell'anello $\mathbb{Z}$, che è PID, sono tutti e soli gli ideali (p), con $p \neq 0$ numero primo. Nell'anello $\mathbb{Z}[x]$ l'elemento x è irriducibile e primo ma l'ideale (x) non è massimale pur essendo primo. Nell'anello $\mathbb{Z}[\sqrt{-5}]$, che non è UFD, l'elemento 2 è irriducibile, ma non primo.

T. 25. Sia A un PID. Allora ogni catena $I_0 \subseteq I_1 \subseteq \dots$ ascendente di ideali di A è stazionaria, i.e. esiste n_0 tale che $I_n = I_{n_0}$ per ogni $n \geq n_0$.

Dimostrazione T. 25 . Data una qualsiasi catena ascendente di ideali I_j in un anello A, l'unione I degli ideali della catena è un ideale, come si verifica facilmente. Inoltre, dato che A è PID, tutti gli ideali sono principali, e dunque

anche I è principale. Sia dunque $I = (a)$; allora esiste n_0 tale che $I_{n_0} \subseteq I = (a) \subseteq I_{n_0}$ e $I_n = I_{n_0}$ per ogni $n \geq n_0$.

Diremo che un dominio A è a *fattorizzazione unica* , abbreviato *UFD*, se soddisfa le seguenti proprietà:

(UFD1) *esistenza di una fattorizzazione in irriducibili*: per ogni elemento $a \in A \setminus \{A^* \cup \{0\}\}$ esistono $b_1, \ldots, b_k \in A$ irriducibili tali che $a = b_1 \cdots b_k$;

(UFD2) *unicità della fattorizzazione*: se $a = b_1 \cdots b_k = c_1 \cdots c_h$ sono due fattorizzazioni di a in elementi irriducibili, allora $k = h$ e, a meno dell'ordine, ogni elemento b_i è associato a c_i, per ogni i.

T. 26. Sia A un dominio per cui vale (UFD1); allora in A vale (UFD2) se e solo se vale

(UFD3): *ogni elemento irriducibile è primo.*

Dimostrazione T. 26 Mostriamo che se A è fattoriale allora vale (UFD3). Supponiamo che a sia un elemento irriducibile e $b, c \in A$ tali che $a|bc$; vogliamo mostrare che a divide b oppure c. Se b oppure c sono 0 abbiamo finito. Possiamo anche supporre che né b né c siano invertibili, dunque che $b, c \in A \setminus \{A^* \cup \{0\}\}$. Esiste allora un $d \in A$ non nullo tale che $da = bc$. Discende da (UFD1) che esistono elementi irriducibili b_i, c_j tali che $b = \prod_i b_i, c = \prod_j c_j,$ e per l'unicità della fattorizzazione (UFD2) esiste allora $e = b_{i_0}$ oppure un $e = c_{j_0}$ tale che a ed e sono associati, visto che a per ipotesi è irriducibile. Avremo allora che $a|b$ nel primo caso oppure $a|c$ nel secondo, come volevamo.

Supponiamo ora che valga (UFD3) e dimostriamo (UFD2): supponiamo che $a \in A \setminus \{A^* \cup \{0\}\}$, e $a = \prod_{i=1}^m a_i = \prod_{j=1}^n b_j$ siano fattorizzazioni in elementi irriducibili. Senza perdita di generalità possiamo assumere che $m \leq n$. Osserviamo ora che $\prod_{j=1}^n b_j \in (a_1)$ che è primo per ipotesi. Pertanto esiste $j_1 \in \{1, \ldots, n\}$ tale che $b_{j_1} \in (a_1)$. Riordinando gli indici, possiamo assumere che $j_1 = 1$; quindi $b_1 = a_1 c_1$, e visto che b_1 è irriducibile e $a_1 \notin A^*$, risulta che $c_1 \in A^*$ e dunque che a_1 e b_1 sono associati. Dopo aver semplificato per a_1 otteniamo che $c_1 \prod_{i=2}^m a_i = \prod_{j=2}^n b_j$, con $c_1 \in A^*$. Ragionando allo stesso modo possiamo dedurre che $b_2 = a_2 c_2$, con $c_2 \in A^*$; dopo m passi avremo

che a_i è associato con b_i per ogni $i = 1, \dots, m$ e $\prod_{j=m+1}^{n} b_j = \prod_{i=1}^{m} c_i \in A^*$. Abbiamo dimostrato allora che, a meno dell'ordine e di elementi invertibili, le due fattorizzazioni di a coincidono.

T. 27. Se A è PID allora A è UFD. Esistono però UFD che non sono PID.

Dimostrazione T. 27 Sappiamo da **T.**24.2, che in un PID ogni elemento irriducibile è anche primo. Dunque, grazie a **T.**26, basta mostrare che ogni elemento non nullo e non invertibile di A si esprime come prodotto di un numero finito di elementi irriducibili. Se per assurdo esistesse un elemento $a_0 \in A \setminus \{A^* \cup \{0\}\}$ che non possiede tale fattorizzazione, esso non sarebbe irriducibile e genererebbe un ideale proprio. Pertanto esistono elementi non invertibili $a_1, b_1 \in A$ che non sono associati e tali che $a = a_1 b_1$. Se entrambi a_1 e b_1 fossero esprimibili come prodotto finito di elementi irriducibili, anche a_0 avrebbe una tale fattorizzazione. Possiamo dunque supporre che a_1 non l'abbia, e dunque che non sia irriducibile. Procedendo in questo modo possiamo costruire una catena di ideali $(a_0) \subsetneq (a_1) \subsetneq \dots$ di A che non è stazionaria, e ciò contraddice **T.**25.

Un esempio di anello a fattorizzazione unica che non è PID è un anello di polinomi A a coefficienti in un anello UFD, con almeno due indeterminate x_1 e x_2. Esso è UFD per il Lemma di Gauss, e non è PID: l'ideale $(x_1, x_2) \subset A$ non può essere generato da un solo elemento d, in quanto per la fattorizzazione unica questo dovrebbe avere almeno $x_1 x_2$ come fattore, e quindi essere di grado almeno 2. Poiché A è un dominio l'uguaglianza $(x_1, x_2) = (d)$ è dunque esclusa per motivi di grado.

Sia A un UFD. Dati due elementi $a, b \in A$ non nulli, un elemento $d \in A$ tale che

i) $d \mid a$ e $d \mid b$ (*divisore comune*);

ii) per ogni $c \in A$ tale che $c \mid a$ e $c \mid b$ si ha che $c \mid d$ (*massimo*);

si chiama *massimo comun divisore* di a e b, e si denota con $\gcd(a, b)$.
Segue immediatamente dalla definizione che se d è massimo comune divisore di a, b allora anche ed, con $e \in A^*$, lo è. Tenendo a mente questo fatto, con un lieve abuso di nomenclatura, chiamiamo un elemento d che soddisfa

le condizioni i) e ii) della definizione precedente *il massimo comun divisore* di a e b, intendendo che esso è unico a meno di associati. Analogamente si introduce la definizione di *minimo comune multiplo*. Sia $\mathcal{R}$ la relazione di equivalenza data dall'essere elementi associati. Se denotiamo con $\mathrm{Irr}(A) = \{p \neq 0 \colon p \text{ primo }\}/\mathcal{R}$ l'insieme degli elementi primi - o, per quanto dimostrato in **T.**24 e **T.**26, irriducibili - modulo la relazione di equivalenza $\mathcal{R}$, per ogni coppia di elementi $a, b \in A \setminus \{A^* \cup \{0\}\}$ possiamo scrivere $a = \prod_{p\in\mathrm{Irr}(A)} p^{a_p}$, e $b = \prod_{p\in\mathrm{Irr}(A)} p^{b_p}$, con a_p e b_p quasi tutti nulli. Risulterà allora che

$$\gcd(a,b) = \prod_{p\in\mathrm{Irr}(A)} p^{\min\{a_p,b_p\}} \quad \text{e} \quad \mathrm{lcm}(a,b) = \prod_{p\in\mathrm{Irr}(A)} p^{\max\{a_p,b_p\}}.$$

Un dominio d'integrità A si dice *dominio euclideo* se esiste un'applicazione $\delta \colon A \setminus \{0\} \longrightarrow \mathbb{N}_{>0}$ detta *grado* tale che
i) per ogni $a, b \in A \setminus \{0\}$, $\delta(a) \leq \delta(ab)$;
ii) per ogni $a \in A$ e $b \in A \setminus \{0\}$, esistono $q, r \in A$ tali che $a = qb + r$ e $r = 0$ oppure $\delta(r) < \delta(b)$.
Tali elementi q ed r si dicono rispettivamente *quoziente* e *resto* della divisione di a per b.

T. 28. Un dominio euclideo è un PID e quindi è un UFD.

***Dimostrazione T.** 28* Sia I un ideale di A. Se $I = (0)$ abbiamo finito. Altrimenti sia $I \neq 0$, e sia δ la funzione grado che rende A euclideo. Allora $\delta(I \setminus \{0\})$ è un sottoinsieme non vuoto di $\mathbb{N}_{>0}$, e dunque ha un minimo. Sia $a \in I \setminus \{0\}$ un elemento per cui $\delta(a)$ sia minimo e mostriamo che $I = (a)$, provando che A è PID e dunque anche UFD, per **T.**27. Sia $b \in I$; per ipotesi esistono $q, r \in A$ tali che $b = qa + r$ con $r = 0$ oppure $\delta(r) < \delta(a)$. Dato che $r = b - qa \in I$, questo secondo caso non si può presentare per la minimalità di $\delta(a)$, dunque $r = 0$, come volevamo.

Esempio 1.6. Gli anelli $\mathbb{Z}$, $K[x]$, con K campo, e $\mathbb{Z}[i]$ sono anelli euclidei e quindi anche PID e UFD.

T. 29. Siano A un UFD e $a \in A$ un elemento non invertibile e diverso da zero; se a è irriducibile, allora l'ideale (a) è irriducibile.

Dimostrazione T. 29 Supponiamo che l'elemento a sia irriducibile, e siano $I, J \subset A$ ideali tali che $(a) = I \cap J$. Allora $(a) \subset I$ e $(a) \subset J$. Supponiamo per assurdo che $(a) \neq I$ e $(a) \neq J$. Allora esistono $b \in I \setminus (a)$ e, $c \in J \setminus (a)$; dal momento che $bc \in I \cap J = (a)$, si ha che $a \not| b$ e $a \not| c$, con $a|bc$, il che è impossibile se a è irriducibile, e quindi primo per **T.**26.

Osserviamo che, se A non è UFD, l'affermazione precedente non vale, cf. **E.**60. Inoltre, anche se A è PID non vale necessariamente che gli ideali irriducibili siano generati da elementi irriducibili. Basta considerare l'ideale $(9) \subset \mathbb{Z}$. L'ideale (9) è irriducibile, dato che se $(9) = (a) \cap (b) = (\mathrm{lcm}(a, b))$ allora $a = 9$ oppure $b = 9$, ma 9 non è un elemento irriducibile. In particolare, un ideale irriducibile non è necessariamente primo. Vale però il viceversa, come già dimostrato.

2

L'anello $K[x_1, \ldots, x_n]$

In questo capitolo studieremo le proprietà di un anello dei polinomi $A = K[x_1, \ldots, x_n]$ in n indeterminate a coefficienti in un campo K. Useremo la notazione compatta $X = x_1, \ldots, x_n$, per cui ad esempio potremo scrivere $A = K[X]$. Denotiamo inoltre con $\mathrm{Mon}(A)$ l'insieme di tutti i monomi di A.

2.1 Ideali monomiali ed $\mathcal{E}$-sottoinsiemi

Dato $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$, ricordiamo che un *monomio* di A è un elemento della forma $x_1^{a_1} \cdots x_n^{a_n} \in A$ che denotiamo con $X^{\mathbf{a}}$ e il cui *esponente* è $\mathbf{a}$. In questo modo risulta definita una corrispondenza 1-1 tra l'insieme $\mathrm{Mon}(A)$ dei monomi di A e gli elementi di $\mathbb{N}^n$; in questa bigezione il monomio 1 corrisponde all'esponente $\mathbf{0} \in \mathbb{N}^n$. Osserviamo che, se $\mathbf{a}, \mathbf{b} \in \mathbb{N}^n$, dire che $X^{\mathbf{a}}$ divide $X^{\mathbf{b}}$ è equivalente a dire che $\mathbf{b} - \mathbf{a} \in \mathbb{N}^n$.
Un elemento $f \in A$ è un *polinomio*, che scriviamo come $f = \sum_{\mathbf{a}} c_{\mathbf{a}} X^{\mathbf{a}}$, con $\mathbf{a} \in \mathbb{N}^n$ e $c_{\mathbf{a}} \in K^*$, per un numero finito di $\mathbf{a} \in \mathbb{N}^n$. Chiamiamo *termine* di f ogni addendo non nullo $c_{\mathbf{a}} X^{\mathbf{a}}$.
Gli ideali di A sono, per definizione, generati da polinomi ovvero da elementi che sono somme e prodotti di monomi. Volendone studiare le proprietà è conveniente cominciare con una classe importante di ideali di A.

Un ideale $I \subseteq A$ è *monomiale* se ha un sistema di generatori composto da monomi.

Il seguente fatto fornisce un criterio per decidere se $f \in A$ appartiene ad I e caratterizza gli ideali monomiali.

T. 30. Sia I un ideale monomiale e sia $f = \sum_{\mathbf{a}} c_{\mathbf{a}} X^{\mathbf{a}}$, con $\mathbf{a} \in \mathbb{N}^n$ e $c_{\mathbf{a}} \in K^*$, un polinomio di A; allora

$$f \in I \iff X^{\mathbf{a}} \in I \text{ per ogni } \mathbf{a}.$$

***Dimostrazione* T. 30** Chiaramente, se $X^{\mathbf{a}} \in I$ per ogni $\mathbf{a}$, allora $f \in I$, dato che I è un ideale. Viceversa, supponiamo che $f \in I$. Allora f si scrive in termini dei generatori di I, che indichiamo qui sotto con $X^{\mathbf{b}}$, come somma finita

$$f = \sum_{\mathbf{b}} p_{\mathbf{b}}(X) X^{\mathbf{b}} = \sum_{\mathbf{b}} (\sum_{\mathbf{a}} c_{\mathbf{b},\mathbf{a}} X^{\mathbf{a}}) X^{\mathbf{b}} = \sum_{\mathbf{b},\mathbf{a}} c_{\mathbf{b},\mathbf{a}} X^{\mathbf{b}+\mathbf{a}},$$

con $p_{\mathbf{b}}(X) \in A$, $c_{\mathbf{b},\mathbf{a}} \in K$ per ogni $\mathbf{a}, \mathbf{b} \in \mathbb{N}^n$. Per il principio di identità dei polinomi, i termini devono coincidere e dunque ogni termine di f appartiene a I, poiché $X^{\mathbf{b}+\mathbf{a}} \in I$ per ogni $\mathbf{a} \in \mathbb{N}^n$.

In particolare, dati un sottoinsieme $E \subseteq \mathbb{N}^n$ e un ideale monomiale $I = (X^{\mathbf{a}} : \mathbf{a} \in E)$, un monomio $X^{\mathbf{b}} \in I$ se e soltanto se esiste $\mathbf{a} \in E$ tale che $\mathbf{b} - \mathbf{a} \in \mathbb{N}^n$.
L'insieme degli esponenti E, e quindi un insieme di generatori di I, a priori non è necessariamente finito, ma vedremo nel seguito che esiste sempre un sottoinsieme finito $E' \subseteq E$ tale che $I = (X^{\mathbf{a}} : \mathbf{a} \in E) = (X^{\mathbf{b}} : \mathbf{b} \in E')$.
Grazie alla bigezione tra monomi ed esponenti, studiare un ideale monomiale diventa equivalente a studiare particolari sottoinsiemi di $\mathbb{N}^n$; per questo introduciamo le seguenti definizioni, che corrispondono a quelle di ideale monomiale e di insieme di generatori, rispettivamente.

Un sottoinsieme $E \neq \emptyset$ di $\mathbb{N}^n$ si dice un $\mathcal{E}$-sottoinsieme se

$$\mathbf{a} \in E \implies \mathbf{a} + \mathbf{b} \in E \text{ per ogni } \mathbf{b} \in \mathbb{N}^n.$$

Un sottoinsieme $F \neq \emptyset$ di un $\mathcal{E}$-sottoinsieme E si dice *una frontiera di* E

se per ogni $\mathbf{a} \in E$ esistono $\mathbf{b} \in F$ e $\mathbf{c} \in \mathbb{N}^n$ tali che $\mathbf{a} = \mathbf{b} + \mathbf{c}$.

Il seguente teorema garantisce che ogni $\mathcal{E}$-sottoinsieme ammette una frontiera finita.

T. 31. [Lemma di Dickson] Ogni $\mathcal{E}$-sottoinsieme ammette una frontiera finita, quindi ogni ideale monomiale di A è finitamente generato.

Dimostrazione T. 31 Dimostriamo la tesi per induzione su n. Se $n = 1$, $E \subset \mathbb{N}$ e $F = \{\min E\}$ è una frontiera finita di E.
Supponiamo ora l'enunciato vero per n e dimostriamolo per $n+1$. Consideriamo la proiezione $\pi\colon \mathbb{N}^{n+1} \longrightarrow \mathbb{N}^n$ definita da $\pi(a_0, \ldots, a_n) = (a_1, \ldots, a_n)$. Chiaramente, $\pi(E) \neq \emptyset$; dato che per ogni $\mathbf{a} \in E$ e $\mathbf{b} \in \mathbb{N}^n$ si ha $\mathbf{a} + (0, \mathbf{b}) \in E$, avremo che $\pi(\mathbf{a}) + \mathbf{b} = \pi(\mathbf{a} + (0, \mathbf{b})) \in \pi(E)$. Dunque $\pi(E)$ è un $\mathcal{E}$-sottoinsieme di $\mathbb{N}^n$ e quindi, per ipotesi induttiva e per la surgettività di π, esiste $F_0 = \{\mathbf{a}_1, \ldots, \mathbf{a}_k\} \subset \mathbb{N}^{n+1}$ tale che $\pi(F_0)$ sia una frontiera finita di $\pi(E)$.
Per completare la costruzione di una frontiera di E poniamo $\overline{a} = \max_i\{a_0^{(i)}\}$, dove $\mathbf{a}_i = (a_0^{(i)}, \ldots, a_n^{(i)})$, e per ogni $0 \leq a < \overline{a}$ consideriamo i sottoinsiemi non vuoti $E_a = E \cap (\{a\} \times \mathbb{N}^n)$ costituiti da tutte le $(n+1)$-uple in E con prima coordinata uguale ad a. Allora $\pi(E_a) \subset \mathbb{N}^n$ è un $\mathcal{E}$-sottoinsieme di $\mathbb{N}^n$ e quindi, per l'ipotesi induttiva, per ogni tale a esiste un insieme finito $F_a = \{\mathbf{a}_1^{(a)}, \ldots, \mathbf{a}_{k_a}^{(a)}\} \subset E_a$ tale che $\pi(F_a)$ sia una frontiera finita di $\pi(E_a)$.
Proviamo ora che $F = F_0 \cup \bigcup_{0 \leq a < \overline{a}} F_a$ è una frontiera di E. Sia $\mathbf{a} = (a_0, \ldots, a_{n+1}) \in E$, dobbiamo dimostrare che esiste $\mathbf{b} \in F$ tale che $\mathbf{a} - \mathbf{b} \in \mathbb{N}^{n+1}$. A tal scopo basta osservare che, per costruzione, se $a_0 \geq \overline{a}$ allora esiste $\mathbf{a}_i \in F_0$ tale che $\mathbf{a} - \mathbf{a}_i \in \mathbb{N}^{n+1}$; altrimenti $\mathbf{a} \in E_{a_0}$ ed esiste un $\mathbf{b} \in F_{a_0}$ tale che $\mathbf{a} - \mathbf{b} \in \mathbb{N}^{n+1}$.

È chiaro che, data una frontiera F di un $\mathcal{E}$-sottoinsieme, se ne può estrarre una frontiera minimale, eliminando gli elementi $\mathbf{b}$ di F che a loro volta si possono scrivere come $\mathbf{a} + \mathbf{c}$, con $\mathbf{a} \in F$ e $\mathbf{c} \in \mathbb{N}^n$.

T. 32. Ogni $\mathcal{E}$-sottoinsieme ha un'unica frontiera finita minimale. Pertanto, ogni ideale monomiale I ha un unico insieme minimale di generatori monomiali.

Dimostrazione T. 32 Siano $F = \{\mathbf{a}_1, \ldots, \mathbf{a}_s\}$ e $F' = \{\mathbf{b}_1, \ldots, \mathbf{b}_t\}$ due frontiere minimali di un $\mathcal{E}$-sottoinsieme E. Allora vale $E = \bigcup_{i=1}^{s}(\mathbf{a}_i + \mathbb{N}^n) = \bigcup_{j=1}^{t}(\mathbf{b}_j + \mathbb{N}^n)$. Dato che $\mathbf{a}_i \in E$, per ogni i possiamo trovare $\mathbf{b}_j \in F'$ tale che $\mathbf{a}_i \in \mathbf{b}_j + \mathbb{N}^n$. Definiamo allora $\eta : \{1, \ldots, s\} \to \{1, \ldots, t\}$ tramite $\eta(i) = \min\{j \ : \ \mathbf{a}_i \in \mathbf{b}_j + \mathbb{N}^n\}$. Questa applicazione è surgettiva perché se non lo fosse si potrebbe scrivere

$$E = \bigcup_{i=1}^{s}(\mathbf{a}_i + \mathbb{N}^n) \subseteq \bigcup_{i=1}^{s}(\mathbf{b}_{\eta(i)} + \mathbb{N}^n) \subsetneq \bigcup_{j=1}^{t}(\mathbf{b}_j + \mathbb{N}^n) = E\,,$$

che è assurdo. Dunque $s \geq t$: ribaltando i ruoli di F e F' si ottiene una mappa surgettiva $\nu : \{1, \ldots, t\} \to \{1, \ldots, s\}$ che dimostra $t \geq s$ e quindi $s = t$. Di conseguenza η e ν sono permutazioni e si ha $\mathbf{a}_i \in \mathbf{b}_{\eta(i)} + \mathbb{N}^n \subseteq \mathbf{a}_{\nu(\eta(i))} + \mathbb{N}^n$: la minimalità di F allora implica $\mathbf{a}_i = \mathbf{a}_{\nu(\eta(i))}$ e quindi $\mathbf{a}_i = \mathbf{b}_{\eta(i)}$ per ogni i.

La frontiera (finita) minimale di un $\mathcal{E}$-sottoinsieme E viene chiamata l'*escalier* di E.

Riassumendo, dato un qualsiasi ideale monomiale $I = (X^{\mathbf{a}} \ : \ X^{\mathbf{a}} \in M)$ e un suo insieme di generatori monomiali M, ad esso corrisponde l'$\mathcal{E}$-sottoinsieme $E = \{\mathbf{a} + \mathbf{b} \ : \ X^{\mathbf{a}} \in M, \mathbf{b} \in \mathbb{N}^n\}$. Per definizione di $\mathcal{E}$-sottoinsieme, ogni frontiera di E corrisponde ad un insieme di generatori di I. In questo modo, il lemma di Dickson, che garantisce l'esistenza di una frontiera finita E' di E, prova che esiste un insieme di generatori finito per ogni ideale monomiale. Inoltre se $F = \{\mathbf{a}_1, \ldots, \mathbf{a}_k\}$ è la frontiera minimale di E, allora l'insieme $M' = \{X^{\mathbf{a}_1}, \ldots, X^{\mathbf{a}_k}\} \subseteq M$ dei corrispondenti monomi è un insieme minimale di generatori di I. Esso è l'insieme dei monomi di I minimali rispetto alla divisibilità. Lo denotiamo con $G(I)$.

Per gli ideali monomiali, è molto semplice calcolare i generatori degli ideali ottenuti dopo aver eseguito le operazioni usuali. Per quanto riguarda la somma di due ideali monomiali I e J con insiemi minimali di generatori $G(I)$ e

$G(J)$, possiamo considerare l'insieme di generatori $G(I) \cup G(J)$ e ridurlo a $G(I+J)$.

Operazioni e ideali monomiali

T. 33. Siano $I = (m_1, \dots, m_s)$ e $J = (n_1, \dots, n_t)$ ideali monomiali di A, con $m_i, n_j \in \mathrm{Mon}(A)$, con $i = 1, \dots, s$, $j = 1, \dots, t$.

1. **Decomposizione.** Siano $m, n \in A$ monomi relativamente primi; allora $(I, mn) = (I, m) \cap (I, n)$.
2. **Intersezione.** L'ideale $I \cap J$ è un ideale monomiale generato dagli elementi $\mathrm{lcm}(m_i, n_j)$, $i = 1, \dots, s$, $j = 1, \dots, t$.
3. **Quoziente.** Sia m un monomio di A, allora l'ideale $I : m$ è un ideale monomiale, generato dai monomi $m_i / \gcd(m_i, m)$, $i = 1, \dots, s$.
4. **Radicale.** Dato un monomio m sia $\sqrt{m} = \prod_{x_h \mid m} x_h$ la sua *parte libera da quadrati*; allora $\sqrt{I} = (\sqrt{m_1}, \dots, \sqrt{m_s})$.

Osserviamo che, da **T.** 33.3, insieme con **E.**18.5, discende che, per un qualsiasi ideale $J = (n_1, \dots, n_t)$, avremo

$$I : J = \bigcap_{j=1}^{t} I : n_j = \bigcap_{j=1}^{t} \left(\frac{m_1}{\gcd(m_1, n_j)}, \dots, \frac{m_s}{\gcd(m_t, n_j)} \right).$$

***Dimostrazione T.** 33* Osserviamo innanzitutto che, se I e J sono monomiali, allora $I \cap J$ è monomiale: infatti se $f \in I \cap J$, tutti i suoi monomi devono stare sia in I che in J, quindi per **T.**30 anche $I \cap J$ è monomiale.

1. È chiaro che $(I, m) \cap (I, n) \supseteq (I, mn)$. Vediamo l'altro contenimento. Innanzitutto osserviamo che se $f = \sum_{\mathbf{a}} c_{\mathbf{a}} X^{\mathbf{a}} \in (I, m) \cap (I, n)$, allora dato che (I, m) e (I, n) sono ancora ideali monomiali, ogni termine $c_{\mathbf{a}} X^{\mathbf{a}} \in (I, m) \cap (I, n)$, quindi è sufficiente considerare il caso in cui f sia un monomio u. Possiamo supporre anche che $u \notin I$, altrimenti avremmo finito; avremo allora che $u = am = bn$ e, dato che m e n sono relativamente primi, $m | b$ e quindi $u = cmn$ per qualche $c \in \mathrm{Mon}(A)$.

2. Indichiamo con $d_{ij} = \mathrm{lcm}(m_i, n_j)$. È chiaro che l'ideale generato dai d_{ij} è contenuto in $I \cap J$.

Sia ora $f \in I \cap J$ che è monomiale, allora ogni monomio di f è del tipo $X^{\mathbf{a}} n_j$ per qualche j e, per **T.**30, deve essere divisibile per un qualche m_i. Dunque $m_i | X^{\mathbf{a}} n_j$ e quindi $d_{ij} | X^{\mathbf{a}} n_j$ e $f \in (d_{ij} \colon i = 1, \dots, s\,,\ j = 1, \dots, t)$.

3. Sia $d_i = \gcd(m_i, m)$ per ogni $i = 1, \dots, s$; allora possiamo scrivere $m_i = a_i d_i$ e $m = b_i d_i$ con $\gcd(a_i, b_i) = 1$, per opportuni a_i, b_i, per ogni i. Dato che $I : m = \{f \in A \ : \ fm \in I\}$, avremo $a_i m = a_i b_i d_i = b_i m_i \in I$, da cui discende che $(a_1, \dots, a_s) \subset I : m$.

Per l'inclusione opposta, se $f = \sum_i c_i n_i$, con $c_i \in K$ e $n_i \in \mathrm{Mon}(A)$, è la scrittura di f come somma di termini e $fm = \sum_i c_i n_i m \in I$, si ha che per ogni i esistono monomi $m_{k_i} \in I$ e $e_i \in \mathrm{Mon}(A)$ tali che $n_i m = e_i m_{k_i} = e_i a_{k_i} d_{k_i}$. Si ha che $n_i m = n_i b_{k_i} d_{k_i}$, dunque $e_i a_{k_i} d_{k_i} = n_i b_{k_i} d_{k_i}$, che implica $a_{k_i} | n_i$, e quindi $f \in (a_1, \dots, a_s)$.

4. L'inclusione $\sqrt{I} \supseteq (\sqrt{m_1}, \dots, \sqrt{m_s})$ è ovvia. Per il viceversa, sia $f = \sum_{\mathbf{a}} c_{\mathbf{a}} X^{\mathbf{a}} \in \sqrt{I}$ e sia $k \in \mathbb{N}$ tale che $f^k \in I$. Allora ogni monomio di f^k appartiene ad I e, in particolare, per ogni $\mathbf{a}$ tale che $c_{\mathbf{a}} \neq 0$ esiste i tale che $m_i | X^{k\,\mathbf{a}}$. Ne segue che $\sqrt{m_i}\,| X^{\mathbf{a}}$ e quindi $f \in (\sqrt{m_1}, \dots, \sqrt{m_s})$.

Ideali monomiali speciali

T. 34. Sia I un ideale monomiale di A con $G(I) = \{m_1, \dots, m_s\}$.

1. **Test di primalità.** I è primo se e solo se per ogni $i \in \{1, \dots, s\}$ esiste $j_i \in \{1, \dots, n\}$ tale che $m_i = x_{j_i}$, ovvero se e solo se I è generato da un insieme di variabili.
2. **Test radicale.** I è radicale se e solo se m_i è libero da quadrati, per ogni $i \in \{1, \dots, s\}$.
3. **Test di irriducibilità.** I è irriducibile se e solo se, per ogni $i \in \{1, \dots, s\}$, esistono $j_i \in \{1, \dots, n\}$ e $b_i > 0$ tali che $m_i = x_{j_i}^{b_i}$, ovvero se e solo se I è generato da potenze pure delle variabili.
4. **Test di primarietà.** I è primario se e solo se $m_i = x_1^{a_1} \cdots x_n^{a_n} \in G(I)$ implica che per ogni $a_i \neq 0$ esiste $m_{j_i} = x_i^{b_i} \in G(I)$ per qualche $b_i > 0$, ovvero se e solo se $G(I)$ contiene una potenza pura di ogni variabile che compare in almeno uno dei monomi $m_1, \dots, m_s$.

Come corollario dell'ultimo fatto otteniamo che se I è un ideale monomiale irriducibile allora è primario, cf. **T.**154.

***Dimostrazione* T. 34** 1. Sia $I = (x_{i_1}, \dots, x_{i_k})$, allora $K[x_1, \dots, x_n]/I$ è un dominio quindi I è primo. Viceversa, per ogni $i \in \{1, \dots, s\}$ esiste $j_i \in \{1, \dots, n\}$ tale che $x_{j_i} | m_i$, ossia $m_i = x_{j_i} n_i$: dato che $G(I)$ è minimale $n_i \notin I$, quindi, visto che I è primo, $x_{j_i} \in I$ e ciò implica $m_i = x_{j_i}$ ancora per la minimalità.

2. Per ogni $i = 1, \dots, s$ si ha che m_i è libero da quadrati se e solo se $m_i = \sqrt{m_i}$ se e solo se $I = \sqrt{I}$, cf. **T.**33.4.

3. Sia I irriducibile. Se esiste $m_i = nm$ con $gcd(n, m) = 1$, allora $I \subsetneq (I, n)$, $I \subsetneq (I, m)$ e $(I, n) \cap (I, m) = I$, per **T.**33.1, contro le ipotesi.

Viceversa, supponendo di aver riordinato le variabili, se necessario, in modo tale che $G(I)$ sia $\{x_1^{a_1}, \dots, x_k^{a_k}\}$ per un certo $k \leq n$, denotiamo $X = x_1, \dots, x_k$ e $Y = x_{k+1}, \dots, x_n$.

Siano J, L ideali di $A = K[x_1, \dots, x_n] = K[X, Y]$, non necessariamente monomiali, tali che $I = J \cap L$; proveremo che esiste $p(Y) \in K[Y]$ tale $p(Y) x_1^{a_1 - 1} \cdots x_k^{a_k - 1} \in I$, da cui troviamo l'assurdo, dato che $I = (x_1^{a_1}, \dots, x_k^{a_k})$. Siano ora $f \in J \setminus I$ e $g \in L \setminus I$, allora $fg \in I$ e possiamo supporre che nessun monomio di f o di g sia in I. Consideriamo f e scriviamolo come polinomio in $K[Y][X]$, $f = \sum_{\mathbf{a}} c_{\mathbf{a}}(Y) X^{\mathbf{a}}$. Sia $X^{\boldsymbol{\delta}}$ il monomio di f di grado totale $|\boldsymbol{\delta}| = \delta_1 + \ldots + \delta_k$ minimale. Allora, per ogni i, $\delta_i < a_i$ e per ogni altro monomio m in f esiste almeno un i tale che $\deg_{x_i} m > \delta_i$. Sia $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_k)$ dato da $\gamma_i = a_i - \delta_i - 1 \geqslant 0$. Per costruzione $X^{\boldsymbol{\gamma} + \boldsymbol{\delta}} = x_1^{a_1 - 1} \cdots x_k^{a_k - 1} \notin I$. Inoltre $X^{\boldsymbol{\gamma}} m \in I$ per ogni monomio m di f diverso da $X^{\boldsymbol{\delta}}$. Quindi otteniamo $X^{\boldsymbol{\gamma}}(f - c_{\boldsymbol{\delta}}(Y) X^{\boldsymbol{\delta}}) \in I \subseteq J$, da cui $c_{\boldsymbol{\delta}}(Y) x_1^{a_1 - 1} \cdots x_k^{\alpha_k - 1} = X^{\boldsymbol{\gamma}} f - X^{\boldsymbol{\gamma}}(f - c_{\boldsymbol{\delta}}(Y) X^{\boldsymbol{\delta}}) \in J$.
Ripetendo il ragionamento per il polinomio $g \in L \setminus I$, troveremo opportuni $\boldsymbol{\varepsilon}$ e $\boldsymbol{\eta}$ e $d_{\boldsymbol{\varepsilon}}(Y)$, tali che $d_{\boldsymbol{\varepsilon}}(Y) x_1^{a_1 - 1} \cdots x_k^{a_k - 1} = X^{\boldsymbol{\eta}} g - X^{\boldsymbol{\eta}}(g - d_{\boldsymbol{\varepsilon}}(Y) X^{\boldsymbol{\varepsilon}}) \in L$.
Da questo segue allora che $p(Y) = c_{\boldsymbol{\delta}}(Y) d_{\boldsymbol{\varepsilon}}(Y)$ ha la proprietà richiesta, dato che $p(Y) x_1^{a_1 - 1} \cdots x_k^{a_k - 1} \in J \cap L = I$.

4. Supponiamo che I sia primario, e sia $m_i = x_k n$; visto che $G(I)$ è un insieme di generatori minimale, avremo che $n \notin I$; allora $x_k^a \in I$.

Viceversa, eventualmente riordinando le variabili, supponiamo che tutti i monomi di $G(I)$ appartengano a $K[x_1, \dots, x_r]$, $r \leq n$; allora per **T.**33.4, dall'ipotesi discende che $\sqrt{I} = (x_1, \dots, x_r)$. Consideriamo l'omomorfismo di

inclusione

$$\phi : K[x_1, \ldots, x_n] \longrightarrow K(x_{r+1}, \ldots, x_n)[x_1, \ldots, x_r].$$

L'ideale $\sqrt{(\phi(I))} = (x_1, \ldots, x_r)$ è massimale in $K(x_{r+1}, \ldots, x_n)[x_1, \ldots, x_r]$ quindi $(\phi(I))$ è primario per **T.**7. Dato che $(\phi(I))^c = I$, perché hanno gli stessi generatori, si ha la tesi.

Esempio 2.1. Sia $I = (x_1^3\, x_2\,,\ x_1^4\, x_2\, x_3^3,\ x_1^7,\ x_1^2\, x_3^3)$. Dato che $x_1^2\, x_3^3 \mid x_1^4\, x_2\, x_3^4$ possiamo ridurre l'insieme dei generatori e ottenere $I = (x_1^3\, x_2,\ x_1^7,\ x_1^2\, x_3^3)$. Usando il monomio $x_1^2\, x_3^3$, per **T.**33.1, possiamo spezzare l'ideale e ottenere $I = (I,\, x_1^2) \cap (I,\, x_3^3) = (x_1^2) \cap (x_1^3\, x_2\,,\ x_1^7,\ x_3^3)$. Ripetendo il procedimento, usando il monomio $x_1^3\, x_2$ e riducendo i generatori ottenuti si ha $I = (\, x_1^2) \cap (x_1^3, x_3^3) \cap (x_1^7, x_2, x_3^3)$. In particolare questa è una decomposizione di I come intersezione di ideali irriducibili, e quindi anche primari.

2.2 Basi di Gröbner

Vogliamo ora estendere ai polinomi in più variabili i concetti di grado e coefficiente direttivo e definire un'operazione di divisione di un polinomio per un insieme di polinomi. A tal scopo, iniziamo definendo un ordinamento sull'insieme $\mathrm{Mon}(A)$, che equivale ad ordinare gli elementi di $\mathbb{N}^n$. Fra gli ordinamenti possibili, siamo interessati ad ordinamenti che soddisfano le seguenti proprietà e che chiameremo *ordinamenti monomiali*.

Ordinamento monomiale

Un ordinamento monomiale è una relazione d'ordine $>$ su $\mathbb{N}^n$ o, equivalentemente, su $\mathrm{Mon}(A)$, che verifica le seguenti proprietà:

i) $>$ è un ordinamento totale;

ii) $>$ è un buon ordinamento cioè ogni sottoinsieme non vuoto di $\mathbb{N}^n$ ha un elemento minimo rispetto a $>$ (o, equivalentemente, ogni catena

decrescente in $\mathbb{N}^n$ è stazionaria, cf. **E.**72 o **T.**150);
iii) per ogni $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n$, $\mathbf{a} > \mathbf{b} \implies \mathbf{a}+\mathbf{c} > \mathbf{b}+\mathbf{c}$.

Tra gli ordinamenti più usati ci sono i seguenti, cf. **E.**73.

Siano $\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{N}^n$; indichiamo con $|\mathbf{a}| = \sum_{i=1}^n a_i$, $|\mathbf{b}| = \sum_{i=1}^n b_i$.

- *ordinamento* **lex** o *lessicografico*,
  $\mathbf{a} >_{\text{lex}} \mathbf{b}$ se e solo se la prima componente non nulla di $\mathbf{a}-\mathbf{b}$ è > 0.
- *ordinamento* **deglex**,
  $\mathbf{a} >_{\text{deglex}} \mathbf{b}$ se e solo se $|\mathbf{a}| > |\mathbf{b}|$ oppure se $|\mathbf{a}| = |\mathbf{b}|$ e $\mathbf{a} >_{\text{lex}} \mathbf{b}$.
- *ordinamento* **degrevlex**,
  $\mathbf{a} >_{\text{degrevlex}} \mathbf{b}$ se e solo se $|\mathbf{a}| > |\mathbf{b}|$ oppure se $|\mathbf{a}| = |\mathbf{b}|$ e l'ultima componente non nulla di $\mathbf{a}-\mathbf{b}$ è < 0.

Dato un ordinamento monomiale $>$ e un polinomio $0 \neq f = \sum_{\mathbf{a}} c_{\mathbf{a}} X^{\mathbf{a}} \in A$, con $c_{\mathbf{a}} \in K$, si introducono le seguenti definizioni:

- il **multigrado** di f: $\text{Deg}(f) = \max_>\{\mathbf{a} \in \mathbb{N}^n : c_{\mathbf{a}} \neq 0\}$;
- il **coefficiente direttore** di f: $\text{lc}(f) = c_{\text{Deg}(f)}$;
- il **monomio di testa** di f: $\text{lm}(f) = X^{\text{Deg}(f)}$;
- il **termine di testa** di f: $\text{lt}(f) = \text{lc}(f)\text{lm}(f) = c_{\text{Deg}(f)} X^{\text{Deg}(f)}$.

Notiamo inoltre che se $f, g \in A$ sono polinomi non nulli, allora si ha:

- $\text{Deg}(fg) = \text{Deg}(f) + \text{Deg}(g)$;
- se $f + g \neq 0$ allora $\text{Deg}(f+g) \leq \max_>\{\text{Deg}(f), \text{Deg}(g)\}$.

Fissato un ordinamento monomiale $>$, possiamo associare ad ogni ideale $0 \neq I \subset A$ l'insieme

$$\text{Deg}(I) = \{\text{Deg}(f) \ : \ f \in I, f \neq 0\}.$$

È facile verificare che è un $\mathcal{E}$-sottoinsieme, che dunque ha un escalier. Per definizione chiamiamo il suo escalier $E(I)$ l'*escalier* di I. Possiamo inoltre associare ad I l'ideale monomiale

$$\mathrm{Lt}\,(I) = (\mathrm{lt}\,(f)\colon f \in I, f \neq 0) = (\mathrm{lm}(f)\colon f \in I, f \neq 0),$$

che si chiama *l'ideale iniziale* o leading term ideal *di I rispetto a $>$*. Per definizione, l'escalier di I coincide con quello del suo ideale iniziale.

In generale, dato un sottoinsieme $F \subseteq A \setminus \{0\}$, definiamo $\mathrm{Lt}(F) = (\mathrm{lt}(f)\colon f \in F)$. Chiaramente, dato un sottoinsieme G di un ideale I, avremo sempre che $\mathrm{Lt}(G) \subseteq \mathrm{Lt}(I)$.

Base di Gröbner

Siano $>$ un ordinamento monomiale e I un ideale di A. Diremo che un insieme $G = \{g_1, \ldots, g_t\} \subset I \setminus \{0\}$ è *una base di Gröbner di I* rispetto all'ordinamento $>$ se

$$\mathrm{Lt}(G) = (\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t)) = \mathrm{Lt}(I).$$

2.2.1 La divisione di polinomi in più variabili

Per il resto di questa sezione supponiamo di avere fissato un ordinamento monomiale $>$.

Siano $f, g \in A \setminus \{0\}$, diciamo che un polinomio f *riduce ad un polinomio $h \in A$ modulo g (in un passo)* se e solo se esiste un termine $t_{\mathbf{b}} = c_{\mathbf{b}} X^{\mathbf{b}}$ in f, tale che $\mathrm{lt}(g) \mid t_{\mathbf{b}}$ e $h = f - \frac{t_{\mathbf{b}}}{\mathrm{lt}(g)} g$. Indichiamo l'operazione di riduzione con $f \xrightarrow{g} h$.

Osserviamo che, con l'operazione di riduzione, tutto il termine $t_{\mathbf{b}}$ viene sostituito con una somma di termini di multigrado strettamente minore di $\mathbf{b}$.

Esempio 2.2. Consideriamo l'anello $K[x, y, z]$ con l'ordinamento lessicografico dato da $x > y > z$. Siano $f = 3x^2y^3z^2 + xy^2z + 2xy$, $\quad g = 2xy - z$ e $t_{\mathbf{b}} = 3x^2y^3z^2$. Allora $\mathrm{lt}(g) = 2xy$ e $f \xrightarrow{g} h = f - \frac{3x^2y^3z^2}{2xy} g = xy^2z + 2xy + \frac{3}{2}xy^2z^3$. Il termine $t_{\mathbf{b}}$ è stato sostituito dal termine $\frac{3}{2}xy^2z^3$ che è di multigrado strettamente minore, dato che $(1, 2, 3) < (2, 3, 2)$ nell'ordinamento lex.

Si può ripetere la riduzione fino a quando nessun termine di f è divisibile per $\mathrm{lt}(g)$, in tal caso scriveremo $f \xrightarrow{g}_* h$ e diremo che h è *ridotto rispetto a* g.

Esempio 2.3. Siano f e g come nell'esempio precedente, allora:

$$f \xrightarrow{g} \frac{3}{2}xy^2z^3 + xy^2z + 2xy \xrightarrow{g} \frac{3}{2}xy^2z^3 + xy^2z + z \xrightarrow{g} xy^2z + \frac{3}{4}yz^4 + z$$
$$\xrightarrow{g}_* \frac{3}{4}yz^4 + \frac{1}{2}yz^2 + z.$$

Possiamo operare in modo analogo rispetto ad un insieme di polinomi.

Siano $f, f_1, \ldots, f_s \in A \setminus \{0\}$. Diciamo che f *riduce ad un polinomio* $r \in A$ *modulo l'insieme* $F = \{f_1, \ldots, f_s\}$ quando esistono indici $i_1, \ldots, i_k \in \{1, \ldots, s\}$ e polinomi $h_1, \ldots, h_{k-1} \in A$ tali che

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \cdots \xrightarrow{f_{i_{k-1}}} h_{k-1} \xrightarrow{f_{i_k}} r.$$

Indichiamo l'operazione di riduzione di f modulo un insieme di polinomi F con $f \xrightarrow{F} r$.

Se inoltre $r = \sum r_{\mathbf{a}} X^{\mathbf{a}} \in A$ è *ridotto* rispetto ad F, ossia se $r = 0$ oppure se $\mathrm{lt}(f_i)$ non divide $r_{\mathbf{a}} X^{\mathbf{a}}$ per ogni $\mathbf{a}$ tale che $r_{\mathbf{a}} \neq 0$ e per ogni $i \in \{1, \ldots, s\}$, e quindi se r non può essere ridotto ulteriormente modulo F, chiamiamo il polinomio r *un resto* di f rispetto a F, e scriviamo $f \xrightarrow{F}_* r$.

Diciamo *un* resto poiché il processo di riduzione dipende dall'ordine in cui si usano i polinomi dell'insieme F. Siano per esempio $f = x_1x_2 - x_2$, $f_1 = x_1 - 1$ e $f_2 = x_1x_2$ elementi di $K[x_1, x_2]$, dotato dell'ordinamento lex con $x_1 > x_2$; allora $f \xrightarrow{f_1}_* 0$ mentre $f \xrightarrow{f_2}_* -x_2$.
L'operazione di riduzione permette tuttavia di definire la divisione di un polinomio per un insieme di polinomi in modo analogo alla divisione per polinomi in una variabile. Eseguiamo la divisione di un polinomio f per un

insieme di polinomi $\{f_1, \ldots, f_s\}$ usando il procedimento descritto dal seguente algoritmo, tralasciando i casi banali in cui f e/o $f_i = 0$.

Algoritmo di divisione

Input $f, f_1, \ldots, f_s \in A \setminus \{0\}$
Output $u_1, \ldots, u_s, r \in A$ tali che:

- $f = \sum_{i=1}^{s} u_i f_i + r$;
- r è ridotto rispetto a $\{f_1, \ldots, f_s\}$;
- se $u_i f_i \neq 0$, allora $\mathrm{Deg}(u_i f_i) \leq \mathrm{Deg}(f)$.

Inizializzazione $p := f$; $u_1 := 0$; $u_2 := 0$; $\ldots$, $u_s := 0$; $r := 0$;

while $p \neq 0$ **repeat**
  if esiste j tale che $\mathrm{lt}(f_j) \,|\, \mathrm{lt}(p)$ **then**
    $i := \min\{j \ : \ \mathrm{lt}(f_j) \,|\, \mathrm{lt}(p)\}$
    $u_i := u_i + \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)}$
    $p := p - \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)} f_i$
  else
    $r := r + \mathrm{lt}(p)$
    $p := p - \mathrm{lt}(p)$
  endif
endwhile
return $\{u_1, \ldots, u_s, r\}$

I polinomi $u_1, \ldots, u_s$ ed r ottenuti col precedente algoritmo soddisfano le seguenti proprietà.

Teorema di divisione

T. 35. Fissato un ordinamento monomiale, per ogni insieme di polinomi $F = \{f_1, \ldots, f_s\}$ e $f \in A$ esistono polinomi $u_1, \ldots, u_s$, $r \in A$ tali che

1. $f = \sum_{i=1}^{s} u_i f_i + r$;
2. r è ridotto rispetto a F;

3. se $u_i f_i \neq 0$, allora $\mathrm{Deg}(u_i f_i) \leq \mathrm{Deg}(f)$.

Dimostrazione T. *35* Bisogna provare che l'algoritmo di divisione termina e che i polinomi $u_1, \ldots, u_s$ e r ottenuti soddisfano le condizioni richieste. Cominciamo col dimostrare che ad ogni passo si ha $f = u_1 f_1 + \ldots + u_s f_s + p + r$. Sicuramente la relazione è vera al primo passo. Supponiamo allora che sia vera al passo $(n-1)$-esimo. Eseguendo il passo n-esimo, l'algoritmo procede in uno dei due modi seguenti:

1. se $\mathrm{lt}(f_i) \mid \mathrm{lt}(p)$, vale che $u_i f_i + p = \left(u_i + \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)}\right) f_i + p - \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)} f_i$ e dunque $u_i f_i + p$ rimane invariato;
2. se si aggiorna il resto, ossia se per ogni i si ha che $\mathrm{lt}(f_i) \nmid \mathrm{lt}(p)$, si ha $p + r = (p - \mathrm{lt}(p)) + (r + \mathrm{lt}(p))$ e dunque $p + r$ rimane invariato.

Quindi in entrambi i casi la relazione continua a valere.
Proviamo ora che l'algoritmo termina. Per farlo, basta ricordare che $>$ è un buon ordinamento e che ad ogni passo, in entrambi i casi a $\mathrm{lt}(p)$ si sostituisce $\mathrm{lt}(p - \mathrm{lt}(p))$ che ha multigrado strettamente minore del multigrado di p.
Per la condizione su r basta osservare che l'algoritmo aggiunge ad r solo monomi non divisibili per nessun $\mathrm{lt}(f_i)$, quindi r è ridotto rispetto ad F.
Infine, verifichiamo che vale la condizione sul grado di $u_i f_i$. Innanzitutto $\mathrm{Deg}(p) \leq \mathrm{Deg}(f)$; quando ad un passo si modifica u_i, lo si fa aggiungendo un addendo del tipo $\frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)}$, dove $\frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)} f_i$ cancella quello che a quel passo risulta essere $\mathrm{lt}(p)$. Quindi $\mathrm{Deg}(u_i f_i) \leq \mathrm{Deg}(p) \leq \mathrm{Deg}(f)$, come voluto.

Osservazione 2.4. Come conseguenza dell'algoritmo si ha immediatamente che il leading monomial di f compare in r oppure in qualcuno tra i leading monomial di $u_i f_i$. Più precisamente

$$\mathrm{lm}(f) = \begin{cases} \max\{\, \max_{u_i \neq 0}\{\, \mathrm{lm}(u_i)\mathrm{lm}(f_i)\,\},\, \mathrm{lm}(r)\,\} & \text{se } r \neq 0; \\ \max_{u_i \neq 0}\{\, \mathrm{lm}(u_i)\mathrm{lm}(f_i)\} & \text{altrimenti.} \end{cases}$$

Osserviamo inoltre che implicitamente l'algoritmo di divisione assume che i polinomi $f_1, \ldots, f_s$ siano ordinati, quando si sceglie il minimo indice i tale che $\mathrm{lt}(f_i) \mid \mathrm{lt}(p)$, e in effetti questa scelta può modificare il risultato della divisione,

cf. **E.**76. In generale anche il resto della divisione può dipendere dall'ordine in cui vengono considerati i polinomi per cui si divide. Vedremo che questo fatto non è più vero se $f_1, \ldots, f_s$ costituiscono una base di Gröbner per l'ideale che generano. Anzi, questa proprietà caratterizza le basi di Gröbner.

2.2.2 Basi di Gröbner: prime proprietà

Ricordiamo la definizione

Base di Gröbner

Siano $>$ un ordinamento monomiale e I un ideale di A. Diremo che un insieme $G = \{g_1, \ldots, g_t\} \subset I \setminus \{0\}$ è *una base di Gröbner di* I rispetto all'ordinamento $>$ se

$$\mathrm{Lt}(G) = (\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t)) = \mathrm{Lt}(I).$$

Equivalentemente G è una base di Gröbner se $\{\mathrm{Deg}(g_1), \ldots, \mathrm{Deg}(g_t)\}$ è una frontiera di $\mathrm{Deg}(I)$, ossia se $\mathrm{Deg}(I) = \bigcup_{i=1}^{t}(\mathrm{Deg}(g_i) + \mathbb{N}^n)$. Diciamo che $\{g_1, \ldots, g_t\} \subset I$ è una base di Gröbner *minimale* rispetto all'ordinamento $>$ se i polinomi g_i sono monici e $\{\mathrm{Deg}(g_1), \ldots, \mathrm{Deg}(g_t)\}$ è l'escalier di $\mathrm{Deg}(I)$. In altre parole, se i polinomi g_i sono monici e l'insieme minimale di generatori monomiali $G(\mathrm{Lt}(I))$ è proprio $\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t)\}$.

T. 36. Siano $I \subset A$ un ideale, $G = \{g_1, \ldots, g_t\} \subset I \setminus \{0\}$ e $>$ un ordinamento monomiale. Sono fatti equivalenti:

1. G è una base di Gröbner di I rispetto a $>$;
2. $f \in I$ se e solo se $f \xrightarrow{G}_* 0$.
3. $f \in I$ se e solo se $f = \sum_{i=1}^{t} u_i g_i$, con $\mathrm{lm}(f) = \max_{u_i \neq 0}\{\mathrm{lm}(u_i)\mathrm{lm}(g_i)\}$.

***Dimostrazione T.** 36* Dato un polinomio $0 \neq f \in A$, dividendo per l'insieme G, per il teorema di divisione otteniamo $f = \sum_{i=1}^{t} u_i g_i + r$ con r ridotto rispetto a G.

$1 \Rightarrow 2$. È sempre vero che, se $f \xrightarrow{G}_* 0$ allora esistono $u_1, \ldots, u_t \in A$ tali che $f = \sum_{i=1}^{t} u_i g_i$; quindi $f \in (G) \subseteq I$.

Supponiamo che $f \in I$; allora $r = \sum r_{\mathbf{a}} X^{\mathbf{a}} \in I$ e se $r \neq 0$ si dovrebbe avere che $\mathrm{lt}(r) \in \mathrm{Lt}(G)$, ma ciò contraddice il fatto che r è ridotto rispetto a G. Si conclude che $r = 0$.

$2 \Rightarrow 3$. Ovviamente, se $f = \sum_{i=1}^{t} u_i g_i$ allora $f \in I$.

Per il viceversa, sia $f \in I$: per ipotesi si ha $f \xrightarrow{G}_* 0$, dunque per l'algoritmo di divisione f è una combinazione dei g_i con coefficienti $u_i \in A$. Infine, l'uguaglianza $\mathrm{lm}(f) = \max_{u_i \neq 0}\{\mathrm{lm}(u_i)\mathrm{lm}(g_i)\}$ segue dall'Osservazione 2.4 e dal fatto che $r = 0$.

$3 \Rightarrow 1$. Proviamo che si ha $\mathrm{Lt}(I) = \mathrm{Lt}(G)$. È sempre vero che $\mathrm{Lt}(G) \subseteq \mathrm{Lt}(I)$; per l'altra inclusione, proviamo che per ogni $0 \neq f \in I$ si ha $\mathrm{lm}(f) \in (\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t))$. Se $f \in I$ allora per ipotesi esistono $u_1, \ldots, u_t$ tali che $f = \sum_{i=1}^{t} u_i g_i$, con $\mathrm{lm}(f) = \max_{u_i \neq 0}\{\mathrm{lm}(u_i)\mathrm{lm}(g_i)\}$, e da ciò discende la tesi.

T. 37. Sia $G = \{g_1, \ldots, g_t\}$ una base di Gröbner di I rispetto a $>$. Allora $I = (g_1, \ldots, g_t)$, ovvero una base di Gröbner di I è un insieme di generatori di I.

Dimostrazione T. 37 È una diretta applicazione di **T.**36. Se $f \in I$ allora $f \xrightarrow{G}_* 0$, ovvero $f = \sum_{i=1}^{t} u_i g_i$ per qualche $u_i \in A$; pertanto $I \subseteq (g_1, \ldots, g_t)$.

Per brevità diremo anche che un insieme $G \subset A$ è una base di Gröbner se è una base di Gröbner per l'ideale (G) che esso genera.
Di fondamentale importanza è il seguente risultato.

T. 38. Sia $G = \{g_1, \ldots, g_t\} \subset I \setminus \{0\}$. Allora G è una base di Gröbner per I rispetto a $>$ se e solo se per ogni $f \in A$ il resto della divisione di f per G è unico.

Dimostrazione T. 38 Sia $f \in A \setminus \{0\}$. Dall'algoritmo di divisione si ha che $f = \sum_{i=1}^{t} u_i g_i + r$, con $r = \sum_{\mathbf{a}} r_{\mathbf{a}} X^{\mathbf{a}}$. Se $r_{\mathbf{a}} \neq 0$ allora $r_{\mathbf{a}} X^{\mathbf{a}} \notin \mathrm{Lt}(G) = \mathrm{Lt}(I)$. Sia r' un altro resto, allora l'elemento $r - r' \in I$ ma nessuno dei suoi monomi diversi da zero può appartenere a $\mathrm{Lt}(I)$. Si deve avere necessariamente $r - r' = 0$.

Viceversa, grazie a **T.**36, ci basta dimostrare che se $0 \neq f \in I$ e $f \xrightarrow{G}_* r$, allora $r = 0$. Una dimostrazione di questo fatto si trova in [AL, Theorem 1.6.7].

Osserviamo che una base di Gröbner rispetto ad un ordinamento monomiale $>$ non è in generale base di Gröbner rispetto ad un altro ordinamento monomiale $>_1$, cf. **E.**75.
Grazie al precedente risultato abbiamo la seguente

Unicità del resto
Data una base di Gröbner G e un polinomio $f \in A$ *esiste un unico* r *ridotto modulo* G *tale che* $f \xrightarrow{G}_* r$. Chiameremo r *il resto* della divisione di f per G e lo indicheremo con la notazione $\overline{f}^G$.

È importante osservare che, mentre il resto della divisione di un polinomio per una base di Gröbner G è unico e indipendente dall'ordine con cui i polinomi sono considerati, questo non è vero per i coefficienti u_i dei polinomi di G nell'espressione di f. Consideriamo ad esempio $G = \{g_1, g_2\} = \{x_1 + x_3, x_2 - x_3\}$ e sia $f = x_1x_2$. Non è difficile verificare che G è una base di Gröbner rispetto all'ordinamento lessicografico dato da $x_1 > x_2 > x_3$. Ciò nonostante, se eseguiamo la divisione dividendo prima per g_1 e poi per g_2 otteniamo $f = x_2\, g_1 - x_3\, g_2 - x_3^2$ mentre se dividiamo prima per g_2 e poi per g_1 si ha $f = x_1\, g_2 + x_3\, g_1 - x_3^2$. Quindi il resto è unico, ma i coefficienti dei polinomi g_1, g_2 nelle due espressioni di f sono diversi.

T. 39. Siano $G = \{g_1, \ldots, g_t\}$ e $G' = \{g'_1, \ldots, g'_{t'}\}$ due basi di Gröbner di $I \subset A$ rispetto ad uno stesso ordinamento monomiale fissato, e siano r ed r' i resti della divisione di un polinomio $f \in A$ per G e G' rispettivamente. Si ha allora $r = r'$.

***Dimostrazione T.** 39* Osserviamo che $r = f - h$ e $r' = f - h'$, con $h, h' \in I$, pertanto $r - r' \in I$. Allora, se per assurdo $r - r' \neq 0$, avremmo che $\mathrm{lt}(r - r') \in \mathrm{Lt}(I)$. Per ipotesi allora esistono $g_i \in G$ e $g'_j \in G'$ tali che $\mathrm{lt}(g_i)$ e $\mathrm{lt}(g'_j)$ lo dividono, ma $\mathrm{lt}(r - r')$ è un termine che proviene o da r o da r'; in

ogni caso si ha una contraddizione, poiché r è ridotto modulo G, r' è ridotto modulo G' e $\mathrm{Lt}(G) = \mathrm{Lt}(G')$.

Come conseguenza dei risultati precedenti otteniamo anche il seguente fondamentale teorema.

Teorema della base di Hilbert

T. 40. Ogni ideale di $A = K[x_1, \ldots, x_n]$ è finitamente generato.

Dimostrazione T. 40 Fissiamo su A un ordinamento monomiale $>$ e sia I un ideale di A. Allora l'ideale iniziale $\mathrm{Lt}(I)$ rispetto a $>$ ha un sistema di generatori monomiale finito, diciamo $\mathrm{Lt}(I) = (m_1, \ldots, m_t)$. Allora esiste $f_i \in I$ tale che $\mathrm{lt}(f_i) = m_i$ per ogni $i = 1, \ldots, t$; da ciò segue che $\{f_1, \ldots, f_t\}$ è una base di Gröbner di I, e dunque da **T.**37 segue che $I = (f_1, \ldots, f_t)$.

Un anello in cui ogni ideale è finitamente generato si dice *noetheriano*, cf. Capitolo 7; l'anello dei polinomi a coefficienti in K è dunque un esempio di tale anello, per quanto appena dimostrato. Per il risultato generale cf. **T.**151.

T. 41. Sia A un anello; allora A è noetheriano se e solo se ogni catena ascendente di ideali di A è stazionaria.

Lasciamo al lettore la dimostrazione di questo fatto per esercizio, in attesa della dimostrazione generale nel caso dei moduli, cf. **T.**152.1.

2.2.3 Costruzione di una base di Gröbner

Abbiamo visto che se G è una base di Gröbner di I allora G è un insieme di generatori di I e per ogni polinomio $f \in I$ esiste un elemento $g_i \in G$ tale che $\mathrm{lt}(g_i)|\mathrm{lt}(f)$. Se invece G è un insieme di generatori qualunque, non è detto che ciò sia vero, perché se $f = \sum_i u_i g_i$ in generale possono intervenire delle cancellazioni tra i termini di multigrado massimo.

Esempio 2.5. Siano $I = (f_1, f_2)$ con $f_1 = x_1x_2^2 + x_1$ e $f_2 = x_1^2x_2 + x_2$; se consideriamo l'ordinamento lessicografico con $x_1 > x_2$, si ha che il polinomio $f = x_1f_1 - x_2f_2 = x_1^2 - x_2^2 \in I$ ma $x_1^2 \notin (x_1x_2^2, x_1^2x_2) = (\mathrm{lt}(f_1), \mathrm{lt}(f_2))$.

Veniamo ora al problema di come costruire una base di Gröbner. Fondamentale a questo proposito sarà la seguente definizione: dati f, g polinomi di A con $\mathrm{Deg}(f) = \mathbf{a}$ e $\mathrm{Deg}(g) = \mathbf{b}$, sia $\mathbf{c} \in \mathbb{N}^n$ il vettore di componenti $c_i = \max\{a_i, b_i\}$, cosicché $X^{\mathbf{c}}$ sia il minimo comune multiplo di $\mathrm{lm}(f)$ e $\mathrm{lm}(g)$.

S-polinomio

Definiamo *l'S-polinomio tra* f *e* g come:

$$S(f, g) = \frac{X^{\mathbf{c}}}{\mathrm{lt}(f)} f - \frac{X^{\mathbf{c}}}{\mathrm{lt}(g)} g.$$

Vale il seguente fondamentale risultato, per la cui dimostrazione rimandiamo il lettore ad un libro di testo, cf. ad esempio [CLS, Chapter 2, §7].

Criterio di Buchberger

Siano $>$ un ordinamento fissato e $I = (g_1, \ldots, g_t)$ un ideale di A; allora $\{g_1, \ldots, g_t\}$ è una base di Gröbner rispetto a $>$ se e solo se $\overline{S(g_i, g_j)}^{G} = 0$, per ogni $i, j = 1, \ldots, t$.

Usando il precedente criterio possiamo ottenere un algoritmo per la costruzione di una base di Gröbner di un ideale $I = (f_1, \ldots, f_s)$. Procederemo calcolando dapprima gli S-polinomi $S(f_i, f_j)$ dei generatori di I e i loro resti rispetto a $\{f_1, \ldots, f_s\}$. Nel caso tali resti non siano zero, li aggiungeremo all'insieme dei generatori dato così da ottenere un nuovo insieme di generatori di I. Ripetendo questo procedimento, continueremo ad aggiungere polinomi, all'insieme $\{f_1, \ldots, f_s\}$ fino a quando tutti i resti degli S-polinomi, ridotti rispetto ai nuovi generatori, saranno zero. Dopo avere dimostrato che questa costruzione termina in un numero finito di passi, il criterio garantirà che il risultato sia una base di Gröbner. Questo procedimento è descritto dal seguente algoritmo.

Algoritmo di Buchberger

Input $I = (f_1, \ldots, f_s) \subseteq A$, $f_i \neq 0$ per $i = 1, \ldots, s$; $>$ ordinamento monomiale.

Output Una base di Gröbner G di I, rispetto a $>$, tale che $\{f_1, \ldots, f_s\} \subseteq G$.

Inizializzazione
  $F := \{f_1, \ldots, f_s\}$
  $G := F$
  $\Sigma := \{(f_i, f_j) \in G \times G \mid f_i \neq f_j\}$
while $\Sigma \neq \emptyset$ **repeat**
  for $(f, g) \in \Sigma$ **repeat**
    $\Sigma := \Sigma \setminus \{(f, g)\}$
    $p := \overline{S(f, g)}^{G}$
    if $p \neq 0$ then
      $\Sigma := \Sigma \cup \{(h, p) \ : \ h \in G\}$
      $G := G \cup \{p\}$
    endif
  endfor
endwhile
Return G

Osserviamo che ad ogni passo l'insieme G costruito dall'algoritmo è sempre contenuto in I, perché G viene aggiornato solo con resti di S-polinomi, quindi elementi di I ridotti rispetto ai generatori già presenti in G.

T. 42. L'algoritmo di Buchberger termina ed è corretto.

Dimostrazione T. 42 Sicuramente l'algoritmo è corretto, perché la condizione di terminazione è che $\overline{S(f_i, f_j)}^{G} = 0$ e questo, per il criterio di Buchberger garantisce che l'output sia effettivamente una base di Gröbner. D'altronde, se l'algoritmo non terminasse, costruiremmo progressivamente una catena ascendente di insiemi $G_1 \subsetneq G_2 \subsetneq \ldots$, ove le inclusioni sono strette perché a

G_i aggiungiamo un elemento di I che non si riduce a zero modulo G_i. Da ciò seguirebbe che in A vi è la catena infinita di ideali $\mathrm{Lt}(G_1) \subsetneq \mathrm{Lt}(G_2) \subsetneq \ldots$, ma questo viola la noetherianità di A per **T.**41.

Concludiamo questa sezione con il seguente corollario, che non dimostriamo, estremamente utile per concludere in certi casi che un insieme G è una base di Gröbner.

T. 43. Siano $G = \{g_1, \ldots, g_t\} \subset A \setminus \{0\}$, e $>$ un ordinamento monomiale. Se $\gcd(\mathrm{lt}(g_i), \mathrm{lt}(g_j)) = 1$ per ogni $i \neq j$, allora G è una base di Gröbner rispetto a $>$.

Dimostrazione T. *43* Una dimostrazione si trova in [CLS, Chapter 2, §9 Proposition 4].

2.2.4 Basi di Gröbner minimali e ridotte

Abbiamo visto che ogni ideale ammette una base di Gröbner G' rispetto ad un ordinamento $>$, e che da essa si può estrarre una base minimale G, rendendo monici i polinomi di G' ed eliminando da G' quegli elementi il cui termine di testa viene diviso da quello di uno degli altri. Queste condizioni determinano però solo quale sia il numero di elementi che compongono una base di Gröbner minimale, che deve essere $|G(\mathrm{Lt}(I))|$, ma non garantiscono l'unicità dei polinomi che la compongono.

Esempio 2.6. Sia $I = (x_1, x_2) \subset K[x_1, x_2]$ allora per ogni $a \in K$ e per ogni $n \in \mathbb{N}$ gli insiemi $\{x_1 + ax_2^n, x_2\}$ sono basi di Gröbner minimali per I, rispetto all'ordinamento lessicografico con $x_1 > x_2$.

Per ottenere un teorema di unicità imponiamo un ulteriore condizione su $G = \{g_1, \ldots, g_t\}$, richiedendo che, per ogni $i = 1, \ldots, t$, g_i sia ridotto modulo $G \setminus \{g_i\}$ e quindi che in g_i non esistano termini diversi da zero divisibili per $\mathrm{lt}(g_j)$, se $j \neq i$.

Base di Gröbner ridotta

Una base di Gröbner $G = \{g_1, \ldots, g_k\}$ di un ideale I, si dice *ridotta* se

i) è minimale, ossia:

- $\mathrm{lc}(g_i) = 1$ per ogni $i = 1, \ldots, t$;
- $\mathrm{lt}(g_i) \notin \mathrm{Lt}(G \setminus \{g_i\})$, per ogni $i = 1, \ldots, t$;

ii) $\overline{g_i}^{G-\{g_i\}} = g_i$, per ogni $i = 1, \ldots, t$.

È sempre possibile costruire una base di Gröbner ridotta usando il seguente procedimento.

Costruzione di una base di Gröbner ridotta

T. 44. Sia $G = \{g_1, \ldots, g_t\}$ una base di Gröbner minimale di un ideale $I \subset A$ rispetto ad un ordinamento $>$. Definiamo elementi $g'_1, \ldots, g'_t$ nella maniera seguente

$$
\begin{aligned}
&g_1 \xrightarrow{G'_1}_* g'_1, && \text{con } G'_1 = \{g_2, \ldots, g_t\};\\
&g_2 \xrightarrow{G'_2}_* g'_2, && \text{con } G'_2 = \{g'_1, g_3, \ldots, g_t\};\\
&g_3 \xrightarrow{G'_3}_* g'_3, && \text{con } G'_3 = \{g'_1, g'_2, g_4, \ldots, g_t\};\\
&\cdot\\
&\cdot\\
&\cdot\\
&g_t \xrightarrow{G'_t}_* g'_t, && \text{con } G'_t = \{g'_1, \ldots, g'_{t-1}\}.
\end{aligned}
$$

Allora $G' = \{g'_1, \ldots, g'_t\}$ è una base di Gröbner ridotta di I.

Dimostrazione T. *44* Dal momento che la base G è minimale, $\mathrm{lt}(g_i) \nmid \mathrm{lt}(g_j)$, per ogni $i \neq j$; quindi $\mathrm{lt}(g_i) = \mathrm{lt}(g'_i)$ per ogni $i = 1, \ldots, t$ e così G' è una base di Gröbner per I. Inoltre, dato che ad ogni passo la riduzione modulo G'_i è fatta usando $\mathrm{lt}(g'_1), \ldots, \mathrm{lt}(g'_{i-1}), \mathrm{lt}(g_{i+1}), \ldots, \mathrm{lt}(g_t)$ e $\mathrm{lt}(g_j) = \mathrm{lt}(g'_j)$ per ogni j, la base G' è ridotta.

T. 45. [Unicità della base ridotta]
Siano $G = \{g_1, \ldots, g_t\}$ e $G' = \{g'_1, \ldots, g'_t\}$ due basi di Gröbner ridotte di un ideale I rispetto ad uno stesso ordinamento $>$. Allora $G = G'$.

Dimostrazione T. *45* Dato che sia G che G' sono minimali, possiamo supporre senza perdita di generalità che $\mathrm{lt}(g_i) = \mathrm{lt}(g'_i)$ per ogni $i = 1, \ldots, t$, cf. **T.**32. Fissato allora un tale i, consideriamo il polinomio $g_i - g'_i \in I$. Se $g_i - g'_i \neq 0$ allora esiste g_j tale che $\mathrm{lm}(g_j)|\mathrm{lm}(g_i - g'_i)$. Dato che $\mathrm{lm}(g_i - g'_i) < \mathrm{lm}(g_i)$, deduciamo che $i \neq j$. Allora $\mathrm{lm}(g_j) = \mathrm{lm}(g'_j)$ divide un termine di $g_i - g'_i$, quindi uno dei termini di g_i o di g'_i, che è assurdo perché sia G che G' sono ridotte.

Osserviamo che una base di Gröbner minimale, o anche ridotta, non è necessariamente costituita da un insieme di generatori minimale di I e viceversa, ovvero un insieme di generatori di I minimale non costituisce in generale un base di Gröbner minimale.

Esempio 2.7. Siano $f_1 = x_1^3$ e $f_2 = x_1^2x_2 - x_2^2$ e $I = (f_1, f_2) \subset K[x_1, x_2]$. Fissiamo l'ordinamento lessicografico con $x_1 > x_2$. La base di Gröbner ridotta di I è $\{f_1, f_2, f_3, f_4\}$ dove $f_3 = x_1x_2^2$ e $f_4 = x_2^3$ e quindi contiene 4 elementi, mentre I può essere generato da solo 2 elementi.

2.2.5 Alcune applicazioni

Abbiamo già visto la dimostrazione del teorema della base di Hilbert come corollario del Lemma di Dickson e dei primi risultati sulle basi di Gröbner. Ora vogliamo applicare i risultati precedenti per rispondere ad alcune domande che è naturale porsi. Pensiamo ad esempio:

1. dato un polinomio $f \in A$ e un ideale $I = (f_1, \ldots, f_s) \subseteq A$, decidere se $f \in I$;
1′. in caso affermativo, trovare $c_1, \ldots, , c_s \in A$ tali che $f = \sum_{i=1}^{s} c_i f_i$;
2. stabilire se due ideali $I, J \subset A$ sono uguali;
3. trovare una rappresentazione canonica per gli elementi nel quoziente A/I;
4. trovare una base di A/I come K-spazio vettoriale;
5. decidere se un elemento è invertibile in A/I e determinarne l'inverso.

Il prossimo enunciato risponde alla prima di queste domande: bisogna calcolare una base di Gröbner G di I e controllare che il resto della divisione di f con G sia 0.

T. 46. [Test di appartenenza - Membership Test]
Siano $f \in A$, I un ideale di A e $>$ un ordinamento fissato; sia $G = \{g_1, \cdots g_t\}$ una base di Gröbner di I rispetto a $>$. Allora

$$f \in I \iff \overline{f}^G = 0$$

Dimostrazione T. 46 La tesi discende immediatamente applicando **T.**36 e **T.**38.

Si può implementare l'algoritmo di Buchberger in modo che nel calcolo di una base di Gröbner G a partire da $\{f_1, \ldots, f_s\}$ vengano memorizzati passo passo i coefficienti delle combinazioni lineari degli f_i che danno origine ai g_j: se $\{h_1, \ldots, h_l\}$ è la base calcolata ad un certo momento dall'algoritmo e un nuovo polinomio g viene aggiunto, avremo che $g = S(h_\alpha, h_\beta) - \sum_{i=1}^{l} v_i h_i$, per certi v_i che vengono esplicitamente calcolati. Come output avremo allora la base di Gröbner G e una matrice M di taglia $t \times s$ a coordinate in A e tale che

$$M[f_1, \ldots, f_s]^{\mathrm{t}} = [g_1, \ldots, g_t]^{\mathrm{t}}. \tag{2.1}$$

Ora, se dividiamo $f \in I$ per $G = \{g_1, \ldots, g_t\}$, otteniamo polinomi $u_1, \ldots, u_t$ tali che $f = \sum_{i=1}^{t} u_i g_i$. Usando la relazione vista sopra, è possibile esprimere ogni polinomio $f \in I$ come combinazione lineare dei polinomi $f_1, \ldots, f_s$. Abbiamo in questo modo risposto anche al quesito $1'$, cf. **E.** 83.

T. 47. [Test di uguaglianza tra ideali]
Siano $I, J \subset A$ due ideali e siano G e G' le basi di Gröbner ridotte di I e J rispettivamente, rispetto ad un ordinamento $>$. Allora,

$$I = J \text{ se e solo se } G = G'.$$

Dimostrazione T. 47 Il risultato segue immediatamente dal teorema di unicità delle basi di Gröbner ridotte **T.**45.

Anche il seguente criterio risulta spesso utile.

T. 48. Siano $I, J \subseteq A$ ideali tali che $I \subseteq J$. Se, per qualche ordinamento $>$, $\mathrm{Lt}(I) = \mathrm{Lt}(J)$ allora $I = J$.

***Dimostrazione* T. 48** Sia G una base di Gröbner di I rispetto a $>$. Vogliamo far vedere che ogni elemento $j \in J$ è anche elemento di I, e per far ciò basta provare che $j \xrightarrow{G}_* 0$. Se chiamiamo r il resto di j, avremmo $r = j - \sum_{i=1}^{t} u_i g_i \in J + I \subseteq J$. Se $r \neq 0$, i suoi monomi non stanno in $\mathrm{Lt}(G) = \mathrm{Lt}(I) = \mathrm{Lt}(J)$ perché r è ridotto; d'altra parte $r \in J$ e $\mathrm{lm}(r) \in \mathrm{Lt}(J)$. Pertanto $r = 0$, come volevamo.

T. 49. Sia I un ideale con base di Gröbner G rispetto a $>$.

1. L'applicazione $\overline{}^G \colon A \longrightarrow A$ definita da $f \longrightarrow \overline{f}^G$ è K-lineare.
2. Dati $f, g \in A$ si ha

$$f \equiv g \mod I \text{ se e solo se } \overline{f}^G = \overline{g}^G.$$

***Dimostrazione* T. 49** 1. Bisogna verificare che $\overline{af + bg}^G = a\overline{f}^G + b\overline{g}^G$, per ogni $f, g \in A$ e per ogni $a, b \in K$. Chiamiamo $r = \overline{f}^G$ e $s = \overline{g}^G$. Allora, $af + bg = a(f - r) + b(g - s) + ar + bs$, ove $f - r$ e $g - s$, e quindi la loro combinazione, sono elementi di I. Mostriamo che allora $ar + bs$ è proprio il resto di $af + bg$ rispetto a G: per fare questo basta osservare che i monomi di $ar + bs$ sono monomi di r oppure di s, che sono ridotti rispetto a G.

2. Abbiamo che $f \equiv g \mod I$ se e solo se $f - g \in I$ se e solo se $\overline{f - g}^G = 0$. Per il punto 1, ciò è equivalente a $\overline{f}^G - \overline{g}^G = 0$.

Dalla dimostrazione segue che $\left\{\overline{f}^G \colon f \in A\right\}$ è un insieme di rappresentanti di A/I. Infatti se $r = \overline{f}^G$ abbiamo che $f - r \in I$ e dunque $\overline{f} = \overline{r}$ in A/I.

T. 50. [K-base di A/I] Siano $I \subset A$ un ideale, $G = \{g_1, \ldots, g_t\}$ una base di Gröbner di I rispetto ad un ordinamento $>$ fissato.

1. Sia $\mathcal{B} = \{X^{\mathbf{a}} \colon \mathrm{lm}(g) \nmid X^{\mathbf{a}}, \text{ per ogni } g \in G\} = \{X^{\mathbf{a}} \colon X^{\mathbf{a}} \notin \mathrm{Lt}(I)\}$. Allora $\overline{\mathcal{B}} = \{\overline{m} \in A/I \colon m \in \mathcal{B}\}$ è una K-base di A/I.

2. Sia $f \in A$ e $\overline{f}^G = \sum_{X^{\mathbf{a}} \in \mathcal{B}} c_{\mathbf{a}} X^{\mathbf{a}}$, le coordinate di $\overline{f}$ rispetto alla base $\overline{\mathcal{B}}$ sono date dal vettore $(c_{\mathbf{a}})_{X^{\mathbf{a}} \in \mathcal{B}}$.

***Dimostrazione T.** 50* 1. Ogni elemento di A/I si può rappresentare tramite la classe $\overline{r}$, con $r = \overline{f}^G$, per un certo $f \in A$. Dato che r è ridotto rispetto a G, $\overline{r}$ risulta essere una combinazione K-lineare di monomi che non sono divisibili per $\mathrm{lt}(g_i)$, per ogni $i = 1, \ldots, t$. Abbiamo così dimostrato che $\mathcal{B}$ è un insieme di generatori.
Per dimostrare l'indipendenza lineare su K supponiamo, per assurdo, che esistano $m_1, \ldots, m_k \in \mathcal{B}$ tali che $\overline{m_1} = \sum_{i=2}^{k} a_i \overline{m_i}$ con $a_i \in K^*$ per $i = 2, \ldots, k$. Allora esiste $g \in I$ tale che $m_1 = g + \sum_{i=2}^{k} a_i m_i$; pertanto in A avremmo che $m_1 \xrightarrow{G}_* m_1$ e $m_1 \xrightarrow{G}_* \sum_{i=2}^{k} a_i m_i$, poiché $m_i \in \mathcal{B}$, e ciò nega l'unicità del resto visto che gli m_i sono ovviamente linearmente indipendenti su K.

2. La seconda affermazione è di verifica immediata.

Il seguente risultato risponde infine in maniera costruttiva alla domanda 5, fornendo un procedimento per calcolare l'inverso di $f \mod I$.

T. 51. Un elemento $f \in A$ è invertibile modulo $I = (f_1, \ldots, f_s)$ se e solo se $(I, f) = 1$.

***Dimostrazione T.** 51* Esiste $g \in A$ tale che $fg = 1 \mod I$ se e solo se $fg - 1 \in I$, cioè se e solo se $1 \in (I, f)$. È sufficiente allora calcolare una base di Gröbner G dell'ideale $(I, f) = (f_1, \ldots, f_s, f)$ rispetto ad un ordinamento $>$. Se questo ideale è proprio, allora f non è invertibile modulo I altrimenti esprimiamo $1 = u_1 g_1 + \ldots + u_t g_t$ come combinazione degli elementi della base G e dunque, usando una matrice di passaggio come in (2.1), determiniamo allora la combinazione $1 = h_1 f_1 + \ldots + h_s f_s + fg$, e dunque anche g.

2.2.6 Eliminazione ed ordinamento lessicografico

Gli ordinamenti lessicografici soddisfano una proprietà importante, che chiamiamo *di eliminazione*, che analizzeremo nel seguito, e che ha alcune applicazioni di rilievo. Per il resto della sezione sia $>$ l'ordinamento lessicografico dato da $x_1 > x_2 > \ldots > x_n$.

Sia $I \subset K[x_1, \ldots, x_n]$; chiamiamo $I_k = I \cap K[x_{k+1}, \ldots, x_n]$, con $k = 1, \ldots, n-1$, il *k-esimo ideale di eliminazione di I*. Esso è la contrazione di I rispetto all'omomorfismo di immersione $K[x_{k+1}, \ldots, x_n] \longrightarrow K[x_1, \ldots, x_n]$.

T. 52. [Teorema di eliminazione delle variabili]
Siano $I \subset A$ un ideale e sia $>$ come sopra. Sia G una base di Gröbner di I rispetto a $>$. Allora $G_k = G \cap K[x_{k+1}, \ldots, x_n]$ è una base di Gröbner del k-simo ideale di eliminazione I_k di I, per ogni $k = 1, \ldots, n-1$.

Dimostrazione T. 52 Sia $1 \leq k \leq n-1$ un intero fissato. Dato che $G_k \subset I_k$, ci serve mostrare che $\mathrm{Lt}(I_k) \subseteq \mathrm{Lt}(G_k)$. Consideriamo allora un polinomio $f \in I_k \subseteq I$ e mostriamo che è divisibile per qualche $\mathrm{lt}(g)$, con $g \in G_k$. Dato che $f \in I$, allora $\mathrm{lt}(f)$ viene diviso da $\mathrm{lt}(g)$ per qualche $g \in G$; visto che $f \in I_k \subseteq K[x_{k+1}, \ldots, x_n]$, $\mathrm{lt}(g)$ deve essere nelle sole variabili $x_{k+1}, \ldots, x_n$. La proprietà cruciale dell'ordinamento che stiamo considerando è questa: ogni monomio che viene diviso da x_i, con $i = 1, \ldots, k$ è più grande di un qualsiasi monomio in $K[x_{k+1}, \ldots, x_n]$. Questo implica che ogni altro termine di g, che è più piccolo di $\mathrm{lt}(g)$, deve essere in $K[x_{k+1}, \ldots, x_n]$, e così tutto g, i.e. $g \in G_k$.

Ecco due applicazioni del precedente risultato.

T. 53. [Calcolo dell'intersezione di ideali]
Siano $I, J \subseteq A$ ideali; siano t una nuova indeterminata e $B = K[t, x_1, \ldots, x_n]$. Allora

$$I \cap J = (tI, (1-t)J) \cap K[x_1, \ldots, x_n].$$

Quindi, eliminando t si ottiene un base di Gröbner di $I \cap J \subseteq A$.

Dimostrazione T. 53 Sia $f \in I \cap J$ allora $f = tf + (1-t)f \in (tI, (1-t)J)$ e un'inclusione è provata. Osserviamo ora che, se $f_1, \ldots, f_s$ e $h_1, \ldots, h_u$ sono rispettivamente generatori di I e di J allora $tf_1, \ldots, tf_s$ e $(1-t)h_1, \ldots, (1-t)h_u$ generano tI e $(1-t)J$. Quindi se $f(X) = g(t, X) + h(t, X) \in (tI, (1-t)J) \cap K[X]$, con $g(t, X) \in tI$ e $h(t, X) \in (1-t)J$, allora per l'osservazione precedente $f(X) = g(1, X) = h(0, X) \in I \cap J$.

Per concludere la dimostrazione ora basta considerare un ordinamento lessicografico tale che $t > x_i$ per ogni $i = 1, \ldots, n$. Applicando **T.**52 all'ideale $(tI, (1-t)J)$ di $B = K[t, x_1, \ldots, x_n]$ abbiamo la tesi.

Osservazione 2.8. [Calcolo del quoziente di ideali] Ricordiamo che, dati ideali I e $J = (f_1, \ldots, f_s)$ in un qualsiasi anello A si ha che $I : J = \cap_{i=1}^{s} I : f_i$, cf. **T.**18.5. Inoltre, per ogni $f \in A$ si ha che $I\colon (f) = \frac{1}{f}(I \cap (f))$, cf. **E.**20. Il calcolo del quoziente si riduce dunque al calcolo di intersezioni di ideali di $K[x_1, \ldots, x_n]$, che possono essere ottenute applicando il risultato precedente.

T. 54. [Test di appartenenza al radicale] Sia $I \subsetneq A = K[x_1, \ldots, x_n]$ un ideale e t un'indeterminata. Allora $f \in \sqrt{I}$ se e solo se $(I, 1 - tf) = A[t]$.

Dimostrazione T. *54* L'enunciato è ovvio per $f = 0$, quindi supponiamo $f \neq 0$. Sia $f \in \sqrt{I}$; allora esiste un intero m tale che $f^m \in I \subseteq (I, 1 - tf)$. Scriviamo allora $1 = t^m f^m + (1 - t^m f^m) = t^m f^m + (1 - tf) \sum_{i=0}^{m-1} t^i f^i$, e otteniamo che $1 \in (I, 1 - tf)$.
Viceversa, se $I = (f_1, \ldots, f_k)$ e $(I, 1 - tf) = (1)$, possiamo scrivere $1 = \sum_{i=1}^{k} h_i(x_1, \ldots, x_n, t) f_i + h(x_1, \ldots, x_n, t)(1 - tf)$. Dal momento che il membro di sinistra dell'uguaglianza non dipende da t, possiamo valutare in $t = 1/f$ e ottenere

$$1 = \sum_{i=1}^{k} h_i(x_1, \ldots, x_n, 1/f) f_i \in K(x_1, \ldots, x_n).$$

Quindi, eliminando i denominatori, esistono polinomi $g_i = g_i(x_1, \ldots, x_n) \in A$ e un intero m positivo tali che $f^m = \sum_{i=1}^{k} g_i f_i \in I$.

3

Varietà algebriche affini

3.1 Definizione e prime proprietà

Siano $F = \{f_1, \ldots, f_s\} \subset A = K[x_1, \ldots, x_n]$ e I un ideale di A. *La varietà affine associata ad* F, rispettivamente ad I, è l'insieme

$$\mathbf{V}(F) = \{(a_1, \ldots, a_n) \in K^n \colon f_i(a_1, \ldots, a_n) = 0 \text{ per ogni } i = 1, \ldots, s\},$$

rispettivamente $\mathbf{V}(I) = \{(a_1, \ldots, a_n) \in K^n \colon f(a_1, \ldots, a_n) = 0 \text{ per ogni } f \in I\}$. Dal teorema della base di Hilbert **T.**40 sappiamo che ogni ideale di A è finitamente generato; inoltre, se $I = (F)$, è immediato verificare che $(a_1, \ldots, a_n) \in K^n$ è tale che $f(a_1, \ldots, a_n) = 0$ per ogni $f \in I$ se e solo se $f(a_1, \ldots, a_n) = 0$ per ogni $f \in F$. Avremo dunque che $\mathbf{V}(I) = \mathbf{V}(F)$, per ogni insieme di generatori F di I.

Viceversa, data una varietà affine $V \subseteq K^n$, chiamiamo *l'ideale associato a* V l'ideale

$$\mathbf{I}(V) = \{f \in A \,:\, f(\alpha) = 0, \text{ per ogni } \alpha \in V\} \subseteq A\,.$$

Vorremmo ora capire che proprietà hanno le funzioni

$$\begin{array}{ccc} \mathcal{Z} = \{V \subseteq K^n \colon \text{varietà affine}\} & \longleftrightarrow & \mathcal{I} = \{I \subseteq A \colon \text{ideale}\} \\ \mathbf{V}(I) & \longleftarrow & I \\ V & \longrightarrow & \mathbf{I}(V)\,. \end{array}$$

Varietà: prime proprietà

T. 55. Siano $I, J \subseteq A$ ideali e siano $V, W \subseteq K^n$ varietà affini; allora

1. $I \subseteq J \Rightarrow \mathbf{V}(I) \supseteq \mathbf{V}(J)$;
2. $I \subseteq \mathbf{I}(\mathbf{V}(I))$;
3. $\mathbf{V}(\mathbf{I}(\mathbf{V}(I))) = \mathbf{V}(I)$;
4. $V \subseteq W \iff \mathbf{I}(V) \supseteq \mathbf{I}(W)$;
5. $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$;
6. $\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$;
7. $\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$;
8. $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$.

Dimostrazione T. 55 1. Sia $\alpha \in \mathbf{V}(J)$; allora si ha $f(\alpha) = 0$ per ogni $f \in J$ e quindi, per ipotesi, si anche che $f(\alpha) = 0$ per ogni $f \in I$ da cui segue che $\alpha \in \mathbf{V}(I)$.

2. Segue immediatamente dalla definizione di $\mathbf{I}(\mathbf{V}(I))$.

3. Certamente $\mathbf{V}(I) \subseteq \mathbf{V}(\mathbf{I}(\mathbf{V}(I)))$. Per l'altro contenimento, basta notare che $I \subseteq \mathbf{I}(\mathbf{V}(I)))$ e dunque, dal punto 1, $\mathbf{V}(\mathbf{I}(\mathbf{V}(I))) \subseteq \mathbf{V}(I)$.

4. Proviamo prima che se $V \subseteq W$ allora $\mathbf{I}(W) \subseteq \mathbf{I}(V)$. Infatti se $f \in \mathbf{I}(W)$ allora $f(\alpha) = 0$ per ogni $\alpha \in W$ e quindi $f(\alpha) = 0$ anche per ogni $\alpha \in V$, ossia $f \in \mathbf{I}(V)$.

Viceversa, se $\mathbf{I}(W) \subseteq \mathbf{I}(V)$ allora, se $\alpha \in V$, per ogni $f \in \mathbf{I}(V)$ si ha $f(\alpha) = 0$ e quindi anche $f(\alpha) = 0$ per ogni $f \in \mathbf{I}(W)$ ossia $\alpha \in \mathbf{V}(\mathbf{I}(W)) = W$, ove l'ultima uguaglianza segue dal punto 3.

5. Dal momento che $I, J \subseteq I + J$, si ha che $\mathbf{V}(I + J) \subseteq \mathbf{V}(I) \cap \mathbf{V}(J)$.

Viceversa, se $\alpha \in \mathbf{V}(I) \cap \mathbf{V}(J)$, per ogni $f = i + j \in I + J$ avremo $f(\alpha) = i(\alpha) + j(\alpha) = 0$ e quindi $\alpha \in \mathbf{V}(I + J)$.

6. $IJ \subseteq I, J$ e dunque $\mathbf{V}(I) \cup \mathbf{V}(J) \subseteq \mathbf{V}(IJ)$.

Per l'altra inclusione, se $\alpha \in \mathbf{V}(IJ)$, allora $fg(\alpha) = 0$ per ogni $f \in I$, $g \in J$. Se $\alpha \notin \mathbf{V}(I)$, allora esiste $f \in I$ tale che $f(\alpha) \neq 0$, e dato che $fg(\alpha) = f(\alpha)g(\alpha) = 0$, $\alpha \in \mathbf{V}(J)$.

7. $I \cap J \subseteq I, J$ e dunque $\mathbf{V}(I) \cup \mathbf{V}(J) \subseteq \mathbf{V}(I \cap J)$.

Per l'altra inclusione, dal momento che $IJ \subseteq I \cap J$, dal punto precedente segue che $\mathbf{V}(I \cap J) \subseteq \mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$.

8. Dato che $I \subseteq \sqrt{I}$, dal punto 1 avremo subito $\mathbf{V}(I) \supseteq \mathbf{V}(\sqrt{I})$.

Se $f \in \sqrt{I}$ allora esiste $m \in \mathbb{N}$ tale che $f^m \in I$. Di conseguenza, dato $\alpha \in \mathbf{V}(I)$ si ha $f^m(\alpha) = 0$, da cui segue che $f(\alpha) = 0$ e quindi $\alpha \in \mathbf{V}(\sqrt{I})$.

In particolare l'intersezione e l'unione di due varietà affini sono varietà affini. Se $V \subset W$ allora diremo che V è una *sottovarietà* di W. Inoltre, per quanto visto sopra, su $X = K^n$ possiamo introdurre una topologia in cui i chiusi sono le varietà affini, cf. **T.**73. Il prossimo risultato dimostra che tale spazio topologico è noetheriano.

T. 56. Ogni catena discendente di varietà affini è stazionaria.

Dimostrazione T. *56* Data $V_1 \supseteq V_2 \supseteq \dots$ una catena discendente di varietà affini di K^n, vi è una catena ascendente di ideali $\mathbf{I}(V_1) \subseteq \mathbf{I}(V_2) \subseteq \dots$ di A. Poiché A è noetheriano, la catena di ideali è stazionaria; necessariamente anche la catena $\mathbf{V}(\mathbf{I}(V_1)) \supseteq \mathbf{V}(\mathbf{I}(V_2)) \supseteq \dots$ è stazionaria, e la conclusione segue allora da **T.**55.3.

Una varietà affine V si dice *irriducibile* se non si può scrivere come unione di due sottovarietà proprie V_1 e V_2, cioè V è irriducibile se e solo se

$$V = V_1 \cup V_2 \quad \text{implica} \quad V = V_1 \text{ oppure } V = V_2.$$

Esempio 3.1. Siano $K = \mathbb{Z}/(2)$, $A = K[x, y]$ e $I = (x + y)$. Allora $A/I \simeq K[x]$ è un dominio, cioè I è primo, mentre $\mathbf{V}(I) = \{(0, 0), (1, 1)\} \subsetneq K^2$ è riducibile in quanto unione di $V_1 = \{(0, 0)\} = \mathbf{V}((x, y))$ e $V_2 = \{(1, 1)\} = \mathbf{V}((x + 1, y + 1))$, ove entrambe sono varietà strettamente contenute in $\mathbf{V}(I)$.

T. 57. Una varietà V è irriducibile se e solo $\mathbf{I}(V)$ è un ideale primo.

Dimostrazione T. *57* Sia $fg \in \mathbf{I}(V)$. Vogliamo provare che $f \in \mathbf{I}(V)$ oppure $g \in \mathbf{I}(V)$ quando V è irriducibile. Consideriamo le varietà $V_1 = V \cap$

$\mathbf{V}(f)$ e $V_2 = V \cap \mathbf{V}(g)$ e proviamo che $V_1 \cup V_2 = V$. Da **T.**55 discende infatti che

$$V_1 \cup V_2 = (V \cap \mathbf{V}(f)) \cup (V \cap \mathbf{V}(g)) = V \cap (\mathbf{V}(f) \cup \mathbf{V}(g)) = V \cap (\mathbf{V}(fg)) = V,$$

ove l'ultima uguaglianza è dovuta al fatto che $\mathbf{V}(fg) \supseteq \mathbf{V}(\mathbf{I}(V)) = V$. Dato che V è irriducibile si deve avere necessariamente $V = V_1$ oppure $V = V_2$; da ciò segue che $\mathbf{V}(f) \supseteq V$ oppure $\mathbf{V}(g) \supseteq V$ e quindi, usando nuovamente **T.**55, che $f \in \mathbf{I}(\mathbf{V}(f)) \subseteq \mathbf{I}(V)$ oppure $g \in \mathbf{I}(\mathbf{V}(g)) \subseteq \mathbf{I}(V)$.
Viceversa, supponiamo che $\mathbf{I}(V)$ sia primo e che $V = V_1 \cup V_2$; passando agli ideali, otteniamo che $\mathbf{I}(V) = \mathbf{I}(V_1 \cup V_2) = \mathbf{I}(V_1) \cap \mathbf{I}(V_2)$, ove l'ultima uguaglianza è di facile verifica. Poiché $\mathbf{I}(V)$ è primo, è anche irriducibile, cf. **T.**13, dunque $\mathbf{I}(V_1) = \mathbf{I}(V)$ oppure $\mathbf{I}(V_2) = \mathbf{I}(V)$. Sfruttando il fatto che $\mathbf{V}(\mathbf{I}(V)) = V$, si ha allora che $V_1 = V$ oppure $V_2 = V$, e dunque V è irriducibile.

T. 58. [Decomposizione in varietà irriducibili]

1. Ogni varietà affine V si decompone come unione di un numero finito di varietà irriducibili, cioè esiste un intero t tale che $V = \cup_{i=1}^{t} V_i$, con V_i irriducibile per $i = 1, \ldots, t$.
2. Se tale decomposizione è minimale, ovvero se $V_i \not\subseteq V_j$ per ogni $i \neq j$, allora essa è unica a meno dell'ordine.

Dimostrazione T. 58 1. Sia

$$\Sigma = \{V : V \text{ varietà affine che non è unione finita di varietà irriducibili}\},$$

ordinato con "$\supseteq$", e supponiamo per assurdo che $\Sigma \neq \emptyset$. Grazie a **T.**56, sappiamo che ogni catena discendente ammette un elemento massimale rispetto a "$\supseteq$" e dunque, per il lemma di Zorn, vi è un elemento minimale in Σ, sia esso W, che non è irriducibile. Pertanto $W = W_1 \cup W_2$, con $W_1, W_2 \subsetneq W$ sottovarietà proprie di W. Per la minimalità di W segue allora che esistono interi r, s e sottovarietà $W_{1,j}$, con $j = 1, \ldots, r$, e $W_{2,h}$, con $h = 1, \ldots, s$ di W_1 e W_2 rispettivamente tali che $W = W_1 \cup W_2 = \bigcup_{j=1}^{r} W_{1,j} \cup \bigcup_{h=1}^{s} W_{2,h}$. Abbiamo dunque scritto W come unione finita di varietà irriducibili, che è assurdo.

2. Supponiamo ora che $V = \cup_{i=1}^{r} V_i = \cup_{j=1}^{s} W_j$ siano due decomposizioni minimali di V. Allora, $V_i = V_i \cap V = \cup_{j=1}^{s}(V_i \cap W_j)$ per ogni $i = 1, \ldots, r$. Dato che V_i è irriducibile si deve avere allora che $V_i = V_i \cap W_{j_0}$, per qualche $j_0 \in \{1, \ldots, s\}$. Allo stesso modo deduciamo che esiste un $i_0 \in \{1, \ldots, r\}$ per cui $W_{j_0} = W_{j_0} \cap V_{i_0}$. Pertanto avremo che per ogni i, $V_i \subseteq W_{j_0} \subseteq V_{i_0}$. Dato che la decomposizione è minimale dobbiamo allora aver che $V_i = W_{j_0}$. Scambiando i ruoli delle decomposizioni arriviamo a concludere che $r = s$ e che le due decomposizioni sono uguali a meno di una permutazione degli indici.

Concludiamo questa parte con un'osservazione sugli ideali associati alle varietà costituite da un solo punto.

T. 59. Sia $V_\alpha = \{\alpha = (a_1, \ldots, a_n)\}$ una varietà costituita da un solo $\alpha \in K^n$; allora $\mathbf{I}(V_\alpha) = (x_1 - a_1, \ldots, x_n - a_n) = \mathfrak{m}_\alpha$ è un ideale massimale.

Dimostrazione T. *59* Sia $f \in A$; dividendo f per i polinomi $x_i - a_i$ otteniamo che $f(x_1, \ldots, x_n) = \sum_i h_i(x_i - a_i) + r$, con $r \in K$; dal momento che i polinomi $x_i - a_i$ sono una base di Gröbner per l'ideale che generano, cf. **T.**43, $f \in \mathbf{I}(V_\alpha)$ se e solo se $f(\alpha) = r = 0$, ovvero quando $f \in (x_1 - a_1, \ldots, x_n - a_n)$. L'ideale $\mathfrak{m}_\alpha$ è massimale: consideriamo $\varphi_\alpha \colon K[x_1, \ldots, x_n] \longrightarrow K$ l'omomorfismo surgettivo di valutazione dato da $\varphi_\alpha(f(x_1, \ldots, x_n)) = f(a_1, \ldots, a_n)$. Dal momento che K è un campo si ha che $\mathfrak{m}_\alpha = \operatorname{Ker} \varphi_\alpha$ è massimale.

Per quanto appena visto, ad ogni punto $\alpha = (a_1, \ldots, a_n) \in K^n$ corrisponde un ideale massimale di $K[x_1, \ldots, x_n]$. È immediato osservare che in generale non vale il viceversa, basta considerare l'ideale $(x^2 + 1) \subset \mathbb{R}[x]$, per cui non esiste $\alpha \in \mathbb{R}$ tale che $\alpha^2 + 1 = 0$.

3.2 Il risultante

Sia A un dominio di integrità e siano $f = \sum_{i=0}^{m} a_i x^i$ e $g = \sum_{i=0}^{n} b_i x^i$ due polinomi in $A[x]$ non entrambi costanti di gradi m ed n rispettivamente. Definiamo *matrice di Sylvester di* f *e* g come la matrice $(m + n) \times (m + n)$

$$\mathrm{Syl}(f,g) = \begin{pmatrix} a_m & a_{m-1} & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & \cdots & a_0 & & \vdots \\ \vdots & & \ddots & \ddots & & & \ddots & 0 \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & \cdots & a_0 \\ b_n & \cdots & b_1 & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & & \ddots & \ddots & & & \vdots \\ \vdots & & \ddots & & & \ddots & & \vdots \\ 0 & \cdots & 0 & b_n & \cdots & b_1 & b_0 & 0 \\ 0 & \cdots & \cdots & 0 & b_n & \cdots & b_1 & b_0 \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \end{matrix}$$

Per l'origine di questa matrice e la sua connessione con l'esistenza di fattori comuni tra f e g, cf. [CLS, Chapter 3, §5].

Definiamo il *risultante di* f, g come $\mathrm{Ris}(f,g) = \det(\mathrm{Syl}(f,g))$.

Se $f, g \in A$ poniamo per definizione $\mathrm{Ris}(f,g) = 1$.

Osserviamo che se $m > 0$, $n = 0$, otteniamo la matrice $m \times m$ diagonale con $g = b_0$ sulla diagonale, per cui $\mathrm{Ris}(f,g) = b_0^m$. Analogamente, se $m = 0$, $n > 0$, $\mathrm{Ris}(f,g) = a_0^n$.

Proprietà del risultante /I

T. 60. 1. $\mathrm{Ris}(f,g) \in A$;

2. $\mathrm{Ris}(f,g) = (-1)^{mn}\,\mathrm{Ris}(g,f)$;

3. $\mathrm{Ris}(af,g) = a^n\,\mathrm{Ris}(f,g)$ e $\mathrm{Ris}(f,bg) = b^m\,\mathrm{Ris}(f,g)$, per ogni $a, b \in A$.

Dimostrazione T. *60* Tutte le affermazioni seguono immediatamente dalle proprietà del determinante.

T. 61. Esistono polinomi $F, G \in A[x]$, con $\deg F < \deg g$ e $\deg G < \deg f$, tali che

$$\mathrm{Ris}(f,g) = Ff + Gg.$$

In particolare, $\mathrm{Ris}(f,g) \in (f,g) \cap A$.

Dimostrazione T. *61* Sommando all'ultima colonna della matrice di Sylvester la colonna i-esima moltiplicata per x^{m+n-i} per ogni $i = 1, \ldots, m+n$, otteniamo

$$\mathrm{Ris}(f,g) = \det \mathrm{Syl}(f,g) = \det \begin{pmatrix} a_m & \cdots & a_0 & & x^{n-1}f(x) \\ & \ddots & & \ddots & \vdots \\ & & a_m & \cdots & f(x) \\ b_n & \cdots & b_1 & b_0 & x^{m-1}g(x) \\ & \ddots & & \ddots & \vdots \\ & & b_n & \cdots & g(x) \end{pmatrix}.$$

Sviluppando ora il determinante rispetto all'ultima colonna è chiaro che f risulta moltiplicato per un polinomio di grado al più $n-1$ e g per un polinomio di grado al più $m-1$, e che la somma di questi è il risultante cercato.

Esempio 3.2. Sia $f = ax^2 + bx + c \in \mathbb{Q}[x]$, $a \neq 0$ allora

$$\mathrm{Syl}(f,f') = \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix} \quad \text{e} \quad \mathrm{Ris}(f,f') = -a(b^2 - 4ac)\ ,$$

quindi $\mathrm{Ris}(f,f') = 0$ se e solo se f e f' hanno una radice in comune, ossia se e solo se f ha una radice doppia.

La proprietà osservata nell'esempio precedente è un caso particolare di un'importante proprietà di $\mathrm{Ris}(f,g)$. Per dimostrare le proprietà fondamentali del risultante abbiamo bisogno di alcuni fatti, che includiamo nel seguente enunciato.

T. 62. Siano m un intero positivo, $Y = y_1, \ldots, y_m$ indeterminate, e $f_m(x) \in A[Y][x] \simeq A[Y,x]$ il polinomio

$$f_m(x) = \prod_{i=1}^{m} (x - y_i) = \sum_{i=0}^{m} a_i^{(m)} x^i.$$

Allora

1. i coefficienti $a_i^{(m)}$ sono funzioni lineari in y_j, per ogni $j = 1, \dots, m$;
2. $a_{i-1}^{(m-1)}(y_1, \dots, y_{m-1}) = a_i^{(m)}(y_1, \dots, y_{m-1}, 0)$, per $0 < i \leq m$; inoltre $a_0^{(m)}(y_1, \dots, y_{m-1}, 0) = 0$;
3. dato un polinomio $g = \sum_{i=0}^{n} b_i x^i$, $b_i \in A \subset A[Y]$, si ha

$$\operatorname{Ris}(f_m(x), g(x)) = g(y_m) \operatorname{Ris}(f_{m-1}(x), g(x)) \in A[Y].$$

Dimostrazione T. *62* 1. I coefficienti di f_m sono le funzioni simmetriche elementari nelle variabili $y_1, \dots, y_m$ e quindi si ha:

$$\begin{aligned} a_m^{(m)} &= 1; \\ a_{m-1}^{(m)} &= -(y_1 + \cdots + y_m); \\ a_{m-2}^{(m)} &= y_1 y_2 + \cdots + y_{m-1} y_m; \\ &\vdots \\ a_0^{(m)} &= (-1)^m y_1 y_2 \cdots y_m; \end{aligned}$$

da cui segue che ogni $a_i^{(m)}$ è lineare in ogni variabile y_j.

2. Scrivendo $f_m(x) = f_{m-1}(x)(x - y_m)$ otteniamo che, per ogni $i > 0$,

$$a_{i-1}^{(m-1)}(y_1, \dots, y_{m-1}) - y_m\, a_i^{(m-1)}(y_1, \dots, y_{m-1}) = a_i^{(m)}(y_1, \dots, y_{m-1}, y_m)$$

Valutando per $y_m = 0$, si ottiene

$$a_{i-1}^{(m-1)}(y_1, \dots, y_{m-1}) = a_i^{(m)}(y_1, \dots, y_{m-1}, 0),$$

come volevamo. L'affermazione per $i = 0$ è ovvia dal punto 1.

3. Consideriamo la matrice di Sylvester

$$\operatorname{Syl}(f_m, g) = \begin{pmatrix} a_m^{(m)} & \cdots & a_0^{(m)} & & \\ & \ddots & & \ddots & \\ & & a_m^{(m)} & \cdots & a_0^{(m)} \\ b_n & \cdots & b_1 & b_0 & \\ & \ddots & & \ddots & \\ & & b_n & \cdots & b_0 \end{pmatrix}.$$

Moltiplicando la colonna i-esima della matrice per y_m^{m+n-i} e sommando il risultato all'ultima colonna per ogni $i = 1, \dots, m+n-1$, dalle proprietà del determinante e da $f_m(y_m) = 0$ discende che:

$$\mathrm{Ris}(f_m, g) = \det \begin{pmatrix} a_m^{(m)} & \cdots & a_0^{(m)} & & & y_m^{n-1} f_m(y_m) \\ & \ddots & & \ddots & & \vdots \\ & & a_m^{(m)} & & \cdots & f_m(y_m) \\ b_n & \cdots & b_1 & b_0 & & y_m^{m-1} g(y_m) \\ & \ddots & & & \ddots & \vdots \\ & & b_n & & \cdots & g(y_m) \end{pmatrix} =$$

$$\det \begin{pmatrix} a_m^{(m)} & \cdots & a_0^{(m)} & & & 0 \\ & \ddots & & \ddots & & \vdots \\ & & a_m^{(m)} & & \cdots & 0 \\ b_n & \cdots & b_1 & b_0 & & y_m^{m-1} g(y_m) \\ & \ddots & & & \ddots & \vdots \\ & & b_n & & \cdots & g(y_m) \end{pmatrix} = g(y_m) \det \begin{pmatrix} a_m^{(m)} & \cdots & a_0^{(m)} & & & 0 \\ & \ddots & & \ddots & & \vdots \\ & & a_m^{(m)} & & \cdots & 0 \\ b_n & \cdots & b_1 & b_0 & & y_m^{m-1} \\ & \ddots & & & \ddots & \vdots \\ & & b_n & & \cdots & 1 \end{pmatrix}.$$

Chiamando M quest'ultima matrice, abbiamo provato che $\mathrm{Ris}(f_m, g) = g(y_m) \det M$.

Ora, dato che A è un dominio, avremo che $\deg_{y_m}(\mathrm{Ris}(f_m, g)) = \deg_{y_m}(g(y_m)) + \deg_{y_m}(\det M)$; allora, visto che $\deg_{y_m}(\mathrm{Ris}(f_m, g)) \leq n$, per il punto 1 e $\deg_{y_m}(g(y_m)) = n$, si deve avere $\deg_{y_m}(\det M) = 0$, quindi possiamo valutare y_m in 0, senza modificare $\det M$. Usando il punto 2 si ottiene allora che

$$\det \begin{pmatrix} a_{m-1}^{(m-1)} & \cdots & a_0^{(m-1)} & 0 & \cdots & 0 \\ & \ddots & & \ddots & & \vdots \\ & & a_{m-1}^{(m-1)} & \cdots & & 0 \\ b_n & \cdots & b_1 & b_0 & & \vdots \\ & \ddots & & & \ddots & 0 \\ & & b_n & \cdots & & 1 \end{pmatrix} = \det \begin{pmatrix} a_{m-1}^{(m-1)} & \cdots & a_0^{(m-1)} & 0 & \cdots & 0 \\ & \ddots & & \ddots & & \vdots \\ & & a_{m-1}^{(m-1)} & \cdots & & a_0^{(m-1)} \\ b_n & \cdots & b_1 & b_0 & & \\ & \ddots & & & \ddots & \\ & & b_n & & \cdots & b_0 \end{pmatrix}$$

$= \mathrm{Ris}(f_{m-1}, g)$, e ciò conclude la dimostrazione.

Proprietà del risultante /II

T. 63. Sia $A = K$ un campo e siano $f = \sum_{i=0}^{m} a_i x^i$ e $g = \sum_{i=0}^{n} b_i x^i$ polinomi in $K[x]$, con $a_m, b_n \neq 0$.

1. Siano $\alpha_1, \ldots, \alpha_m$ e $\beta_1, \ldots, \beta_n$ le radici di f e g in $\overline{K}$ rispettivamente; allora

$$\mathrm{Ris}(f,g) \;=\; a_m^n \prod_{i=1}^{m} g(\alpha_i) \;=\; (-1)^{mn} b_n^m \prod_{j=1}^{n} f(\beta_j) \in \overline{K}.$$

2. $\mathrm{Ris}(f,g) = a_m^n b_n^m \prod_{i,j}(\alpha_i - \beta_j) \in \overline{K}$.

3. Se $K = \overline{K}$, $\mathrm{Ris}(f,g) = 0$ se e solo se f e g hanno una radice in comune.

4. $\mathrm{Ris}(f,g) = 0$ se e solo se f e g hanno un fattore comune di grado positivo.

***Dimostrazione T.** 63* 1. Dato che $\alpha_1, \ldots, \alpha_m \in \overline{K}$ sono le radici di f allora $f = a_m \prod_{i=1}^{m}(x - \alpha_i)$ e $\mathrm{Ris}(f,g) = a_m^n \mathrm{Ris}(\hat{f}, g)$, ove $\hat{f} = \prod_{i=1}^{m}(x - \alpha_i)$, per **T.**60.3. Quindi, applicando m volte **T.**62.3 a $\hat{f}$ e g, e valutando il risultato in $y_1 = \alpha_1, \ldots, y_m = \alpha_m$, otteniamo $\mathrm{Ris}(f,g) = a_m^n \prod_{i=1}^{m} g(\alpha_i) \cdot \mathrm{Ris}(1, g(x)) = a_m^n \prod_{i=1}^{m} g(\alpha_i)$. Per ottenere l'altra relazione osserviamo che, per **T.**60.2, $\mathrm{Ris}(f,g) = (-1)^{mn} \mathrm{Ris}(g,f) = (-1)^{mn} b_n^m \prod_{j=1}^{n} f(\beta_j)$.

2. Segue dal punto precedente, osservando che, da $f = a_m \prod_{i=1}^{m}(x - \alpha_i)$, discende che

$$\prod_{j=1}^{n} f(\beta_j) = a_m^n \prod_{j=1}^{n}\prod_{i=1}^{m}(\beta_j - \alpha_i) = (-1)^{mn} a_m^n \prod_{j=1}^{n}\prod_{i=1}^{m}(\alpha_i - \beta_j)\ .$$

3. Segue immediatamente dalle relazioni dimostrate in 1.

4. Basta osservare che se $\alpha \in \overline{K}$ è una radice comune di f e g allora il suo polinomio minimo $h \in K[x]$ divide sia f che g.

Concludiamo questa parte con un'osservazione che ci sarà utile nella dimostrazione del teorema di estensione **T.**65.

T. 64. Siano f, g polinomi in $A = K[x_1, \ldots, x_s]$ di grado in x_1 rispettivamente m e n. Se esiste $\beta = (a_2, \ldots, a_s) \in K^{s-1}$ tale che $f(x_1, \beta)$ e $g(x_1, \beta)$ hanno ancora grado in x_1 rispettivamente m e n allora

$$\mathrm{Ris}_{x_1}(f, g)(\beta) = \mathrm{Ris}_{x_1}(f(x_1, \beta), g(x_1, \beta)).$$

Dimostrazione T. 64 Sia $h = h(x_2, \ldots, x_s) = \mathrm{Ris}_{x_1}(f, g)$, con $f = \sum_{i=0}^{m} c_i(x_2, \ldots, x_s)x_1^i$, $g = \sum_{j=0}^{n} d_i(x_2, \ldots, x_s)x_1^i$. Allora

$$h(\beta) = \det \begin{pmatrix}
c_m(\beta) & c_{m-1}(\beta) & \cdots & \cdots & c_0(\beta) & 0 & \cdots & 0 \\
0 & c_m(\beta) & c_{m-1}(\beta) & \cdots & \cdots & c_0(\beta) & & \vdots \\
\vdots & & \ddots & \ddots & & & \ddots & 0 \\
0 & \cdots & 0 & c_m(\beta) & c_{m-1}(\beta) & \cdots & \cdots & c_0(\beta) \\
d_n(\beta) & \cdots & d_1(\beta) & d_0(\beta) & 0 & \cdots & \cdots & 0 \\
0 & \ddots & & \ddots & \ddots & & & \vdots \\
\vdots & & \ddots & & & \ddots & & \vdots \\
0 & \cdots & 0 & d_n(\beta) & \cdots & d_1(\beta) & d_0(\beta) & 0 \\
0 & \cdots & \cdots & 0 & d_n(\beta) & \cdots & d_1(\beta) & d_0(\beta)
\end{pmatrix}$$

e dalla nostra ipotesi discende che questo determinante è proprio quello della matrice di Sylvester di $f(x_1, \beta)$ e $g(x_1, \beta)$.

3.3 Il teorema di estensione

Prima di dimostrare il teorema di estensione ricordiamo i seguenti fatti. Un campo K algebricamente chiuso è infinito; infatti se fosse finito, diciamo $K = \{a_1, \ldots, a_s\}$, il polinomio $\prod_{i=1}^{s}(x - a_i) + 1$ non avrebbe soluzioni in K, che è assurdo. Di conseguenza è facile verificare che un polinomio in n variabili a coefficienti in un campo algebricamente chiuso è non nullo se e solo se esiste $\alpha \in K^n$ tale che $f(\alpha) \neq 0$.

Sia $I = (f_1, \ldots, f_s)$ un ideale di $A = K[x_1, \ldots, x_n]$. Allora la varietà associata ad I corrisponde all'insieme delle soluzioni del sistema $\Sigma = \{f_i = 0 : i = 1, \ldots, s\}$. Siano ora k un intero fissato, con $1 \leq k \leq n-1$, e I_k il k-esimo

ideale di eliminazione di I. Chiamiamo $(a_{k+1}, \ldots, a_n)$ *una soluzione parziale* del sistema quando $(a_{k+1}, \ldots, a_n) \in \mathbf{V}(I_k)$.

Teorema di estensione delle soluzioni

T. 65. Siano $K = \overline{K}$ un campo algebricamente chiuso, $I = (f_1, \ldots, f_s)$ un ideale di A e $I_1 = I \cap K[x_2, \ldots, x_n]$ il primo ideale di eliminazione di I. Per ogni $i = 1, \ldots, s$, scriviamo

$$f_i = c_i(x_2, \ldots, x_n)x_1^{N_i} + f_i' \text{ con } \deg_{x_1} f_i' < N_i \text{ e } c_i \in K[x_2, \ldots, x_n] \setminus \{0\}.$$

Sia $\beta = (a_2, \ldots, a_n) \in \mathbf{V}(I_1)$ una soluzione parziale; se $\beta \notin \mathbf{V}(c_1, \ldots, c_s)$, allora esiste $a_1 \in K$ tale che $(a_1, \beta) = (a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$.

Dimostrazione ***T.*** *65* $\boxed{s = 2}$ Consideriamo $I = (f, g)$, con

$$f = d_l x_1^l + \ldots + d_0, \quad g = e_m x_1^m + \ldots + e_0,$$

ove $d_0, \ldots, d_l, e_0, \ldots, e_m \in K[x_2, \ldots, x_n]$, $d_l, e_m \neq 0$. Per ipotesi esiste una soluzione parziale $\beta = (a_2, \ldots, a_n) \in \mathbf{V}(I_1)$ tale che $d_l(\beta) \neq 0$ oppure $e_m(\beta) \neq 0$. Trattiamo prima il caso in cui entrambi siano diversi da zero; sia $h = h(x_2, \ldots, x_n) = \mathrm{Ris}_{x_1}(f, g)$. Da **T.**61 discende che $h \in K[x_2, \ldots, x_n] \cap I = I_1$. Dunque, dato che $\beta \in \mathbf{V}(I_1)$, si ha $h(\beta) = 0$. Dal momento che $d_l(\beta)$ e $e_m(\beta)$ sono diversi da zero, $f(x_1, \beta), g(x_1, \beta)$ hanno ancora grado l e m e dunque da **T.**64 segue che $0 = h(\beta) = \mathrm{Ris}_{x_1}(f(x_1, \beta), g(x_1, \beta))$. Da **T.**63.2 segue allora che $f(x_1, \beta)$ e $g(x_1, \beta)$ hanno una radice comune a_1, ovvero $f(a_1, \beta) = g(a_1, \beta) = 0$; questo mostra che $(a_1, \beta) \in \mathbf{V}(I)$ è l'estensione della soluzione parziale cercata.

Supponiamo ora che $d_l(\beta) = 0$ ed $e_m(\beta) \neq 0$, l'altro caso sarà del tutto analogo. Consideriamo il polinomio $p = x_1^r g + f$, dove r è scelto in modo tale che $\deg_{x_1}(x_1^r g + f) > \deg_{x_1}(f)$. Allora $I = (f, g) = (p, g)$; dato che $\mathrm{lc}(p) = e_m$ in questo modo ci si riconduce al caso precedente, e la dimostrazione di questo caso è completa.

$\boxed{\text{Caso generale}}$ Sia $\beta = (a_2, \ldots, a_n) \in \mathbf{V}(I_1)$ una soluzione parziale e consideriamo l'omomorfismo di valutazione $\varphi\colon A \longrightarrow K[x_1]$, $f(x_1, \ldots, x_n) \mapsto f(x_1, \beta)$, che è surgettivo. Avremo allora che $\varphi(I)$ è un ideale di $K[x_1]$, che

è PID, pertanto $\varphi(I) = \{f(x_1, \beta)\colon f \in I\} = (g(x_1, \beta))$ per qualche $g \in I$. È sufficiente dimostrare che $g(x_1, \beta)$ ha almeno una radice e, dato che K è algebricamente chiuso, basterà allora provare che $g \notin K^*$. Infatti, sia a_1 una radice di $g(x_1, \beta)$; dato che $g(x_1, \beta)$ genera $\varphi(I)$, da ciò segue che $f(a_1, \beta) = 0$ per ogni $f \in I$, e dunque $(a_1, \beta) \in \mathbf{V}(I)$ è l'estensione cercata della soluzione parziale β.

In primo luogo osserviamo che $g(x_1, \beta) \neq 0$. Infatti, dato che $\beta \notin \mathbf{V}(c_1, \ldots, c_s)$, esiste un c_i tale che $c_i(\beta) \neq 0$. Il polinomio f_i corrispondente avrà allora grado in x_1 positivo dato che $\beta \in \mathbf{V}(I_1)$; infatti se fosse $N_i = 0$ avremmo $f_i = c_i$ con $f_i = f_i(x_2, \ldots, x_n) \in I_1$ e $0 = f_i(\beta) = c_i(\beta) \neq 0$. Pertanto $0 \neq \varphi(f_i) \in \varphi(I)$. In particolare $g \neq 0$ e, per concludere la dimostrazione, è sufficiente applicare il caso $s = 2$ all'ideale $J = (f_i, g)$ con β soluzione parziale in $\mathbf{V}(J_1)$.

3.4 Il Nullstellensatz e le sue conseguenze

Come nella sezione precedente assumiamo che $K = \overline{K}$ sia algebricamente chiuso. Nel seguito è utile ricordare che, dato un termine $cX^{\mathbf{a}}$, con $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$ e $c \in K^*$, il suo *grado (totale)* è la quantità $|\,\mathbf{a}\,| = \sum_{i=1}^n a_i$. Un polinomio si dice *omogeneo* se risulta essere somma di termini tutti dello stesso grado. Più formalmente, un polinomio $f = f(x_1, \ldots, x_n)$ si dice *omogeneo di grado d* se $f(tx_1, tx_2, \ldots, tx_n) = t^d f(x_1, \ldots, x_n)$. "Collezionando" i termini dello stesso grado, ogni polinomio $f \in A$ si può scrivere come somma finita di polinomi omogenei tutti di grado diverso: il grado di f è il massimo di questi gradi.

Nel seguente fatto serve solo che K sia infinito.

T. 66. Sia $f \in A = K[x_1, x_2, \ldots, x_n]$ un polinomio di grado $N \geq 1$; allora esistono $a_2, \ldots, a_n \in K$ e un cambiamento lineare di coordinate $\varphi\colon K[x_1, \ldots, x_n] \longrightarrow K[y_1, \ldots, y_n]$ definito da

$$\begin{aligned} x_1 &\longmapsto \quad y_1 \\ x_i &\longmapsto y_i + a_i y_1 \ \text{ per ogni } i = 2, \ldots, n \end{aligned}$$

tale che $\varphi(f) = cy_1^N + f'$ con $c \in K^*$ e $\deg_{y_1} f' < N$.

Dimostrazione T. 66 Scriviamo $f = f_N + f_{N-1} + \ldots + f_0$, con ognuno degli f_i omogeneo di grado totale i. Applicando φ, si ha che $\varphi(f) = f(y_1, y_2 + a_2 y_1, \ldots, y_n + a_n y_1)$. Osservando che un monomio $X^{\mathbf{a}}$, con $\sum_{i=1}^{n} a_i = N$ viene mappato in $y_1^{a_1}(y_2 + a_2 y_1)^{a_2} \cdots (y_n + a_n y_1)^{a_n}$, possiamo scrivere $\varphi(f) = f_N(1, a_2, \ldots, a_n) y_1^N + f'$, con $\deg_{y_1} f' < N$.
Dal momento che $0 \neq f_N(x_1, \ldots, x_n) = x_1^N f_N\left(1, \frac{x_2}{x_1}, \ldots, \frac{x_n}{x_1}\right)$, allora, dato che il campo K è infinito, esistono $a_2, \ldots, a_n \in K$ tali che $f_N(1, a_2, \ldots, a_n) = c \neq 0$.

Teorema degli zeri di Hilbert

T. 67. [Nullstellensatz, forma debole] Siano K un campo algebricamente chiuso e $I \subseteq A = K[x_1, x_2, \ldots, x_n]$ un ideale; allora

$$\mathbf{V}(I) = \emptyset \quad \text{se e solo se} \quad I = (1).$$

T. 68. [Nullstellensatz, forma forte] Siano K un campo algebricamente chiuso e $I \subseteq A = K[x_1, x_2, \ldots, x_n]$ un ideale; allora

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

Dimostrazione T. 67 È chiaro che se $I = (1)$ allora $\mathbf{V}(I) = \emptyset$.
Dimostriamo il viceversa per induzione sul numero di variabili n. Se $n = 1$ allora $K[x]$ è un PID, dunque $I = (f)$ e poiché K è algebricamente chiuso, gli unici polinomi senza radici sono costanti e quindi $I = (1)$.
Supponiamo la tesi vera per ogni $i < n$ e proviamo che vale per n. Sia dunque $I = (f_1, \ldots, f_s)$ tale che $\mathbf{V}(I) = \emptyset$. Se $f_1 \in K$ allora la tesi vale. Altrimenti supponiamo che f_1 abbia grado totale $N \geq 1$. Per **T.**66 esiste un cambiamento lineare di coordinate φ tale che $\varphi(f_1) = c y_1^N + f'$ con $c \in K^*$ e $\deg_{y_1} f' < N$. Dal momento che φ è un isomorfismo, avremo che $\varphi(I)$ è un ideale di $K[y_1, \ldots, y_n]$ e $\mathbf{V}(\varphi(I)) = \emptyset$. Dal teorema di estensione segue allora che $\mathbf{V}(\varphi(I)_1) = \emptyset$; infatti se così non fosse, un elemento $\beta \in \mathbf{V}(\varphi(I)_1)$ verrebbe sicuramente esteso ad un elemento $\alpha \in \mathbf{V}(\varphi(I))$, poiché $c \in K^*$ e $\mathbf{V}((c)) = \emptyset$. Dall'ipotesi induttiva segue allora che $1 \in \varphi(I)_1 \subseteq \varphi(I)$, e da questo segue che $1 \in I$, come volevamo.

Dimostrazione T. 68 L'inclusione $\sqrt{I} \subseteq \mathbf{I}(\mathbf{V}(I))$ è sempre vera: infatti, da **T.**55, $\sqrt{I} \subseteq \mathbf{I}(\mathbf{V}(\sqrt{I})) = \mathbf{I}(\mathbf{V}(I))$.
Per l'inclusione opposta, sia $f \in \mathbf{I}(\mathbf{V}(I))$. Consideriamo l'ideale $J = (I, 1 - tf) \subseteq K[t, x_1, \ldots, x_n]$ e proviamo che $\mathbf{V}(J) = \emptyset$; in questo caso, dal teorema degli zeri, forma debole, segue che $1 \in J$ e dunque la conclusione discende dal test di appartenenza al radicale **T.**54. Sia dunque $\alpha = (b, \beta) \in K^{n+1}$, con $\beta = (a_1, \ldots, a_n) \in K^n$. Ora, se $\beta \in \mathbf{V}(I)$, allora $f(\beta) = 0$ e $(1 - tf)(b, \beta) = 1 - bf(\beta) = 1$; da ciò si conclude che $\alpha \notin \mathbf{V}(J)$. Se invece $\beta \notin \mathbf{V}(I)$, esiste i per cui $f_i(\beta) \neq 0$; allora, pensando f_i come un polinomio in $K[t, x_1, \ldots, x_n]$ che non dipende da t, avremo che $f_i(b, \beta) \neq 0$, ovvero anche in questo caso $\alpha \notin \mathbf{V}(J)$.

Il teorema degli zeri ha alcune immediate conseguenze. La prima che riportiamo è la caratterizzazione degli ideali massimali in $K[x_1, \ldots, x_n]$, quando $K = \overline{K}$, cf. **T.**59.

T. 69. Sia $K = \overline{K}$ un campo algebricamente chiuso. Allora $\mathfrak{m} \subset K[x_1, \ldots, x_n]$ è un ideale massimale se e solo se esiste $\alpha = (a_1, \ldots, a_n) \in K^n$ tale che $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$.

Dimostrazione T. 69 Abbiamo già visto in **T.**59 che un ideale della forma $(x_1 - a_1, \ldots, x_n - a_n)$ è massimale. Proviamo dunque che se $K = \overline{K}$ vale anche il viceversa. Sia $\mathfrak{m} \subset K[x_1, \ldots, x_n]$ un ideale massimale. Dalla forma debole del Nullstellensatz discende che $\mathbf{V}(\mathfrak{m}) \neq \emptyset$; esiste quindi $\alpha \in \mathbf{V}(\mathfrak{m})$. Da questo segue che

$$(x_1 - a_1, \ldots, x_n - a_n) = \mathbf{I}(\{\alpha\}) \supseteq \mathbf{I}(\mathbf{V}(\mathfrak{m})) = \sqrt{\mathfrak{m}} = \mathfrak{m},$$

ove la penultima uguaglianza è data dalla forma forte. La tesi segue dalla massimalità di $\mathfrak{m}$.

T. 70. Sia $K = \overline{K}$. Per ogni ideale $I \subseteq A = K[x_1, \ldots, x_n]$, l'insieme $\mathrm{Min}(I)$ dei primi minimali contenenti I è finito. In particolare, $\sqrt{I}$ si scrive come intersezione finita di primi di A.

Dimostrazione T. 70 Consideriamo $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$, per **T.**55.8, e sia $\mathbf{V}(I) = V_1 \cup \ldots \cup V_r$ una sua decomposizione minimale in sottovarietà irriducibili. Passando agli ideali associati, per la forma forte del Nullstellensatz, avremo che

$$\sqrt{I} = \mathbf{I}(\mathbf{V}(I)) = \mathbf{I}(V_1 \cup \ldots \cup V_r) = \mathbf{I}(V_1) \cap \ldots \cap \mathbf{I}(V_r) \ .$$

Grazie a **T.**57 possiamo concludere che abbiamo scritto $\sqrt{I}$ come intersezione di un numero finito di ideali primi. Poiché la decomposizione della varietà è minimale, tale intersezione è anch'essa minimale, ovvero non ci sono inclusioni tra i primi che intersechiamo. Infine, ricordando che un ideale è minimale su I se e solo se è minimale su $\sqrt{I}$, da **T.**12.2 e **T.**14 deduciamo che tali primi sono tutti e soli gli elementi $\mathrm{Min}(I)$.

Vedremo però più avanti che questa proprietà è vera in generale per ogni ideale in un anello noetheriano, cf. **T.**154 e **T.**159; a posteriori quindi, nel caso dell'anello dei polinomi, l'ipotesi che $K = \overline{K}$ può venire rimossa.

3.5 Sistemi di equazioni polinomiali

Vediamo in questa sezione un'applicazione del teorema degli zeri al problema della risoluzione di sistemi di equazioni polinomiali. Siano $\Sigma = \{f_i = 0 \colon i = 1, \ldots, s\}$ un sistema di equazioni polinomiali, con $f_i \in A = K[x_1, \ldots, x_n]$, $I = (f_1, \ldots, f_s)$ e G una base di Gröbner di I rispetto ad un qualunque ordinamento monomiale fissato.

Test di risolubilità di un sistema polinomiale

Il sistema Σ ha soluzione in $\overline{K}^n$ se e solo se $I \neq (1)$, cioè se e solo se $1 \notin G$.

Infatti, Σ ha soluzioni se e solo se $\mathbf{V}(I) \neq \emptyset$, cioè se e solo se $I \neq (1)$ per il teorema degli zeri, e possiamo controllare se questo sia vero grazie alle basi di Gröbner.
Una volta accertata l'esistenza o meno delle soluzioni del sistema Σ vorremo determinare di quante soluzioni si tratta, ovvero trovare la cardinalità di $\mathbf{V}(I)$.

T. 71. Siano $K = \overline{K}$ e $I = (G) \subset A = K[x_1, \ldots, x_n]$, ove G è una base di Gröbner di I rispetto ad un ordinamento fissato. I seguenti fatti sono equivalenti:

1. $\mathbf{V}(I)$ è finita.
2. Esistono $c_i \in \mathbb{N}$ e $g_{l_i} \in G$ tale che $\mathrm{lm}(g_{l_i}) = x_i^{c_i}$ per ogni $i = 1, \ldots, n$.
3. Il K-spazio vettoriale A/I ha dimensione finita, i.e. $\dim_K(A/I) < \infty$.

Dimostrazione T. 71 Dimostriamo che $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$.

$1. \Rightarrow 2.$ Se $\mathbf{V}(I) = \emptyset$, allora dalla forma debole del Nullstellensatz avremo che $I = (1)$, $1 \in G$ e $x_i^0 = 1$ per ogni $i = 1, \ldots, n$. Altrimenti, sia $\mathbf{V}(I) = \{\alpha_1, \ldots, \alpha_s\}$, con $\alpha_j = (a_{j1}, \ldots, a_{jn}) \in K^n$ per ogni $j = 1, \ldots, s$. Per ogni $i = 1, \ldots, n$ consideriamo allora il polinomio $f_i(X) = \prod_{j=1}^{s}(x_i - a_{ji})$; avremo che $f_i(\alpha_j) = 0$ per ogni $j = 1, \ldots, s$, e pertanto $f_i \in \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ per la forma forte del Nullstellensatz. Allora, per ogni $i = 1, \ldots, n$ esiste $d_i \in \mathbb{N}$ tale che $f_i^{d_i} \in I$; il suo leading monomial, che è $x_i^{sd_i}$, sta in $\mathrm{Lt}(I) = \mathrm{Lt}(G)$, e da ciò segue che per ogni $i = 1, \ldots, n$ esiste un elemento g_{l_i} di G il cui leading monomial è $\mathrm{lm}(g_{l_i}) = x_i^{c_i}$, per qualche $c_i \in \mathbb{N}$, con $c_i \leq sd_i$.

$2. \Rightarrow 3.$ Alla luce di **T.**50.1, è sufficiente dimostrare che l'insieme $\mathcal{B} = \{X^{\mathbf{a}} : \mathrm{lm}(g) \nmid X^{\mathbf{a}}, \text{ per ogni } g \in G\}$ è finito. Ora, se $X^{\mathbf{a}} \in \mathcal{B}$, dall'ipotesi discende che $a_1 < c_1, \ldots, a_n < c_n$, e pertanto il numero di tali $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$ è finito.

$3. \Rightarrow 1.$ Sia $d = \dim_K A/I$. Per ogni $i = 1, \ldots, n$, l'insieme $\{\overline{1}, \overline{x_i}, \ldots, \overline{x_i}^d\}$ è un insieme di vettori linearmente dipendenti; esiste pertanto una combinazione K-lineare non banale nulla $\sum_{j=0}^{d} b_{ij}\overline{x_i}^j = 0$. Pertanto $\sum_{j=0}^{d} b_{ij}x_i^j \in I \cap K[x_i]$ per ogni $i = 1, \ldots, n$. Sia ora $\alpha = (a_1, \ldots, a_n) \in \mathbf{V}(I)$; per quanto appena visto ogni a_i deve essere radice di un polinomio in una variabile non nullo, e quindi per ogni i ci sono solo un numero finito di possibilità. Da ciò possiamo concludere che gli elementi di $\mathbf{V}(I)$ sono in numero finito.

Osserviamo che nella dimostrazione $K = \overline{K}$ è stato usato solo in $1 \Rightarrow 2$. Senza l'ipotesi di K algebricamente chiuso vale anche $3 \Rightarrow 2$.

T. 72. Siano $K = \overline{K}$ e $\mathbf{V}(I)$ finita. Se I è radicale allora $|\mathbf{V}(I)| = \dim_K A/I$; inoltre I è un ideale zero dimensionale, i.e. $\dim(A/I) = 0$, e l'anello A/I è somma diretta di un numero finito di campi.

***Dimostrazione* T. 72** Se $K = \overline{K}$, $\mathbf{V}(I) = \{\alpha_1, \ldots, \alpha_s\}$ è finita e I è radicale, allora $I = \sqrt{I} = \mathbf{I}(\mathbf{V}(I)) = \mathbf{I}(\{\alpha_1, \ldots, \alpha_s\}) = \cap_{i=1}^s \mathbf{I}(\{\alpha_i\})$, e quindi da **T.**69 discende che $I = \cap_{i=1}^s \mathfrak{m}_{\alpha_i}$. Dato che tali ideali sono massimali e dunque comassimali avremo

$$A/I = A/\cap_{i=1}^s \mathfrak{m}_{\alpha_i} = A/\mathfrak{m}_{\alpha_1} \cdots \mathfrak{m}_{\alpha_s} \simeq \prod_{i=1}^s A/\mathfrak{m}_{\alpha_i} \simeq K^s.$$

In questa situazione l'anello A/I è un anello noetheriano - poiché gli ideali in A/I sono in corrispondenza 1:1 con gli ideali di A che contengono I, e tutti gli ideali di A sono finitamente generati - di dimensione 0. L'anello A/I risulta essere allora somma diretta finita di anelli locali noetheriani di dimensione 0. Questo è un fatto che vale più in generale, cf. **T.**168 e **T.**171.

Sappiamo che, in generale, $I \subseteq \sqrt{I}$. Sia $>$ un ordinamento fissato. Grazie a **T.**50, sappiamo che $\dim_K(A/I) = \dim_K(A/\mathrm{Lt}(I)) \geq \dim_K(A/\mathrm{Lt}(\sqrt{I})) = \dim_K(A/\sqrt{I})$, ove la disuguaglianza è dovuta al fatto che $\mathrm{Lt}(I) \subseteq \mathrm{Lt}(\sqrt{I})$. Inoltre, per **T.**48, vale l'uguaglianza se e solo se I è radicale. Per quanto riguarda la dimensione di Krull invece, da **T.**14 discende che $\dim(A/I) = \dim(A/\sqrt{I})$, pertanto I è zero dimensionale se e solo se $\sqrt{I}$ è zero dimensionale.

Osservazione 3.3. Se $K = \overline{K}$ e $\mathbf{V}(I)$ è finita o, equivalentemente $\dim_K(A/I)$ è finita, allora

$$|\mathbf{V}(I)| = |\mathbf{V}(\sqrt{I})| = \dim_K(A/\sqrt{I}) \leq \dim_K(A/I) < \infty.$$

Inoltre I è un ideale zero dimensionale.

Ora, se $K \subset \overline{K}$ e $I = (f_1, \ldots, f_s)$, avremo che $\mathbf{V}(I) = \{\alpha \in K^n \colon f_i(\alpha) = 0, i = 1, \ldots, s\} \subseteq \{\alpha \in \overline{K}^n \colon f_i(\alpha) = 0, i = 1, \ldots, s\} = \mathbf{V}_{\overline{K}}(\{f_i \colon i = 1, \ldots, s\}) = \mathbf{V}_{\overline{K}}(I\overline{K}[X])$. Pertanto, se la varietà dei punti nella chiusura

algebrica di K è finita, sicuramente lo è anche la varietà di partenza $\mathbf{V}(I)$. In questo caso avremo

$$|\mathbf{V}(I)| \leq |\mathbf{V}_{\overline{K}}(I\overline{K}[X])| \leq \dim_{\overline{K}}(\overline{K}[X]/I\overline{K}[X]) = \dim_K(K[X]/I) < \infty.$$

Come si giustifica l'ultima uguaglianza? Possiamo concludere anche in questo caso che A/I è zero dimensionale ?

3.6 Approfondimento: topologia di Zariski

T. 73. Sia $X = K^n$ lo spazio affine. Diciamo che Y è un chiuso di X se Y è una varietà affine, e A è un aperto di X se il suo complementare è un chiuso. Sia τ la famiglia degli aperti di A; allora τ è una topologia su X detta *topologia di Zariski* .

***Dimostrazione T.** 73* Tutto lo spazio $X = \mathbf{V}((0))$ e l'insieme vuoto $\emptyset = \mathbf{V}((1))$ sono chiusi. Inoltre è facile verificare, come nella dimostrazione di **T.**55 punti 5. e 6., che l'unione finita di chiusi è chiusa e che l'intersezione di una famiglia qualsiasi di chiusi è un chiuso.

Siano ora S un sottoinsieme di K^n e $\mathbf{I}(S) = \{f \in A\colon f(\alpha) = 0, \text{ per ogni } \alpha \in S\}$; osserviamo che $\mathbf{I}(S)$ è un ideale e consideriamo la varietà $\overline{S} = \mathbf{V}(\mathbf{I}(S))$. Chiamiamo $\overline{S}$ *chiusura di Zariski di* S, alla luce del seguente risultato.

T. 74. La varietà $\overline{S} = \mathbf{V}(\mathbf{I}(S))$ è la più piccola varietà affine che contiene S.

***Dimostrazione T.** 74* Dalla definizione discende immediatamente che $\overline{S}$ è una varietà affine che contiene S. Se poi $W \supseteq S$ è una varietà che contiene S, allora $\mathbf{I}(W) \subseteq \mathbf{I}(S)$, da cui segue che $W = \mathbf{V}(\mathbf{I}(W)) \supseteq \mathbf{V}(\mathbf{I}(S)) = \overline{S}$ e dunque $\overline{S}$ è l'intersezione di tutte le varietà affini che contengono S.

T. 75. [Teorema di chiusura] Siano $K = \overline{K}$, $I \subset A$ un ideale, I_k il k-esimo ideale di eliminazione di I, $V = \mathbf{V}(I)$ e $\pi_k : K^n \longrightarrow K^{n-k}$ la proiezione sulle ultime $n-k$ coordinate, $\pi(a_1, \ldots, a_n) = (a_{k+1}, \ldots, a_n)$. Allora

$$\overline{\pi_k(V)} = \mathbf{V}(I_k).$$

Dimostrazione T. *75* Siano $f \in I_k$ e $\alpha = (a_1, \ldots, a_n) \in V$, allora f si annulla in α e $f = f(x_{k+1}, \ldots, x_n)$. Dunque $f(\alpha) = f(a_{k+1}, \ldots, a_n) = f(\pi_k(\alpha)) = 0$, ovvero f si annulla su tutti i punti di $\pi_k(V)$. Abbiamo allora provato che $\pi_k(V) \subseteq \mathbf{V}(I_k)$, e da **T.**74 segue la prima inclusione.

Viceversa, sia $f \in \mathbf{I}(\pi_k(V)) \subseteq K[x_{k+1}, \ldots, x_n]$: per ogni $\alpha \in V$, se consideriamo f come polinomio in A, si ha $f(\alpha) = f(a_{k+1}, \ldots, a_n) = 0$. Quindi $f \in \mathbf{I}(V) = \sqrt{I}$ per la forma forte del Nullstellensatz, ed esiste allora un intero m tale che $f^m \in I \cap K[x_{k+1}, \ldots, x_n] = I_k$. Da questo segue che $f \in \sqrt{I_k}$ e dunque $\mathbf{I}(\pi_k(V)) \subseteq \sqrt{I_k}$. Passando alle varietà avremo allora $\mathbf{V}(I_k) = \mathbf{V}(\sqrt{I_k}) \subseteq \mathbf{V}(\mathbf{I}(\pi_k(V)) = \overline{\pi_k(V)}$.

T. 76. Sia V una varietà affine e sia $W \subseteq V$ una sottovarietà; allora

1. $V = W \cup (\overline{V \setminus W})$;
2. $\mathbf{V}(I : J) \supseteq \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}$;
3. se $K = \overline{K}$ è algebricamente chiuso e I è radicale allora

$$\mathbf{V}(I : J) = \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}.$$

Dimostrazione T. *76* 1. Dato che $V \supseteq W, V \setminus W$, allora avremo anche che $V \supseteq \overline{V \setminus W}$ e l'inclusione "$\supseteq$" è verificata. Per l'inclusione opposta avremo $V = W \cup (V \setminus W) \subseteq W \cup \overline{(V \setminus W)}$.

2. Ci basta provare che $I : J \subseteq \mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))$: infatti la tesi segue subito passando alle varietà. A questo scopo prendiamo un polinomio $f \in I : J$ e un punto $\alpha \in \mathbf{V}(I) \setminus \mathbf{V}(J)$. Allora avremo che $fg \in I$ per ogni $g \in J$ e $f(\alpha)g(\alpha) = fg(\alpha) = 0$ per ogni $g \in J$. Dato che $\alpha \notin \mathbf{V}(J)$, esiste un $g \in J$ tale che $g(\alpha) \neq 0$, e pertanto $f(\alpha) = 0$ per ogni tale α.

3. Come sopra, ci basta provare che $I : J \supseteq \mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))$. Sia allora $f \in \mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))$ e $g \in J$, bisogna verificare che $fg \in I = \sqrt{I}$. Il polinomio fg si annulla su ogni $\alpha \in \mathbf{V}(I)$ poiché un tale α annulla f se è in $\mathbf{V}(I) \setminus \mathbf{V}(J)$ o annulla g altrimenti. Per il Nullstellensatz allora $fg \in \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$, come desiderato.

Dotiamo ora *lo spettro di un anello* A, $\operatorname{Spec} A$, di una topologia. Siano $X = \operatorname{Spec} A$ ed E un sottoinsieme di A: definiamo

$$\mathcal{V}(E) = \{\mathfrak{p} \in \operatorname{Spec} A \ : \ E \subseteq \mathfrak{p}\}.$$

Topologia di Zariski

T. 77. Siano $E, E' \subseteq A$ sottoinsiemi e $I, J, I_\alpha \subseteq A$ ideali; allora

1. $\mathcal{V}(\{0\}) = X, \ \mathcal{V}(A) = \emptyset$;
2. $E \subseteq E' \Longrightarrow \mathcal{V}(E) \supseteq \mathcal{V}(E')$;
3. $\mathcal{V}(E) = \mathcal{V}((E)) = \mathcal{V}\left(\sqrt{(E)}\right)$;
4. $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J) = \mathcal{V}(IJ)$ (Unione finita);
5. $\bigcap_\alpha \mathcal{V}(I_\alpha) = \mathcal{V}(\bigcup_\alpha I_\alpha)$ (Intersezione qualunque).

Possiamo allora definire *topologia di Zariski su* X la topologia i cui chiusi sono gli insiemi $\mathcal{V}(E)$, con E sottoinsieme di A.

Dimostrazione T. 77 Chiaramente $X = \mathcal{V}(\{0\})$ e $\emptyset = \mathcal{V}(A)$ e quindi X e $\emptyset$ sono chiusi; il punto 2. è ovvio. Osserviamo poi che, dato che (E) è il più piccolo ideale che contiene E, ogni primo che contiene E contiene anche (E) e $\sqrt{(E)} = \bigcap_{(E)\subset\mathfrak{p}} \mathfrak{p}$. Quindi per ogni sottoinsieme E di A, si ha $\mathcal{V}(E) = \mathcal{V}((E)) = \mathcal{V}(\sqrt{(E)})$, dunque basta considerare gli insiemi $V(I)$ con I ideale radicale di A.

Per provare che l'unione finita di chiusi è un chiuso dimostriamo il punto 3., la tesi per un'unione finita segue poi facilmente. Da $IJ \subseteq I \cap J \subseteq I, J$ segue $\mathcal{V}(IJ) \supseteq \mathcal{V}(I \cap J) \supseteq \mathcal{V}(I) \cup \mathcal{V}(J)$.
Ricordiamo ora che se $I \cap J \subseteq \mathfrak{p}$ allora $I \subseteq \mathfrak{p}$ oppure $J \subseteq \mathfrak{p}$, cf. **T.**12.2, e se $IJ \subseteq \mathfrak{p}$ allora $I \subseteq \mathfrak{p}$ o $J \subseteq \mathfrak{p}$, per definizione di ideale primo. Da ciò si deduce che $\mathcal{V}(I) \cup \mathcal{V}(J) \supseteq \mathcal{V}(I \cap J)$ e $\mathcal{V}(I) \cup \mathcal{V}(J) \supseteq \mathcal{V}(IJ)$, e abbiamo dimostrato le uguaglianze volute.
Infine, $\mathfrak{p} \supseteq \bigcup_\alpha I_\alpha$ se e solo se $\mathfrak{p} \supseteq I_\alpha$ per ogni α, cioè se e solo se $\mathfrak{p} \in \bigcap_\alpha \mathcal{V}(I_\alpha)$.

T. 78. Siano A un anello e $X = \operatorname{Spec} A$ dotato della topologia di Zariski; allora gli insiemi

$$X_f = X \setminus \mathcal{V}(\{f\}) = \{\mathfrak{p} \in X \colon f \notin \mathfrak{p}\}$$

sono una base di aperti per X.

Dimostrazione T. *78* Bisogna verificare che ogni aperto $X \setminus \mathcal{V}(I)$ si scrive come unione di X_f. Da **T.**77.4 segue che $\mathcal{V}(I) = \bigcap_{f \in I} \mathcal{V}(f)$, e dunque

$$X \setminus \mathcal{V}(I) = X \setminus \Big(\bigcap_{f \in I} \mathcal{V}(f) \Big) = \bigcup_{f \in I} (X \setminus \mathcal{V}(f)) = \bigcup_{f \in I} X_f \ .$$

T. 79. Siano A un anello e $X = \operatorname{Spec} A$ dotato della topologia di Zariski; allora X è compatto.

Dimostrazione T. *79* Uno spazio topologico X è compatto se e solo se da ogni ricoprimento aperto formato da aperti della base si può estrarre un sottoricoprimento finito. Sia

$$X = \bigcup_{\alpha \in \Lambda} X_{f_\alpha} = \bigcup_{\alpha \in \Lambda} (X \setminus \mathcal{V}(f_\alpha)) = X \setminus \bigcap_{\alpha \in \Lambda} \mathcal{V}(f_\alpha) = X \setminus \mathcal{V}(\bigcup_{\alpha \in \Lambda} \{f_\alpha\}) \, .$$

Allora $\mathcal{V}(\bigcup_{\alpha \in \Lambda} \{f_\alpha\}) = \emptyset$, ossia gli $\{f_\alpha\}_{\alpha \in \Lambda}$ generano A. Pertanto esiste un sottoinsieme finito $\Lambda' \subseteq \Lambda$ ed elementi $g_\lambda \in A$, tali che $1 = \sum_{\lambda \in \Lambda'} g_\lambda f_\lambda$. Da ciò segue che $\mathcal{V}(\bigcup_{\lambda \in \Lambda'} \{f_\lambda\}) = \emptyset$ e quindi $X = \bigcup_{\lambda \in \Lambda'} X_{f_\lambda}$, ossia $\{X_{f_\lambda} \colon \lambda \in \Lambda'\}$ è un sottoricoprimento finito.

T. 80. Siano A un anello e $X = \operatorname{Spec} A$ dotato della topologia di Zariski; sia $Y \subset X$ e $\overline{Y}$ la sua chiusura. Allora $\overline{Y} = \mathcal{V}(\bigcap_{\mathfrak{p} \in Y} \mathfrak{p})$.

Dimostrazione T. *80* Dato che $\overline{Y}$ è chiuso, avremo che $\overline{Y} = \mathcal{V}(I)$ con I ideale di A. Chiaramente si ha $Y \subseteq \mathcal{V}(\bigcap_{\mathfrak{p} \in Y} \mathfrak{p})$, perché se $\mathfrak{q} \in Y$ allora $\mathfrak{q} \supseteq \bigcap_{\mathfrak{p} \in Y} \mathfrak{p}$ e quindi $\mathfrak{q} \in \mathcal{V}(\bigcap_{\mathfrak{p} \in Y} \mathfrak{p})$. Inoltre $\mathcal{V}(I) \supseteq \mathcal{V}(\bigcap_{\mathfrak{p} \in Y} \mathfrak{p})$: basta infatti verificare che $I \subseteq \bigcap_{\mathfrak{p} \in Y} \mathfrak{p}$ e questo è vero perché $\mathfrak{p} \in Y \subseteq \mathcal{V}(I) \Longrightarrow \mathfrak{p} \supseteq I$.
Dunque $Y \subseteq \mathcal{V}(\bigcap_{\mathfrak{p} \in Y} \mathfrak{p}) \subseteq \mathcal{V}(I) = \overline{Y}$ e passando alla chiusura si ha la tesi.

T. 81. Siano A un anello di dimensione positiva e $X = \operatorname{Spec} A$ dotato della topologia di Zariski; allora X è uno spazio topologico T_0 ma non T_1. In particolare, X non è uno spazio di Hausdorff.

Dimostrazione T. 81 Usando **T.**80, deduciamo che se $\mathfrak{p}$ è primo allora $\overline{\{\mathfrak{p}\}} = \mathcal{V}(\mathfrak{p})$ e quindi $\overline{\{\mathfrak{p}\}} = \{\mathfrak{p}\}$ se e solo se $\mathfrak{p}$ è massimale. Quindi X non è T_1, in quanto sono chiusi solo certi punti di X, ma non tutti perché se tutti i primi fossero massimali A avrebbe dimensione 0. A fortiori, X non è T_2. Proviamo che X è T_0. Consideriamo $\mathfrak{p}_1, \mathfrak{p}_2$ due punti distinti di X. Allora esiste, ad esempio, $f \in \mathfrak{p}_1$ e $f \notin \mathfrak{p}_2$ e quindi $X_f = X \setminus \mathcal{V}(f)$ è un aperto che contiene $\mathfrak{p}_2$ e non $\mathfrak{p}_1$.

T. 82. Sia $\phi : A \to B$ un omomorfismo di anelli; allora $\phi^* : \operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ data da $\phi^*(\mathfrak{q}) = \phi^{-1}(\mathfrak{q})$ è continua.

Dimostrazione T. 82 Sappiamo che la contrazione di un ideale primo è un ideale primo e dunque la funzione ϕ^* è ben definita. Poniamo $X = \operatorname{Spec} A$ e $Y = \operatorname{Spec} B$ e proviamo che la controimmagine di un aperto della base di X è aperta in Y verificando che se $f \in A$, allora $(\phi^*)^{-1}(X_f) = Y_{\phi(f)}$. Infatti, abbiamo che

$$\begin{aligned}(\phi^*)^{-1}(X_f) &= \{\mathfrak{q} \in Y \,:\, \phi^*(\mathfrak{q}) \in X_f\} = \{\mathfrak{q} \in Y \,:\, f \notin \phi^*(\mathfrak{q})\} \\ &= \{\mathfrak{q} \in Y \,:\, f \notin \phi^{-1}(\mathfrak{q})\} = \{\mathfrak{q} \in Y \,:\, \phi(f) \notin \mathfrak{q}\} = Y_{\phi(f)}\,.\end{aligned}$$

T. 83. Sia $\mathcal{N}(A)$ il nilradicale di A; allora X e $\operatorname{Spec}(A/\mathcal{N}(A))$ sono omeomorfi.

Dimostrazione T. 83 Per l'esercizio precedente $\pi^* : \operatorname{Spec}(A/\mathcal{N}(A)) \longrightarrow \operatorname{Spec} A$ indotta da $\pi : A \longrightarrow A/\mathcal{N}(A)$ è continua. Inoltre π^* è biunivoca, dato che π stabilisce una corrispondenza biunivoca tra gli ideali (primi) di $A/\mathcal{N}(A)$ e gli ideali (primi) di A che contengono $\mathcal{N}(A)$, cioè tutti gli ideali primi di A. Dato che $\pi^*(\mathcal{V}(I)) = \mathcal{V}(\pi^{-1}(I))$ per ogni ideale I di $A/\mathcal{N}(A)$, allora π^* è chiusa e quindi un omeomorfismo.

T. 84. X è irriducibile come spazio topologico se e solo se $\mathcal{N}(A)$ è primo, i.e. se e solo se $|\operatorname{Min} A| = 1$.

***Dimostrazione T.** 84* Ricordiamo che uno spazio topologico X si dice irriducibile se e solo se per ogni coppia di aperti non vuoti $A, B \subset X$ si ha $A \cap B \neq \emptyset$ o, equivalentemente, se e solo se per ogni aperto $A \neq \emptyset$ si ha $\overline{A} = X$.
Per il risultato precedente possiamo supporre che l'anello A sia ridotto, ossia $\sqrt{(0)} = (0)$ e provare che X è irriducibile se e solo se (0) è primo.
Siano $f, g \in A$ tali che $fg = 0$: allora

$$\begin{aligned} X_f \cap X_g &= (X \setminus \mathcal{V}(f)) \cap (X \setminus \mathcal{V}(g)) = X \setminus (\mathcal{V}(f) \cup \mathcal{V}(g)) \\ &= (X \setminus \mathcal{V}(fg)) = X \setminus \mathcal{V}(0) = \emptyset\,. \end{aligned}$$

Se X è irriducibile allora $X_f = \emptyset$ oppure $X_g = \emptyset$, ossia $\mathcal{V}(f) = X$ oppure $\mathcal{V}(g) = X$. Questo equivale a dire che per ogni primo $\mathfrak{p}$, $f \in \mathfrak{p}$ e quindi $f \in \mathcal{N}(A) = (0)$ o, analogamente, $g = 0$.
Viceversa supponiamo che (0) sia primo e siano $X - \mathcal{V}(I)$ e $X - \mathcal{V}(J)$ due aperti non vuoti. Dato che $\mathcal{V}(I) \neq X$ e $\mathcal{V}(J) \neq X$ si ha che $I \neq (0)$ e $J \neq (0)$ e quindi $(0) \in (X - \mathcal{V}(I)) \cap (X - \mathcal{V}(J))$, ossia l'intersezione è non vuota.

4

Moduli

4.1 Moduli e sottomoduli: definizioni e prime proprietà

Sia A un anello. Un insieme M si dice un A-modulo se $(M,+)$ è un gruppo abeliano ed esiste un'applicazione di *prodotto esterno* $\cdot\colon A \times M \longrightarrow M$, $(a,m) \longrightarrow a \cdot m = am$ tale che, per ogni $a,b,c \in A$ e per ogni $m,n \in M$ si abbia:

i) $(a+b)m = am + bm$;

ii) $a(m+n) = am + an$;

iii) $(ab)m = a(bm)$;

iv) $1_A\, m = m$.

Esempi 4.1. 1. Ogni anello A è naturalmente un A-modulo con l'operazione di prodotto esterno data dalla moltiplicazione, o prodotto interno, di A.

2. Sia A un sottoanello di B; allora $A \times B \longrightarrow B$ data dalla moltiplicazione di a per b come elementi di B verifica le proprietà richieste e quindi B è un A-modulo.

3. Quando $A = \mathbb{Z}$ un A-modulo è esattamente un gruppo abeliano.

4. Quando $A = K$ è un campo, un A-modulo è esattamente un K-spazio vettoriale.

Dato un A-modulo M, un sottoinsieme $N \subseteq M$ si dice A-*sottomodulo* di M quando

i) $(N,+)$ è un sottogruppo di $(M,+)$;

ii) N è chiuso rispetto al prodotto esterno: per ogni $a \in A$ e per ogni $n \in N$, si ha che $an \in N$.
Un modulo si dice *semplice* se non possiede sottomoduli non banali.

Esempi 4.2. 1. $\{0\}$ è un sottomodulo di qualsiasi modulo, scriveremo semplicemente 0.

2. I sottomoduli dell'A-modulo A sono tutti e soli gli ideali di A.

3. Dato un A-modulo M, per ogni ideale $I \subset A$, l'insieme

$$IM = \left\{ \sum_{i=1}^{s} a_i m_i \colon a_i \in I,\ m_i \in M,\ \text{per qualche } s \in \mathbb{N} \right\}$$

è un sottomodulo di M.

Dato un sottomodulo N di un A-modulo M, si può definire in modo naturale una struttura di A-modulo sul gruppo quoziente M/N definendo $a\,\overline{m} = \overline{am}$, per ogni $a \in A$ e $\overline{m} \in M/N$.
Inoltre dato un ideale $I \subset A$, sul modulo quoziente M/IM, oltre alla struttura di A-modulo, si può definire anche una struttura di A/I-modulo ponendo $\bar{a}\overline{m} = \overline{am}$, per ogni $\bar{a} \in A/I$ e $\overline{m} \in M/IM$. Il lettore avrà cura di verificarne la buona definizione, cf **E.**112.

Restrizione di scalari

Siano $f \colon A \longrightarrow B$ un omomorfismo di anelli e M un B-modulo. Possiamo dotare M di una struttura di A-modulo tramite f, ponendo

$$\cdot \colon A \times M \longrightarrow M, \quad (a, m) \mapsto f(a)m.$$

Si dice allora che M è un A-modulo *per restrizione di scalari* tramite f .

Questa definizione generalizza quanto visto nell'Esempio 4.1.2 dove $A \subseteq B$, $M = B$ e f è l'omomorfismo dato dall'immersione di A in B.

Operazioni fra sottomoduli

Sia $\{M_h\}_{h\in H}$ una famiglia qualsiasi di sottomoduli di un A-modulo M, allora i seguenti insiemi:

- **Somma di sottomoduli**

$$\sum_{h\in H} M_h = \left\{ \sum_h a_h m_h \colon \ a_h \in A, m_h \in M_h, a_h = 0 \ \text{ per quasi ogni } h \right\}$$

- **Intersezione di sottomoduli**

$$\bigcap_h M_h = \{m \in M \colon \ m \in M_h \ \text{ per ogni } h\}$$

sono sottomoduli di M.

È facile verificare che i sottoinsiemi di M sopra definiti sono effettivamente A-sottomoduli di M. È utile ricordare che in generale l'unione di sottomoduli non è un sottomodulo, a meno che essi non siano contenuti uno nell'altro in catena.
Dato che il prodotto fra elementi di un modulo non è definito non vi è un analogo del quoziente di ideali; si considera invece il seguente insieme.

Siano M un A-modulo e N, P sottomoduli di M. Si definisce l'insieme $N \colon P = \{a \in A \colon aP \subseteq N\}$. In particolare se $N = 0$ allora $0 : P$ viene denotato anche con $\operatorname{Ann} P$ e viene chiamato *l'annullatore di* P.

È facile vedere che $N : P$ e, in particolare, $\operatorname{Ann} P$ sono ideali di A, cf. **E.**115.

T. 85. Siano M un A-modulo e $I \subseteq A$ un ideale; se $I \subseteq \operatorname{Ann} M$ si definisce su M una struttura di A/I-modulo in maniera naturale, tramite il prodotto esterno $\overline{a}m = am$, per ogni $a \in A$ e $m \in M$.

***Dimostrazione* T.** *85* L'unica cosa da verificare è la buona definizione dell'operazione, essendo le condizioni di linearità sicuramente soddisfatte: dobbiamo provare che per ogni $a, b \in A$ tali che $\overline{a} = \overline{b} \in A/I$ si ha $am = bm \in M$ per ogni $m \in M$. Questo è vero se e solo se $(a - b)m = 0$, i.e. quando

$a - b \in \operatorname{Ann} M$ e ciò è garantito dal fatto che $a - b \in I \subseteq \operatorname{Ann} M$, per ipotesi.

Questa estensione risulta particolarmente utile nel caso in cui I sia un ideale massimale: in tal caso infatti si può definire su M una struttura di spazio vettoriale.

4.2 Omomorfismi di moduli

Siano M, N due A-moduli. Un'applicazione $f\colon M \longrightarrow N$ si dice *omomorfismo di A-moduli* se è un omomorfismo di gruppi ed è *A-lineare*, i.e. se, per ogni $m, n \in M$ e $a \in A$,
i) $f(m+n) = f(m) + f(n)$;
ii) $f(am) = af(m)$.
Se $M = N$ un omomorfismo si chiama anche *endomorfismo*.

Il modulo $\operatorname{Hom}_A(M, N)$

T. 86. L'insieme $\operatorname{Hom}_A(M, N)$ di tutti gli omomorfismi $f\colon M \longrightarrow N$ di A-moduli dotato delle operazioni

$$(f + g)(m) = f(m) + g(m), \quad (af)(m) = a\,(f(m)), \forall a \in A \text{ e } \forall m \in M,$$

è un A-modulo.
Inoltre, per ogni A-modulo M vale che $\operatorname{Hom}_A(A, M) \simeq M$.

L'A-modulo $\operatorname{Hom}_A(M, M)$ degli endomorfismi di M si denota con $\operatorname{End}_A M$.

Dimostrazione T. 86 Le proprietà della struttura di A-modulo sono conseguenze immediate della definizione (verificarlo!).

Sia $f\colon M \longrightarrow \operatorname{Hom}_A(A, M)$ la funzione definita da $f(m) = f_m$, dove $f_m(a) = am$. Tale applicazione è A-lineare: infatti si verifica facilmente che $f(\alpha m_1 + \beta m_2) = f_{\alpha m_1 + \beta m_2}$ è la funzione $\alpha f_{m_1} + \beta f_{m_2}$, per ogni $\alpha, \beta \in A$. È iniettiva, infatti $f(m) = 0$ se e solo se $f_m = 0$, i.e. $am = 0$ per ogni $a \in A$; quindi, in particolare, per $a = 1$ si ottiene $m = 0$. È inoltre surgettiva: ogni omomorfismo di A-moduli da A in M è individuato per A-linearità dall'immagine di 1: se $\varphi \in \operatorname{Hom}_A(A, M)$ è tale che $\varphi(1) = m$, allora $\varphi = f_m = f(m)$.

Dato un omomorfismo di moduli $f\colon M \longrightarrow N$, risultano definiti i seguenti sottomoduli:

- $\operatorname{Ker} f = \{m \in M \ : \ f(m) = 0\}$;
- $\operatorname{Im} f = f(M) \subseteq N$.

Definiamo inoltre il *conucleo di* f come il quoziente $\operatorname{Coker} f = N/\operatorname{Im} f$. È immediato verificare che f è iniettiva se e solo se $\operatorname{Ker} f = 0$ e f è surgettiva se e solo se $\operatorname{Coker} f = 0$.

Esempio 4.3. Siano $a \in A$ e M un A-modulo. L'applicazione di moltiplicazione per a, $\cdot a\colon M \longrightarrow M$ è un omomorfismo di A-moduli, e dunque un endomorfismo di M. Il suo nucleo è $\{m \in M\colon am = 0\}$, la sua immagine è $aM = (a)M$, e il suo conucleo è M/aM.

Teoremi di omomorfismo di moduli

T. 87. Siano M, N e P A-moduli.

I. Sia $f\colon M \longrightarrow N$ un omomorfismo di A-moduli; allora

$$M/\operatorname{Ker} f \simeq \operatorname{Im} f.$$

II. Siano $P \subseteq N \subseteq M$; allora

$$(M/P)/(N/P) \simeq M/N.$$

III. Siano N e P sottomoduli di M; allora

$$(N + P)/P \simeq N/(N \cap P).$$

Dimostrazione T. 87 **I.** La dimostrazione è analoga al corrispondente teorema per anelli: si dimostra facilmente che la mappa $\tilde{f} : M/\operatorname{Ker} f \to \operatorname{Im} f$ definita da $\tilde{f}(\overline{m}) = f(m)$ è ben definita ed è un isomorfismo.

II. Osserviamo dapprima che N/P è un sottomodulo di M/P; inoltre $f\colon M/P \longrightarrow M/N$ definito da $f(\overline{m}) = \overline{\overline{m}}$ è un omomorfismo ben definito: infatti se $\overline{m} = \overline{n}$ allora $m - n \in P \subseteq N$ e $\overline{\overline{m}} = \overline{\overline{n}}$. È ovvio che f è surgettivo; infine $\overline{m} \in \operatorname{Ker} f$ se e solo se $\overline{\overline{m}} = 0$, i.e. se $m \in N$ e $\overline{m} \in N/P$.

III. Consideriamo l'omomorfismo $\pi \circ j\colon N \xrightarrow{j} N + P \xrightarrow{\pi} (N + P)/P$, dove j è l'omomorfismo di inclusione di N in $N + P$ e π è la proiezione canonica

sul quoziente. Esso è chiaramente surgettivo. Sia $n \in N$ allora $(\pi \circ j)(n) = \overline{n} = 0$ se e solo se $n \in N \cap P$, dunque per il primo teorema di omomorfismo $(N + P)/P \simeq N/(N \cap P)$.

Diamo ora alcune importanti definizioni, che generalizzano quelle ben note nel caso di spazi vettoriali.

Generatori, insiemi liberi e basi

Sia M un A-modulo e sia $S \subseteq M$ un suo sottoinsieme.

- L'insieme

$$\langle S \rangle = \langle S \rangle_A = \left\{ \sum_{i=1}^{k} a_i s_i : \ a_i \in A \ s_i \in S, \ \text{ per qualche } k \in \mathbb{N} \right\} \subseteq M$$

costituito da tutte le combinazioni lineari finite di elementi di S a coefficienti in A, è un sottomodulo di M che si chiama il sottomodulo *generato* da S.

- Si dice che S è un *insieme di generatori* per M, e dunque che S *genera* M, se $\langle S \rangle = M$, ossia se per ogni $m \in M$ esistono $a_1, \ldots, a_k \in A$ e $s_1, \ldots, s_k \in S$ tali che $m = \sum_{i=1}^{k} a_i s_i$.
- Si dice che S è *libero*, e in tal caso i suoi elementi si dicono *linearmente indipendenti*, se per ogni $a_1, \ldots, a_k \in A$ e $s_1, \ldots, s_k \in S$, tali che $\sum_{i=1}^{k} a_i s_i = 0$ si ha $a_i = 0$, per ogni $i = 1, \ldots, k$.
- Un insieme di generatori libero di un modulo M si chiama *base* di M.

Dalla definizione di sottomodulo segue immediatamente che $\langle S \rangle$ è il più piccolo sottomodulo di M che contiene S.

Dato $M = \langle S \rangle$, se S è finito, allora M si dice *finitamente generato*; se $S = \{s\}$, allora M si dice *ciclico*; se S è libero allora M si dice *libero*. Quindi, per definizione, un modulo è libero se ammette una base.

Esempi 4.4. 1. Ogni anello A è un A-modulo libero, con base $\{1\}$.

2. $\mathbb{Z}/(n)$ è libero come modulo su se stesso, ma non è uno $\mathbb{Z}$-modulo libero.

3. L'anello A^n è un A-modulo libero e gli elementi $e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)$ ne costituiscono una base, detta *base canonica*.

T. 88. Sia M un A-modulo generato da un insieme S. Allora M è libero con base S se e solo se ogni elemento di M si scrive in maniera unica come combinazione lineare di elementi di S.

Dimostrazione T. 88 "$\Rightarrow$" Dato che S è un insieme di generatori, ogni elemento di M si scrive come combinazione di un numero finito di elementi di S. Se $\sum_i a_i s_i = \sum_j b_j s_j$ fossero due scritture dello stesso elemento, riordinando gli indici troveremmo $\sum_i (a_i - b_i)s_i = 0$, e poiché S è libero da ciò segue $a_i = b_i$ per ogni i, ovvero l'unicità della scrittura.
"$\Leftarrow$" Una combinazione lineare nulla di elementi di S è una scrittura dello 0 come combinazione di elementi di S: per l'unicità della scrittura segue subito che tale combinazione deve essere banale.

Osservazione 4.5. Non tutte le proprietà degli insiemi di generatori e degli insiemi liberi che valgono nel caso degli spazi vettoriali si generalizzano. In particolare:

1. Due insiemi di generatori minimali di un modulo non hanno necessariamente lo stesso numero di elementi.
2. Un insieme di generatori minimale di un modulo non è necessariamente una sua base.
3. Un sottoinsieme libero massimale non è necessariamente una base.
4. Un sottomodulo di un modulo finitamente generato non è necessariamente finitamente generato.
5. Non tutti i moduli hanno una base.
6. Un sottomodulo di un modulo libero non è necessariamente libero.

Ad esempio, consideriamo lo $\mathbb{Z}$-modulo $M = \mathbb{Z}$, gli insiemi $S = \{1\}$, $S_1 = \{2, 3\}$ e $S_2 = \{6, 10, 15\}$ sono tre insiemi di generatori minimali di cardinalità diverse, ma solo S è una base di M, dato che S_1 e S_2 non sono liberi. Inoltre, l'insieme $S_3 = \{2\}$ è libero e massimale ma non è una base di M.
Sia ora $A = K[x_1, x_2, \ldots, x_n, \ldots]$ l'anello dei polinomi in infinite variabili, a coefficienti in un campo K. Allora l'A-modulo A è finitamente generato da

1, ma l'ideale $N = (x_1, x_2, \ldots)$ è un sottomodulo di A che non è finitamente generato.
Se consideriamo lo $\mathbb{Z}$-modulo $N = \mathbb{Z}/(n)$, con $n \neq 0$, constatiamo che non esistono elementi linearmente indipendenti (e quindi basi) di N su $\mathbb{Z}$, dato che $n \cdot m = 0$ per ogni $m \in N$.
Infine, osserviamo che $\mathbb{Z}/(6)$ è libero come modulo su se stesso, ma il sottomodulo $P = (2)\mathbb{Z}/(6) = (\overline{2})$ non è uno $\mathbb{Z}/(6)$-modulo libero perché $\overline{3}P = 0$.

Se M è un A-modulo è libero, cioè ha una base, tutte le sue basi hanno la stessa cardinalità.

T. 89. [**Rango di un modulo libero**] Sia M un A-modulo libero; allora tutte le basi di M hanno la stessa cardinalità.
Chiamiamo tale numero il *rango* di M e lo denotiamo con $\operatorname{rank} M$, o $\operatorname{rank}_A M$ in caso di possibili ambiguità.

Dimostrazione T. 89 Dimostriamo che, se $\mathcal{B} = \{m_i\}_{i\in I}$ è una base di M come A-modulo, allora per ogni ideale massimale $\mathfrak{m}$ di A l'insieme $\overline{\mathcal{B}} = \{\overline{m_i}\}_{i\in I}$ è una base dell'$A/\mathfrak{m}$-spazio vettoriale $M/\mathfrak{m}M$. La tesi seguirà allora dal corrispondente risultato: le basi di uno spazio vettoriale sono equipotenti.
$\overline{\mathcal{B}}$ è un insieme di generatori: dato che ogni $m \in M$ si scrive come $\sum_i a_i m_i$ per certi $a_i \in A$, ogni elemento $\overline{m} \in M/\mathfrak{m}M$ si scrive come $\overline{m} = \overline{\sum_i a_i m_i} = \sum_i \overline{a_i m_i} = \sum_i \bar{a}_i \overline{m_i}$.
$\overline{\mathcal{B}}$ è un insieme libero: se $0 = \sum_i \bar{a}_i \overline{m_i} = \overline{\sum_i a_i m_i}$, allora $\sum_i a_i m_i \in \mathfrak{m}M$ e quindi esistono elementi $c_j \in \mathfrak{m}$ tali che $\sum_i a_i m_i = \sum_j c_j m_j$, ove per definizione, tutte le somme considerate sono finite. Riordinando gli indici possiamo scrivere che $\sum_i (a_i - c_i) m_i = 0$. Dato che $\mathcal{B}$ è una base di M, questo implica che $a_i = c_i \in \mathfrak{m}$ per ogni i, ossia $\bar{a}_i = 0$ per ogni i, come volevamo.

4.3 Somma e prodotto diretto di moduli

Data una famiglia $\{M_h\}_{h\in H}$ di A-moduli, possiamo definirne la *somma diretta*:

$$\bigoplus_{h\in H} M_h = \{(m_h)_{h\in H} : \ m_h \in M_h \ \text{ e } \ m_h = 0 \ \text{ per quasi ogni } h\}.$$

Togliendo il vincolo che gli elementi non nulli nella somma siano in numero finito, otteniamo la definizione di *prodotto diretto*:

$$\prod_{h\in H} M_h = \{(m_h)_{h\in H} \colon \ m_h \in M_h\}.$$

Dotando questi insiemi di una somma e di un prodotto esterno definiti componente per componente, si definisce su di essi una struttura di A-modulo. Osserviamo che in questo modo il primo modulo risulta essere un sottomodulo del secondo. Inoltre, nel caso di un numero finito di componenti, i.e. se $|H| < +\infty,$ le due strutture coincidono.

Osservazione 4.6. 1. Nel caso degli anelli ci siamo limitati alle somme e prodotti diretti per un numero finito di componenti perché la somma diretta di infiniti anelli commutativi con unità è ancora un anello commutativo ma senza unità, visto che questa appartiene solo al corrispondente prodotto diretto infinito. Dati anelli $A_1, \ldots, A_k$ useremo dunque indistintamente le notazioni $A_1 \times \cdots \times A_k$ e $A_1 \oplus \cdots \oplus A_k$, e le corrispondenti notazioni compatte $\prod_{i=1}^{k} A_i$ e $\bigoplus_{i=1}^{k} A_i$.
2. Dato un insieme S, finito o infinito, l'A-modulo libero

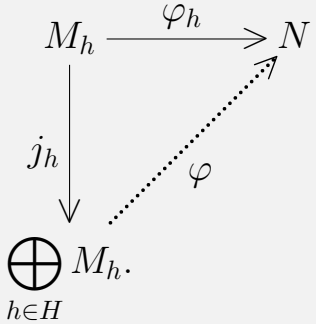
$$A^S = \bigoplus_{s\in S} A,$$

è la somma diretta di tante copie di A quanti sono gli elementi di S, con base canonica $\{e_s \colon s \in S\}$.
Se S è un sottoinsieme di un A-modulo M, l'assegnazione $e_s \mapsto s$ definisce un omomorfismo surgettivo $A^S \longrightarrow \bigoplus_{s\in S} \langle s\rangle$, ove $\langle s\rangle$ sono gli A-moduli ciclici $\langle s\rangle_A = As$ generati dagli elementi di S.

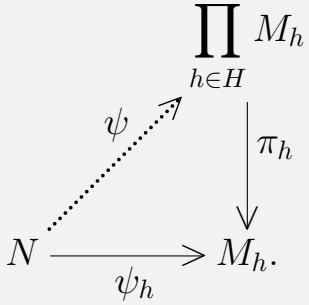
Proprietà universali della somma e del prodotto diretto

T. 90. Siano $\{M_h\}_{h\in H}$ una famiglia di A-moduli e N un A-modulo.

1. Per ogni $h \in H$ siano $j_h \colon M_h \longrightarrow \bigoplus_{h\in H} M_h$ gli omomorfismi di inclusione. Supponiamo che, per ogni $h \in H$, esista un omomorfismo $\varphi_h \colon M_h \longrightarrow N$; allora esiste un unico omomorfismo $\varphi \colon \bigoplus_{h\in H} M_h \longrightarrow N$ per cui i seguenti diagrammi commutano, per ogni $h \in H$:



2. Per ogni $h \in H$ siano $\pi_h \colon \prod_{h\in H} M_h \longrightarrow M_h$ gli omomorfismi di proiezione. Supponiamo che, per ogni $h \in H$, esista un omomorfismo $\psi_h \colon N \longrightarrow M_h$; allora esiste un unico omomorfismo $\psi \colon N \longrightarrow \prod_{h\in H} M_h$ per cui i seguenti diagrammi commutano, per ogni $h \in H$:



Dimostrazione T. *90* 1. L'omomorfismo $\varphi \colon \bigoplus_{h\in H} M_h \longrightarrow N$ dato da $m = (m_h)_{h\in H} \mapsto \sum_{h\in H} \varphi_h(m_h)$ è ben definito perché per ogni elemento $m \in \bigoplus_h M_h$ esistono solo un numero finito di $m_h \neq 0$ e quindi la somma è una somma finita di elementi di N. Inoltre è facile verificare che $\varphi \circ j_h = \varphi_h$ per ogni $h \in H$. Se poi φ' è un altro omomorfismo tale che $\varphi' \circ j_h = \varphi_h$ per ogni $h \in H$, si ha che

$$\varphi'(m) = \varphi'(\sum_{h\in H} j_h(m_h)) = \sum_{h\in H} \varphi'(j_h(m_h)) = \sum_{h\in H} \varphi_h(m_h) = \varphi(m)$$

per ogni $m \in \bigoplus_{h\in H} M_h$.

2. Sia $m = (m_h)_{h\in H} \in \prod_{h\in H} M_h$. Definiamo l'omomorfismo $\psi\colon N \longrightarrow \prod_{h\in H} M_h$ come $\psi(n) = (\psi_h(n))_{h\in H}$; è immediato vedere che ψ è tale che $\pi_h \circ \psi = \psi_h$ per ogni $h \in H$. Se poi ψ' è un omomorfismo tale che $\pi_h \circ \psi' = \psi_h$ e $\psi'(n) = (n_h)_{h\in H}$, con $n \in N$, allora, $n_h = \pi_h \circ \psi'(n) = \psi_h(n)$ per ogni $n \in N$, e dunque $\psi = \psi'$.

Esempio 4.7. Siano A un anello e x una indeterminata, e consideriamo i moduli ciclici $M_i = \langle x^i\rangle = Ax^i$ per ogni $i \in \mathbb{N}$; allora, dalle relative proprietà universali **T.**90.1 e 2 discendono degli isomorfismi canonici di A-moduli

$$\bigoplus_{i\in\mathbb{N}} M_i \simeq A[x] \qquad \text{e} \qquad \prod_{i\in\mathbb{N}} M_i \simeq A[[x]].$$

Concludiamo questa sezione con due caratterizzazioni per i moduli liberi.

T. 91. Un A-modulo $M = \langle S\rangle$ è libero con base S se e solo se per ogni A-modulo N e ogni applicazione $f\colon S \longrightarrow N$ esiste un unico omomorfismo di A-moduli $\tilde{f}\colon M \longrightarrow N$ tale che $\tilde{f}_{|S} = f$.

Dimostrazione T. 91 Abbiamo verificato in **T.**88 che se M è libero con base S allora ogni elemento di $m \in M$ si scrive in maniera unica come combinazione $m = \sum_i a_i s_i$ di elementi di S. Se vogliamo che $\tilde{f}$ sia un omomorfismo tale che $\tilde{f}_{|S} = f$, dobbiamo necessariamente definire

$$\tilde{f}(m) = \tilde{f}(\sum_i a_i s_i) = \sum_i a_i \tilde{f}(s_i) = \sum_i a_i f(s_i)\ ,$$

per ogni $m \in M$: dunque $\tilde{f}$ è univocamente determinato.

Mostriamo il viceversa, ovvero che S è libero. Consideriamo $N = A^S$ e $f\colon S \longrightarrow A^S$ che associa ad ogni $s \in S$ l'elemento e_s della base canonica dell'A-modulo libero A^S. Questa mappa si solleva ad un omomorfismo $\tilde{f}$ tale che $\tilde{f}(s) = f(s) = e_s$ per ogni $s \in S$. Inoltre è surgettivo, dato che ogni elemento di A^S è del tipo $\sum_i a_i e_{s_i}$, che è l'immagine di $\sum_i a_i s_i$, poiché

$\tilde{f}$ è un omomorfismo. È anche iniettivo: infatti dato $m = \sum_i a_i s_i$, avremo $0 = \tilde{f}(m) = \sum_i a_i \tilde{f}(s_i) = \sum_i a_i e_{s_i}$ se e solo se $a_i = 0$ per ogni i. Quindi M è isomorfo all'A-modulo libero A^S e ha base S.

T. 92. Ogni A-modulo M è quoziente di un A-modulo libero. In particolare, se M è finitamente generato da n elementi, allora M è quoziente di A^n.

Dimostrazione T. 92 Sia $\{m_h\}_{h\in H}$ un insieme di generatori per M; consideriamo il modulo libero A^H e l'omomorfismo definito da $f(e_h) = m_h$, ove $\{e_h\}_{h\in H}$ denota la base canonica di A^H. Tale f risulta essere surgettivo e dunque $M \simeq A^H/\operatorname{Ker} f$. La seconda parte dell'enunciato si deduce immediatamente.

T. 93. Un A-modulo M è libero se e solo se esistono A-moduli $\{M_i\}_{i\in H}$ tali che $M \simeq \oplus_{i\in H} M_i$, ove $M_i \simeq A$ per ogni i.

Dimostrazione T. 93 Nella dimostrazione di **T.**91 abbiamo visto che se M è libero con base S allora $M \simeq A^S$.

4.4 Lemma di Nakayama e sue conseguenze

Il prossimo risultato che riportiamo è di importanza fondamentale per lo sviluppo della teoria dei moduli, sebbene sia largamente noto con il nome di lemma e sia una diretta conseguenza del teorema di Cayley-Hamilton, che ricordiamo qui sotto.

T. 94. [**Teorema di Cayley-Hamilton**] Siano M un A-modulo finitamente generato da n elementi e I un ideale di A. Sia inoltre $\varphi \in \operatorname{End}_A M$ un endomorfismo di M tale che $\varphi(M) \subseteq IM$; allora esistono $a_0, \ldots, a_{n-1} \in I$ tali che

$$\varphi^n + \sum_{i=0}^{n-1} a_i \varphi^i = 0_{\operatorname{End}_A M} \ .$$

Dimostrazione T. 94 Sia $M = \langle m_1, \dots, m_n \rangle$. Dato che $\varphi(m_i) \in IM$, si ha $\varphi(m_i) = \sum_{j=1}^{n} c_{ij} m_j$, per certi $c_{ij} \in I$. In questo modo otteniamo n equazioni lineari

$$\varphi(m_i) - \sum_{j=1}^{n} c_{ij} m_j \;=\; \sum_{j=1}^{n} (\delta_{ij}\varphi - c_{ij}) m_j \;=\; 0$$

che possiamo rappresentare nel seguente modo:

$$T_\varphi \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} \varphi - c_{11} & -c_{12} & \cdots & -c_{1n} \\ -c_{21} & \varphi - c_{22} & & \vdots \\ \vdots & & \ddots & \\ -c_{n1} & \cdots & & \varphi - c_{nn} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Osserviamo che T_φ è una matrice $n \times n$ a coefficienti in $A[\varphi] \subset \mathrm{End}_A(M)$. Anche se l'anello $\mathrm{End}_A(M)$ degli endomorfismi di M non è commutativo, $A[\varphi]$ lo è, e quindi possiamo considerare la matrice aggiunta T_φ^* di T_φ e il suo determinante $\det T_\varphi \in A[\varphi]$. Avremo allora che

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = T_\varphi^* \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = T_\varphi^* T_\varphi \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} \det T_\varphi & 0 & \cdots & 0 \\ 0 & \det T_\varphi & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & \det T_\varphi \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix}.$$

Di conseguenza, $\det(T_\varphi) m_i = 0$ per ogni $i = 1, \dots, n$. Poiché $\det(T_\varphi) = \varphi^n + \sum a_i \varphi^i \in A[\varphi]$, con $a_i \in I$ per ogni i dato che $c_{ij} \in I$ per ogni i, j, è un endomorfismo che si annulla su ognuno dei generatori di M, esso coincide con l'omomorfismo nullo, da cui discende la tesi.

Il Lemma di Nakayama ha diverse formulazioni strettamente legate una all'altra, come si vedrà nelle dimostrazioni, ma non equivalenti. Ne presentiamo tre tra le più comuni.

Lemma di Nakayama

T. 95. Sia M un A-modulo finitamente generato.

I forma. Sia I un ideale di A tale che $M = IM$; allora esiste un elemento $a \in A$ tale che $a \equiv 1 \mod I$ e $aM = 0$.

II forma. Siano $\mathcal{J}(A)$ il radicale di Jacobson di A e $I \subseteq \mathcal{J}(A)$ un ideale di A tale che $IM = M$; allora $M = 0$.

III forma. Siano $N \subseteq M$ un sottomodulo e $I \subseteq \mathcal{J}(A)$ un ideale di A tale che $M = IM + N$; allora $M = N$.

Dimostrazione T. 95 I forma. Per il teorema di Cayley-Hamilton applicato all'endomorfismo identità id_M, otteniamo dei coefficienti $a_i \in I$ tali che $\mathrm{id}_M + \sum_{i=0}^{n-1} a_i \mathrm{id}_M = 0$. Di conseguenza, per ogni $m \in M$, si ha $(1 + \sum a_i)m = 0$. Ponendo $a = 1 + \sum a_i$ si ha $aM = 0$ e $a \equiv 1 \mod I$.
II forma. Per la prima forma del lemma di Nakayama, esiste un elemento a tale che $a \equiv 1 \pmod I$ e $aM = 0$. Di conseguenza, $1 - a \in I \subseteq \mathcal{J}(A)$ e dunque $a \in A^*$, cf. **T.**15. Pertanto $aM = 0$ implica $M = 0$, come volevamo.
III forma. Per la seconda forma del lemma di Nakayama, ci basta verificare che $M/N = I(M/N)$. Dal momento che

$$\begin{aligned} I\left({}^{M}\!/_{N}\right) &= \{\textstyle\sum a_i(m_i + N) \colon \ a_i \in I,\ m_i \in M\} \\ &= \{\textstyle\sum a_i m_i + N \colon \ a_i \in I,\ m_i \in M\} = {}^{(IM+N)}\!/_{N} = {}^{M}\!/_{N} \end{aligned}$$

anche questo enunciato risulta provato.

Esempio 4.8. Consideriamo $\mathbb{Q}$ come $\mathbb{Z}$-modulo: ovviamente $\mathbb{Q}$ non è finitamente generato (verificare), e il lemma di Nakayama non si applica in questo caso. Per esempio per ogni primo p si ha $p\mathbb{Q} = \mathbb{Q}$ ma non esiste $a \equiv 1 \mod p$ tale che $a\mathbb{Q} = 0$.

Grazie al lemma di Nakayama dato un A-modulo finitamente generato M, con $(A, \mathfrak{m}, K)$ locale, possiamo collegare la cardinalità di un insieme di generatori minimale di M come A-modulo alla dimensione di $M/\mathfrak{m}M$ come spazio vettoriale.

T. 96. Siano $(A, \mathfrak{m}, K)$ un anello locale e M un A-modulo finitamente generato; siano inoltre $\overline{m_1}, \ldots, \overline{m_k}$ una base del K-spazio vettoriale $M/\mathfrak{m}M$ e

$\pi\colon M \longrightarrow M/\mathfrak{m}M$ la proiezione canonica. Se $m_1, \dots, m_k \in M$ sono tali che $\pi(m_i) = \overline{m_i}$, allora $M = \langle m_1, \dots, m_k \rangle_A$.

Dimostrazione T. *96* Sia $N = \langle m_1, \dots, m_k \rangle \subseteq M$ e consideriamo l'omomorfismo

$$N \xrightarrow{j} M \xrightarrow{\pi} {}^{M}\!/_{\mathfrak{m}M},$$

dove j è l'inclusione di N in M. Per ipotesi, $\pi \circ j$ è un omomorfismo surgettivo, dunque $M = N + \mathfrak{m}M$: infatti $N + \mathfrak{m}M \subseteq M$ e per ogni $m \in M$ esiste un $n \in N$ tale che $\overline{n} = \overline{m}$, da cui segue che $n - m \in \mathfrak{m}M$ e $m = n + (m - n) \in N + \mathfrak{m}M$. Dato che l'anello è locale, $\mathfrak{m} = \mathcal{J}(A)$ e quindi, per la terza forma del lemma di Nakayama, $M = N$.

T. 97. Siano $(A, \mathfrak{m}, K)$ un anello locale e M un A-modulo finitamente generato; allora ogni insieme di generatori minimale di M ha la stessa cardinalità, $\dim_K M/\mathfrak{m}M$. La si indica spesso con $\mu(M)$ oppure $\beta_0(M)$.

Dimostrazione T. *97* Siano $d = \dim_K M/\mathfrak{m}M$ e $\{m_1, \dots, m_k\}$ un insieme di generatori minimale di M. Se $k < d$ avremmo che $\overline{m}_1, \dots, \overline{m}_k$ genera $M/\mathfrak{m}M$, che non è possibile. Se $k > d$, allora $\overline{m_1}, \dots, \overline{m_k}$ non sarebbero linearmente indipendenti e potremmo estrarre un sottoinsieme di d elementi che forma una base di $M/\mathfrak{m}M$. Dal risultato precedente, seguirebbe allora che un sottoinsieme proprio di $\{m_1, \dots, m_k\}$ genera M, contro l'ipotesi di minimalità.

Nel caso degli spazi vettoriali finitamente generati, sappiamo che ogni endomorfismo surgettivo o iniettivo è un isomorfismo. Nel caso dei moduli, ciò non è più vero: basta pensare a $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ definita da $f(1) = 2$ che è un endomorfismo di $\mathbb{Z}$ iniettivo ma non surgettivo. Vale però il seguente risultato.

T. 98. Siano M un A-modulo finitamente generato e $f \in \mathrm{End}_A M$ un endomorfismo surgettivo; allora f è iniettivo.

Dimostrazione T. *98* Dotiamo M di una struttura di $A[x]$-modulo definendo il prodotto esterno in questo modo: dato $p(x) = \sum_i a_i x^i$ e $m \in M$, sia

$$p(x)m = \sum_i a_i f^i(m)\,.$$

Dato che f è surgettivo si ha $M = f(M) = xM$ e quindi dal lemma di Nakayama, I forma, segue che esiste $p(x) \in A[x]$, $p(x) \equiv 1 \mod (x)$ tale che $p(x)M = 0$. Scriviamo $p(x) = 1 + xq(x)$ e consideriamo $m \in \operatorname{Ker} f$: otteniamo $m = (p(x) - xq(x))m = p(x)m - xq(x)m = 0$, da cui segue che $\operatorname{Ker} f = 0$ e quindi che f è iniettivo.

Concludiamo questa parte con la seguente proprietà dei moduli liberi.

T. 99. Sia M un A-modulo libero di rango r. Ogni insieme di generatori costituito da r elementi è una base di M.

Dimostrazione T. 99 Siano $S = \{m_1, \ldots, m_r\}$ e $\{n_1, \ldots, n_r\}$ rispettivamente una base e un insieme di generatori di M. L'assegnazione $f\colon S \longrightarrow M$ data da $m_i \mapsto n_i$ per ogni $i = 1, \ldots, r$ induce per **T.**91 un endomorfismo surgettivo $\tilde{f}$ di M. Per **T.**98, $\tilde{f}$ è un isomorfismo. Pertanto anche $\{n_1, \ldots, n_r\}$ è un insieme libero.

4.5 Categorie e funtori

Spendiamo due parole in questa breve sezione sui concetti di categoria e funtore, che sono concetti chiave in Teoria delle Categorie e Algebra omologica, le quali diventano, dopo la pubblicazione del testo fondamentale di H. Cartan e S. Eilenberg [CE], parti cruciali del sapere matematico. Si può dire che il linguaggio offerto dalla Teoria delle Categorie permette un più alto livello di astrazione. Introduciamo solamente qualche idea, affinché lo studente possa iniziare a pensare in questa ottica, rimandandolo a corsi futuri e ai libri di testo per una vera introduzione.

Una *categoria* è una coppia di dati $\mathcal{C} = (\mathrm{Obj}(\mathcal{C}), \mathrm{Mor}(\mathcal{C}))$ formata da $\mathrm{Obj}(\mathcal{C})$, gli *oggetti* di $\mathcal{C}$, e $\mathrm{Mor}(\mathcal{C})$, i *morfismi* di $\mathcal{C}$. Si pensi alle categorie $\mathcal{S}et$, $\mathcal{R}ing$, $\mathcal{T}op$, ove gli oggetti sono gli insiemi, gli anelli, gli spazi topologici, e i morfismi sono le funzioni tra insiemi, gli omomorfismi di anelli, le funzioni continue, rispettivamente.

Una categoria deve essere dotata di una *legge di composizione* $\circ$ per gli elementi di $\mathrm{Mor}(\mathcal{C})$, che deve verificare due proprietà:

- [associatività] per ogni $A, B, C, D \in \mathrm{Obj}(\mathcal{C})$ e per ogni $f, g, h \in \mathrm{Mor}(\mathcal{C})$, con $f\colon A \longrightarrow B$, $g\colon B \longrightarrow C$, $h\colon C \longrightarrow D$, si deve avere $h\circ(g\circ f) = (h\circ g)\circ f$;
- [esistenza dell'identità] per ogni $A \in \mathrm{Obj}(\mathcal{C})$ esiste in $\mathrm{Mor}(\mathcal{C})$ un morfismo $\mathrm{id}_A\colon A \longrightarrow A$ tale che, per ogni $B \in \mathrm{Obj}(\mathcal{C})$ e $g, h \in \mathrm{Mor}(\mathcal{C})$, con $g\colon A \longrightarrow B$ e $h\colon B \longrightarrow A$, si ha che $g \circ \mathrm{id}_A = g$, $\mathrm{id}_A \circ h = h$.

Per mettere in relazione due categorie, diciamo $\mathcal{C}$ e $\mathcal{D}$, si usa il concetto di funtore: è una mappa $F\colon \mathcal{C} \longrightarrow \mathcal{D}$ che trasforma oggetti in oggetti e mappe in mappe. Più precisamente si vuole che

- per ogni $A \in \mathrm{Obj}(\mathcal{C})$, $F(A) \in \mathrm{Obj}(\mathcal{D})$;
- per ogni $f \in \mathrm{Mor}(\mathcal{C})$, $F(f) \in \mathrm{Mor}(\mathcal{D})$;
- per ogni $A \in \mathrm{Obj}(\mathcal{C})$, $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$;
- F deve essere compatibile con la composizione. Dobbiamo distinguere due casi: sia $f \in \mathrm{Mor}(\mathcal{C})$, $f\colon A \longrightarrow B$,

1. se $F(f)\colon F(A) \longrightarrow F(B)$, allora F si dice *covariante*;
2. se $F(f)\colon F(B) \longrightarrow F(A)$, allora F si dice *contravariante*.

Nel primo caso si richiede che $F(g\circ f) = F(g)\circ F(f)$, per ogni $f, g \in \mathrm{Mor}(\mathcal{C})$, $f\colon A \longrightarrow B$, $g\colon B \longrightarrow C$. Nel secondo invece richiederemo che $F(g \circ f) = F(f) \circ F(g)$, per ogni $f, g \in \mathrm{Mor}(\mathcal{C})$, $f\colon A \longrightarrow B$, $g\colon B \longrightarrow C$.

Come primi esempi di funtori si possono considerare il *funtore costante* e il *funtore dimenticante*.

- Date due categorie qualsiasi $\mathcal{C}$ e $\mathcal{D}$, il funtore costante manda ogni oggetto di $\mathcal{C}$ in un oggetto X di $\mathcal{D}$ fissato, e ogni elemento di $\mathrm{Mor}(\mathcal{C})$ in $\mathrm{id}_X \in \mathrm{Mor}(\mathcal{D})$.
- Siano $\mathcal{C} = \mathcal{R}ing$ e $\mathcal{D} = \mathcal{G}rp$ le categorie degli anelli con omomorfismi di anello e dei gruppi con omomorfismi di gruppi, rispettivamente; il funtore dimenticante $F\colon \mathcal{C} \longrightarrow \mathcal{D}$ lascia oggetti e omomorfismi invariati, dimenticandosi della moltiplicazione e della struttura che ne deriva. È ovviamente un funtore covariante.

Nel seguito vedremo alcuni importanti esempi di funtore in Algebra Commutativa, quali $\mathrm{Hom}_A(M,\bullet)$, $\mathrm{Hom}_A(\bullet,N)$, $\bullet\otimes_A N$, $S^{-1}\bullet$, tutti definiti sulla categoria degli A-moduli.

4.6 Successioni esatte

Siano $\{M_i\}$ una famiglia di A-moduli e $\{\varphi_i\colon M_{i-1}\longrightarrow M_i\}$ una famiglia di omomorfismi. La *successione*, o *sequenza*, di A-moduli

$$\ldots\longrightarrow M_{i-1}\xrightarrow{\varphi_i} M_i\xrightarrow{\varphi_{i+1}} M_{i+1}\longrightarrow\ldots$$

si dice *complesso di A-moduli* se la composizione di due qualsiasi omomorfismi del complesso è nulla, i.e. se $\varphi_{i+1}\circ\varphi_i=0$ per ogni i, ossia se e solo se $\operatorname{Im}\varphi_i\subseteq\operatorname{Ker}\varphi_{i+1}$ per ogni i. Se il complesso è limitato a sinistra e/o a destra, ovvero se $M_i=0$ definitivamente a sinistra e/o a destra, ne scriviamo solo la parte non nulla, inserendo solo uno 0 a sinistra e/o a destra. Nel seguito tutti i complessi avranno solo un numero finito di moduli non nulli.

Una successione si dice *esatta in M_i* se $\operatorname{Im}\varphi_i=\operatorname{Ker}\varphi_{i+1}$; si dice che una successione è *esatta* se è esatta in ogni M_i. Una successione esatta

$$0\longrightarrow M\xrightarrow{f} N\xrightarrow{g} P\longrightarrow 0 \tag{4.1}$$

si dice *esatta corta*. Dalla definizione abbiamo subito che $0\longrightarrow M\xrightarrow{f}N$ è esatta se e solo se f è iniettiva, $N\xrightarrow{g}P\longrightarrow 0$ è esatta se e solo se g è surgettiva, e $0\longrightarrow M\xrightarrow{f}N\xrightarrow{g}P\longrightarrow 0$ è esatta se e solo se f è iniettiva, g è surgettiva e $\operatorname{Coker} f=N/\operatorname{Im} f=N/\operatorname{Ker} g\simeq P$.

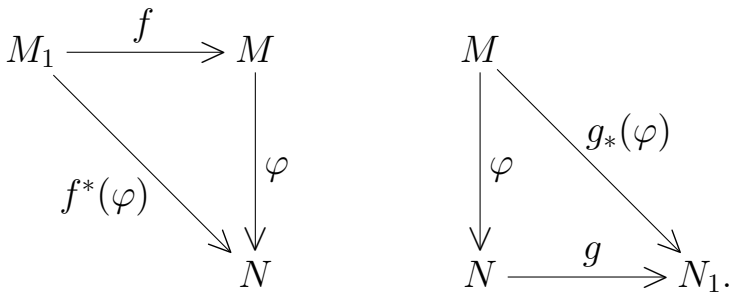
Tipicamente le sequenze esatte corte vengono usate col seguente scopo. Supponiamo di avere tre moduli M,N,P in sequenza esatta corta come in (4.1), e di volerne studiare un invariante ρ o una proprietà $\mathcal{P}$. Dalla conoscenza di ρ per due dei tre moduli è spesso possibile determinare, o perlomeno stimare, il ρ del terzo modulo; similmente, sapendo che la proprietà $\mathcal{P}$ vale per due dei tre moduli, è spesso possibile dire che $\mathcal{P}$ vale per il terzo modulo. Ad esempio, se i moduli in questione sono K-spazi vettoriali, si può pensare a $\rho=\dim_K$; si veda **T.**152.2 per un esempio, quando $\mathcal{P}$ è "essere noetheriano".

4.6.1 I funtori $\mathbf{Hom}_A(M, \bullet)$ e $\mathbf{Hom}_A(\bullet, N)$

Dati A-moduli M, M_1, N e N_1 e omomorfismi $f : M_1 \longrightarrow M$ e $g : N \longrightarrow N_1$ possiamo definire omomorfismi

$$f^*\colon \mathrm{Hom}_A(M,N) \longrightarrow \mathrm{Hom}_A(M_1,N) \quad \varphi \mapsto \varphi \circ f \qquad \text{e} \qquad g_*\colon \mathrm{Hom}_A(M,N) \longrightarrow \mathrm{Hom}_A(M,N_1) \quad \varphi \mapsto g \circ \varphi$$

in modo che i seguenti diagrammi commutino



Valgono inoltre le seguenti proprietà:

- se $f\colon M \longrightarrow M$ è id_M allora $f^* = \mathrm{id}_{\mathrm{Hom}(M,N)}$ per ogni N;
- se $g\colon N \longrightarrow N$ è id_N allora $g_* = \mathrm{id}_{\mathrm{Hom}(M,N)}$ per ogni M;
- per ogni A-modulo M_2 e omomorfismo $f'\colon M_2 \longrightarrow M_1$, si ha

$$(f \circ f')^* = f'^* \circ f^* \ ;$$

- per ogni A-modulo N_2 e omomorfismo $g'\colon N_1 \longrightarrow N_2$, si ha

$$(g' \circ g)_* = g'_* \circ g_* \, .$$

Fissato N si ha che $\mathrm{Hom}_A(\bullet, N)$ fornisce un'operazione che trasforma un qualsiasi A-modulo M in un altro A-modulo, $\mathrm{Hom}_A(M, N)$; trasforma inoltre un'omomorfismo A-lineare $f\colon M_1 \longrightarrow M$ in un altro omomorfismo A-lineare $\mathrm{Hom}_A(f, N) = f^*$, e gli omomorfismi identità in omomorfismi identità. Infine, si comporta bene rispetto alla composizione di mappe. Nel linguaggio dell'algebra omologica si dice che $\mathrm{Hom}_A(\bullet, N)$ è un funtore dalla categoria degli A-moduli in se stessa. Visto poi che $\mathrm{Hom}_A(f \circ f', N) = \mathrm{Hom}_A(f', N) \circ \mathrm{Hom}_A(f, N)$, ovvero l'ordine nella composizione viene scambiato, si dice che $\mathrm{Hom}_A(\bullet, N)$ è un funtore contravariante.

Fissato M, anche $\mathrm{Hom}_A(M, \bullet)$ è un funtore, ma è covariante per via di $\mathrm{Hom}_A(M, g' \circ g) = \mathrm{Hom}_A(M, g') \circ \mathrm{Hom}_A(M, g)$.

T. 100. [Esattezza a sinistra di $\mathrm{Hom}(\bullet, N)$ e $\mathrm{Hom}(M, \bullet)$]

1. Sia $M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ una successione esatta di A-moduli. Allora, per ogni A-modulo N, la successione
$$0 \longrightarrow \mathrm{Hom}_A(M_2, N) \xrightarrow{g^*} \mathrm{Hom}_A(M, N) \xrightarrow{f^*} \mathrm{Hom}_A(M_1, N)$$
è esatta .
2. Sia $0 \longrightarrow N_1 \xrightarrow{f} N \xrightarrow{g} N_2$ una successione esatta di A-moduli. Allora, per ogni A-modulo M, la successione
$$0 \longrightarrow \mathrm{Hom}_A(M, N_1) \xrightarrow{f_*} \mathrm{Hom}_A(M, N) \xrightarrow{g_*} \mathrm{Hom}_A(M, N_2)$$
è esatta.

Diremo pertanto che i funtori $\mathrm{Hom}_A(\bullet, N)$ e $\mathrm{Hom}_A(M, \bullet)$ sono *esatti a sinistra* riferendoci a queste proprietà.

I viceversa di entrambe le affermazioni di **T.**100 sono ancora veri.

T. 101. 1. Sia $M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ una successione di A-moduli tale che, per ogni A-modulo N, la successione
$$0 \longrightarrow \mathrm{Hom}_A(M_2, N) \xrightarrow{g^*} \mathrm{Hom}_A(M, N) \xrightarrow{f^*} \mathrm{Hom}_A(M_1, N)$$
è esatta; allora $M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ è esatta.
2. Sia $0 \longrightarrow N_1 \xrightarrow{f} N \xrightarrow{g} N_2$ una successione di A-moduli tale che, per ogni A-modulo M, la successione
$$0 \longrightarrow \mathrm{Hom}_A(M, N_1) \xrightarrow{f_*} \mathrm{Hom}_A(M, N) \xrightarrow{g_*} \mathrm{Hom}_A(M, N_2)$$
è esatta; allora $0 \longrightarrow N_1 \xrightarrow{f} N \xrightarrow{g} N_2$ è esatta.

Dimostrazione T. 100 1. Dobbiamo provare che la successione è esatta, per ogni A-modulo N.

$\boxed{\text{In } \mathrm{Hom}_A(M_2, N)}$ ovvero g^* è iniettiva.

Sia $\varphi \in \mathrm{Hom}_A(M_2, N)$ e supponiamo che $g^*(\varphi) = \varphi \circ g = 0$. Dato che g è surgettiva per ipotesi, per ogni $m_2 \in M_2$ esiste $m \in M$ tale che $m_2 = g(m)$ e dunque $\varphi(m_2) = \varphi(g(m)) = 0$; quindi $\varphi = 0$ e $\mathrm{Ker}\, g^* = 0$.

$\boxed{\text{In } \mathrm{Hom}_A(M, N)}$ ovvero $\mathrm{Im}\, g^* = \mathrm{Ker}\, f^*$.
Dato che vale $f^* \circ g^* = (g \circ f)^* = 0$ si ha immediatamente che $\mathrm{Im}\, g^* \subseteq \mathrm{Ker}\, f^*$. Proviamo ora che $\mathrm{Ker}\, f^* \subseteq \mathrm{Im}\, g^*$: sia $\psi \in \mathrm{Ker}\, f^*$, dobbiamo costruire $\varphi \in \mathrm{Hom}(M_2, N)$ tale che $g^*(\varphi) = \varphi \circ g = \psi$. Dato che g è surgettiva, per ogni $m_2 \in M_2$ esiste $m \in M$ tale che $m_2 = g(m)$ e possiamo dunque definire φ ponendo $\varphi(m_2) = \psi(m)$. Bisogna però verificare che φ è ben definita. Sicuramente φ è a valori in N. Siano $m, n \in g^{-1}(m_2)$, allora $m - n \in \mathrm{Ker}\, g = \mathrm{Im}\, f$ e quindi esiste $m_1 \in M_1$ tale che $m - n = f(m_1)$. Ma allora $\psi(m-n) = \psi(f(m_1)) = f^*(\psi)(m_1) = 0$, poiché $\psi \in \mathrm{Ker}\, f^*$. Quindi φ è ben definita, poiché la definizione non dipende dalla scelta dell'elemento nella controimmagine.

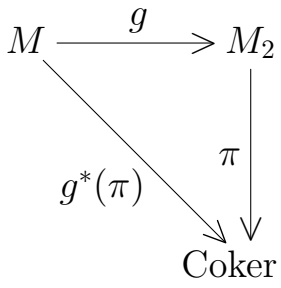
2. La dimostrazione è analoga a quella del punto precedente. Dobbiamo provare che la seconda successione è esatta per ogni A-modulo M.

$\boxed{\text{In } \mathrm{Hom}_A(M, N_1)}$ ovvero f_* è iniettiva.
Sia $\varphi \in \mathrm{Hom}_A(M, N_1)$ tale che $f_*(\varphi) = f \circ \varphi = 0$; da ciò deduciamo che $\mathrm{Im}\, \varphi \subseteq \mathrm{Ker}\, f$ e, dall'iniettività di f, che $\varphi = 0$.

$\boxed{\text{In } \mathrm{Hom}_A(M, N)}$ ovvero $\mathrm{Im}\, f_* = \mathrm{Ker}\, g_*$.
Dato che vale $g_* \circ f_* = (g \circ f)_* = 0$ si ha immediatamente che $\mathrm{Im}\, f_* \subseteq \mathrm{Ker}\, g_*$. Per l'altra inclusione, sia $\psi \in \mathrm{Ker}\, g_*$, e dunque $g \circ \psi = 0$. Dobbiamo definire $\varphi \in \mathrm{Hom}_A(M, N_1)$ tale che $f_*(\varphi) = \psi$; lo facciamo ponendo $\varphi(m) = f^{-1}(\psi(m))$ per ogni $m \in M$. Tale applicazione è ben definita perché f è iniettiva e per ipotesi $\mathrm{Im}\, \psi \subseteq \mathrm{Ker}\, g = \mathrm{Im}\, f$.

Dimostrazione T. *101* 1. Dato che la successione degli Hom è esatta per ogni A-modulo N, scegliamo allora degli opportuni N per dedurre l'esattezza della successione di partenza.

$\boxed{\text{In } M_2}$ ovvero g è surgettiva.
Scegliamo $N = \mathrm{Coker}\, g = M_2/\mathrm{Im}\, g$ e proviamo che $N = 0$. Consideriamo il diagramma

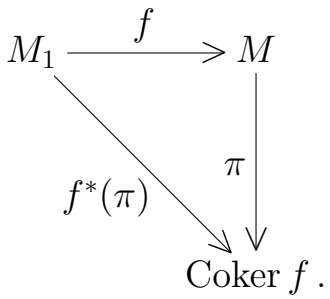


Per dimostrare che $N = 0$ proviamo che la proiezione π è l'omomorfismo nullo. Per costruzione $g^*(\pi) = 0$ e la conclusione segue pertanto dall'ipotesi che g^* è iniettiva per ogni A-modulo N.

$\boxed{\text{In } M}$ ovvero $\operatorname{Ker} g = \operatorname{Im} f$.

Che $\operatorname{Ker} g \supseteq \operatorname{Im} f$ segue dal fatto che $(g \circ f)^* = f^* \circ g^* = 0$. Infatti, preso $N = M_2$, abbiamo $0 = (g \circ f)^*(\mathrm{id}_{M_2}) = \mathrm{id}_{M_2} \circ g \circ f = g \circ f = 0$, ovvero $\operatorname{Im} f \subseteq \operatorname{Ker} g$.

Per provare che $\operatorname{Ker} g \subseteq \operatorname{Im} f$ scegliamo $N = \operatorname{Coker} f = M/\operatorname{Im} f$ e consideriamo il diagramma

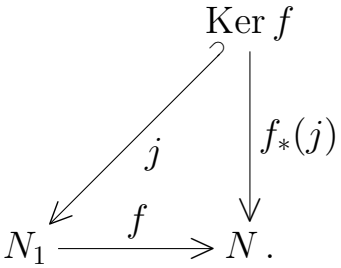


Per costruzione abbiamo che $\operatorname{Im} f = \operatorname{Ker} \pi$ e che $f^*(\pi) = 0$; di conseguenza $\pi \in \operatorname{Ker} f^* = \operatorname{Im} g^*$ ed esiste $\varphi \in \operatorname{Hom}(M_2, N)$ tale che $g^*(\varphi) = \varphi \circ g = \pi$; abbiamo quindi ottenuto che $\operatorname{Im} f = \operatorname{Ker} \pi \supseteq \operatorname{Ker} g$.

2. Analogamente al precedente dimostriamo che la successione di partenza è esatta scegliendo degli opportuni moduli M per la successione degli Hom.

$\boxed{\text{In } N_1}$ ovvero f è iniettiva.

Scegliamo $M = \operatorname{Ker} f$: consideriamo l'immersione $j\colon \operatorname{Ker} f \longrightarrow N_1$ e il diagramma

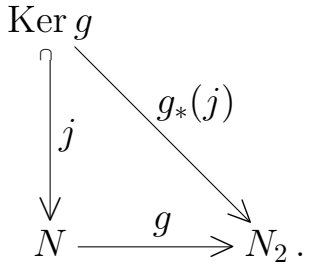


Per costruzione, $f_*(j) = 0$ e, dato che per ipotesi f_* è iniettiva per ogni M, si ottiene che $j = 0$, cioè f è iniettiva.

In N ovvero $\operatorname{Ker} g = \operatorname{Im} f$.

Dimostriamo le inclusioni $\operatorname{Im} f \subseteq \operatorname{Ker} g$ e $\operatorname{Im} f \supseteq \operatorname{Ker} g$. La prima segue dal fatto che $(g \circ f)_* = g_* \circ f_* = 0$. Infatti, prendendo $M = N_1$ e $\mathrm{id}_{N_1} \in \operatorname{Hom}_A(M, N_1)$, deduciamo che $g \circ f = 0$, ovvero $\operatorname{Im} f \subseteq \operatorname{Ker} g$.

Per dimostrare che $\operatorname{Im} f \supseteq \operatorname{Ker} g$ scegliamo $M = \operatorname{Ker} g$ e consideriamo il diagramma



Per costruzione, $g_*(j) = 0$, cioè $j \in \operatorname{Ker} g_* = \operatorname{Im} f_*$ e dunque esiste $\varphi \in \operatorname{Hom}_A(\operatorname{Ker} g, N_1)$ tale che $f_*(\varphi) = f \circ \varphi = j$. Dato che j è l'omomorfismo di inclusione di $\operatorname{Ker} g$ in N, da quest'ultima uguaglianza discende che $\operatorname{Im} f \supseteq \operatorname{Im} j = \operatorname{Ker} g$, come volevamo.

Alternativamente, la conclusione discende scegliendo $M = A$ e osservando che, per **T.** 86, nel diagramma

$$\begin{array}{ccccccc} 0 & \longrightarrow & \operatorname{Hom}_A(A, N_1) & \xrightarrow{f_*} & \operatorname{Hom}_A(A, N) & \xrightarrow{g_*} & \operatorname{Hom}_A(A, N_2) \\ & & \downarrow \simeq & & \downarrow \simeq & & \downarrow \simeq \\ 0 & \longrightarrow & N_1 & \xrightarrow{f} & N & \xrightarrow{g} & N_2, \end{array}$$

le frecce verticali sono isomorfismi e i quadrati commutano.

4.6.2 Successioni che spezzano

Dalla definizione di somma diretta di A-moduli segue che, per ogni M, N, la successione

$$0 \longrightarrow M \xrightarrow{i_M} M \oplus N \xrightarrow{\pi_N} N \longrightarrow 0$$

dove $i_M(m) = (m, 0)$ e $\pi_N(m, n) = n$, è esatta. Però non è sempre vero che una successione esatta corta

$$0 \longrightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} P \longrightarrow 0$$

fornisce una decomposizione di N in termini di M e P. Le successioni che hanno questa proprietà sono caratterizzate dalla seguente proposizione.

T. 102. Sia $0 \longrightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} P \longrightarrow 0$ una successione esatta di A-moduli. Le seguenti condizioni sono equivalenti:

1. esiste un isomorfismo $N \xrightarrow{\varphi} M \oplus P$ per cui il seguente diagramma commuta:

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

2. esiste un omomorfismo $r\colon N \longrightarrow M$ tale che $r \circ \alpha = \mathrm{id}_M$, ossia r è un inverso sinistro di α;
3. esiste un omomorfismo $s\colon P \longrightarrow N$ tale che $\beta \circ s = \mathrm{id}_P$, ossia s è un inverso destro di β.

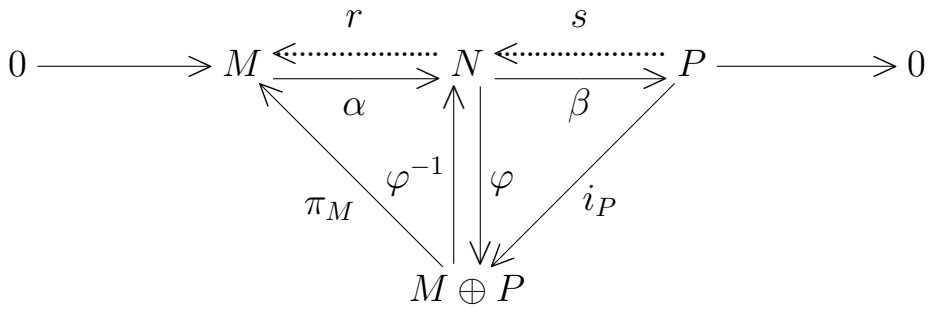
Se vale una delle suddette condizioni equivalenti si dice che la successione *spezza*; in questo caso r si dice una *retrazione di* α e s una *sezione di* β.

Dimostrazione T. 102

Osserviamo prima di tutto che, se abbiamo una successione esatta corta

$$0 \longrightarrow M \xrightarrow{i_M} M \oplus N \xrightarrow{\pi_N} N \longrightarrow 0$$

allora le immersioni e le proiezioni canoniche giocano il ruolo di sezioni e retrazioni, i.e. $i_M \circ \pi_M = \mathrm{id}_M$ e $\pi_P \circ i_P = \mathrm{id}_P$. Consideriamo allora il seguente diagramma



$1 \Rightarrow 2$. Basta definire r ponendo, per ogni $n = \varphi^{-1}(m,p) \in N$, $r(n) = \pi_M(m,p) = m$, i.e. $r(n) = (\pi_M \circ \varphi)(n)$.

$1 \Rightarrow 3$. Poiché β è surgettivo, per ogni $p \in P$ esiste $n \in N$ tale che $\beta(n) = p$. Definiamo allora $s(p) = (\varphi^{-1} \circ i_P)(p)$: si ha $\varphi(s(p)) = i_P(p)$ e quindi

$$p = \pi_P(i_P(p)) = \pi_P(\varphi(s(p))) = \beta(s(p))\,.$$

$2 \Rightarrow 1$. Per ogni $n \in N$ scriviamo $n = (n - \alpha(r(n))) + \alpha(r(n))$ e notiamo che $r(n - \alpha(r(n))) = r(n) - (r \circ \alpha)(r(n)) = 0$. Si ha allora che $N = \operatorname{Ker} r + \operatorname{Im} \alpha$ e la somma è diretta. Infatti, se $u \in \operatorname{Ker} r \cap \operatorname{Im} \alpha$, allora $u = \alpha(m)$, per qualche $m \in M$; inoltre, dato che $r \circ \alpha = \mathrm{id}_M$ e $u \in \operatorname{Ker} r$, si ottiene che $0 = r(u) = r(\alpha(m)) = m$ e quindi $u = 0$. Dato che $\operatorname{Im} \alpha = \operatorname{Ker} \beta$, si ha che $\beta_{|\operatorname{Ker} r}$ è un isomorfismo: dunque $\operatorname{Im} \alpha \simeq M$, poiché α è iniettiva, e $\operatorname{Ker} r \simeq \operatorname{Im} \beta = P$. L'isomorfismo φ è definito da

$$\varphi(n) = (r(\alpha(r(n))), \beta(n - \alpha(r(n)))) = (r(n), \beta(n))\ .$$

Le verifiche sulla commutatività del diagramma sono immediate

$$\varphi(\alpha(m)) = (r(\alpha(m)), \beta(\alpha(m)) = (m, 0) = i_M(m)$$

e

$$\pi_P(\varphi(n)) = \pi_P(r(n), \beta(n)) = \beta(n)\ .$$

$3 \Rightarrow 1$. È analoga alla precedente: per ogni $n \in N$ consideriamo $n = (n - s(\beta(n))) + s(\beta(n))$. Poiché $n - s(\beta(n)) \in \operatorname{Ker} \beta = \operatorname{Im} \alpha$ e $\operatorname{Im} \alpha \cap \operatorname{Im} s = 0$, otteniamo che $N = \operatorname{Im} \alpha \oplus \operatorname{Im} s \simeq M \oplus P$.

Dalla dimostrazione segue immediatamente che se la successione di partenza spezza, anche la successione $0 \longrightarrow P \xrightarrow{s} N \xrightarrow{r} M \longrightarrow 0$ è esatta.

4.6.3 Lemma del serpente

Concludiamo questa sezione con un risultato di grande utilità, noto come *Lemma del serpente*.

T. 103. [**Lemma del serpente**] Dato il seguente diagramma commutativo di A-moduli con successioni orizzontali esatte

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

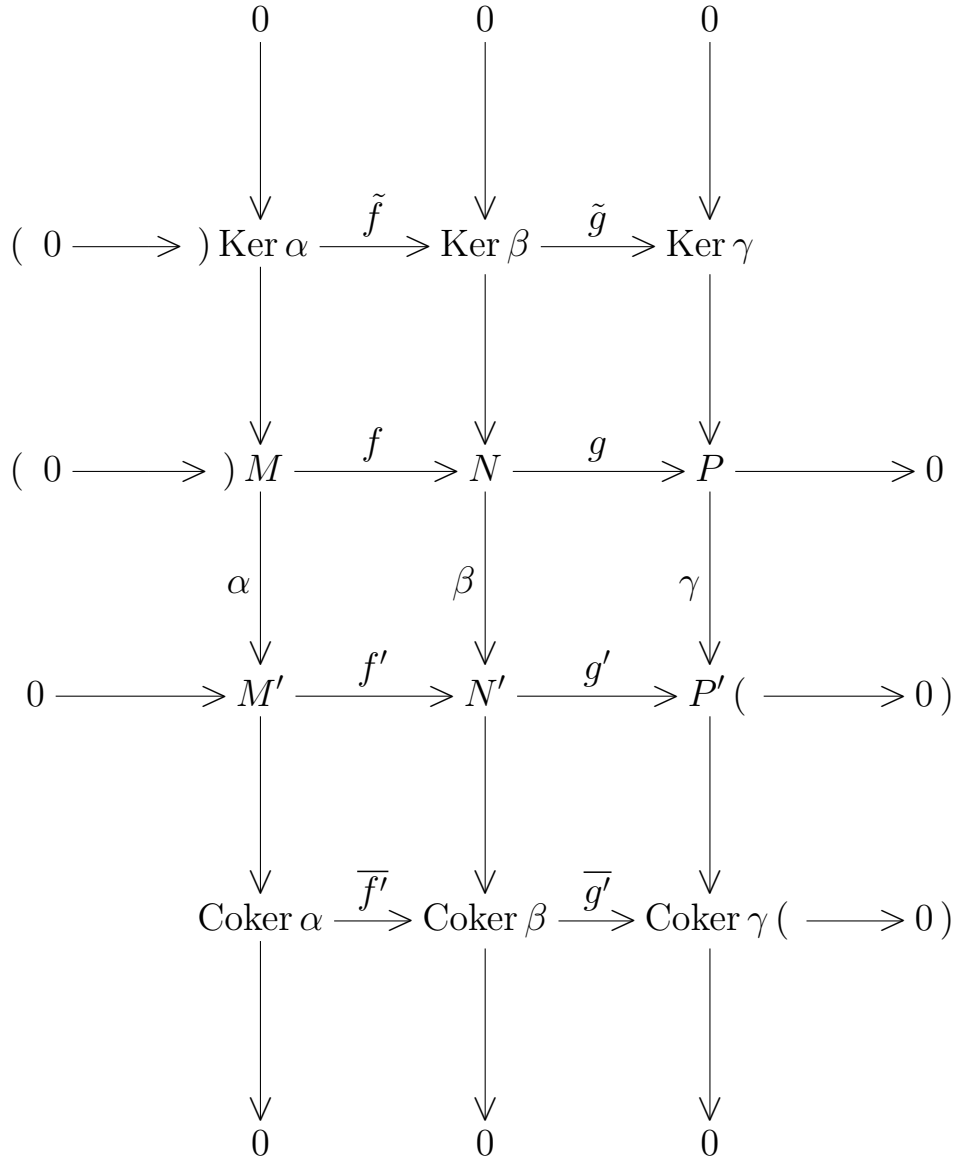
esiste una successione esatta

$$\operatorname{Ker}\alpha \xrightarrow{\tilde{f}} \operatorname{Ker}\beta \xrightarrow{\tilde{g}} \operatorname{Ker}\gamma \xrightarrow{\delta} \operatorname{Coker}\alpha \xrightarrow{\overline{f'}} \operatorname{Coker}\beta \xrightarrow{\overline{g'}} \operatorname{Coker}\gamma \ .$$

Inoltre, se f è iniettivo anche $\tilde{f}$ è iniettivo e se g' è surgettivo anche $\overline{g'}$ lo è.

L'omomorfismo δ viene detto *omomorfismo connettivo*.

Dimostrazione T. 103 Consideriamo il seguente diagramma



in cui i quadrati centrali commutano per ipotesi e le colonne sono successioni esatte per costruzione.

In primo luogo studiamo la buona definizione degli altri omomorfismi. Le mappe $\tilde{f}$ e $\tilde{g}$ sono definite come le restrizioni $f|_{\operatorname{Ker} f}$ e $g|_{\operatorname{Ker} g}$: $\tilde{f}$ è ben definito dato che, se $m \in \operatorname{Ker} \alpha$, allora $\beta(f(m)) = f'(\alpha(m)) = 0$, ossia $f(m) \in \operatorname{Ker} \beta$. La verifica del fatto che $\tilde{g}$ sia ben definito è analoga.

Gli omomorfismi $\overline{f'}$ e $\overline{g'}$ sono dati da $\overline{f'}(\overline{m}) = \overline{f'(m)}$ e $\overline{g'}(\overline{n}) = \overline{g'(n)}$; allora $\overline{f'}$ è ben definito dato che, se $\overline{m} = \overline{m'} \in \operatorname{Coker} \alpha$ avremo che $m - m' = \alpha(a)$ e dunque $f'(m - m') = f'(\alpha(a)) = \beta(f(a)) \in \operatorname{Im} \beta$, da cui discende che

$\overline{f'(m)} = \overline{f'(m')} \in \operatorname{Coker}\beta$. La verifica del fatto che $\overline{g'}$ sia ben definito è simile.

La costruzione dell'omomorfismo δ è centrale nella dimostrazione. Vogliamo definire un omomorfismo

$$\delta\colon \operatorname{Ker}\gamma \longrightarrow \operatorname{Coker}\alpha;$$

la sua definizione, come la dimostrazione delle altre parti essenziali dell'enunciato, avviene secondo la strategia del *diagram chasing*, ovvero della caccia nel diagramma nel modo seguente.

Sia $p \in \operatorname{Ker}\gamma \subset P$ e sia $n \in N$ tale che $g(n) = p$; un tale n esiste poiché g è surgettivo. Dato che $0 = \gamma(g(n)) = g'(\beta(n))$, si ha che $\beta(n) \in \operatorname{Ker} g' = \operatorname{Im} f'$ e quindi esiste un unico $m \in M'$ tale che $f'(m) = \beta(n)$, poiché f' è iniettivo. Definiamo dunque

$$\delta(p) = \overline{m} \in \operatorname{Coker}\alpha.$$

Per accertarci che δ sia ben definito dobbiamo provare che, se $n' \in N$ è tale che $g(n') = p$ e $m' \in M'$ è l'elemento tale che $f'(m') = \beta(n')$, allora $\overline{m} = \overline{m'} \in \operatorname{Coker}\alpha$, i.e. $m - m' \in \operatorname{Im}\alpha$. Abbiamo che $n - n' \in \operatorname{Ker} g = \operatorname{Im} f$, quindi esiste $b \in M$ tale che $f(b) = n - n'$, cosicché $f'(m - m') = \beta(n - n') = \beta(f(b)) = f'(\alpha(b))$. Dato che f' è iniettivo, $m - m' = \alpha(b)$, come volevamo. È immediato vedere che δ è un omomorfismo.

Possiamo ora verificare l'esattezza della successione della tesi.

$\boxed{\text{In } \operatorname{Ker}\beta}$ Chiaramente, $\tilde{g} \circ \tilde{f} = 0$ dato che $g \circ f = 0$, e dunque $\operatorname{Im}\tilde{f} \subseteq \operatorname{Ker}\tilde{g}$.

Sia $n \in \operatorname{Ker}\beta$ un elemento tale che $\tilde{g}(n) = 0$; allora $g(n) = 0$ e quindi $n \in \operatorname{Ker} g = \operatorname{Im} f$ ed esiste pertanto $m \in M$ tale che $f(m) = n$. Dobbiamo provare che tale $m \in \operatorname{Ker}\alpha$. Dato che $f'(\alpha(m)) = \beta(f(m)) = \beta(n) = 0$, ciò segue dall'iniettività di f'.

$\boxed{\text{In } \operatorname{Ker}\gamma}$ Sia $n \in \operatorname{Ker}\beta$. Vogliamo verificare che $\delta(\tilde{g}(n)) = 0$; dato che $\beta(n) = 0$ avremo che $\beta(n) = f'(0)$ e quindi $\delta(\tilde{g}(n))$ è nullo, per definizione di δ. Abbiamo ottenuto in questo modo che $\delta \circ \tilde{g} = 0$.

Per l'inclusione opposta, sia $p \in \operatorname{Ker}\delta$. Scrivendo $p = g(n)$, per un certo $n \in N$, si ha che $\beta(n) = f'(m)$ con $m \in \operatorname{Im}\alpha$. Sia allora $u \in M$ tale che $\alpha(u) = m$; avremo che $\beta(f(u)) = f'(\alpha(u)) = \beta(n)$ e quindi $f(u) - n \in \operatorname{Ker}\beta$.

Infine, $\tilde{g}(n - f(u)) = g(n) - g(f(u)) = g(n) = p$, ossia abbiamo verificato che, se $p \in \operatorname{Ker}\delta$ allora $p \in \operatorname{Im}\tilde{g}$.

In $\operatorname{Coker}\alpha$ Sia $p \in \operatorname{Ker}\gamma$. Scrivendo $p = g(n)$ e $\beta(n) = f'(m)$ si ha che $\delta(p) = \overline{m} \in \operatorname{Coker}\alpha$; abbiamo allora che $\overline{f'}(\delta(p)) = \overline{f'(m)} = 0 \in \operatorname{Coker}\beta$, dato che $f'(m) \in \operatorname{Im}\beta$, quindi $\operatorname{Im}\delta \subseteq \operatorname{Ker}\overline{f'}$.

Sia ora $\overline{m} \in \operatorname{Ker}\overline{f'}$; allora $f'(m) \in \operatorname{Im}\beta$. Siano $n \in N$ tale che $f'(m) = \beta(n)$ e $p = g(n)$. Allora, $\gamma(g(n)) = g'(\beta(n)) = g'(f'(m)) = 0$, quindi $p \in \operatorname{Ker}\gamma$ e di conseguenza, per definizione di δ, $\delta(p) = \overline{m}$, ovvero $\overline{m} \in \operatorname{Im}\delta$, come volevamo.

In $\operatorname{Coker}\beta$ Certamente $\overline{g'} \circ \overline{f'} = 0$, i.e. $\operatorname{Im}\overline{f'} \subseteq \operatorname{Ker}\overline{g'}$.

Sia ora $\overline{n'} \in \operatorname{Ker}\overline{g'} \subseteq \operatorname{Coker}\beta$; allora $g'(n') \in \operatorname{Im}\gamma$ ed esiste $p \in P$ tale che $g'(n') = \gamma(p)$. Sia $n \in N$ tale che $g(n) = p$ e consideriamo l'elemento $n' - \beta(n)$. Avremo dunque che $g'(n' - \beta(n)) = g'(n') - g'(\beta(n)) = g'(n') - \gamma(g(n)) = \gamma(p) - \gamma(p) = 0$; pertanto $n' - \beta(n) \in \operatorname{Ker}g' = \operatorname{Im}f'$ ed esiste $m' \in M'$ tale che $f'(m') = n' - \beta(n)$. Otteniamo allora che $\overline{n'} = \overline{n' - \beta(n)} = \overline{f'(m')} = \overline{f'}(\overline{m'})$, e anche l'altra inclusione è ora provata.

Inoltre, se f è iniettivo l'esattezza

in $\operatorname{Ker}\tilde{f}$ discende subito dal fatto che $\tilde{f}$ è una restrizione di f.

Infine, se g' è surgettivo l'esattezza

in $\operatorname{Coker}\gamma$ segue dal fatto che per ogni $\overline{p} \in \operatorname{Coker}\gamma$ esiste $n' \in N'$ tale che $g'(n') = p$: dunque $\overline{p} = \overline{g'}(\overline{n})$ e anche $\overline{g'}$ è surgettivo.

T. 104. Dato il seguente diagramma commutativo di A-moduli con righe esatte

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

se due qualunque degli omomorfismi α, β, γ sono isomorfismi, allora anche il terzo è un isomorfismo.

***Dimostrazione T.** 104* Supponiamo che α, β siano isomorfismi, e dunque che $\operatorname{Ker}\alpha = \operatorname{Ker}\beta = \operatorname{Coker}\alpha = \operatorname{Coker}\beta = 0$; dal lemma del serpente otteniamo allora la successione esatta $0 \longrightarrow 0 \longrightarrow 0 \longrightarrow \operatorname{Ker}\gamma \longrightarrow 0 \longrightarrow 0 \longrightarrow \operatorname{Coker}\gamma \longrightarrow 0$, e pertanto $\operatorname{Ker}\gamma = \operatorname{Coker}\gamma = 0$, i.e. γ è un isomorfismo. La verifica degli altri due casi è del tutto simile.

4.7 Moduli proiettivi

Abbiamo già visto in **T.**100 che per ogni successione esatta $0 \longrightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ e per ogni A-modulo N, sono esatte a sinistra anche le successioni

$$0 \longrightarrow \operatorname{Hom}_A(M_2, N) \xrightarrow{g^*} \operatorname{Hom}_A(M, N) \xrightarrow{f^*} \operatorname{Hom}_A(M_1, N)$$

$$0 \longrightarrow \operatorname{Hom}_A(N, M_1) \xrightarrow{f_*} \operatorname{Hom}_A(N, M) \xrightarrow{g_*} \operatorname{Hom}_A(N, M_2)$$

mentre in generale queste successioni non sono esatte a destra. Consideriamo per esempio la successione esatta di $\mathbb{Z}$-moduli

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\mu_n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/(n) \longrightarrow 0,$$

dove $\mu_n(m) = nm$ è la moltiplicazione per n e π è la proiezione canonica. Fissiamo lo $\mathbb{Z}$-modulo $N = \mathbb{Z}/(n)$ e applichiamo i funtori $\operatorname{Hom}_{\mathbb{Z}}(\bullet, N)$ e $\operatorname{Hom}_{\mathbb{Z}}(N, \bullet)$. Risultano definite le due successioni

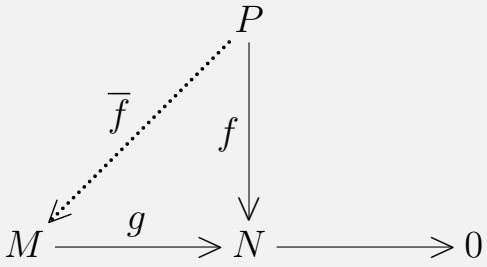
$$0 \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(n)) \xrightarrow{\pi^*} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/(n)) \xrightarrow{\mu_n^*} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/(n))$$

$$0 \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}) \xrightarrow{\mu_{n*}} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}) \xrightarrow{\pi_*} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(n))$$

rispettivamente. Per ogni $g \in \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/(n))$ vale $\mu_n^*(g)(m) = g \circ \mu_n(m) = g(nm) = ng(m) = 0$ per ogni $m \in \mathbb{Z}$: quindi $\mu_n^* = 0$ non è surgettiva, poiché per **T.**86 $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/(n)) \simeq \mathbb{Z}/(n) \neq 0$. Inoltre, π_* certamente non è surgettiva, dato che $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}) = 0$.
Per caratterizzare i moduli M per cui il funtore $\operatorname{Hom}_A(M, \bullet)$ è esatto anche a destra, introduciamo la seguente definizione.

Moduli proiettivi

Un A-modulo P si dice *proiettivo* se, per ogni coppia di A-moduli M, N ed omomorfismi $g : M \longrightarrow N$ e $f : P \longrightarrow N$, con g surgettivo, esiste un omomorfismo $\overline{f} : P \longrightarrow M$ che fa commutare il diagramma

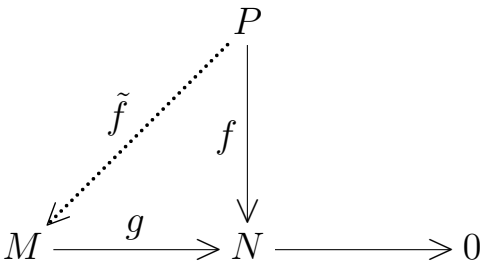


$$\boxed{g \circ \overline{f} = f.}$$

Osserviamo che il modulo nullo è un modulo proiettivo.

T. 105. Ogni modulo libero è proiettivo.

Dimostrazione T. 105 Sia P un A-modulo libero e sia $\mathcal{B}$ una sua base. Consideriamo il seguente diagramma



con g surgettiva. Allora per ogni $b \in \mathcal{B} \subseteq P$ esiste $m_b \in M$ tale che $g(m_b) = f(b)$. Definiamo $\tilde{f}$ sugli elementi di $\mathcal{B}$, ponendo $\tilde{f}(b) = m_b$ per ogni $b \in \mathcal{B}$. Da **T.**91 otteniamo che $\tilde{f}$ si estende in maniera unica ad un omomorfismo $\overline{f}$ tale che $g \circ \overline{f} = f$: dunque P è proiettivo.

T. 106. [Caratterizzazione dei moduli proiettivi] Sia P un A-modulo. I seguenti fatti sono equivalenti:

1. P è proiettivo.
2. Per ogni successione esatta corta di A-moduli

$$0 \longrightarrow N_1 \xrightarrow{f} N \xrightarrow{g} N_2 \longrightarrow 0$$

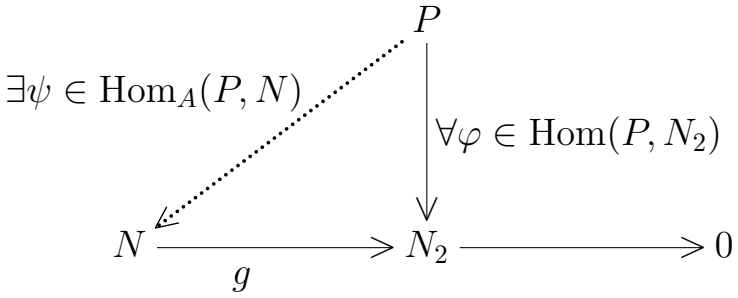
la successione

$$0 \longrightarrow \mathrm{Hom}_A(P, N_1) \xrightarrow{f_*} \mathrm{Hom}_A(P, N) \xrightarrow{g_*} \mathrm{Hom}_A(P, N_2) \longrightarrow 0$$

è esatta.

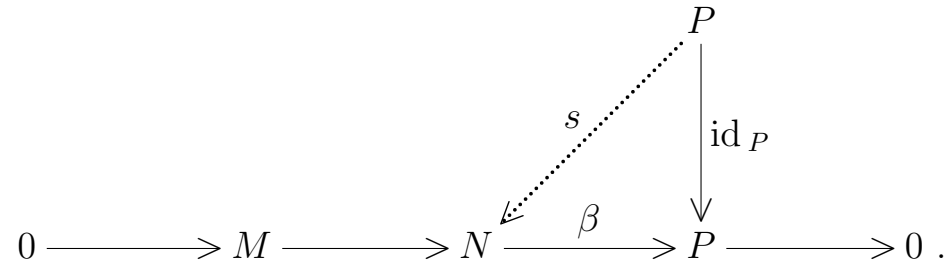
3. Ogni successione esatta $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$ spezza.
4. P è addendo diretto di ogni modulo di cui è quoziente.
5. P è addendo diretto di un modulo libero.

Dimostrazione T. *106* 1 $\Leftrightarrow$ 2. L'equivalenza segue direttamente dalla definizione di modulo proiettivo: dato $g : N \to N_2$ surgettivo



tale che $g_*(\psi) = g \circ \psi = \varphi$.

1 $\Rightarrow$ 3. Consideriamo la successione esatta $0 \longrightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} P \longrightarrow 0$. Poiché P è proiettivo, esiste un omomorfismo s che fa commutare il diagramma

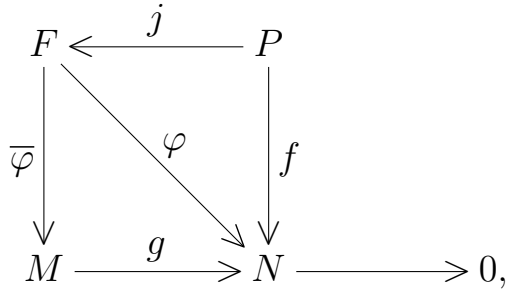


Pertanto $s : P \longrightarrow N$ è una sezione di β, e la successione spezza, cf. **T.**102.

3 $\Rightarrow$ 4. Sia M un modulo di cui P è quoziente; abbiamo allora una successione esatta $0 \longrightarrow \mathrm{Ker}\,\pi \longrightarrow M \xrightarrow{\pi} P \longrightarrow 0$ che per ipotesi spezza, e dunque $M \cong \mathrm{Ker}\,\pi \oplus P$.

4 $\Rightarrow$ 5. Per **T.**92, ogni A-modulo è quoziente di un modulo libero.

$5 \Rightarrow 1$. Siano $f\colon P \longrightarrow N$ e $g\colon M \longrightarrow N$ omomorfismi, con g surgettivo. Vogliamo trovare un omomorfismo $\overline{f}\colon P \longrightarrow M$ tale che $g \circ \overline{f} = f$. Per ipotesi esiste un A-modulo libero F tale che $F = Q \oplus P$; sia dunque $j\colon P \longrightarrow F$ l'omomorfismo di inclusione. Per la proprietà universale della somma diretta **T.**90, considerando l'omomorfismo $f'\colon Q \longrightarrow N$, $f' = 0$, possiamo estendere f ad un unico omomorfismo $\varphi\colon F \longrightarrow N$ tale che $\varphi|_Q = 0$ e $f = \varphi \circ j$. Dato che F è libero, e quindi proiettivo, esiste $\overline{\varphi}\colon F \longrightarrow M$ tale che $\varphi = g \circ \overline{\varphi}$, e quindi abbiamo costruito un diagramma



ove i triangoli commutano. Basta ora definire $\overline{f}$ come $\overline{\varphi} \circ j$.

T. 107. Sia $P = \oplus_{i \in I} P_i$. Allora P è proiettivo se e solo se P_i è proiettivo per ogni $i \in I$.

***Dimostrazione T.** 107* Sia P proiettivo: per **T.**106 esistono A-moduli Q ed F, con F libero, tali che $F = Q \oplus P$. Di conseguenza, per ogni i, $(Q \oplus (\oplus_{j \neq i} P_j)) \oplus P_i = F$, e dunque, per ogni i, P_i è addendo diretto di un modulo libero. Applicando nuovamente **T.**106, abbiamo allora che ogni P_i è proiettivo.

Viceversa, se ogni P_i è proiettivo, esistono A-moduli Q_i tali che $Q_i \oplus P_i$ è libero per ogni i. Detto $Q = \oplus_i Q_i$, si ha allora che $P \oplus Q$ è libero, cioè che P è proiettivo.

Esempio 4.9. Consideriamo l'anello $A = \mathbb{Z}[\sqrt{-6}]$ e gli ideali $I = (2, \sqrt{-6})$ e $J = (3, \sqrt{-6})$. È facile verificare che

- $I + J = A$ e $IJ = (\sqrt{-6}) \simeq A$;

- I e J non sono ideali principali e non sono A-moduli liberi;
- la successione di A-moduli

$$\begin{array}{ccccccccc} 0 & \longrightarrow & IJ & \longrightarrow & I \oplus J & \longrightarrow & A & \longrightarrow & 0 \\ & & a & \longrightarrow & (a, -a) & & & & \\ & & & & (a, b) & \longrightarrow & a + b & & \end{array}$$

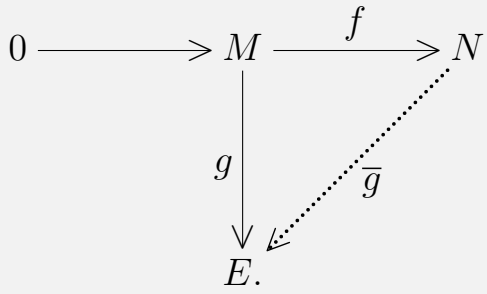
è esatta, cf. **E.**144.

Dato che A è libero e quindi proiettivo, la successione spezza e si ha $I \oplus J \simeq A \oplus IJ \simeq A \oplus A = A^2$. Dunque I e J sono proiettivi come addendi diretti di un modulo libero.

Concludiamo questo paragrafo menzionando solamente che, con lo stesso principio, si introduce la definizione di modulo iniettivo, per caratterizzare quei moduli M per cui $\mathrm{Hom}_A(\bullet, M)$ è esatto, per qualche dettaglio cf. **E.**150, **E.**151 e **E.**152.

Moduli iniettivi

Un A-modulo E si dice *iniettivo* se, per ogni coppia di A-moduli M, N ed omomorfismi $g\colon M \longrightarrow E$ e $f\colon M \longrightarrow N$, con f iniettivo, esiste un omomorfismo $\overline{g} : N \longrightarrow E$ che fa commutare il diagramma



$\boxed{\overline{g} \circ f = g}$

4.8 Moduli su PID

Studiamo ora più nel dettaglio i moduli su un dominio A ad ideali principali. Abbiamo già osservato che in generale se un modulo è libero o finitamente generato i suoi sottomoduli non sono dotati necessariamente di queste proprietà, cf. Osservazione 4.5; diversa è la situazione se A è PID. Ricordiamo che in generale tutte le basi di un modulo libero M sono equipotenti, cf. **T.**89, e tale cardinalità è per definizione $\operatorname{rank} M$.

Proprietà dei sottomoduli

T. 108. Siano A un dominio a ideali principali, M un A-modulo e $0 \neq N \subseteq M$ un sottomodulo di M.

1. Se M è libero, allora N è libero e $\operatorname{rank} N \leq \operatorname{rank} M$.
2. Se M è finitamente generato, allora N è finitamente generato.

Dimostrazione T. 108 1. L'enunciato ha validità generale, ci limitiamo al caso in cui M sia finitamente generato, per il caso generale cf. [L, Appendix 2, §2]. Procediamo dunque per induzione sul rango di M, ovvero sulla cardinalità di una sua base. Se M è ciclico, e dunque $M \simeq A$, i suoi sottomoduli sono isomorfi ad ideali di A. Poiché A è un dominio ad ideali principali e $N \neq 0$, esiste $0 \neq a \in A$ tale che $N \simeq (a)$; inoltre, per ogni $0 \neq c \in A$, $ca = 0$ implica $a = 0$, dato che A è un dominio e quindi N è libero. Inoltre $\operatorname{rank} N = \operatorname{rank} M = 1$.
Supponiamo ora che M abbia rango $r+1$ e assumiamo vera la tesi per tutti i moduli liberi di rango minore o uguale a r. Sia $\{m_1, \dots, m_{r+1}\}$ una base di M. Definiamo $N_r = N \cap \langle m_1, \dots, m_r \rangle$. Ora, se $N = N_r$ allora N è libero di rango $\leq \operatorname{rank}\langle m_1, \dots, m_r \rangle = r < \operatorname{rank} M$, altrimenti si ha $N_r \subsetneq N$ e N_r libero. Ricordando che, per ogni $n \in N$, esistono unici $b_1, \dots, b_r$ e $a_n \in A$, tali che $n = b_1 m_1 + \cdots + b_r m_r + a_n m_{r+1}$, definiamo

$$I = \{a_n \in A \colon n \in N\};$$

I è un ideale di A, dal momento che $a_{n_1} + a_{n_2} = a_{n_1+n_2}$ e $ca_n = a_{cn}$, e $I \neq 0$ perché $N_r \neq N$. Poiché A è PID, esistono allora $0 \neq a \in A$ e $n_0 \in N \setminus N_r$, con $n_0 = b_1 m_1 + \cdots + b_r m_r + a m_{r+1}$ e $I = (a)$. Per concludere dimostriamo che $N \simeq N_r \oplus \langle n_0 \rangle$. Sia $n \in N$, allora $a_n = ka$, per qualche $k \in A$. Di conseguenza, $n - kn_0 \in N_r$ e quindi $n = (n - kn_0) + kn_0 \in N_r + \langle n_0 \rangle$. Dato che $m_1, \dots, m_r, n_0$ sono linearmente indipendenti segue anche che $N_r \cap \langle n_0 \rangle = 0$. La conclusione discende dall'ipotesi induttiva, una volta osservato che $\langle n_0 \rangle$ è libero. Infine, avremo anche in questo caso che $\operatorname{rank} N = \operatorname{rank} N_r + 1 \leq r + 1 = \operatorname{rank} M$.

2. Dato un insieme di generatori di M formato da r elementi, possiamo definire un'omomorfismo $A^r \xrightarrow{f} M \longrightarrow 0$ surgettivo, per cui risulta che $f^{-1}(N)$ è un sottomodulo di A^r, e dunque è libero e finitamente generato. Di conseguenza, N è finitamente generato.

T. 109. Sia M un A-modulo, con A PID; allora M è proiettivo se e solo se è libero.

Dimostrazione T. 109 Supponiamo che M sia proiettivo; allora è addendo diretto di un modulo libero, cf. **T.**106, ed è dunque isomorfo ad un sottomodulo di un modulo libero, che è libero per **T.**108; quindi M è libero. Il viceversa è sempre vero, cf. **T.**105.

Vogliamo nel seguito presentare una dimostrazione costruttiva del teorema di struttura dei moduli finitamente generati su domini ad ideali principali. Prima di introdurre alcuni fatti sulle matrici a coefficienti in un PID e la forma normale di Smith, iniziamo con la seguente osservazione.
Indichiamo con $\mathcal{C}_n = \left\{e_1^{(n)}, \ldots, e_n^{(n)}\right\}$ la base canonica del modulo A^n. Sia $M = \langle m_1, \ldots, m_r\rangle$ un A-modulo finitamente generato; come abbiamo visto M è isomorfo ad un quoziente di A^r, tramite l'omomorfismo $f : A^r \longrightarrow M$ definito da $f(e_i^{(r)}) = m_i$. Abbiamo inoltre la successione esatta

$$0 \longrightarrow \operatorname{Ker} f \longrightarrow A^r \xrightarrow{f} M \longrightarrow 0;$$

dato che $\operatorname{Ker} f \subseteq A^r$, è anche esso libero, di rango $s \leq r$, per **T.**108.1; fissata allora una sua base $w_1, \ldots, w_s$, possiamo definire un omomorfismo $\varphi\colon A^s \longrightarrow A^r$, ponendo $\varphi(e_i^{(s)}) = w_i$. In questo modo, $\operatorname{Ker} f \simeq \operatorname{Im}\varphi$, da cui segue che

$$M \simeq A^r / \operatorname{Ker} f \simeq \operatorname{Coker}\varphi.$$

Inoltre, fissate delle basi di A^s e A^r possiamo rappresentare l'omomorfismo φ con una matrice X di taglia $r \times s$.

Scelte le basi canoniche $\mathcal{C}_s$ e $\mathcal{C}_r$, otteniamo una matrice $X = (x_{ij})$ *le cui colonne generano le relazioni fra i generatori di* M; in altri termini, $(a_1, \ldots, a_r) \in A^r$ è tale che $a_1 m_1 + \ldots + a_r m_r = 0$, i.e. $(a_1, \ldots, a_r) \in \operatorname{Ker} f$

$$\Updownarrow$$

esiste $u \in A^s$ tale che $Xu^{\mathrm{t}} = (a_1, \ldots, a_r)^{\mathrm{t}}$, i.e. $(a_1, \ldots, a_r)^t \in \operatorname{Im} \varphi$,

ove $^{\mathrm{t}}$ denota l'usuale trasposizione di vettori.

Questo spiega perché, al fine di studiare gli A-moduli finitamente generati, possiamo passare attraverso lo studio delle matrici a coefficienti in A.

4.8.1 La forma normale di Smith

Sia X una matrice $r \times s$ a coefficienti in un dominio a ideali principali A. Come già visto nel corso di Algebra Lineare, su X possiamo eseguire le seguenti *operazioni elementari di riga*: scambiare due righe, sommare ad una riga un multiplo non nullo di un'altra riga, moltiplicare una riga per un elemento *invertibile* di A. Analogamente possiamo operare sulle colonne. Ognuna di queste operazioni si ottiene moltiplicando - a sinistra se lavoriamo sulle righe, a destra se lavoriamo sulle colonne - la matrice data per le *matrici elementari* corrispondenti, ovvero quelle ottenute eseguendo sulla matrice identica la corrispondente operazione elementare.
Diciamo che due matrici $X, Y \in M_{rs}(A)$ sono *equivalenti* se esistono matrici $R \in M_r(A)$ e $S \in M_s(A)$ invertibili - ovvero con $\det R, \det S \in A^*$ - tali che $Y = RXS$; è facile verificare che in questo modo si introduce effettivamente una relazione d'equivalenza su $M_{rs}(A)$. Diciamo che una matrice, non necessariamente quadrata, $D = (d_{ij}) \in M_{rs}$ è *diagonale* se $d_{ij} = 0$, per $i \neq j$.

Data una matrice X a coefficienti in A, consideriamo gli ideali

$$\Delta_i(X) = (\det X_i \colon X_i \text{ sottomatrice } i \times i \text{ di } X) \subseteq A.$$

T. 110. Siano X e Y matrici equivalenti; allora $\Delta_i(X) = \Delta_i(Y)$ per ogni i.

Dimostrazione T. 110 Ci basta dimostrare che, data una una matrice invertibile R, $\Delta_i(RX) = \Delta_i(X)$. Infatti da ciò seguirà anche che $\Delta_i(XS) =$

$\Delta_i((XS)^{\mathrm{t}}) = \Delta_i(S^{\mathrm{t}}X^{\mathrm{t}}) = \Delta_i(X^{\mathrm{t}}) = \Delta_i(X)$, e di conseguenza la tesi. Iniziamo osservando che le righe di RX sono combinazioni lineari delle righe di X e quindi, per la multilinearità del determinante, i determinanti delle sottomatrici $i \times i$ di RX sono combinazione lineare dei determinanti delle sottomatrici $i \times i$ di X. Di conseguenza, $\Delta_i(RX) \subseteq \Delta_i(X)$. D'altronde R è invertibile e dunque vale anche $\Delta_i(RX) \supseteq \Delta_i(R^{-1}RX) = \Delta_i(X)$, come volevamo.

T. 111. Sia A un dominio ad ideali principali. Allora ogni matrice a coefficienti in A è equivalente ad una matrice diagonale.

Dimostrazione T. 111 Consideriamo una matrice $X = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ ad entrate in A, con a, b non entrambi nulli, e indichiamo con $0 \neq x = \gcd(a, b)$ il loro massimo comune divisore; allora esistono $s, t \in A$ tali che $sa + tb = x$. Consideriamo la matrice $R = \begin{pmatrix} s & t \\ -bx^{-1} & ax^{-1} \end{pmatrix}$, che ha determinante 1, ed è dunque invertibile; moltiplicando a sinistra per R otteniamo

$$RX = \begin{pmatrix} s & t \\ -bx^{-1} & ax^{-1} \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} x & * \\ 0 & * \end{pmatrix},$$

che è triangolare superiore e il cui primo elemento diverso da zero nella prima colonna è proprio il massimo comune divisore degli elementi della prima colonna di X.
Osserviamo anche che moltiplicando R^{t} a destra di X^t, che ha gli elementi a, b nella prima riga, otteniamo similmente una matrice triangolare inferiore

$$X^{\mathrm{t}}R^{\mathrm{t}} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} s & -bx^{-1} \\ t & ax^{-1} \end{pmatrix} = \begin{pmatrix} x & 0 \\ * & * \end{pmatrix}$$

in cui il primo elemento diverso da zero della prima riga è uguale al massimo comune divisore degli elementi della prima riga di X^t.
Sia ora X una matrice $r \times s$. Consideriamo la prima colonna di X. Se è nulla passiamo alla seconda colonna, altrimenti eventualmente con scambi di

righe, ossia moltiplicando a sinistra per opportune matrici elementari, possiamo applicare la costruzione precedente alle prime due righe e colonne di X, trovare una matrice $R = \left(\begin{array}{c|c} R_2 & 0 \\ \hline 0 & I_{r-2} \end{array}\right)$ tale che $RX = \left(\begin{array}{cc|c} x & * & * \\ 0 & * & \\ \hline * & & * \end{array}\right)$.
Ripetendo questo passo con tutte le matrici 2×2 ottenibili con le prime due colonne di X, otteniamo una matrice equivalente ad X con una prima colonna nulla eccetto per l'elemento x_1 di posto $(1,1)$ che è il massimo comun divisore degli elementi della prima colonna di X. Nello stesso modo, moltiplicando a destra la matrice ottenuta per opportune matrici invertibili si può sostituire x_1 con un elemento x_2 che è il massimo comun divisore di tutti gli elementi sulla prima riga e azzerare tutti gli altri elementi della prima riga. In questo modo però possono ricomparire elementi diversi da zero nella prima colonna e quindi si deve ripetere il procedimento sulla prima colonna. Con successive applicazioni di questo metodo si costruisce, al posto $(1,1)$, una successione elementi $x_1, x_2, \ldots, x_i, \ldots$, che sono alternativamente il massimo comun divisore degli elementi della prima colonna e il massimo comun divisore degli elementi della prima riga, e quindi tali che $x_{i+1} | \, x_i$. Dal momento che A è PID, da questo segue che esiste n tale che $x_n = x_{n+1}$, cf. **T.**25, ma questo dice che x_n è il massimo comun divisore sia degli elementi della prima colonna che della prima riga, e quindi si possono azzerare tutti gli altri elementi sia della prima riga che della prima colonna con operazioni elementari. Iterando il procedimento sulla matrice ottenuta cancellando la prima riga e la prima colonna si ottiene che la matrice può essere diagonalizzata.

La forma normale di Smith

Sia A un dominio ad ideali principali. Una matrice $D = (d_{ij}) \in M_{rs}(A)$ è *in forma (normale) di Smith* se

- D è diagonale;
- $d_{11} \mid d_{22} \mid \cdots \mid d_{tt}$, ove $t = \min\{r, s\}$.

Osserviamo che è possibile che $d_{jj} = 0$ per $t \geq j > k$ per qualche indice k.

T. 112. Ogni matrice X a coefficienti in A è equivalente ad una matrice in forma di Smith.

Dimostrazione T. 112 Grazie a **T.**111, possiamo assumere che $X = (x_{ij})$ sia in forma diagonale. Se la matrice non è in forma di Smith, siano i il minimo indice tale che esiste $j > i$ con $x_{ii} \nmid x_{jj}$ e supponiamo che j sia minimo con questa proprietà; a meno di scambi di riga e colonna, possiamo supporre senza perdita di generalità che $i = 1$ e $j = 2$.
Siano allora $x = \gcd(x_{11}, x_{22})$ e $s, t \in A$ tali che $sx_{11}+tx_{22} = x$ e consideriamo le matrici

$$R = \left(\begin{array}{cc|c} s & t & \\ -x_{22}x^{-1} & x_{11}x^{-1} & 0 \\ \hline 0 & & I_{r-2} \end{array}\right), \quad S = \left(\begin{array}{cc|c} 1 & -tx_{22}x^{-1} & \\ 1 & sx_{11}x^{-1} & 0 \\ \hline 0 & & I_{s-2} \end{array}\right).$$

La matrice prodotto $RXS = (y_{ij})$ è ancora diagonale, con $y_{jj} = x_{jj}$ se $j > 2$, $y_{11} = x$ e $y_{22} = x_{11}x_{22}x^{-1}$, quindi tale che $y_{11}|y_{22}$. A meno di ulteriori scambi di riga e colonna otteniamo una matrice diagonale (z_{ij}), dove $z_{hh} = x_{hh}$ per $h \neq i, j$, $z_{ii} = y_{11}$ e $z_{jj} = y_{22}$, tale che, per ogni $1 \leq h \leq i-1$, $z_{hh} \mid z_{h+\ell,h+\ell}$ per ogni $\ell > 0$ e $z_{ii} \mid z_{hh}$ per ogni $i < h \leq j$. Iterando il procedimento si ottiene la tesi.

T. 113. Sia X una matrice equivalente ad una matrice $D = (d_{ij})$ in forma di Smith; allora

1. $\Delta_1(X) = (d_{11})$;
2. $\Delta_i(X) = (d_{ii})\Delta_{i-1}(X)$ per ogni $i > 1$.

Quindi, se $\Delta_i(X) = (\delta_i)$, possiamo prendere $d_{11} = \delta_1$, $d_{ii} = \delta_i/\delta_{i-1}$, per ogni $i > 1$ tale che $\delta_{i-1} \neq 0$. In particolare, gli elementi d_{ii} sono unici solo a meno di elementi invertibili in A. In questo senso possiamo dire che la forma della matrice X è *essenzialmente* unica, e diciamo che D è la forma di Smith di X; chiamiamo gli elementi d_{ii} *fattori invarianti* di X. Da quanto detto sopra segue dunque che due matrici sono equivalenti se e solo se gli elementi corrispondenti nelle rispettive forme di Smith sono associati.

***Dimostrazione T.** 113* Per **T.** 110, abbiamo che $\Delta_i(X) = \Delta_i(D) = (d_{11} \cdots d_{ii})$, ove la seconda uguaglianza è dovuta al fatto che D è diagonale e alle relazioni di divisibilità $d_{11}|d_{22}| \cdots |d_{tt}$ tra i d_{ii}. Dunque $\Delta_1(D) = (d_{11}) = \Delta_1(X)$. Inoltre $\Delta_i(X) = \Delta_i(D) = (d_{ii})\Delta_{i-1}(X)$, per ogni $1 < i \leq t$.

Osservazione 4.10. Ricordiamo che le operazioni elementari consentite, descritte all'inizio della sezione, non alterano i $\Delta_i(X)$; se si procede al calcolo dei $\Delta_i(X)$ tramite l'eliminazione di Gauss si deve quindi prestare attenzione ad usare solo quelle. Per esempio $\begin{pmatrix} 2 & 4 \\ 3 & 8 \end{pmatrix}$ si riduce a $\begin{pmatrix} 2 & 0 \\ 3 & 2 \end{pmatrix}$, sottraendo alla seconda colonna 2 volte la prima, ma non a $\begin{pmatrix} 2 & 4 \\ 0 & 2 \end{pmatrix}$ che si otterrebbe sottraendo alla seconda riga $\frac{3}{2}$ volte la prima, e nemmeno a $\begin{pmatrix} 2 & 4 \\ 0 & 4 \end{pmatrix}$, sottraendo al doppio della seconda riga 3 volte la prima.

4.8.2 Il teorema di struttura per moduli finitamente generati

Dall'esistenza della forma normale di Smith e dalle sue proprietà discende una classificazione dei moduli finitamente generati su domini ad ideali principali. Fissiamo dapprima la seguente notazione. Dato $N = \langle w_1, \ldots, w_s \rangle$ un sottomodulo di un modulo $L = \langle l_1, \ldots, l_r \rangle$, esistono elementi $x_{ij} \in A$ tali che $w_h = \sum_{k=1}^{r} x_{kh} l_k$, per ogni $h = 1, \ldots, s$. Se $X = (x_{ij})$ è la matrice $r \times s$ formata con gli elementi x_{ij}, possiamo scrivere queste relazioni usando la notazione matriciale $(w_1, \ldots, w_s) = (l_1, \ldots, l_r)X$.

T. 114. Siano L un A-modulo libero di rango r e $0 \neq N \subseteq L$ un sottomodulo; allora esistono una base $\{v_1, \ldots, v_r\}$ di L e scalari $d_1, \ldots, d_s \in A$, con $s \leq r$, tali che $\{d_1 v_1, \ldots, d_s v_s\}$ è una base di N.

***Dimostrazione T.** 114* Siano $l_1, \ldots, l_r$ una base di L e $w_1, \ldots, w_s$ una base di N, che è sottomodulo di un modulo libero e quindi libero, per **T.**108.1, di rango $s \leq r$; allora esiste X matrice $r \times s$ a coefficienti in A tale che $(w_1, \ldots, w_s) = (l_1, \ldots, l_r)X$. Per quanto provato prima, cf. **T.**112, X è equivalente ad una matrice in forma di Smith D e quindi esistono

matrici invertibili R e S di taglia $r \times r$ e $s \times s$ rispettivamente tali che $RXS = D$. Siano $d_1, \dots, d_k$ gli elementi non nulli della diagonale di D. Otteniamo allora che $(w_1, \dots, w_s)S = (l_1, \dots, l_r)XS = (l_1, \dots, l_r)R^{-1}D$. Ponendo $(v_1, \dots, v_r) = (l_1, \dots, l_r)R^{-1}$, otteniamo che $\{v_1, \dots, v_r\}$ è una base di L. Inoltre, $(w_1, \dots, w_s)S = (v_1, \dots, v_r)D = (d_1v_1, \dots, d_kv_k, 0, \dots, 0)$, con $k \leq s$. Dal momento che anche S è invertibile, segue che $k = s$ e $\{d_1v_1, \dots, d_sv_s\}$ è una base di N.

Nella dimostrazione precedente si osserva che i coefficienti d_i sono le entrate diagonali di un'opportuna matrice in forma di Smith. Inoltre notiamo che $dv_i \in N$ se e solo se $d_i | d$, dunque $(d_i) = N : \langle v_i \rangle$ per ogni $i = 1, \dots, s$, cf. anche **T.**115, ed è banalmente vera per $i > s$.

T. 115. Con le stesse notazioni di **T.**114,

1. $L/N \simeq \langle \overline{v_1} \rangle \oplus \dots \oplus \langle \overline{v_r} \rangle$.
2. $L/N \simeq A/(d_1) \oplus \dots \oplus A/(d_s) \oplus A^{r-s}$.

Dimostrazione T. *115* 1. Certamente $\overline{v_1}, \dots, \overline{v_r}$ generano L/N; proviamo allora che la somma è diretta. Per qualche $i = 1, \dots, r$, sia $a\overline{v_i} \in \sum_{j \neq i} \langle \overline{v_j} \rangle$, con $a \in A$; allora $a\overline{v_i} = \sum_{j \neq i} a_j \overline{v_j}$ da cui segue che $av_i - \sum_{i \neq j} a_j v_j \in N$. Esistono quindi $b_1, \dots, b_s \in A$ tali che $av_i - \sum_{j \neq i} a_j v_j = \sum_{k=1}^{s} b_k d_k v_k$, da cui segue che $a = 0$ se $i > s$ e $a = b_i d_i$ se $i \leq s$. In ogni caso $a\overline{v}_i = 0$ e quindi la somma è diretta.

2. Osserviamo che l'assegnazione $1 \mapsto \overline{v_i}$ induce un omomorfismo surgettivo $A \longrightarrow \langle \overline{v_i} \rangle$ il cui nucleo è $\operatorname{Ann} \overline{v_i} = 0 : \langle \overline{v_i} \rangle$. Sia allora $a\overline{v_i} = 0$: se $i \leq s$ questo accade se e solo se $av_i = \sum_{j=1}^{s} b_j d_j v_j$, cioè se e solo se $a \in (d_i)$, mentre se $i > s$ ciò è vero se e solo se $a = 0$. Quindi $\langle \overline{v_i} \rangle \simeq A/\operatorname{Ann} \overline{v_i}$ che a sua volta è isomorfo a $A/(d_i)$ se $i \leq s$ e ad A se $i > s$. La conclusione segue ora dal punto 1.

Teorema di struttura / I

T. 116. Sia A un PID e $M = \langle m_1, \dots, m_r \rangle$ un A-modulo finitamente generato; allora esistono ideali principali $I_1 \supseteq I_2 \supseteq \dots \supseteq I_r$ tali che

$$M \simeq \bigoplus_{i=1}^{r} {}^{A}\!/_{I_i}.$$

Dimostrazione T. *116* Siano $M = \langle m_1, \ldots, m_r \rangle$ e $f : A^r \longrightarrow M$ l'omomorfismo definito da $f(e_i) = m_i$. Dal momento che $\operatorname{Ker} f$ è libero, diciamo di rango s, esistono una base $v_1, \ldots, v_r$ di A^r e costanti $d_1, \ldots, d_s$ tali che $\{d_1 v_1, \ldots, d_s v_s\}$ è una base di $\operatorname{Ker} f$. La tesi segue immediatamente dal corollario precedente, dato che $M \simeq A^r / \operatorname{Ker} f$ e gli ideali $I_i = (d_i) = 0$: $f(v_i)$ verificano le relazioni di contenimento poiché $d_1 | d_2 | \cdots | d_s$ e $I_{s+1} = \ldots = I_r = 0$.

È importante osservare che, per quanto visto in precedenza, ogni matrice a coefficienti in A è equivalente ad una matrice in forma normale di Smith, che è essenzialmente unica; è chiaro allora che, scegliendo un'altra base $w'_1, \ldots, w'_s$ del modulo delle relazioni $\operatorname{Ker} f$ la rappresentazione di M come somma diretta di moduli ciclici rimane la stessa. Non è evidente a priori però cosa sarebbe successo se fossimo partiti da un altro insieme di generatori $\{n_1, \ldots, n_{r'}\}$ di $M = \langle m_1, \ldots, m_r \rangle$. Il seguente risultato chiarisce la situazione.

T. 117. Sia A un anello e siano $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_r$ e $J_1 \supseteq J_2 \supseteq \cdots \supseteq J_{r'}$ ideali di A, con $r \leq r'$, e supponiamo che

$$M \simeq \bigoplus_{i=1}^{r} {}^{A}\!/_{I_i} \simeq \bigoplus_{h=1}^{r'} {}^{A}\!/_{J_h}.$$

Allora

1. $J_1 = J_2 = \cdots = J_{r'-r} = A$;
2. $J_{r'-r+i} = I_i$, per ogni $i = 1, \ldots, r$.

Dimostrazione T. *117* 1. Supponiamo $r < r'$, consideriamo $B = {}^{A}\!/_{J_1}$ e dimostriamo che $B = 0$. Notiamo subito che, per ipotesi, $J_1 + J_h = J_1$ per ogni $h > 1$, e quindi da **E.**116 segue che

$$B^{r'} \simeq \bigoplus_{h=1}^{r'} {}^{A}\!/_{J_1} \simeq \bigoplus_{h=1}^{r'} {}^{A}\!/_{(J_1 + J_h)} \simeq {}^{M}\!/_{J_1 M} \simeq \bigoplus_{i=1}^{r} {}^{A}\!/_{(J_1 + I_i)}.$$

Proiettando B^r su $\bigoplus_{i=1}^{r} {}^{A}\!/_{(J_1 + I_i)}$ otteniamo dunque per composizione un omomorfismo surgettivo da B^r in $B^{r'}$; dato che $r < r'$ questo implica che $B = 0$, cf. **E.**118. Iterando il ragionamento otteniamo similmente che $J_2 = \cdots = J_{r'-r} = A$.

2. Per il punto precedente, possiamo supporre che $r = r'$ e, per simmetria, ci basta dimostrare che $I_h \subseteq J_h$, per ogni $h = 1, \ldots, r$. Sia allora $a \in I_h$; da **E.**117 discende che

$$aM \simeq a \left(\bigoplus_{i=1}^{r} {}^{A}\!/_{I_i} \right) \simeq \bigoplus_{i=1}^{r} {}^{A}\!/_{(I_i : a)}.$$

Poiché $I_i \subseteq I_{i-1}$, abbiamo anche che $a \in I_i$ per ogni $i \leq h$ e quindi $I_i : a = A$ per tali i. Di conseguenza avremo che

$$\bigoplus_{i=h+1}^{r} {}^{A}\!/_{(I_i : a)} \simeq aM \simeq a \left(\bigoplus_{i=1}^{r} {}^{A}\!/_{J_i} \right) \simeq \bigoplus_{i=1}^{r} {}^{A}\!/_{(J_i : a)}.$$

Dal punto 1 discende allora che $J_i : a = A$ per ogni $i \leq h$ e dunque che $a \in J_h$.

Per concludere questa parte vogliamo arrivare ad una seconda formulazione del teorema di struttura. In primo luogo introduciamo la seguente definizione.

Sottomodulo di torsione

Dati un dominio A e un A-modulo M il *sottomodulo di torsione* $T(M)$ *di* M è definito come l'insieme

$$T(M) = \{m \in M \ : \ am = 0 \text{ per qualche } a \in A \setminus \{0\}\};$$

i suoi elementi si dicono *di torsione*. Si dice infine che M è un modulo *di torsione* se $M = T(M)$ e che M *è libero da torsione* se $T(M) = 0$.

T. 118. Siano A un dominio a ideali principali e M un A-modulo finitamente generato. Allora,

1. il sottomodulo di torsione $T(M)$ di M è finitamente generato;
2. $M \simeq T(M) \oplus A^k$, per qualche $k \geq 0$;
3. $0 : T(M) \neq 0$.

Dimostrazione T. 118 1. È un caso particolare di **T.**108.2.

2. Dal teorema di struttura **T.**116, sappiamo che esistono ideali principali $I_1 = (d_1) \supseteq I_2 = (d_2) \supseteq \cdots \supseteq I_r = (d_r)$ tali che $M \simeq \bigoplus_{i=1}^{r} {}^{A}\!/_{I_i}$. Se $I_i = 0$ per ogni i, allora $M \simeq A^r$ e $T(M) = 0$. Altrimenti, sia s tale che $I_h \neq 0$ per $h \leq s$ e $I_i = 0$ per $i > s$; allora ci basta osservare che $T(M) = \bigoplus_{i=1}^{s} {}^{A}\!/_{I_i}$ e $M \simeq T(M) \oplus A^k$, con $k = r - s$.

3. Abbiamo osservato sopra che $T(M) = \bigoplus_{i=1}^{s} {}^{A}\!/_{I_i}$; allora segue subito che $0 : T(M) = I_s = (d_s)$, e tanto basta per concludere.

Il risultato precedente mostra come ogni modulo M finitamente generato su un dominio ad ideali principali A si possa decomporre come somma diretta della sua parte libera e della sua parte di torsione. Per decomporre ulteriormente M introduciamo la seguente definizione.
Dati un A-modulo M e $p \in A$ definiamo la *p-componente* di M come

$$M_p = \{m \in M : \ p^k m = 0 \text{ per qualche } k \in \mathbb{N}\} = \bigcup_{k \in \mathbb{N}} 0 :_M p^k .$$

Questa risulta essere un sottomodulo di M, cf. **E.**154.

Nel caso in cui p sia un elemento primo e $M = M_p$ allora M si dice *p-primario* .

Teorema di struttura / II

Sia A un dominio ad ideali principali.

T. 119. Siano $p \in A$ un elemento primo e M un A-modulo p-primario finitamente generato. Allora

$$M \simeq {}^{A}\!/_{(p^{k_1})} \oplus {}^{A}\!/_{(p^{k_2})} \oplus \cdots \oplus {}^{A}\!/_{(p^{k_s})},$$

per certi $k_1 \leq k_2 \leq \ldots \leq k_s$.

T. 120. Sia M un A-modulo finitamente generato. Allora,

$$M \simeq \bigoplus_{i=1}^{h} {}^{A}\!/_{(q_i)} \oplus A^k$$

con $(q_i) \subset A$ ideali primari per ogni i e h, k interi positivi o nulli.
Inoltre, l'insieme degli ideali primari che compaiono nella decomposizione è unico, la decomposizione è unica a meno dell'ordine degli addendi, e un ideale può comparire più di una volta. Gli elementi q_i sono unici a meno di associati e si chiamano i *divisori elementari* di M.

Dimostrazione T. 119 Osserviamo innanzitutto che in un PID gli ideali primari sono potenze di elementi primi, cf. **E.**57.
Per il teorema di struttura **T.** 116 esistono ideali principali $I_1 = (d_1) \supseteq I_2 = (d_2) \supseteq \cdots \supseteq I_r = (d_r)$ tali che $M \simeq \bigoplus_{i=1}^{r} {}^{A}\!/_{I_i}$. Dato che $M = M_p$ ogni ideale I_i contiene una potenza positiva di p, ma se $p^n \in I_i$ allora $p^n = bd_i$ e da questo si ottiene $I_i = (d_i) = (p^{k_i})$, come volevamo. Le disuguaglianze tra i k_i sono dovute alle inclusioni tra gli ideali I_i.

Dimostrazione T. 120 Per il teorema di struttura **T.**116 esistono ideali principali $I_1 = (d_1) \supseteq I_2 = (d_2) \supseteq \cdots \supseteq I_r = (d_r)$ tali che $M \simeq \bigoplus_{i=1}^{r} {}^{A}\!/_{I_i}$. Siano $d_1, \ldots, d_s \neq 0$ e $d_i = \prod_{j=1}^{h_i} p_{ij}^{e_{ij}}$ la decomposizione di d_i come prodotto di primi distinti, per $i = 1, \ldots, s$. Avremo che $M \simeq \bigoplus_{i=1}^{s} {}^{A}\!/_{I_i} \oplus A^{r-s}$; inoltre, per il teorema cinese del resto, si ha che ${}^{A}\!/_{I_i} \simeq \bigoplus_{j=1}^{h_i} {}^{A}\!/_{(p_{ij}^{e_{ij}})}$ e quindi

$$M \simeq \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{h_i} {}^{A}\!/_{(p_{ij}^{e_{ij}})} \oplus A^{r-s},$$

ove gli ideali $(p_{ij}^{e_{ij}})$ sono gli ideali primari cercati.

Osservazione 4.11. Osserviamo che se $M \simeq \operatorname{Coker} \varphi$ è un A-modulo generato da r elementi e φ è rappresentato da una matrice X di taglia $r \times r'$,

allora il rango della parte libera di M coincide con il numero delle righe di zeri della forma di Smith di X, cf. anche **T.**115.

4.9 Approfondimento: la forma canonica razionale e la forma di Jordan

Possiamo applicare i risultati della sezione precedente ai gruppi abeliani, ossia agli $\mathbb{Z}$-moduli, finitamente generati ottenendo così ben noti teoremi di classificazione. In questa ultima parte vediamo una ulteriore applicazione della teoria al caso degli spazi vettoriali.

Sia $V \neq 0$ un K-spazio vettoriale di dimensione finita n e sia $\varphi \in \mathrm{End}_K(V)$ un endomorfismo di V. Definiamo su V una struttura di $K[x]$-modulo tramite φ in questo modo: dati $p(x) = \sum_{i=0}^{t} a_i x^i$ e $v \in V$ poniamo

$$p(x)v = \sum_{i=0}^{t} a_i \varphi^i(v),$$

cf. la dimostrazione di **T.**98.
Nel seguito considereremo fissato l'endomorfismo φ e la struttura di $K[x]$-modulo su V appena introdotta; dato un sottoinsieme $W \subseteq V$ denoteremo con $\langle W \rangle$ il $K[x]$-sottomodulo di V da esso generato.

T. 121. Con le stesse notazioni, valgono i seguenti fatti.

1. L'annullatore $\mathrm{Ann}\, V = 0 :_{K[x]} V$ di V è un ideale proprio e non nullo di $K[x]$; il suo generatore monico viene detto *il polinomio minimo* di φ.
2. Per ogni $0 \neq v \in V$, $\mathrm{Ann}\langle v \rangle$ è un ideale proprio e non nullo di $K[x]$.
3. Una qualsiasi base $\mathcal{B}$ di un sottospazio vettoriale W di V è un insieme di generatori di $\langle W \rangle$, ma non è mai una base di $\langle W \rangle$.
4. Dato un $K[x]$-sottomodulo $W \subseteq V$, W è un sottospazio vettoriale φ-*invariante* di V, ossia tale che $\varphi(W) \subseteq W$. Visto che φ è fissato, diremo semplicemente invariante.
5. Siano $0 \neq v \in V$, $f_v(x)$ il generatore monico di $\mathrm{Ann}\langle v \rangle$ e d il suo grado; allora la dimensione di $\langle v \rangle$ come K-spazio vettoriale è d e $\{v, \varphi(v), \ldots, \varphi^{d-1}(v)\}$ è una sua base. Inoltre $\langle v \rangle$ è il più piccolo sottospazio invariante di V che contiene v.

***Dimostrazione T.** 121* 1. Dato che $f(x)v = 0$ se e solo se $f(\varphi)(v) = 0$, si ha $f(x) \in \operatorname{Ann} V$ se e solo se $f(\varphi)$ è l'endomorfismo nullo. Dal momento che gli n^2+1 vettori $\mathrm{id}_V, \varphi, \dots, \varphi^{n^2} \in \operatorname{End}_K(V)$ sono linearmente dipendenti, possiamo trovare una combinazione K-lineare non banale $\sum_{i=0}^{n^2+1} a_i\varphi^i = 0$; allora il polinomio $0 \neq f(x) = \sum_{i=0}^{n^2+1} a_i x^i \in K[x]$ è tale che $f(\varphi) = 0$ in $\operatorname{End}_K(V)$, i.e. $f(x) \in \operatorname{Ann} V$.

2. Dato che $\langle v \rangle$ è un sottomodulo di V, dal punto 1 segue subito che $0 \neq \operatorname{Ann} V \subseteq \operatorname{Ann}\langle v \rangle \subsetneq K[x]$.

3. La prima affermazione discende dal fatto che, se $a \in K$ e $v \in V$ allora il prodotto av in V come K-spazio vettoriale o come $K[x]$-modulo è lo stesso. Dal momento però che, per il punto 1, V come $K[x]$-modulo è di torsione, certamente V non è libero, e dunque non ammette base.

4. Per ogni $w \in W$ si ha $p(x)w \in W$; in particolare $\varphi(w) = xw \in W$ per ogni $w \in W$, cioè $\varphi(W) \subseteq W$.

5. Osserviamo che, per il punto 2, $d > 0$; inoltre, $\langle v \rangle = \{p(x)v \colon p(x) \in K[x]\}$ è generato da v su $K[x]$ e dunque da $\{\varphi^i(v) \colon i \in \mathbb{N}\}$ su K, visto che per ogni i si ha che $\varphi^i(v) = x^i v$. Dato che $f_v v = 0$ e f_v è monico, possiamo scrivere $\varphi^d(v)$, e dunque anche $\varphi^{d+h}(v)$ per ogni $h \in \mathbb{N}$, come combinazione K-lineare di $v, \varphi(v), \dots, \varphi^{d-1}(v)$. Abbiamo quindi dimostrato che ogni elemento di $\langle v \rangle$ si può scrivere come combinazione K-lineare di $v, \varphi(v), \dots, \varphi^{d-1}(v)$, ovvero $v, \varphi(v), \dots, \varphi^{d-1}(v)$ generano $\langle v \rangle$ come K-spazio vettoriale.
Se per assurdo esistesse una combinazione K-lineare non banale $\sum_{i=0}^{d-1} a_i\varphi^i(v)$ uguale a 0, avremmo un polinomio non nullo $f(x) = \sum_{i=0}^{d-1} a_i x^i \in \operatorname{Ann}\langle v \rangle = (f_v(x))$ di grado minore di d, che non è possibile.

Il sottospazio $\langle v \rangle$ è invariante, come visto nel punto precedente; inoltre, dato un altro sottospazio W invariante che contiene v, induttivamente avremo che $\varphi^i(v) \subseteq \varphi^i(W) \subseteq \varphi(W) \subseteq W$ per ogni i, cioè $\langle v \rangle \subseteq W$.

Dal momento che $K[x]$ è PID, il $K[x]$-modulo finitamente generato V che, come osservato nella dimostrazione di **T.**121.3, è di torsione, si decompone come somma diretta di moduli ciclici

$$V = \langle v_1 \rangle \oplus \cdots \oplus \langle v_s \rangle \simeq K[x]/\operatorname{Ann}\langle v_1 \rangle \oplus \cdots \oplus K[x]/\operatorname{Ann}\langle v_s \rangle,$$

per il teorema di struttura **T.**116.
Consideriamo allora, per ogni $i = 1, \dots, s$, il polinomio monico $f_i = f_{v_i}$ che genera $\mathrm{Ann}\langle v_i \rangle$, cf. **T.**121.5; per ogni i, il grado d_i di f_i è positivo e scriviamo $f_i = \sum_{j=0}^{d_i} a_j^{(i)} x^j$, per certi $a_j^{(i)} \in K$.

La forma canonica razionale

T. 122. Con le notazioni precedenti, sia data una decomposizione $V = \langle v_1 \rangle \oplus \cdots \oplus \langle v_s \rangle$ di V come somma diretta di $K[x]$-moduli ciclici; allora

1. $\{v_1, \varphi(v_1), \dots, \varphi^{d_1-1}(v_1), \dots, v_s, \varphi(v_s), \dots, \varphi^{d_s-1}(v_s)\}$ è una base di V;
2. la matrice M associata a φ rispetto a questa base è una matrice a blocchi,

$$M = \begin{pmatrix} M_{f_1} & 0 & \dots & 0 \\ 0 & M_{f_2} & \dots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \dots & M_{f_s} \end{pmatrix},$$

dove ogni blocco è dato dalla *matrice compagna* di f_i

$$M_{f_i} = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0^{(i)} \\ 1 & 0 & \dots & 0 & -a_1^{(i)} \\ 0 & 1 & \dots & 0 & -a_2^{(i)} \\ \vdots & & \ddots & & \vdots \\ 0 & & \dots & 1 & -a_{d_i-1}^{(i)} \end{pmatrix}.$$

M viene detta *forma canonica razionale* di φ.

***Dimostrazione T.** 122* 1. Per **T.**121.5 ogni insieme $\{v_i, \dots, \varphi^{d_i-1}(v_i)\}$ è una base di $\langle v_i \rangle$ come K-spazio vettoriale. La conclusione segue dal fatto che V è la somma diretta su $K[x]$ e quindi anche su K dei sottospazi $\langle v_1 \rangle, \dots, \langle v_s \rangle$.
2. È una immediata conseguenza del punto precedente.

Ricordiamo che, per il teorema di struttura, i polinomi f_i che definiscono la forma canonica razionale di φ soddisfano la condizione $f_1 \mid f_2 \mid \cdots \mid f_s$.

Esempio 4.12. Sia $V = \mathbb{Q}^4$ e $\varphi \in \mathrm{End}_{\mathbb{Q}}(V)$ l'endomorfismo dato da $\varphi(v) = Av$ dove

$$A = (a_{ij}) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & -2 & 0 \\ -2 & -1 & 2 & 0 \\ -2 & -1 & -2 & 1 \end{pmatrix}.$$

Vogliamo trovare una decomposizione di V come somma diretta di $\mathbb{Q}[x]$-moduli ciclici e determinare la forma canonica razionale di A.

Sia $\mathcal{B} = \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4\}$ la base canonica di V; per **T.**121.3, $\mathcal{B}$ costituisce un insieme di generatori di V come $\mathbb{Q}[x]$-modulo. Sia dunque $f : \mathbb{Q}[x]^4 \longrightarrow V$ definito da $f(p_1, p_2, p_3, p_4) = p_1(x)\mathbf{e}_1 + p_2(x)\mathbf{e}_2 + p_3(x)\mathbf{e}_3 + p_4(x)\mathbf{e}_4$; allora f è un omomorfismo surgettivo e la successione

$$0 \longrightarrow \mathrm{Ker}\, f \longrightarrow \mathbb{Q}[x]^4 \xrightarrow{f} V \longrightarrow 0$$

è esatta. Determiniamo ora il sottomodulo $\mathrm{Ker}\, f$; dato che

$$x\mathbf{e}_1 = \varphi(\mathbf{e}_1) = A\mathbf{e}_1 = \sum_{h=1}^{4} a_{h1}\mathbf{e}_h,$$

si ha

$$f(x - a_{11}, -a_{21}, -a_{31}, -a_{41}) = 0\ .$$

Definendo $\mathbf{r}_1 = (x - a_{11}, -a_{21}, -a_{31}, -a_{41})$ otteniamo quindi un elemento in $\mathrm{Ker}\, f$. Analogamente possiamo definire $\mathbf{r}_2$, $\mathbf{r}_3$ e $\mathbf{r}_4$ tali che il sottomodulo $\langle \mathbf{r}_i : i = 1, \ldots, 4 \rangle$ sia contenuto in $\mathrm{Ker}\, f$.
Adesso sia $\mathbf{p} = (p_1, p_2, p_3, p_4) \in \mathbb{Q}[x]^4$, dividendo per gli $x - a_{ii}$ possiamo scrivere $p_i = h_i(x - a_{ii}) + c_i$ dove, per ogni i, $c_i \in \mathbb{Q}$ e $\deg h_i < \deg p_i$. Dunque

$$\begin{aligned}\begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{pmatrix} &= \begin{pmatrix} h_1(x-a_{11})+c_1 \\ h_2(x-a_{22})+c_2 \\ h_3(x-a_{33})+c_3 \\ h_4(x-a_{44})+c_4 \end{pmatrix} \\ &= h_1\mathbf{r}_1 + h_2\mathbf{r}_2 + h_3\mathbf{r}_3 + h_4\mathbf{r}_4 + \begin{pmatrix} h_2a_{12}+h_3a_{13}+h_4a_{14}+c_1 \\ h_1a_{21}+h_3a_{23}+h_4a_{24}+c_2 \\ h_1a_{31}+h_2a_{32}+h_4a_{34}+c_3 \\ h_1a_{41}+h_2a_{42}+h_3a_{43}+c_4 \end{pmatrix} \\ &= h_1\mathbf{r}_1 + h_2\mathbf{r}_2 + h_3\mathbf{r}_3 + h_4\mathbf{r}_4 + \begin{pmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \end{pmatrix} \quad ,\end{aligned}$$

per certi polinomi $q_1, \ldots, q_4$ tali che $\max_i\{\deg\, q_i\} < \max_i\{\deg\, p_i\}$. Iterando questo procedimento, dato che gli $x - a_{ii}$ sono lineari, possiamo dunque scrivere

$$\begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{pmatrix} = g_1\mathbf{r_1} + g_2\mathbf{r_2} + g_3\mathbf{r_3} + g_4\mathbf{r_4} + \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix}$$

per certi $g_1, \ldots, g_4 \in K[x]$ e $d_1, \ldots, d_4 \in \mathbb{Q}$. Di conseguenza, se $\mathbf{p} = (p_1, p_2, p_3, p_4) \in \operatorname{Ker}\, f$, si ha

$$0 = f(\mathbf{p}) = f(d_1, d_2, d_3, d_4) = d_1\mathbf{e}_1 + d_2\mathbf{e}_2 + d_3\mathbf{e}_3 + d_4\mathbf{e}_4,$$

che implica $d_i = 0$ per ogni i dal momento che $\mathcal{B}$ è una base di V, i.e. $\mathbf{p} \in \langle \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4 \rangle$. Abbiamo dunque dimostrato che $\langle \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4 \rangle = \operatorname{Ker} f$. Per trovare la decomposizione di V è sufficiente ora trovare la forma di Smith della matrice delle relazioni che ha per colonne i vettori $\mathbf{r}_i$, ovvero la matrice $xI - A$, che cambiata di segno è

$$A - xI = \begin{pmatrix} a_{11}-x & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22}-x & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33}-x & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44}-x \end{pmatrix}$$
$$= \begin{pmatrix} 1-x & 0 & 1 & 0 \\ 0 & 1-x & -2 & 0 \\ -2 & -1 & 2-x & 0 \\ -2 & -1 & -2 & 1-x \end{pmatrix}$$

ovvero la *matrice caratteristica* di A.
La sua forma di Smith è la matrice

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x-1 & 0 \\ 0 & 0 & 0 & x^3-4x^2+5x-2 \end{pmatrix},$$

quindi $V \simeq \mathbb{Q}[x]/(x-1) \oplus \mathbb{Q}[x]/(x^3-4x^2+5x-2)$.

La forma canonica razionale M di A è composta da due blocchi, che sono le matrici compagne di $f_1 = a_1^{(1)}x - a_0^{(1)} = x-1$ e $f_2 = a_3^{(2)}x^3 - a_2^{(2)}x^2 + a_1^{(2)}x + a_0^{(2)} = x^3 - 4x^2 + 5x - 2$. Avremo pertanto

$$M = \left(\begin{array}{c|c} M_{f_1} & 0 \\ \hline 0 & M_{f_2} \end{array}\right) = \left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & -5 \\ 0 & 0 & 1 & 4 \end{array}\right).$$

Dalla decomposizione $V = \bigoplus_{i=1}^{s} \langle v_i \rangle \simeq \bigoplus_{i=1}^{s} K[x]/(f_i)$ e utilizzando la fattorizzazione unica dei polinomi in $K[x]$, con il teorema cinese del resto possiamo anche scomporre ulteriormente gli addendi come

$$\langle v_i \rangle \simeq K[x]/(f_i) \simeq \bigoplus_{j=1}^{t_i} K[x]/(f_{ij}^{e_{ij}}),$$

dove gli f_{ij} sono i fattori irriducibili distinti di f_i, cf. **E.** 156. Questa scrittura ci riconduce alle componenti f_{ij}-primarie dei $K[x]/(f_i)$, mentre la componente

f_{ij}-primaria di V risulta esserne la somma diretta. Date le relazioni di divisibilità tra gli f_i è ovvio che componenti f_{ij}-primarie non banali compaiano anche nei $K[x]/(f_k)$ successivi, cioè per $k \geq i$.

In particolare, nel caso in cui K sia algebricamente chiuso, possiamo decomporre ogni polinomio $f_i = \prod_{j=1}^{t_i} \left(x - \lambda_j^{(i)}\right)^{e_{ij}}$ come prodotto di potenze di polinomi lineari, con $\lambda_j^{(i)} \in K$ e $\lambda_j^{(i)} \neq \lambda_h^{(i)}$ se $j \neq h$. Dunque e_{ij} è la molteplicità di $\lambda_j^{(i)}$ come radice di f_i. Come ricordato sopra, $\lambda_j^{(i)}$ comparirà in generale come radice degli f_k con $k \geq 1$.

Possiamo quindi scrivere per ogni i

$$\langle v_i \rangle = \langle w_1^{(i)} \rangle \oplus \ldots \oplus \langle w_{t_i}^{(i)} \rangle,$$

dove $\operatorname{Ann} \langle w_j^{(i)} \rangle = \left(x - \lambda_j^{(i)}\right)^{e_{ij}}$ e ottenere una decomposizione di V come somma diretta di $K[x]$-moduli ciclici primari

$$V = \langle w_1^{(1)} \rangle \oplus \ldots \oplus \langle w_{t_1}^{(1)} \rangle \oplus \ldots \oplus \langle w_1^{(s)} \rangle \oplus \ldots \oplus \langle w_{t_s}^{(s)} \rangle .$$

La forma di Jordan

T. 123. Sia K algebricamente chiuso e, come sopra, sia

$$V = \langle w_1^{(1)} \rangle \oplus \ldots \oplus \langle w_{t_1}^{(1)} \rangle \oplus \ldots \oplus \langle w_1^{(s)} \rangle \oplus \ldots \oplus \langle w_{t_s}^{(s)} \rangle .$$

Definiamo $\psi = \bigoplus_{i,j} \psi_{ij}$, con $\psi_{ij} = (\varphi - \lambda_j^{(i)} I)_{|\langle w_j^{(i)} \rangle}$; allora

1. $\Big\{ w_1^{(1)},\ \psi_{11}(w_1^{(1)}),\ \ldots,\ \psi_{11}^{e_{11}-1}(w_1^{(1)}),\ \ldots,\ w_{t_1}^{(1)},\ \psi_{1t_1}(w_{t_1}^{(1)}),\ \ldots,$
   $\psi_{1t_1}^{e_{1t_1}-1}(w_{t_1}^{(1)}),\ \ldots,\ w_1^{(s)},\ \psi_{s1}(w_1^{(s)}),\ \ldots,\ \psi_{s1}^{e_{s1}-1}(w_1^{(s)}),\ \ldots,\ w_{t_s}^{(s)},$
   $\psi_{st_s}(w_{t_s}^{(s)}),\ \ldots,\ \psi_{st_s}^{e_{st_s}-1}(w_{t_s}^{(s)}) \Big\}$ è una base di V;
2. la matrice associata a φ rispetto a tale base è una matrice diagonale a blocchi

$$\begin{pmatrix} J_{\lambda_1^{(1)}} & & & & & & & & \\ & J_{\lambda_2^{(1)}} & & & & & & & \\ & & \ddots & & & & 0 & & \\ & & & J_{\lambda_{t_1}^{(1)}} & & & & & \\ & & & & J_{\lambda_1^{(2)}} & & & & \\ & & & & & \ddots & & & \\ & & & & & & J_{\lambda_{t_{s-1}}^{(s-1)}} & & \\ & & 0 & & & & & J_{\lambda_1^{(s)}} & \\ & & & & & & & & \ddots \\ & & & & & & & & J_{\lambda_{t_s}^{(s)}} \end{pmatrix},$$

ove ogni blocco $J_{\lambda_j^{(i)}}$ è una matrice di Jordan di taglia e_{ij}, della forma

$$J_{\lambda_j^{(i)}} = \begin{pmatrix} \lambda_j^{(i)} & 0 & \dots & & 0 \\ 1 & \lambda_j^{(i)} & 0 & \dots & \vdots \\ 0 & 1 & \lambda_j^{(i)} & 0 & \dots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & 0 & & \dots\ 1 & \lambda_j^{(i)} \end{pmatrix}.$$

Dimostrazione T. *123* Dal momento che V è somma diretta, possiamo limitarci a considerare l'azione di ψ su ognuno dei sottospazi $\langle w_j^{(i)} \rangle$, su cui, per definizione, ψ coincide con $\psi_{ij} = \varphi - \lambda_j^{(i)} I$. Per semplicità di notazione poniamo $w_j^{(i)} = w$, $\lambda_j^{(i)} = \lambda$, $\operatorname{Ann} \langle w \rangle = (x - \lambda)^e$, per cui risulta $\psi = \varphi - \lambda I$ e lo spazio vettoriale che stiamo considerando è $\langle w \rangle \simeq K[x]/(x - \lambda)^e$ che ha dimensione e su K.

1. Da **E.** 121.5 sappiamo che $\{w, \varphi(w), \dots, \varphi^{e-1}(w)\}$ è una base del K-spazio vettoriale $\langle w \rangle$.
Per definizione di ψ si ha che $\varphi^i(w) = (\psi + \lambda I)^i(w) \in \langle w, \psi(w), \dots, \psi^{e-1}(w) \rangle$ e quindi anche $\{w, \psi(w), \dots, \psi^{e-1}(w)\}$ è una base di $\langle w \rangle$.

2. Controlliamo l'azione di φ su $\langle w \rangle$

$$\varphi(\psi^i(w)) = (\psi + \lambda I)(\psi^i(w)) = \begin{cases} \psi^{i+1}(w) + \lambda\psi^i(w) & \text{se } 0 \leq i < e-1 \\ \\ \lambda\psi^{e-1}(w) & \text{se } i = e-1\,, \end{cases}$$

dove l'ultima uguaglianza segue dal fatto che $\psi^e(w) = (x-\lambda)^e w = 0$. Quindi rispetto alla base $\{w, \psi(w), \ldots, \psi^{r-1}(w)\}$ la matrice che rappresenta φ è esattamente

$$J_\lambda = \begin{pmatrix} \lambda & 0 & \ldots & \ldots & 0 \\ 1 & \lambda & 0 & \ldots & 0 \\ 0 & 1 & \lambda & \ldots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 & \lambda \end{pmatrix}.$$

Esempio 4.13. Troviamo la forma di Jordan su $\mathbb{C}$ della matrice A dell'Esempio 4.12. Fattorizziamo i polinomi $x-1$ e $x^3-4x^2+5x-2 = (x-1)^2(x-2)$, e di conseguenza ottieniamo che la forma di Jordan di A è

$$\left(\begin{array}{c|cc|c} 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 2 \end{array}\right).$$

Osserviamo infine che la componente $(x-1)$-primaria è rappresentata dal blocco 3×3 in alto a sinistra, composto a sua volta da due blocchi: uno, di dimensione 1, proveniente da M_{f_1} e uno, di dimensione 2, proveniente da M_{f_2}.

5

Il prodotto tensoriale

Siano A un anello e M, N, P A-moduli.
Diciamo che un'applicazione $f\colon M \times N \longrightarrow P$ è *A-bilineare* se per ogni $m \in M$ la mappa $f_{(m,\cdot)}\colon N \longrightarrow P$, $f_{(m,\cdot)}(n) \mapsto f(m,n)$, e per ogni $n \in N$ la mappa $f_{(\cdot,n)}\colon M \longrightarrow P$, $f_{(\cdot,n)}(m) = f(m,n)$ sono A-lineari, ovvero omomorfismi di A-moduli.
In maniera analoga, dati A-moduli $M_1, \dots, M_k$ e P, un'applicazione $f\colon M_1 \times \cdots \times M_k \longrightarrow P$ si dice *multilineare* se è lineare su ogni componente.
Denotiamo l'insieme di tutte le mappe A-bilineari definite da $M \times N$ in P con $\mathrm{Bil}(M, N; P)$; lo dotiamo di una struttura di A-modulo ponendo, per ogni $f, g \in \mathrm{Bil}(M, N; P)$ e $a \in A$

$$(f+g)(m,n) = f(m,n) + g(m,n) \quad \text{e} \quad (af)(m,n) = af(m,n),$$

per ogni $m \in M, n \in N$, cf. **E.**179.

T. 124. Siano A un anello e M, N, P A-moduli; allora

$$\mathrm{Bil}(M, N; P) \simeq \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)).$$

Dimostrazione T. *124* Sia $\Phi\colon \mathrm{Bil}(M, N; P) \longrightarrow \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$ l'applicazione che ad ogni forma bilineare b associa la mappa $\varphi_b\colon M \longrightarrow \mathrm{Hom}_A(N, P)$ definita da $(\varphi_b(m))(n) = b_{(m,\cdot)}(n) = b(m,n)$. Sia inoltre $\Psi\colon \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)) \longrightarrow \mathrm{Bil}(M, N; P)$ l'applicazione che manda un omomorfismo φ nella mappa bilineare $b_\varphi \in \mathrm{Bil}(M, N; P)$ definita da $b_\varphi(m,n) = \varphi(m)(n)$, per ogni $m \in M$, $n \in N$. Dopo averne verificato la buona definizione, ovvero che φ_b sia un omomorfismo e che b_φ sia bilineare, si verifica

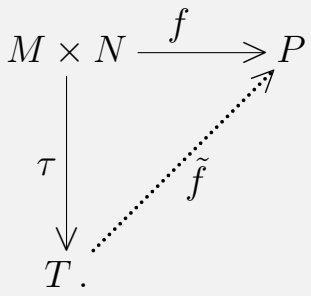
anche che Φ e Ψ sono omomorfismi di A-moduli; la conclusione segue poi dal fatto, facile da vedere, che Φ e Ψ sono uno l'inverso dell'altro.

Il prodotto tensoriale viene definito unicamente attraverso la sua proprietà universale, come segue; si procede poi a dimostrarne l'esistenza e unicità.

Il prodotto tensoriale e la sua proprietà universale

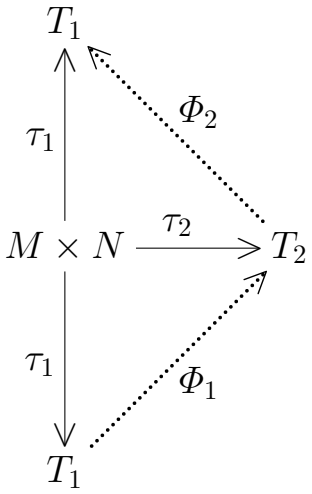
Siano A un anello e M, N due A-moduli. Si definisce *prodotto tensoriale di M e N* la coppia (T, τ), data da un A-modulo T insieme con un'applicazione A-bilineare $\tau\colon M \times N \longrightarrow T$ che verificano la seguente proprietà universale:

per ogni $f \in \mathrm{Bil}(M, N; P)$ esiste un unico omomorfismo $\tilde{f}\colon T \longrightarrow P$ che rende commutativo il diagramma



T. 125. Siano A un anello e M, N due A-moduli; allora il prodotto tensoriale di M ed N esiste ed è unico (a meno di isomorfismi).

Dimostrazione T. 125 Unicità Supponiamo che (T_1, τ_1) e (T_2, τ_2) siano due prodotti tensoriali di M ed N, e consideriamo i seguenti diagrammi



ove gli omomorfismi Φ_1 e Φ_2 sono dati dalle proprietà universali, sono unici e sono tali che $\tau_2 = \Phi_1 \circ \tau_1$ e $\tau_1 = \Phi_2 \circ \tau_2$.
Componendo, troviamo che $\Phi_2 \circ \Phi_1$ è un omomorfismo di T_1 in sé tale che $(\Phi_2 \circ \Phi_1) \circ \tau_1 = \tau_1$; osservando che anche id_{T_1} ha la stessa proprietà, per l'unicità di un tale omomorfismo concludiamo che $\Phi_2 \circ \Phi_1 = \mathrm{id}_{T_1}$. Analogamente, $\Phi_1 \circ \Phi_2 = \mathrm{id}_{T_2}$; possiamo pertanto concludere che $T_1 \simeq T_2$.
Esistenza Consideriamo l'A-modulo libero $F = A^{M \times N}$, la sua base canonica $\mathcal{B} = \{e_{(m,n)} \colon (m,n) \in M \times N\}$ e la mappa

$$\mathrm{i} \colon M \times N \longrightarrow F, \ \ (m,n) \mapsto e_{(m,n)}.$$

Sia

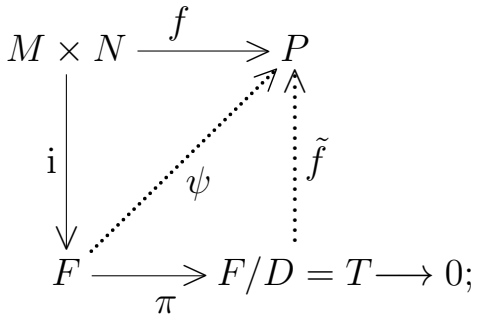
$$\tau = \pi \circ \mathrm{i} \colon M \times N \longrightarrow F \longrightarrow F/D,$$

ove $\pi \colon F \longrightarrow F/D$ è la proiezione canonica e D è il sottomodulo di F generato da tutti gli elementi in F che devono ridursi a 0 per imporre la bilinearità di τ, ovvero

$$\begin{aligned} D \ = \ \langle \ & \mathrm{i}(m_1 + m_2, n) - \mathrm{i}(m_1, n) - \mathrm{i}(m_2, n), \\ & \mathrm{i}(am, n) - a\mathrm{i}(m, n), \\ & \mathrm{i}(m, n_1 + n_2) - \mathrm{i}(m, n_1) - \mathrm{i}(m, n_2) \\ & \mathrm{i}(m, an) - a\mathrm{i}(m, n) \colon m, m_1, m_2 \in M, n, n_1, n_2 \in N, a \in A \rangle. \end{aligned}$$

Per costruzione τ è bilineare. Mostriamo ora che la coppia $(T = F/D, \tau)$ è un prodotto tensoriale di M e N provando che vale la proprietà universale.

Siano P un A-modulo, $f \in \mathrm{Bil}(M, N; P)$ e consideriamo il seguente diagramma



dobbiamo dimostrare che esiste un unico omomorfismo $\tilde{f}$ tale che $\tilde{f} \circ \tau = \tilde{f} \circ \pi \circ \mathrm{i} = f$.

Dato che F è libero esiste un unico omomorfismo ψ che fa commutare il triangolo sinistro, i.e. $f = \psi \circ \mathrm{i}$. Dimostriamo ora che esiste unico $\tilde{f}$ cercato, definendolo in modo tale che $\tilde{f} \circ \pi = \psi$; in questo modo avremo che $\tilde{f} \circ \tau = \tilde{f} \circ \pi \circ \mathrm{i} = \psi \circ \mathrm{i} = f$. Sia dunque

$$\tilde{f} \colon F/D \longrightarrow P, \quad \overline{x} \mapsto \psi(x) \ \text{ per ogni } \ x \in F.$$

Per costruzione avremo che il diagramma commuta, nel momento che saremo sicuri della buona definizione di $\tilde{f}$, ovvero bisogna verificare che $\psi_{|_D} = 0$. Basta verificarlo sui generatori di D: ad esempio, $\psi(\mathrm{i}(m + m', n) - \mathrm{i}(m, n) - \mathrm{i}(m', n)) = \psi \circ \mathrm{i}(m + m', n) - \psi \circ \mathrm{i}(m, n) - \psi \circ \mathrm{i}(m', n) = f(m + m', n) - f(m, n) - f(m', n) = 0$, poiché f è bilineare.

Rimane dunque da mostrare che tale $\tilde{f}$ è unica. Siano dunque $\tilde{f}_1, \tilde{f}_2$ due omomorfismi con la proprietà che $\tilde{f}_1 \circ \pi \circ \mathrm{i} = \tilde{f}_2 \circ \pi \circ \mathrm{i}$. Dunque $\tilde{f}_1 \circ \pi$ e $\tilde{f}_2 \circ \pi$ coincidono sugli elementi della base canonica di F e quindi su tutto F; allora per ogni $x \in F/D$ esiste $y \in F$ tale che $\tilde{f}_1(x) = \tilde{f}_1(\pi(y)) = \tilde{f}_2(\pi(y)) = \tilde{f}_2(x)$, pertanto la dimostrazione è conclusa.

Alla luce di quanto appena visto, il prodotto tensoriale di M ed N esiste sempre ed è unico: lo denotiamo con $M \otimes_A N$, o semplicemente con $M \otimes N$ quando non vi sia ambiguità sull'anello sul quale stiamo lavorando. Denotiamo inoltre con $m \otimes_A n$, o semplicemente $m \otimes n$, l'elemento $\tau(m, n)$. Tali elementi $m \otimes n$, con $m \in M$ e $n \in N$ si dicono *tensori elementari* o monomiali. Un *tensore* è un elemento di $M \otimes N$.

Dalla costruzione di τ discende immediatamente che

per ogni $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, $a \in A$,

$$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n,$$

$$m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2,$$

$$a(m \otimes n) = am \otimes n = m \otimes an.$$

T. 126. Siano A un anello, M, N due A-moduli.

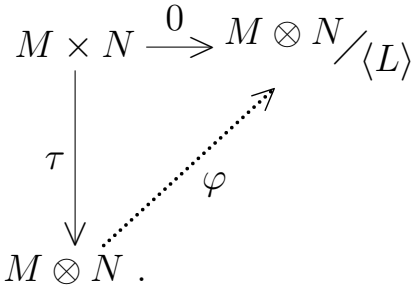
1. $m \otimes 0 = 0 \otimes n = 0$ per ogni $m \in M$, $n \in N$.
2. L'insieme $\{m \otimes n \colon m \in M, n \in N\}$ dei tensori elementari è un insieme di generatori di $M \otimes N$.
3. Se $\mathcal{G}_1$ e $\mathcal{G}_2$ sono insiemi di generatori di M e N rispettivamente, allora l'insieme dei tensori elementari dato da $\mathcal{G}_1 \otimes \mathcal{G}_2 = \{m \otimes n \colon m \in \mathcal{G}_1, n \in \mathcal{G}_2\}$ è un insieme di generatori di $M \otimes N$.
4. Se M e N sono finitamente generati, allora $M \otimes N$ è finitamente generato.

In particolare, da **T.**126.2 segue dunque che un tensore è una combinazione A-lineare finita di tensori elementari.

Dimostrazione T. *126* 1. Basta osservare, ad esempio, che $0 \otimes n = (0 + 0) \otimes n = 0 \otimes n + 0 \otimes n$.

2. Segue direttamente dalla definizione.

3. Dire che L genera $M \otimes N$ equivale a dire che $(M \otimes N)/\langle L \rangle = 0$. Sia $L = \mathcal{G}_1 \otimes \mathcal{G}_2$ e consideriamo il diagramma



Senz'altro $\varphi = 0$ fa commutare il diagramma. Inoltre, sia $(m, n) \in M \times N$, ove $m = \sum_{i=1}^{h} a_i m_i$, $m_i \in \mathcal{G}_1$, $a_i \in A$, $i = 1, \dots, h$, e $n = \sum_{j=1}^{k} b_j n_j$, $n_j \in \mathcal{G}_2$, $b_j \in A$, $j = 1, \dots, k$. Allora, indicando con π la proiezione $M \otimes N \to (M \otimes N)/\langle L \rangle$, si ha

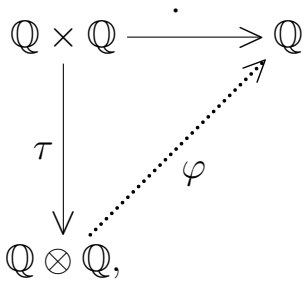
$$\pi(\tau(m,n)) = \pi(m \otimes n) = \pi\left(\sum_{i=i}^{h} a_i m_i \otimes \sum_{j=1}^{h} b_j n_j\right) = \sum_{i,j} a_i b_j \pi(m_i \otimes n_j) = 0,$$

dove abbiamo usato che π è un omomorfismo, $\otimes$ è bilineare e $m_i \in \mathcal{G}_1$, $n_j \in \mathcal{G}_2$. Dunque anche $\varphi = \pi$ fa commutare il diagramma e, per l'unicità nella proprietà universale, $\pi = 0$, cioè $M \otimes N = \langle L \rangle$.

4. Segue immediatamente dal punto precedente.

Esempi 5.1. 1. Mostriamo che $\mathbb{Z}/(5) \otimes_{\mathbb{Z}} \mathbb{Z}/(7) = 0$. Osserviamo che $5(\overline{a} \otimes \overline{b}) = 5\overline{a} \otimes \overline{b} = \overline{5a} \otimes \overline{b} = 0 \otimes \overline{b} = 0$, per **T.**126.1; analogamente $7(\overline{a} \otimes \overline{b}) = 0$. Pertanto, per ogni tensore elementare $m \otimes n$ avremo $m \otimes n = 1(m \otimes n) = (21-20)m \otimes n = 0$. La conclusione segue allora da **T.**126.2.

2. Dimostriamo che $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}$. Consideriamo il diagramma



ove $\cdot(x, y) = xy$ è l'usuale moltiplicazione in $\mathbb{Q}$, che è $\mathbb{Z}$-bilineare. Esiste dunque un unico omomorfismo φ tale che $\cdot = \varphi \circ \tau$, i.e. tale che $\varphi(x \otimes y) = xy$. Vogliamo dimostrare che φ è un isomorfismo. Dato che, per ogni $x \in \mathbb{Q}$, $\varphi(x \otimes 1) = x$, avremo che esso è surgettivo. Osserviamo ora che $L = \{x \otimes 1 \colon x \in \mathbb{Q}\}$ è un insieme di generatori di $\mathbb{Q} \otimes \mathbb{Q}$. A questo scopo, se consideriamo un tensore elementare $m \otimes n$, con $n = a/b$, avremo $m \otimes \frac{a}{b} = \frac{mb}{b} \otimes \frac{a}{b} = \frac{m}{b} \otimes a = \frac{am}{b} \otimes 1$, con $\frac{am}{b} \in \mathbb{Q}$, e l'osservazione è provata. Avremmo potuto concludere che L è un insieme di generatori direttamente da **T.**126.2. Da questo segue che ogni

elemento di $\mathbb{Q} \otimes \mathbb{Q}$, che è combinazione lineare a coefficienti in $\mathbb{Z}$ di tensori elementari, si può scrivere come $x \otimes 1$, per un opportuno $x \in \mathbb{Q}$. Possiamo ora procedere a dimostrare l'iniettività: se $\varphi(x \otimes 1) = 0$ allora $x = 0$ da cui $x \otimes 1 = 0$.

3. Quando si utilizza la proprietà universale e si vuole dimostrare che φ è iniettiva, come nel punto precedente, bisogna procedere con cautela, poiché in generale non è detto che ogni tensore sia un tensore elementare, come si evidenzia nel seguente esempio.

Si consideri $\mathbb{C}$ con la struttura di $\mathbb{R}$-modulo data dalla restrizione di scalari tramite l'omomorfismo di inclusione di anelli $\mathbb{R} \longrightarrow \mathbb{C}$, ovvero si consideri $\mathbb{C}$ dotato della usuale struttura di $\mathbb{R}$-spazio vettoriale: esso è libero con base $\{1, i\}$. Sia dunque $M = N = \mathbb{C}$ e studiamo $M \otimes_{\mathbb{R}} N = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. Un tensore elementare in $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ è dunque del tipo

$$\begin{aligned} x \otimes y =& (a + ib) \otimes (c + id) \\ =& a \otimes c + a \otimes id + ib \otimes c + ib \otimes id \\ =& ac(1 \otimes 1) + ad(1 \otimes i) + bc(i \otimes 1) + bd(i \otimes i), \end{aligned}$$

per certi $a, b, c, d \in \mathbb{R}$. Consideriamo ora l'elemento $1 \otimes 1 + i \otimes i \in \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. Affinché esso sia un tensore elementare deve essere $ac = 1,\ ad = 0,\ bc = 0,\ bd = 1$, che non ha soluzioni in $\mathbb{R}$.

Consideriamo gli A-moduli $M = A[x]$, $N = A[y]$ e il loro prodotto tensoriale $A[x] \otimes_A A[y]$. Mostriamo che esso è isomorfo a $A[x, y]$. Come A-moduli M ed N sono generati rispettivamente da $\{x^i : i \in \mathbb{N}\}$, $\{y^j : j \in \mathbb{N}\}$. Pertanto $M \otimes_A N$ è generato da $\{x^i \otimes y^j : (i, j) \in \mathbb{N}^2\}$. Costruiamo il diagramma

$$\begin{array}{ccc} A[x] \times A[y] & \xrightarrow{\cdot} & A[x, y] \\ \Big\downarrow{\scriptstyle \tau} & \nearrow{\scriptstyle \varphi} & \\ A[x] \otimes_A A[y], & & \end{array}$$

ove $\cdot(x^i, y^j) = x^i y^j$ è l'usuale moltiplicazione in $A[x, y]$, che è A-bilineare, e $\varphi(\sum_{i,j} a_{ij}(x^i \otimes y^j)) = \sum_{i,j} a_{ij} x^i y^j$. Chiaramente φ è surgettiva: dato un

qualsiasi polinomio $p(x,y) = \sum_{i,j} a_{ij} x^i y^j \in A[x,y]$ avremo che $\varphi(\sum_{i,j} a_{ij}(x^i \otimes y^j)) = p$. Se poi $\varphi(\sum_{i,j} a_{ij}(x^i \otimes y^j)) = \sum_{i,j} a_{ij} x^i y^j = 0$, allora $a_{ij} = 0$ per ogni i, j, e dunque φ è anche iniettiva.

È importante osservare che $M \otimes N$ *può essere uguale a zero anche se* $M \neq 0$ *e* $N \neq 0$, come evidenziato dal primo esempio.

Proprietà del prodotto tensoriale

T. 127. Siano A un anello, I un ideale di A, e siano M, N, P A-moduli. Allora

1. $A \otimes M \simeq M$;
2. $M \otimes N \simeq N \otimes M$;
3. $(M \otimes N) \otimes P \simeq M \otimes (N \otimes P) \simeq M \otimes N \otimes P$;
4. $(M \oplus N) \otimes P \simeq (M \otimes P) \oplus (N \otimes P)$;
5. $M \otimes (A/I) \simeq M/IM$;
6. se M e N sono liberi di rango m e n rispettivamente, allora $M \otimes N$ è libero di rango mn.

Osserviamo anche che il prodotto tensoriale e la somma diretta commutano, mentre questo in generale non è vero per il prodotto diretto, cf. **E.**186.

Dimostrazione T. *127* 1. L'applicazione $f\colon A \times M \longrightarrow M$, $f(a,m) = am$ è A-bilineare; per la proprietà universale esiste allora un omomorfismo surgettivo $\tilde{f}\colon A \otimes M \longrightarrow M$ tale che $\tilde{f}(a \otimes m) = am$. Consideriamo l'omomorfismo $g\colon M \longrightarrow A \otimes M$, definito da $g(m) = 1 \otimes m$. Avremo allora che $g \circ \tilde{f}(a \otimes m) = g(am) = 1 \otimes am = a \otimes m$, per ogni tensore elementare $a \otimes m$; quindi $\tilde{f}$ è anche iniettivo ed è l'isomorfismo cercato.

2. L'applicazione $f\colon N \times M \longrightarrow M \otimes N$ definita da $f(n,m) = m \otimes n$ è bilineare e quindi induce un omomorfismo $\tilde{f}\colon N \otimes M \longrightarrow M \otimes N$, tale che $\tilde{f}(n \otimes m) = m \otimes n$. In modo analogo troviamo un omomorfismo $\tilde{g}\colon M \otimes N \longrightarrow N \otimes M$, tale che $\tilde{g}(m \otimes n) = n \otimes m$. Questi due omomorfismi sono uno l'inverso dell'altro e quindi i due moduli sono isomorfi.

3. Sia $m \in M$, l'applicazione

$$f_m : N \times P \longrightarrow (M \otimes N) \otimes P$$

$$f_m(n,p) = (m \otimes n) \otimes p$$

è bilineare e quindi definisce un omomorfismo $\widetilde{f_m} : N \otimes P \longrightarrow (M \otimes N) \otimes P$. Se poi consideriamo l'applicazione

$$g\colon M \times (N \otimes P) \longrightarrow (M \otimes N) \otimes P,$$

definita da $g(m, n \otimes p) = \widetilde{f_m}(n \otimes p) = (m \otimes n) \otimes p$, anch'essa è bilineare e quindi induce un omomorfismo

$$\tilde{g} : M \otimes (N \otimes P) \longrightarrow (M \otimes N) \otimes P.$$

Dal momento che gli elementi del tipo $(m \otimes n) \otimes p$ generano il prodotto tensoriale, questo omomorfismo è unico. In modo analogo si può costruire un unico omomorfismo

$$\tilde{h}\colon (M \otimes N) \otimes P \longrightarrow M \otimes (N \otimes P), \text{ definito da } \tilde{h}((m \otimes n) \otimes p) = m \otimes (n \otimes p),$$

che è l'inverso di $\tilde{g}$, da cui la tesi.
Per l'ultimo isomorfismo rimandiamo a [AM, Proposition 2.14].
4. L'omomorfismo di A moduli

$$f : (M \oplus N) \times P \longrightarrow (M \otimes P) \oplus (N \otimes P)$$

$$f((m,n),p) = (m \otimes p, n \otimes p)$$

è bilineare e quindi induce un unico omomorfismo

$$\tilde{f} : (M \oplus N) \otimes P \longrightarrow (M \otimes P) \oplus (N \otimes P)$$

per provare che $\tilde{f}$ è un isomorfismo costruiamo il suo inverso. A partire dalle applicazioni bilineari

$$g : M \times P \longrightarrow (M \oplus N) \otimes P, \quad g(m,p) \mapsto (m,0) \otimes p;$$

$$h : N \times P \longrightarrow (M \oplus N) \otimes P, \quad h(n,p) \mapsto (0,n) \otimes p,$$

costruiamo gli omomorfismi $\tilde{g}\colon M \otimes P \longrightarrow (M \oplus N) \otimes P$ e $\tilde{h}\colon N \otimes P \longrightarrow (M \oplus N) \otimes P$. Per la proprietà universale della somma diretta otteniamo così un omomorfismo

$$(M \otimes P) \oplus (N \otimes P) \longrightarrow (M \oplus N) \otimes P$$

$$(m \otimes p, n \otimes q) \longmapsto \tilde{g}(m \otimes p) + \tilde{h}(n \otimes q)$$

che è l'inverso di $\tilde{f}$ cercato.

5. L'applicazione $f\colon A/I \times M \longrightarrow M/IM$ tale che $(\overline{a}, m) \longmapsto \overline{am}$ è ben definita e bilineare, ed induce pertanto un omomorfismo $\tilde{f}\colon A/I \otimes M \longrightarrow M/IM$ tale che $\tilde{f}(\overline{a} \otimes m) = \overline{am}$. Consideriamo ora l'omomorfismo $M/IM \longrightarrow A/I \otimes M$ definito da $\overline{m} \longmapsto \overline{1} \otimes m$. Esso è ben definito: se $\overline{m} = \overline{n}$, allora $m - n \in IM$ e dunque $m - n = \sum_i a_i m_i$, per certi $a_i \in I$, $m_i \in M$ in numero finito. Avremo allora che $1 \otimes m - 1 \otimes n = 1 \otimes (m-n) = 1 \otimes \sum_i a_i m_i = \sum_i \overline{a_i} \otimes m_i = 0$. Ora basta verificare che i due omomorfismi sono uno l'inverso dell'altro, sui tensori elementari:

$$\overline{a} \otimes m \mapsto \overline{am} \mapsto \overline{1} \otimes am = \overline{a} \otimes m, \quad \overline{m} \mapsto \overline{1} \otimes m \mapsto \overline{m}.$$

6. La dimostrazione del caso in cui M ed N sono finitamente generati segue immediatamente dai punti precedenti: dimostriamo per induzione su m che, per ogni $n \in \mathbb{N}$ si ha $A^m \otimes A^n \simeq A^{mn}$. Il caso $m = 1$ segue dal punto 1; per il caso generale siano $M \simeq A^m$, $N \simeq A^n$. Allora

$$\begin{aligned} M \otimes N = A^m \otimes A^n &= (A^{m-1} \oplus A) \otimes A^n \\ &\simeq (A^{m-1} \otimes A^n) \oplus (A \otimes A^n) \\ &\simeq A^{(m-1)n} \oplus A^n \simeq A^{mn}. \end{aligned}$$

Per la dimostrazione generale bisogna utilizzare la proprietà universale, cf. **E.**182.

T. 128. Siano A un anello, e M, N, P A-moduli. Allora,

$$\mathrm{Hom}_A(M \otimes_A N, P) \simeq \mathrm{Bil}(M, N; P) \simeq \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)).$$

L'isomorfismo tra $\mathrm{Hom}_A(M \otimes_A N, P)$ e $\mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P))$ viene talvolta chiamato *formula di aggiunzione* Hom-$\otimes$.

***Dimostrazione T.** 128* Abbiamo già dimostrato il secondo isomorfismo in **T.**124. Per ogni $f \in \mathrm{Bil}(M,N;P)$, dalla proprietà universale discende che esiste un unico omomorfismo $\tilde{f}$ tale che $\tilde{f}(m \otimes n) = f(m,n)$. Definiamo dunque $\Phi\colon \mathrm{Bil}(M,N;P) \longrightarrow \mathrm{Hom}_A(M \otimes_A N, P)$ ponendo $\Phi(f) = \tilde{f}$. Sia $\tilde{f} = \Phi(f) = \Phi(g) = \tilde{g}$; allora $f(m,n) = \tilde{f}(m \otimes n) = \tilde{g}(m \otimes n) = g(m,n)$, per ogni $m \in M$, $n \in N$, cioè Φ è iniettiva. La mappa Φ è anche surgettiva: data $f \in \mathrm{Hom}_A(M \otimes_A N, P)$, definiamo $\underline{f}\colon M \times N \longrightarrow P$ ponendo $\underline{f}(m,n) = f(m \otimes n)$. Essa è bilineare e pertanto esiste $\widetilde{\underline{f}}$ tale che $\widetilde{\underline{f}}(m \otimes n) = \underline{f}(m,n) = f(m \otimes n)$, per ogni $m \in M$, $n \in N$. Segue pertanto che $f = \widetilde{\underline{f}} = \Phi(\underline{f})$.

5.1 Il prodotto tensoriale come funtore

Dati $f\colon M \longrightarrow M'$ e $g\colon N \longrightarrow N'$ omomorfismi di A-moduli, si definisce l'omomorfismo

$$f \otimes g\colon M \otimes N \longrightarrow M' \otimes N' \qquad (f \otimes g)(m \otimes n) = f(m) \otimes g(n);$$

esso è ben definito, cf. **E.**184.

In virtù di **E.**185, dato un A-modulo N, possiamo considerare $\bullet \otimes N$ come un funtore covariante dalla categoria degli A-moduli in sé: esso trasforma un A-modulo M in $M \otimes_A N$ e un omomorfismo $f\colon M \longrightarrow M'$ in $f \otimes \mathrm{id}_N\colon M \otimes_A N \longrightarrow M' \otimes_A N$. Lo stesso possiamo fare con $N \otimes \bullet$, anche se in realtà possiamo identificare i due funtori in quanto *equivalenti*, cosa che non definiremo né verificheremo in questa sede. Esso costituisce un esempio di un funtore esatto a destra ma non esatto.

T. 129. [Esattezza a destra di $\bullet \otimes N$]
Sia $M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ una successione esatta. Allora, per ogni A-modulo N, la successione

$$M_1 \otimes N \xrightarrow{f\otimes \mathrm{id}_N} M \otimes N \xrightarrow{g\otimes \mathrm{id}_N} M_2 \otimes N \longrightarrow 0$$

è esatta.

Dimostrazione T. 129 Per **T.**100.1, l'esattezza di $M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ implica quella di

$$\begin{aligned} 0 \longrightarrow \mathrm{Hom}(M_2, \mathrm{Hom}(N, Q)) &\longrightarrow \mathrm{Hom}(M, \mathrm{Hom}(N, Q)) \\ &\longrightarrow \mathrm{Hom}(M_1, \mathrm{Hom}(N, Q)) \end{aligned}$$

per ogni A-modulo Q. Segue allora da **T.**128 l'esattezza della successione

$$0 \longrightarrow \mathrm{Hom}(M_2 \otimes N, Q) \longrightarrow \mathrm{Hom}(M \otimes N, Q) \longrightarrow \mathrm{Hom}(M_1 \otimes N, Q)$$

sempre per ogni Q. Per **T.**101.1, ciò implica l'esattezza di

$$M_1 \otimes N \xrightarrow{f\otimes \mathrm{id}_N} M \otimes N \xrightarrow{g\otimes \mathrm{id}_N} M_2 \otimes N \longrightarrow 0,$$

dopo aver controllato la compatibilità delle mappe che compaiono nelle varie successioni.

Analogamente a quanto visto per i funtori $\mathrm{Hom}_A(M, \bullet)$ e $\mathrm{Hom}_A(\bullet, N)$, cf. **T.**100 e **T.**101, della precedente proposizione vale anche il viceversa.

T. 130. Sia $M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ una successione di A-moduli tale che, per ogni A-modulo N, la successione

$$M_1 \otimes N \xrightarrow{f\otimes \mathrm{id}_N} M \otimes N \xrightarrow{g\otimes \mathrm{id}_N} M_2 \otimes N \longrightarrow 0$$

è esatta; allora $M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ è esatta.

Dimostrazione T. 130 Ponendo $N = A$, la tesi discende subito da **T.**127.1.

Un A-modulo Q tale che $\bullet \otimes_A Q$ trasforma successioni esatte corte in successioni esatte corte si dice *piatto*. Chiaramente non tutti i moduli sono piatti. Per esempio siano $A = \mathbb{Z} = M = N$, $Q = \mathbb{Z}/(2)$ e consideriamo la successione $0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/(2) \longrightarrow 0$, che è esatta corta. Tensorizzando

con Q avremo che $0 \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(2) \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(2)$ non è più esatta, perché l'omomorfismo $2 \otimes \mathrm{id}_{\mathbb{Z}/(2)}$ è nullo, e non può essere iniettiva poiché $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(2) \simeq \mathbb{Z}/(2) \neq 0$.

5.2 Estensione di scalari

Abbiamo visto in precedenza, cf. la restrizione degli scalari nella Sezione 4.1, che se A e B sono anelli e $f\colon A \longrightarrow B$ è un omomorfismo è possibile definire su ogni B-modulo M una struttura di A-modulo via f definendo il prodotto

$$A \times M \longrightarrow M \quad (a, m) \longmapsto f(a)m.$$

Possiamo anche interpretare la restrizione di scalari come un funtore covariante tra la categoria dei B-moduli e quella degli A-moduli: un omomorfismo di B-moduli $u\colon M \longrightarrow N$ induce un omomorfismo $\tilde{u}$ di A-moduli fra le restrizioni di M e N, dato che, presi $m \in M$ e $a \in A$, avremo $\tilde{u}(am) = u(f(a)m) = f(a)u(m) = au(m) = a\tilde{u}(m)$.

Sia $f\colon A \longrightarrow B$ un omomorfismo di anelli. L'anello B è in maniera naturale un modulo su se stesso. Inoltre possiamo considerare su B la sua struttura di A-modulo definita tramite f. Le due operazioni di moltiplicazione per uno scalare commutano, ossia $(ab)b' = (f(a)b)b' = f(a)bb' = a(bb')$ per $b, b' \in B$ e $a \in A$. Si dice pertanto che B è un (A, B)-bimodulo.

Sia ora M un A-modulo. Il prodotto tensoriale $B \otimes_A M = M_B$ ha naturalmente una struttura di A-modulo. Dal momento che B è un B-modulo, su M_B risulta definita anche una struttura di B-modulo, data da

$$B \times M_B \longrightarrow M_B, \quad (b, b' \otimes m) \longmapsto bb' \otimes m.$$

Diremo che la struttura di B-modulo su M_B è definita *per estensione di scalari*. Osserviamo che il modulo M_B ottenuto per estensione di scalari è un (A, B)-bimodulo.

Alcuni esempi classici di estensione di scalari si hanno quando A è un dominio e $B = Q(A)$ è il suo campo dei quozienti oppure quando si considerano due campi $k \subset K$, dove l'estensione di scalari trasforma uno spazio vettoriale su k in uno spazio vettoriale su K.

Analogamente a quanto fatto per la restrizione di scalari, possiamo interpretare l'estensione di scalari come un funtore covariante, questa volta dalla categoria degli A-moduli a quella dei B moduli, dato da $B \otimes_A \bullet$.

Il seguente fatto, che enunciamo senza dimostrazione, risulta essere di grande utilità.

T. 131. Siano A e B anelli, M un A modulo, N un (A, B)-bimodulo e P un B-modulo; allora

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

Osserviamo che su entrambi i moduli $(M \otimes_A N) \otimes_B P$ e $M \otimes_A (N \otimes_B P)$ è definita una struttura di (A, B)-bimodulo. Infatti, l'A-modulo $M \otimes_A N$ ha una struttura di B-modulo, e quindi di (A, B)-bimodulo, ponendo $b(m \otimes n) = m \otimes bn$; analogamente il B-modulo $N \otimes_B P$ ha una struttura di A-modulo, e quindi di (A, B)-bimodulo, ponendo $a\,(n \otimes p) = an \otimes p$.

6

Localizzazione

6.1 Anelli di frazioni

Vogliamo descrivere in questa sezione una costruzione, detta *localizzazione*, che generalizzi la costruzione del campo dei numeri razionali a partire dagli interi e quella del campo dei quozienti di un dominio di integrità. Localizzeremo anelli arbitrari usando come denominatori gli elementi di particolari sottoinsiemi S, i sottoinsiemi moltiplicativi.

Sia A un anello; diciamo che un sottoinsieme $S \subseteq A$ è *moltiplicativamente chiuso* o *moltiplicativo* se $1 \in S$ e $st \in S$ per ogni $s, t \in S$.

T. 132. La relazione

$$(a, s) \sim (b, t) \iff \text{esiste} \quad u \in S \ \text{ tale che } \quad u(at - bs) = 0$$

definisce una relazione di equivalenza su $A \times S$.

Dimostrazione T. 132 La relazione è certamente riflessiva e simmetrica. Proviamo che è transitiva: siano $(a, s) \sim (b, t)$ e $(b, t) \sim (c, r)$. Allora esistono $u, v \in S$ tali che $u(at - bs) = 0$ e $v(br - ct) = 0$, da cui $vru(at - bs) = 0$ e $vus(br - ct) = 0$. Sommando queste relazioni otteniamo $vruat - vusct = 0$, ossia $vut(ar - sc) = 0$, e quindi $(a, s) \sim (c, r)$, dato che $vut \in S$.

Denotiamo $A \times S / \sim$ con $S^{-1}A$; indichiamo inoltre con $\frac{a}{s}$ la classe di equivalenza di un elemento (a, s).

Anello delle frazioni

Siano A un anello e $S \subset A$ un sottoinsieme moltiplicativo di A.

T. 133. L'insieme $S^{-1}A = {}^{A \times S}\!/\!_{\sim}$ dotato delle operazioni di somma e prodotto definite da

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st},$$

con $a, b \in A$ e $s, t \in S$ è un anello commutativo con $0 = \frac{0}{1}$ e $1 = \frac{1}{1}$.

Tale anello viene detto l'*anello delle frazioni di A rispetto a S* o la *localizzazione* di A in S.

L'applicazione $\sigma = \sigma_S \colon A \longrightarrow S^{-1}A$ definita da $\sigma(a) = \frac{a}{1}$ è un omomorfismo di anelli, detto l'*omomorfismo canonico*.

***Dimostrazione T.** 133* È sufficiente dimostrare che le operazioni sono ben definite; l'esistenza dell'elemento neutro per la somma e per il prodotto, l'associatività, la distributività e la commutatività delle operazioni si ricavano direttamente da quelle di A. Supponiamo allora che $\frac{a}{s} = \frac{a'}{s'}$ e $\frac{b}{t} = \frac{b'}{t'}$. Proviamo che $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} = \frac{a't'+b's'}{s't'} = \frac{a'}{s'} + \frac{b'}{t'}$. Per ipotesi, esistono $u, v \in S$ tali che $u(as' - a's) = 0$ e $v(bt' - b't) = 0$. Da questo segue $uvtt'(as' - a's) = 0$ e $uvss'(bt' - b't) = 0$, sommando si ha la relazione cercata. Lo stesso tipo di verifica si effettua per il prodotto.

T. 134. Sia S un sottoinsieme moltiplicativo di A e σ l'omomorfismo canonico. Allora,

1. σ è iniettivo se e solo se $S \cap \mathcal{D}(A) = \emptyset$;
2. $S^{-1}A = 0$ se e solo se $S \cap \mathcal{N}(A) \neq \emptyset$.

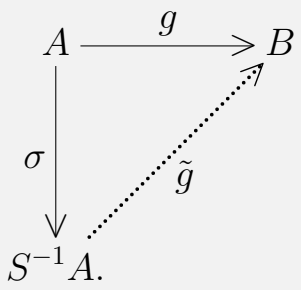
***Dimostrazione T.** 134* 1. Per definizione esiste $a \neq 0$ tale che $\sigma(a) = \frac{a}{1} = 0$ se e solo se esiste $u \in S$ tale che $ua = 0$ ossia se e solo se $u \in S \cap \mathcal{D}(A)$.

2. $S^{-1}A = 0$ se e solo se $\frac{0}{1} = \frac{1}{1}$ ossia, per costruzione, se e solo se $0 \in S$. Quindi, dato che S è moltiplicativo, se e solo se S contiene un elemento nilpotente.

Una fondamentale proprietà della localizzazione $S^{-1}A$ è che ogni omomorfismo g di A in un anello B in cui tutti gli elementi di $g(S)$ sono invertibili, si fattorizza attraverso $S^{-1}A$.

Proprietà universale dell'anello delle frazioni

T. 135. Sia $g\colon A \longrightarrow B$ un omomorfismo di anelli tale che $g(S) \subseteq B^*$; allora esiste un unico omomorfismo di anelli $\tilde{g}\colon S^{-1}A \longrightarrow B$ tale che $\tilde{g} \circ \sigma = g$, ossia tale che il seguente diagramma commuti



Dimostrazione T. 135 Se un tale omomorfismo $\tilde{g}$ esiste, allora per ogni $a \in A$ si deve avere che $\tilde{g}(\frac{a}{1}) = \tilde{g}\sigma(a) = g(a)$; inoltre se $s \in S$, $\tilde{g}(\frac{1}{s}) = \tilde{g}((\frac{s}{1})^{-1}) = \tilde{g}(\frac{s}{1})^{-1} = g(s)^{-1}$. Pertanto

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

Un tale $\tilde{g}$ è dunque determinato da g ed è pertanto unico.
Proviamo allora che $\tilde{g}\colon S^{-1}A \longrightarrow B$ è ben definito. Se questo, come vedremo, è il caso, sarà senz'altro un omomorfismo di anelli poiché g lo è. Siano allora $\frac{a}{s} = \frac{b}{t}$ e $u \in S$ tale che $u(at-bs) = 0$; avremo che $g(u)(g(a)g(t)-g(b)g(s)) = 0$ e, dato che $g(u) \in B^*$, da ciò segue che $\tilde{g}\left(\frac{a}{s}\right) = g(a)g(s)^{-1} = g(b)g(t)^{-1} = \tilde{g}\left(\frac{b}{t}\right)$, come volevamo.

T. 136. Con le notazioni precedenti, supponiamo che:

i. $g(a) = 0$ implica che esiste $s \in S$ tale che $as = 0$;
ii. per ogni $b \in B$ esistono $a \in A$, $s \in S$ tali che $b = g(a)g(s)^{-1}$;

allora $\tilde{g}\colon S^{-1}A \longrightarrow B$ è un isomorfismo.

Dimostrazione ***T.*** *136* Ricordando che $\tilde{g}(\frac{a}{s}) = g(a)g(s)^{-1}$, dalla seconda condizione segue subito la surgettività. La prima condizione implica l'iniettività: infatti se $\tilde{g}(\frac{a}{s}) = 0$, allora $g(a) = 0$ e per ipotesi esiste $t \in S$ tale che $at = 0$; quindi in $S^{-1}A$ avremo $\frac{a}{s} = 0$.

Esistono due casi di particolare importanza nella costruzione di anelli di frazioni. Il primo è quando $S = S_f = \{f^n\}_{n\in\mathbb{N}}$ è costituito dalle potenze di un elemento $f \in A$; in questo caso $S^{-1}A$ si indica con A_f. È chiaro che affinché $A_f \neq 0$ si deve avere che $f \notin \mathcal{N}(A)$.
Il secondo caso è quando si considerano un ideale primo $\mathfrak{p} \in \operatorname{Spec} A$ e l'insieme moltiplicativo $S = A \setminus \mathfrak{p}$ complementare di $\mathfrak{p}$ in A; in questo caso indichiamo $S^{-1}A$ con $A_{\mathfrak{p}}$. Il nome localizzazione viene da questo caso ed è giustificato dal seguente fatto.

T. 137. $A_{\mathfrak{p}}$ è un anello locale con ideale massimale $\mathfrak{p}A_{\mathfrak{p}} = \{\frac{a}{s}\colon a \in \mathfrak{p},\ s \in S\}$.

Dimostrazione ***T.*** *137* Sia $\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$: è un ideale di $A_{\mathfrak{p}}$, infatti dati $\frac{a}{s}, \frac{b}{t} \in \mathfrak{m}$ e $\frac{\alpha}{\beta} \in A_{\mathfrak{p}}$ si ha $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} \in \mathfrak{m}$ e $\frac{\alpha a}{\beta s} \in \mathfrak{m}$.

Inoltre esso è proprio: se $\frac{a}{s} = \frac{1}{1}$ per qualche $a \in \mathfrak{p}$, esisterebbe $u \in A \setminus \mathfrak{p}$ tale che $ua = us \in A \setminus \mathfrak{p}$, che non è possibile.

Infine osserviamo che, se $\frac{a}{s} \notin \mathfrak{m}$, allora $a \in S$ e $\frac{s}{a} \in A_{\mathfrak{p}}$, quindi $\frac{a}{s}$ è invertibile. Pertanto $A_{\mathfrak{p}}$ è locale con ideale massimale $\mathfrak{m}$.

Generalizzando, è immediato verificare che per ogni insieme di primi $\{\mathfrak{p}_h \in \operatorname{Spec} A\colon\ h \in H\}$, $S = A \setminus \bigcup_{h\in H} \mathfrak{p}_h$ è un sistema moltiplicativo.

Ideali estesi e ideali contratti rispetto a σ_S

T. 138. Siano A un anello, S un insieme moltiplicativo e $\sigma = \sigma_S$ l'omomorfismo canonico.

1. Siano $I \subset A$ un ideale e $I^e = (\sigma(I))$ la sua estensione in $S^{-1}A$; allora
   a) $I^e = \left\{\frac{a}{s}\colon a \in I,\ s \in S\right\} = S^{-1}I$;
   b) $S^{-1}I = S^{-1}A$ se e solo se $I \cap S \neq \emptyset$;

c) $I^{ec} = \{a \in A \colon as \in I \text{ per qualche } s \in S\} = \bigcup_{s\in S} I : s$.

2. Siano $J \subset S^{-1}A$ un ideale e $J^c = \sigma^{-1}(J)$ la sua contrazione in A; allora $J = J^{ce}$, i.e. ogni ideale di $S^{-1}A$ è un ideale esteso.

Dimostrazione ***T.*** *138* 1.a) È chiaro che $S^{-1}I \subset I^e$. Viceversa sia $i \in I^e$; allora $i = \sum_{h=1}^{k} \frac{a_h}{s_h}\frac{i_h}{1}$, per certi $\frac{a_1}{s_1}, \dots, \frac{a_k}{s_k} \in S^{-1}A$ e $i_1, \dots, i_k \in I$. Possiamo allora scrivere $i = \frac{\sum_{h=1}^{k} b_h i_h}{s_1 \cdots s_k}$, per certi $b_1, \dots, b_k \in A$. Dato che il numeratore di questa frazione è un elemento di I e il denominatore un elemento di S abbiamo verificato che $i \in S^{-1}I$.

1.b) Se $s \in I \cap S$ allora $1 = \frac{s}{s} \in S^{-1}I$ e quindi $S^{-1}I = S^{-1}A$. Viceversa, se $I^e = S^{-1}I = S^{-1}A$, allora $\frac{1}{1} \in I^e$ e quindi esistono $a \in I$ e $s \in S$ tali che $\frac{a}{s} = \frac{1}{1}$. Per definizione della relazione di equivalenza, esiste perciò $t \in S$ tale che $st = at \in I$, da cui segue che $st \in I \cap S$.

1.c) Sia $a \in \bigcup_{s\in S} I : s$; allora esiste $s \in S$ tale che $as \in I$. Dato che $\frac{a}{1} = \frac{as}{s}$, avremo che $\frac{a}{1} \in S^{-1}I = I^e$ e quindi $a \in I^{ec}$.

Sia ora $b \in I^{ec}$; allora esistono $a \in I$ e $s \in S$ tali che $\frac{b}{1} = \frac{a}{s} \in S^{-1}I = I^e$. Esiste quindi $t \in S$ tale che $stb = ta \in I$, da cui segue che $b \in I : st$, con $st \in S$, e l'altra inclusione è provata.

2. Vale sempre che $J \supseteq J^{ce}$, basta pertanto provare che $J \subseteq J^{ce}$. Consideriamo $\frac{a}{s} \in J$; allora anche $\frac{a}{1} \in J$ e quindi $a \in J^c$ e $\frac{a}{s} = \frac{1}{s}\frac{a}{1} \in J^{ce}$.

T. 139. Siano A un anello e $S \subset A$ un insieme moltiplicativo.

Se $\mathfrak{p} \subset A$ è un ideale primo tale che $\mathfrak{p} \cap S = \emptyset$ allora $\mathfrak{p} = \mathfrak{p}^{ec}$; inoltre $\mathfrak{p}^e$ è un ideale primo di $S^{-1}A$.

In particolare, vi è una corrispondenza biunivoca tra gli ideali primi di $S^{-1}A$ e gli ideali primi di A che non intersecano S.

$$\operatorname{Spec} S^{-1}A \overset{1:1}{\longleftrightarrow} \{\mathfrak{p} \in \operatorname{Spec} A \colon \mathfrak{p} \cap S = \emptyset\}.$$

Dimostrazione ***T.*** *139* Vale sempre che $\mathfrak{p} \subseteq \mathfrak{p}^{ec}$. Sia $a \in \mathfrak{p}^{ec}$; per **T.**138.c) esiste $s \in S$ tale che $a \in \mathfrak{p} : s$. Dal momento che $\mathfrak{p} \cap S = \emptyset$ si deve avere $a \in \mathfrak{p}$, e quindi $\mathfrak{p}^{ec} \subseteq \mathfrak{p}$.

Proviamo la seconda affermazione. Dall'ipotesi e **T.**138.1.b) avremo intanto che $S^{-1}\mathfrak{p} \subsetneq S^{-1}A$.

Siano $\frac{a}{s}, \frac{b}{t} \in S^{-1}A$ tali che $\frac{a}{s}\frac{b}{t} \in \mathfrak{p}^e$. Allora esistono $p \in \mathfrak{p}$ e $u \in S$ tali che $\frac{ab}{st} = \frac{p}{u}$, per **T.**138.1.a), ed esiste $v \in S$ tale che $vuab = vstp \in \mathfrak{p}$. Dato che $vu \in S$ e per ipotesi $\mathfrak{p} \cap S = \emptyset$ otteniamo che $ab \in \mathfrak{p}$; quindi o $\frac{a}{s} \in S^{-1}\mathfrak{p}$ oppure $\frac{b}{t} \in S^{-1}\mathfrak{p}$, come volevamo.

Localizzazione ed operazioni fra ideali

T. 140. Siano $I, J \subset A$ ideali; allora

1. $S^{-1}(I+J) = S^{-1}I + S^{-1}J$;
2. $S^{-1}(IJ) = S^{-1}I\ S^{-1}J$;
3. $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$;
4. $S^{-1}\sqrt{I} = \sqrt{S^{-1}I}$. In particolare, $S^{-1}\mathcal{N}(A) = \mathcal{N}(S^{-1}A)$.

Dimostrazione T. *140* 1 e 2 seguono immediatamente dalle proprietà dell'estensione di ideali.

3. Certamente $S^{-1}(I \cap J) \subseteq S^{-1}I \cap S^{-1}J$. Sia $\alpha = \frac{i}{s} = \frac{j}{t}$, con $i \in I$, $j \in J$ e $s, t \in S$, un elemento di $S^{-1}I \cap S^{-1}J$; allora esiste $u \in S$ tale che $u(it - js) = 0$. Quindi $uti = usj \in I \cap J$ e $\alpha = \frac{uti}{uts} \in S^{-1}(I \cap J)$.

4. Sia $\alpha \in S^{-1}\sqrt{I}$ allora esistono $i \in \sqrt{I}$ e $s \in S$ tali che $\alpha = \frac{i}{s}$. Se $i^n \in I$ allora $\alpha^n = \frac{i^n}{s^n} \in S^{-1}I$, da cui $\alpha \in \sqrt{S^{-1}I}$.

Per l'altra inclusione, sia $\beta = \frac{a}{t} \in \sqrt{S^{-1}I}$; allora esiste n tale che $\beta^n = \frac{a^n}{t^n} \in S^{-1}I$ e quindi $\beta^n = \frac{i}{s}$, con $i \in I$ e $s \in S$. Da ciò segue che esiste $u \in S$ tale che $ua^n s = ut^n i \in I$, quindi $uas \in \sqrt{I}$ e $\beta = \frac{aus}{ust} \in S^{-1}\sqrt{I}$.

Concludiamo osservando che nella costruzione della localizzazione è possibile che si "aggiungano" non solo gli inversi degli elementi di S, ma che risultino invertibili anche altri elementi. Ad esempio, se $S = \{6^n\}_{n\in\mathbb{N}} \subset \mathbb{Z}$, allora in $S^{-1}\mathbb{Z}$ anche $\frac{2}{1}$ è invertibile: $\frac{2}{1}\frac{3}{6} = \frac{1}{1}$. Di fatto tutti gli elementi dell'insieme $T = \{2^n 3^m\}_{n,m\in\mathbb{N}}$ risultano invertibili. Per un'analisi di questo fenomeno si veda la sezione in appendice a questo capitolo.

6.2 Moduli di frazioni

La costruzione descritta per gli anelli può essere generalizzata al caso dei moduli: localizziamo un A-modulo M in un sottoinsieme moltiplicativamente chiuso $S \subset A$, ottenendo $S^{-1}M$, che è un $S^{-1}A$-modulo.

Più precisamente,

$$(m,s) \sim (n,t) \iff \text{esiste } u \in S \text{ tale che } u(tm - sn) = 0,$$

con $m, n \in M$, $s, t \in S$, definisce una relazione di equivalenza su $M \times S$. Indichiamo con $\frac{m}{s}$ la classe di equivalenza di un elemento (m,s). Denotiamo inoltre con $S^{-1}M$ l'insieme $M \times S / \sim$.

Modulo delle frazioni

Siano M un A-modulo e $S \subset A$ un sottoinsieme moltiplicativo.

L'insieme $S^{-1}M$ dotato delle operazioni definite da:

$$\frac{m}{s} + \frac{n}{t} = \frac{tm + sn}{st}, \quad \frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st},$$

con $m, n \in M$, $s, t \in S$ e $a \in A$, è un $S^{-1}A$-modulo.

Tale modulo si chiama il *modulo delle frazioni di M rispetto ad S* o la *localizzazione* di M in S.

Osserviamo che se $\mathrm{Ann}(M) \cap S \neq \emptyset$ allora $S^{-1}M = 0$. Infatti se esiste $s \in \mathrm{Ann}(M) \cap S$, preso un qualunque elemento $\frac{m}{t} \in S^{-1}M$, avremo $sm = 0$ e quindi $\frac{m}{t} = \frac{0}{1}$.

Analogamente a quanto fatto per gli anelli, denotiamo $S^{-1}M$ con M_f oppure $M_{\mathfrak{p}}$ rispettivamente quando $S = \{f^n\}_{n \in \mathbb{N}}$ oppure $S = A \setminus \mathfrak{p}$.

Considerando l'omomorfismo canonico $\sigma \colon A \longrightarrow S^{-1}A$ di anelli, per restrizione di scalari, qualsiasi $S^{-1}A$-modulo è dotato di una struttura di A-modulo, con $am = \frac{a}{1}m$, per ogni $a \in A$ e $m \in M$. Pertanto $S^{-1}M$ ha una naturale struttura di A-modulo.

Con un lieve abuso di notazione indichiamo ancora con $\sigma = \sigma_S$ l'omomorfismo canonico per i moduli.

La mappa $\sigma\colon M \longrightarrow S^{-1}M$, definita da $\sigma(m) = \frac{m}{1}$, è un omomorfismo di A-moduli.

Per definire la proprietà universale del modulo delle frazioni, in analogia a quanto visto per gli anelli, dobbiamo tenere conto del fatto che M e $S^{-1}M$ sono moduli a priori su anelli diversi, quindi abbiamo bisogno di oggetti che abbiano una doppia struttura, quella di A-modulo e quella di $S^{-1}A$-modulo, e che queste strutture siano compatibili.

T. 141. Siano A un anello, $S \subset A$ un insieme moltiplicativo e N un A-modulo. È possibile definire su N una struttura di $S^{-1}A$-modulo compatibile con la struttura di A-modulo data, cioè tale che $an = \frac{a}{1}n$ per ogni $a \in A$ e $n \in N$, se e solo se per ogni $s \in S$ la moltiplicazione $\mu_s\colon N \xrightarrow{\cdot s} N$ è biunivoca. In tale caso la struttura di $S^{-1}A$-modulo su N è unica.

***Dimostrazione T.** 141* Osserviamo che, per ogni $s, t \in S$, si ha che μ_s e μ_t commutano e, se sono invertibili, chiaramente commutano anche le loro inverse.

Sia N dotato di una struttura di $S^{-1}A$-modulo compatibile con quella di A-modulo e sia $s \in S$. Allora $\mu_s = \mu_{\frac{s}{1}}$ e quindi $\mu_s \circ \mu_{\frac{1}{s}} = \mu_{\frac{1}{s}} \circ \mu_s = \mu_1 = \mathrm{id}_N$. Dunque μ_s è biunivoca per ogni $s \in S$.

Viceversa, sia N un A-modulo; dobbiamo definire su N un prodotto esterno compatibile con la struttura di A-modulo: deve essere $\frac{a}{1}n = an$ e $\frac{1}{s}n = \left(\frac{s}{1}\right)^{-1} n$. Dunque definiamo $\frac{1}{s}n$ come quell'unico elemento $n' \in N$ tale che $\mu_s(n') = sn' = n$, ottenendo

$$\frac{a}{s}n = an' = a\mu_s^{-1}(n).$$

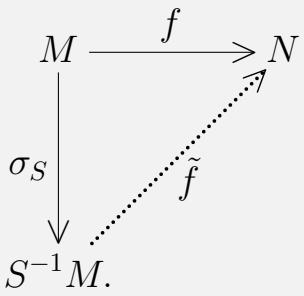
Per vedere che questa è una buona definizione verifichiamo che è indipendente dal rappresentante di $\frac{a}{s}$. Siano allora $\frac{a}{s} = \frac{b}{t}$ e $u \in S$ tale che $u(at - bs) = 0$. Ne segue che $(at - bs)un = 0$ per ogni $n \in N$ e di conseguenza, dato che μ_u è iniettiva, $atn = bsn$ cioè $a\mu_t(n) = b\mu_s(n)$ per ogni $n \in N$. Pertanto si ha

$$\frac{a}{s}n = a\mu_s^{-1}(n) = a\mu_t\mu_t^{-1}\mu_s^{-1}(n) = b\mu_s\mu_t^{-1}\mu_s^{-1}(n) = b\mu_s\mu_s^{-1}\mu_t^{-1}(n) = \frac{b}{t}n\,.$$

Le verifiche che con questa definizione N abbia una struttura unica di $S^{-1}A$-modulo compatibile sono ora ovvie.

Proprietà universale del modulo delle frazioni

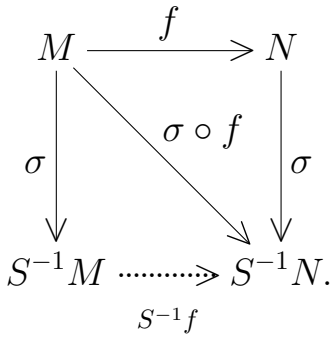
Siano $S \subset A$ un sottoinsieme moltiplicativo, M ed N due A-moduli con N tale che μ_s è biunivoca su N per ogni $s \in S$.
Per ogni omomorfismo di A-moduli $f\colon M \longrightarrow N$ esiste un unico omomorfismo di $S^{-1}A$-moduli $\tilde{f}\colon S^{-1}M \longrightarrow N$ tale che $\tilde{f}\left(\frac{m}{s}\right) = \frac{1}{s}f(m)$, ossia tale che il seguente diagramma commuti



Osserviamo che, per quanto visto in **T.**141, si richiede che N sia un $(A, S^{-1}A)$-bimodulo. Inoltre, l'omomorfismo $\tilde{f}$ è per restrizione di scalari anche un omomorfismo di A-moduli.

6.3 Il funtore S^{-1}

Per poter considerare l'operazione di localizzazione come funtore, dobbiamo capire come trasforma gli omomorfismi. Siano M e N due A-moduli, $f\colon M \longrightarrow N$ un omomorfismo di A-moduli e consideriamo il seguente diagramma:



È facile verificare che la mappa definita da

$$S^{-1}f\left(\frac{m}{s}\right) = \frac{f(m)}{s}$$

è un omomorfismo di $S^{-1}A$-moduli che rende il diagramma commutativo; alternativamente, si può osservare che $S^{-1}N$ è un $S^{-1}A$- e A-modulo e le due strutture sono compatibili; pertanto per **T.**141, le moltiplicazioni per elementi di S sono mappe biunivoche e dunque per la proprietà universale si ha $S^{-1}f = \widetilde{\sigma \circ f}$.

Inoltre, dato un omomorfismo di A-moduli $g\colon N \longrightarrow P$, si ha

$$S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f.$$

L'operazione di localizzazione allora può essere anche interpretata come funtore covariante dalla categoria degli A-moduli a quella degli $S^{-1}A$-moduli.

T. 142. [Esattezza di S^{-1}] S^{-1} è esatto ossia, per ogni successione esatta $M \xrightarrow{f} N \xrightarrow{g} P$ la successione $S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}P$ è esatta.
In particolare, se f è un omomorfismo iniettivo, allora $S^{-1}f$ è iniettivo, se g è un omomorfismo surgettivo, allora $S^{-1}g$ è surgettivo.

Dimostrazione T. *142* Dato che $S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f) = 0$ si ha che $\operatorname{Im} S^{-1}f \subseteq \operatorname{Ker} S^{-1}g$. Sia ora $\frac{n}{s} \in \operatorname{Ker} S^{-1}g$; allora $\frac{g(n)}{s} = \frac{0}{1}$ e quindi esiste $t \in S$ tale che $g(tn) = tg(n) = 0$, ossia $tn \in \operatorname{Ker} g = \operatorname{Im} f$. Quindi esiste $m \in M$ tale che $f(m) = tn$; in $S^{-1}N$ otteniamo allora che $\frac{n}{s} = \frac{tn}{ts} = \frac{f(m)}{ts} = S^{-1}f(\frac{m}{ts}) \in \operatorname{Im} S^{-1}f$.

Localizzazione ed operazioni fra moduli

T. 143. Siano M, N, P A-moduli.

1. Se $M, N \subseteq P$, allora $S^{-1}(M + N) = S^{-1}M + S^{-1}N$.
2. $S^{-1}(M \cap N) = S^{-1}M \cap S^{-1}N$.
3. Se $N \subseteq P$, allora $S^{-1}N \subseteq S^{-1}P$ e $S^{-1}(P/N) \simeq S^{-1}P/S^{-1}N$.
4. Se M è finitamente generato, allora $S^{-1}\operatorname{Ann}_A(M) = \operatorname{Ann}_{S^{-1}A}(S^{-1}M)$.

5. Se M, N sono sottomoduli di P, e N è finitamente generato, allora $S^{-1}(M : N) = S^{-1}M : S^{-1}N$.

***Dimostrazione* T.** *143* 1. Si ha $\frac{m+n}{s} = \frac{m}{s} + \frac{n}{s}$ quindi $S^{-1}(M+N) \subseteq S^{-1}M + S^{-1}N$.

Si ha anche che $\frac{m}{s} + \frac{n}{t} = \frac{tm+sn}{st}$, da cui segue l'altra inclusione.

2. $S^{-1}(M \cap N) \subseteq S^{-1}M \cap S^{-1}N$ segue immediatamente dal fatto che $M \cap N$ è contenuto sia in M che in N.

Viceversa sia $\alpha \in S^{-1}M \cap S^{-1}N$. Allora esistono $m \in M, n \in N, s, t \in S$ tali che $\alpha = \frac{m}{s} = \frac{n}{t}$, ed $u \in S$ tali che $u(tm - sn) = 0$; da ciò discende che $utm = usn \in M \cap N$ e pertanto $\frac{m}{s} = \frac{utm}{uts} = \frac{usn}{uts} \in S^{-1}(M \cap N)$.

3. Applicando S^{-1} alla successione esatta $0 \longrightarrow N \xrightarrow{j} P \xrightarrow{\pi} {}^{P}\!/_{N} \longrightarrow 0$, ove j è l'omomorfismo di inclusione e π la proiezione canonica, otteniamo la successione esatta $0 \longrightarrow S^{-1}N \xrightarrow{S^{-1}j} S^{-1}P \xrightarrow{S^{-1}\pi} S^{-1}{}^{P}\!/_{N} \longrightarrow 0$ per **T.**142. Consideriamo il seguente diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S^{-1}N & \xrightarrow{S^{-1}j} & S^{-1}P & \xrightarrow{S^{-1}\pi} & S^{-1}{}^{P}\!/_{N} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & S^{-1}N & \xrightarrow{S^{-1}j} & S^{-1}P & \xrightarrow{\eta} & S^{-1}{}^{P}\!/_{S^{-1}N} & \longrightarrow & 0, \end{array}$$

dove η è la proiezione canonica sul quoziente, $\eta\left(\frac{p}{s}\right) = \frac{p}{s} + S^{-1}N$, $\alpha = \mathrm{id}_{S^{-1}N}$, $\beta = \mathrm{id}_{S^{-1}P}$, e $\gamma(\frac{\overline{p}}{s}) = \frac{p}{s} + S^{-1}N$, dove $p \in P$ è un qualsiasi elemento congruo a $\overline{p}$ modulo N. La γ è ben definita: osserviamo che $\frac{\overline{p}}{s} = \frac{\overline{q}}{t}$ implica che esiste $u \in S$ tale che $ut\overline{p} = us\overline{q}$, i.e. $utp - usq = n$, per un certo $n \in N$. Allora

$$\gamma\left(\frac{\overline{p}}{s}\right) = \frac{p}{s} + S^{-1}N = \frac{utp}{uts} + S^{-1}N = \frac{usq}{uts} + \frac{n}{uts} + S^{-1}N = \frac{q}{t} + S^{-1}N = \gamma\left(\frac{\overline{q}}{t}\right).$$

Il quadrato a sinistra senz'altro commuta, mentre per il secondo avremo che $\gamma \circ (S^{-1}\pi)\left(\frac{p}{s}\right) = \gamma\left(\frac{\overline{p}}{s}\right) = \eta\left(\frac{p}{s}\right)$. La conclusione segue allora da **T.**104.

4. Procediamo per induzione sul numero di generatori di M. Se $M = 0$ non c'è nulla da dimostrare, quindi supponiamo che $M = \langle m \rangle_A \neq 0$ sia un A-modulo

ciclico; allora $M \simeq A/\operatorname{Ann}_A m$ e, per il punto 3, $S^{-1}M \simeq S^{-1}A/S^{-1}\operatorname{Ann}_A M$. Con lo stesso ragionamento, sfruttando il fatto che $S^{-1}M = \langle \frac{m}{1} \rangle_{S^{-1}A}$, si ottiene $S^{-1}M \simeq S^{-1}A/\operatorname{Ann}_{S^{-1}A} S^{-1}M$. La tesi segue dal lemma del serpente applicato al diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S^{-1}\operatorname{Ann}_A M & \longrightarrow & S^{-1}A & \longrightarrow & {S^{-1}A}\big/{S^{-1}\operatorname{Ann}_A M} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \mathrm{id}_{S^{-1}A}} & & \downarrow{\scriptstyle \beta} & & \\ 0 & \longrightarrow & \operatorname{Ann}_{S^{-1}A} S^{-1}M & \longrightarrow & S^{-1}A & \longrightarrow & {S^{-1}A}\big/{\operatorname{Ann}_{S^{-1}A} S^{-1}M} & \longrightarrow & 0, \end{array}$$

dove β è un isomorfismo e α l'omomorfismo di inclusione.
Dimostriamo ora il passo induttivo: scriviamo $M = N_1 + N_2$ con N_1 e N_2 due A-moduli con un numero di generatori strettamente minore del numero di generatori di M. Allora, per i punti 1 e 2 e le proprietà dell'annullatore, avremo che

$$\begin{aligned} S^{-1}\operatorname{Ann}_A M &= S^{-1}\operatorname{Ann}_A(N_1 + N_2) = S^{-1}(\operatorname{Ann}_A N_1 \cap \operatorname{Ann}_A N_2) \\ &= S^{-1}\operatorname{Ann}_A N_1 \cap S^{-1}\operatorname{Ann}_A N_2 \\ &= \operatorname{Ann}_{S^{-1}A} S^{-1}N_1 \cap \operatorname{Ann}_{S^{-1}A} S^{-1}N_2 \\ &= \operatorname{Ann}_{S^{-1}A}(S^{-1}N_1 + S^{-1}N_2) \\ &= \operatorname{Ann}_{S^{-1}A}(S^{-1}(N_1 + N_2)) = \operatorname{Ann}_{S^{-1}A} S^{-1}M \ , \end{aligned}$$

ove la quarta uguaglianza è giustificata dall'ipotesi induttiva.
5. Osserviamo che $a \in M : N \iff aN \subseteq M \iff a\left({N + M}/{M}\right) = 0$, i.e. $M : N = \operatorname{Ann}_A\left({N + M}/{M}\right)$. Adesso basta osservare che N finitamente generato implica che anche ${N + M}/{M}$ è finitamente generato e applicare le proprietà dimostrate ai punti precedenti:

$$\begin{aligned} S^{-1}(M : N) &= S^{-1}\operatorname{Ann}_A\left({N + M}/{M}\right) \\ &= \operatorname{Ann}_{S^{-1}A}\left(S^{-1}\left({N + M}/{M}\right)\right) \\ &= \operatorname{Ann}_{S^{-1}A}\left({S^{-1}(N + M)}/{S^{-1}M}\right) \\ &= \operatorname{Ann}_{S^{-1}A}\left({S^{-1}N + S^{-1}M}/{S^{-1}M}\right) = S^{-1}M : S^{-1}N \ . \end{aligned}$$

Esempio 6.1. Osserviamo che il punto 4 è un caso particolare di 5, e le affermazioni non valgono in generale. Per esempio consideriamo $A = K\left[t, \frac{x}{t^n} \ : \ n \in \mathbb{N}\right]$, con K campo, x e t indeterminate, $M = \langle x \rangle_A$, $N = \langle \frac{x}{t^n} \ : \ n \in \mathbb{N} \rangle_A$ e $S = \{t^n \ : \ n \in \mathbb{N}\}$. Allora

$$M \ : \ N = \left\{a \in A \ : \ \frac{ax}{t^n} \in M \text{ per ogni } n \in \mathbb{N}\right\} = \left(\frac{x}{t^n} \colon n \in \mathbb{N}\right) = N$$

e dunque $S^{-1}(M \colon N) = S^{-1}N = S^{-1}(x) = S^{-1}M$ e infine $S^{-1}M \ : \ S^{-1}N = S^{-1}A$.

Vediamo infine quali sono alcune relazioni con il prodotto tensoriale.

Localizzazione e prodotto tensoriale

T. 144. Siano A un anello, S un sottoinsieme moltiplicativo di A e M un A-modulo. Allora abbiamo isomorfismi canonici

1. $S^{-1}M \simeq S^{-1}A \otimes_A M$;
2. $S^{-1}(M \otimes_A N) \simeq S^{-1}M \otimes_{S^{-1}A} S^{-1}N$.

Dimostrazione T. *144* 1. Definiamo $f \colon S^{-1}A \times M \longrightarrow S^{-1}M$ come $f\left(\frac{a}{s}, m\right) = \frac{am}{s}$. Tale f è ben definita e A-bilineare e quindi, per la proprietà universale del prodotto tensoriale, esiste un unico omomorfismo di A-moduli

$$\tilde{f} \colon S^{-1}A \otimes_A M \longrightarrow S^{-1}M, \qquad \text{definito da} \qquad \tilde{f}\left(\frac{a}{s} \otimes_A m\right) = \frac{am}{s}.$$

Poiché f è surgettiva anche $\tilde{f}$ è surgettiva.

Osserviamo ora che se $\alpha \in S^{-1}A \otimes_A M$, allora $\alpha = \sum_{i=1}^k \frac{a_i}{s_i} \otimes m_i$; quindi, ponendo $s = \prod_{i=1}^k s_i$, $t_i = \frac{s}{s_i}$ e $n = \sum_{i=1}^k a_i t_i m_i$ si può scrivere $\alpha = \sum_{i=1}^k \frac{a_i t_i}{t_i s_i} \otimes m_i = \frac{1}{s} \otimes \sum_{i=1}^k a_i t_i m_i = \frac{1}{s} \otimes n$. Proviamo ora che $\tilde{f}$ è iniettiva. Supponiamo che $\alpha \in \operatorname{Ker} \tilde{f}$; allora $0 = \tilde{f}(\alpha) = \tilde{f}\left(\frac{1}{s} \otimes n\right) = \frac{n}{s}$, ed esiste dunque $u \in S$ tale $un = 0$. Da ciò si ottiene che

$$\alpha = \frac{1}{s} \otimes n = \frac{u}{us} \otimes n = \frac{1}{us} \otimes un = 0,$$

come volevamo.

2. Per il punto precedente, le proprietà del prodotto tensoriale **T.**127 e **T.**131, si ha

$$\begin{aligned} S^{-1}M \otimes_{S^{-1}A} S^{-1}N &\simeq (M \otimes_A S^{-1}A) \otimes_{S^{-1}A} (S^{-1}A \otimes_A N) \\ &\simeq M \otimes_A (S^{-1}A \otimes_{S^{-1}A} S^{-1}A) \otimes_A N \\ &\simeq M \otimes_A S^{-1}A \otimes_A N \\ &\simeq S^{-1}A \otimes_A (M \otimes_A N) \simeq S^{-1}(M \otimes_A N). \end{aligned}$$

6.4 Proprietà locali

Una proprietà $\mathcal{P}$ di un anello A si dice *locale* se

$$\begin{array}{c} \mathcal{P} \text{ vale per } A \\ \Updownarrow \\ \mathcal{P} \text{ vale per ogni localizzazione } A_{\mathfrak{p}}, \text{ con } \mathfrak{p} \in \operatorname{Spec} A. \end{array}$$

Allo stesso modo, una proprietà $\mathcal{P}$ di un A-modulo M si dice *locale* se

$$\begin{array}{c} \mathcal{P} \text{ vale per l'} A\text{-modulo } M \\ \Updownarrow \\ \mathcal{P} \text{ vale per l'} A_{\mathfrak{p}}\text{-modulo } M_{\mathfrak{p}}, \text{ per ogni } \mathfrak{p} \in \operatorname{Spec} A. \end{array}$$

Una proprietà locale fondamentale è la seguente.

T. 145. Sia M un A-modulo. Sono fatti equivalenti:

1. $M = 0$;
2. $M_{\mathfrak{p}} = 0$ per ogni ideale primo $\mathfrak{p} \subset A$;
3. $M_{\mathfrak{m}} = 0$ per ogni ideale massimale $\mathfrak{m} \subset A$.

Dimostrazione T. *145* Le implicazioni $1 \Rightarrow 2 \Rightarrow 3$ sono ovvie, quindi basta provare che $3 \Rightarrow 1$ Supponiamo per assurdo che $M \neq 0$. Allora esiste $0 \neq m \in M$ tale che $\operatorname{Ann} m \subsetneq A$ e quindi esiste un ideale massimale $\operatorname{Ann} m \subseteq \mathfrak{m}$. Per ipotesi $M_{\mathfrak{m}} = 0$ e quindi $\frac{m}{1} = \frac{0}{1}$ ed esiste $u \in S = A \setminus \mathfrak{m}$ tale che $um = 0$ ma dato che $\operatorname{Ann} m \subseteq \mathfrak{m}$ questo non è possibile.

Alcune proprietà locali

T. 146. Siano A un anello, M, N due A-moduli, $f\colon M \longrightarrow N$ un omomorfismo. Le seguenti sono proprietà locali:

1. A è ridotto;
2. f è iniettivo;
3. f è surgettivo;
4. M è piatto.

Dimostrazione T. 146 1. Segue subito da $S^{-1}\mathcal{N}(A) = \mathcal{N}(S^{-1}A)$, cf. **T.**140, e da **T.**145.

2. Indichiamo con $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ l'omomorfismo indotto da f sulle localizzazioni, tramite $M \xrightarrow{f} N \xrightarrow{\sigma} N_{\mathfrak{p}}$. Dimostriamo che $(\operatorname{Ker} f)_{\mathfrak{p}} = \operatorname{Ker} f_{\mathfrak{p}}$ per ogni primo $\mathfrak{p}$. Infatti, si ha che $\frac{m}{s} \in \operatorname{Ker} f_{\mathfrak{p}} \Leftrightarrow \frac{f(m)}{s} = f_{\mathfrak{p}}\left(\frac{m}{s}\right) = 0$, dunque esiste $u \in S = A \setminus \mathfrak{p}$ tale che $f(um) = uf(m) = 0$. Allora $\frac{m}{s} = \frac{um}{us} \in (\operatorname{Ker} f)_{\mathfrak{p}}$.
Per l'inclusione opposta, $\frac{m}{s} \in (\operatorname{Ker} f)_{\mathfrak{p}} \Longrightarrow \frac{m}{s} = \frac{n}{t}$ per qualche $n \in \operatorname{Ker} f$. Dunque esiste $u \in S$ tale che $utm = usn$ e

$$f_{\mathfrak{p}}\left(\frac{m}{s}\right) = f_{\mathfrak{p}}\left(\frac{utm}{uts}\right) = f_{\mathfrak{p}}\left(\frac{usn}{uts}\right) = \frac{f(usn)}{uts} = 0\ ,$$

i.e. $\frac{m}{s} \in \operatorname{Ker} f_{\mathfrak{p}}$.
Adesso per **T.**145 si ha $\operatorname{Ker} f = 0 \iff (\operatorname{Ker} f)_{\mathfrak{p}} = 0 \iff \operatorname{Ker} f_{\mathfrak{p}} = 0$ per ogni primo $\mathfrak{p}$.

3. Analogamente a quanto fatto al punto precedente, si dimostra che $\operatorname{Im} f_{\mathfrak{p}} = (\operatorname{Im} f)_{\mathfrak{p}}$ e, di conseguenza, $\operatorname{Coker} f_{\mathfrak{p}} = (\operatorname{Coker} f)_{\mathfrak{p}}$. La tesi segue applicando di nuovo **T.**145.

4. Dal fatto che S^{-1} è un funtore esatto e da **T.**144 segue che $S^{-1}A$ è piatto. Dato che il prodotto tensoriale di moduli piatti è piatto, cf. **E.**187, la piattezza di M implica la piattezza di $M_{\mathfrak{p}}$ per ogni primo $\mathfrak{p}$, ancora per **T.**144.
Viceversa sia $f\colon N \to N'$ un omomorfismo iniettivo di A-moduli; vogliamo verificare che $\mathrm{id}_M \otimes f\colon M \otimes N \longrightarrow M \otimes N'$ è iniettivo. Dato che, in generale, $(M \otimes_A N)_{\mathfrak{p}} \simeq M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}}$, segue che $(\mathrm{id}_M \otimes f)_{\mathfrak{p}} = \mathrm{id}_{M_{\mathfrak{p}}} \otimes f_{\mathfrak{p}}$. Pertanto, $0 = \operatorname{Ker}(\mathrm{id}_{M_{\mathfrak{p}}} \otimes f_{\mathfrak{p}}) = (\operatorname{Ker}(\mathrm{id}_M \otimes f))_{\mathfrak{p}}$ per ogni primo $\mathfrak{p}$. Dunque, per **T.**145, $\operatorname{Ker}(\mathrm{id}_M \otimes f) = 0$ ed M è piatto.

Esempio 6.2. 1. Essere un dominio non è una proprietà locale: basta considerare l'anello $\mathbb{Z}/(6)$ i cui unici ideali primi sono $(\overline{2})$ e $(\overline{3})$. È facile verificare che $(\mathbb{Z}/(6))_{(\overline{2})} \simeq \mathbb{Z}/(2)$ e $(\mathbb{Z}/(6))_{(\overline{3})} \simeq \mathbb{Z}/(3)$ che sono entrambi domini, mentre $\mathbb{Z}/(6)$ non è un dominio.

2. Essere un anello noetheriano non è una proprietà locale: definiamo $A = (\mathbb{Z}/(2))[x_i : i \in \mathbb{N}]/I$ con $I = (x_i^2 - x_i \ : \ i \in \mathbb{N})$. Sicuramente A non è noetheriano. Preso un qualsiasi ideale primo $\mathfrak{p}$, allora $A_\mathfrak{p}$ è un anello locale per **T.**137; dalla definizione di I e dal fatto che la caratteristica è 2 si ha che ogni elemento di $A_\mathfrak{p}$ è idempotente. Dato che in un anello locale, gli unici elementi idempotenti sono 0 e 1, cf. **E.**14, si ha allora che $A_\mathfrak{p} = \mathbb{Z}/(2)$ è noetheriano per ogni $\mathfrak{p} \in \operatorname{Spec} A$.

6.5 Approfondimento: la saturazione di un insieme

In questa appendice ci proponiamo di spiegare brevemente il procedimento della saturazione che è strettamente connesso alla descrizione dell'insieme degli invertibili in un anello di frazioni. È possibile infatti che l'insieme $\left\{\frac{t}{s} \in S^{-1}A \ : \ t \in S\right\}$ non esaurisca $(S^{-1}A)^*$.
Consideriamo un sistema moltiplicativo $S \subset A$. Osserviamo che $\frac{a}{s} \in (S^{-1}A)^*$ se e solo se esistono $b \in A$ e $u \in S$ tale che $uab \in S$. Infatti, $\frac{a}{s} \in (S^{-1}A)^*$ se e solo se esiste $\frac{b}{t} \in S^{-1}A$ tale che $\frac{ab}{st} = \frac{1}{1}$, e quindi se e solo se esiste $u \in S$ tale che $uab = ust \in S$.

Diciamo che un insieme moltiplicativo $S \subset A$ è *saturato* se dati $s, t \in A$ tali che $st \in S$ allora $s, t \in S$.

Per esempio, il gruppo delle unità A^* di A e il sottoinsieme dei non divisori di zero $S = A \setminus \mathcal{D}(A)$ sono sottoinsiemi moltiplicativi saturati.
Se S è saturato, allora $S = \{a \in A \ : \ \frac{a}{1} \in (S^{-1}A)^*\}$. Infatti, come visto sopra, $\frac{a}{1} \in (S^{-1}A)^*$ se e solo se $uab \in S$ per qualche $b \in A$ e $u \in S$, e quindi se e solo se $a \in S$, per definizione di saturato.

T. 147. Un insieme moltiplicativo S è saturato se e solo se

$$S = A \setminus \bigcup_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \cap S = \emptyset}} \mathfrak{p}.$$

Dimostrazione T. 147 Consideriamo l'insieme $P = \{\mathfrak{p} \in \operatorname{Spec}(A) \colon \mathfrak{p} \cap S = \emptyset\}$; allora sicuramente $S \subseteq A \setminus \bigcup_{\mathfrak{p} \in P} \mathfrak{p}$.

Sia S saturato; per provare l'altra inclusione, supponiamo che $a \notin S$ e proviamo che esiste un primo $\mathfrak{p} \in P$ tale che $a \in \mathfrak{p}$. Dato che $a \notin S$, l'elemento $\frac{a}{1}$ non è invertibile in $S^{-1}A$ e quindi esiste un ideale massimale $\mathfrak{m} \subset S^{-1}A$ tale che $\frac{a}{1} \in \mathfrak{m}$. Per la corrispondenza tra gli ideali primi di $S^{-1}A$ e i primi di A che non intersecano S, esiste allora $\mathfrak{p} \subset A$ primo tale che $\mathfrak{p} \cap S = \emptyset$ e $\mathfrak{m} = S^{-1}\mathfrak{p}$. Quindi $\frac{a}{1} = \frac{b}{t}$ con $b \in \mathfrak{p}$ e $t \in S$. Esiste quindi $u \in S$ tale che $uta = ub \in \mathfrak{p}$ da cui segue che $a \in \mathfrak{p}$.

Viceversa, abbiamo già osservato che il complementare di un'unione di ideali primi è un insieme moltiplicativo. Inoltre se $st \in S$ allora per ogni $\mathfrak{p} \in P$ si ha $st \notin \mathfrak{p}$ e quindi $s, t \in S$, da cui segue che S è saturato.

Definiamo la *saturazione* di un insieme $S \subseteq A$ come il sottoinsieme

$$\overline{S} = \{t \in A \colon \exists\, a \in A \text{ tale che } at \in S\} .$$

Si verifica facilmente che la saturazione di un insieme moltiplicativo è un insieme moltiplicativo saturato, cf. **E.**235.

Con il prossimo risultato dimostriamo tra le altre cose una caratterizzazione dell'essere saturato e delle unità di $S^{-1}A$.

Proprietà della saturazione

T. 148. Siano $S \subset A$ un sottoinsieme moltiplicativo e $\overline{S}$ la sua saturazione; allora

1. $S \subseteq \overline{S}$;
2. sia $T \subset A$ un insieme moltiplicativo saturato, con $S \subseteq T$; allora $\overline{S} \subseteq T$;

3. $\overline{S} = A \setminus \bigcup_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \cap S = \emptyset}} \mathfrak{p}$;
4. $(S^{-1}A)^* = \left\{ \frac{a}{s} \ : \ a \in \overline{S}, s \in S \right\}$;
5. $\sigma_S^{-1}((S^{-1}A)^*) = \overline{S}$;
6. $\overline{S}^{-1}A \simeq S^{-1}A$.

Dimostrazione T. 148 1. Sia $s \in S$; allora $s1 \in S$ e quindi $s \in \overline{S}$.

2. Sia $s \in \overline{S}$; allora esiste $t \in A$ tale che $st \in S \subseteq T$ e quindi, dato che T è saturato $s \in T$.

3. Sia $T = A \setminus \bigcup_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \cap S = \emptyset}} \mathfrak{p}$: questo insieme è saturato per **T.**147, e contiene S, quindi dal punto 2 segue che $\overline{S} \subseteq T$.

D'altra parte anche $\overline{S}$ è saturato e contiene S, quindi, di nuovo per **T.**147,

$$\overline{S} = A \setminus \bigcup_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \cap \overline{S} = \emptyset}} \mathfrak{p} \supseteq A \setminus \bigcup_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \cap S = \emptyset}} \mathfrak{p} = T.$$

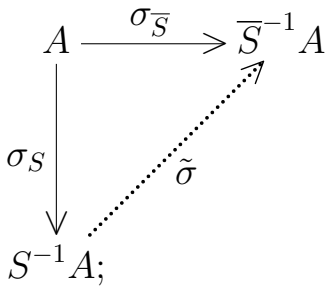
4. Consideriamo $\frac{a}{s}$ con $a \in \overline{S}$; allora esiste $t \in A$ tale che $at \in S$ e quindi $\frac{a}{s}\frac{st}{at} = \frac{1}{1}$, ossia $\frac{a}{s} \in (S^{-1}A)^*$.

Per l'altra inclusione, siano $\frac{a}{s}, \frac{b}{t} \in (S^{-1}A)^*$ tali che $\frac{a}{s}\frac{b}{t} = 1$; allora esiste $u \in S$ tale che $abu = stu \in S$ e quindi $a \in \overline{S}$, come volevamo.

5. Dal punto 4 segue subito che $\sigma_S(\overline{S}) \subseteq (S^{-1}A)^*$.

Per l'altra inclusione, sia $u \in \sigma_S^{-1}((S^{-1}A)^*)$; allora $\frac{u}{1} \in (S^{-1}A)^*$, e quindi esiste $\frac{b}{t}$ tale che $\frac{u}{1}\frac{b}{t} = \frac{1}{1}$. Pertanto esiste $s \in S$ tale che $sbu = st \in S$ e quindi $u \in \overline{S}$.

6. Usiamo la proprietà universale dell'anello delle frazioni e **T.**136, considerando il seguente diagramma



se proviamo che

a) per ogni $s \in S$ si ha che $\sigma_{\overline{S}}(s) \in (\overline{S}^{-1}A)^*$;
b) per ogni $a \in A$ tale che $\sigma_{\overline{S}}(a) = 0$ esiste $s \in S$ tale che $as = 0$;
c) per ogni $\frac{a}{t} \in \overline{S}^{-1}A$ esistono $b \in A$ e $s \in S$ tali che $\frac{a}{t} = \sigma_{\overline{S}}(b)\sigma_{\overline{S}}(s)^{-1}$,

allora $\tilde{\sigma}\colon S^{-1}A \longrightarrow \overline{S}^{-1}A$ definita da $\tilde{\sigma}(\frac{a}{s}) = \sigma_{\overline{S}}(a)\sigma_{\overline{S}}(s)^{-1} = \frac{a}{s}$ è un isomorfismo.

Si osserva che a) vale per i punti 1 e 5.
b) Sia $a \in A$ tale che $\frac{a}{1} = \sigma_{\overline{S}}(a) = \frac{0}{1}$; allora esiste $t \in \overline{S}$ tale che $ta = 0$ e dunque, dalla definizione di saturato, esiste $u \in A$ tale che $ut \in S$, e quindi esiste $s = ut \in S$ tale che $sa = 0$.
c) Sia $\frac{a}{t} \in \overline{S}^{-1}A$; dobbiamo trovare $\frac{b}{s} \in S^{-1}A$ tale che $\frac{a}{t} = \frac{b}{s}$: Basta prendere $u \in A$ tale che $ut \in S$ per ottenere $\frac{a}{t} = \frac{ua}{ut} \in S^{-1}A$.

In generale, se $S \subset T$ sono due insiemi moltiplicativi di A non è vero che $S^{-1}A \subset T^{-1}A$: vale invece il seguente

T. 149. Siano S, T sottoinsiemi moltiplicativi di A, allora

$$S^{-1}A = T^{-1}A \quad \text{se e solo se} \quad \overline{S} = \overline{T}.$$

***Dimostrazione* T. 149** Se $S^{-1}A = T^{-1}A$, allora i loro elementi invertibili sono gli stessi e per **T.**148.5, $\overline{S} = {\sigma_S}^{-1}((S^{-1}A)^*) = {\sigma_T}^{-1}((T^{-1}A)^*) = \overline{T}$.
Viceversa se $\overline{S} = \overline{T}$, allora, per **T.**148.6, si ha $S^{-1}A = \overline{S}^{-1}A = \overline{T}^{-1}A = T^{-1}A$.

Esempio 6.3. Siano $A = \mathbb{Z}/(6)$ e $S = \{1, 5\} = A^* \subset T = \{1, 5, 2, 4\} = \mathbb{Z}/(6) \setminus (\overline{3})$; allora avremo che $S^{-1}A = \mathbb{Z}/(6)$ e $T^{-1}A = \mathbb{Z}/(3)$.

7

Moduli noetheriani e artiniani. Decomposizione primaria

Sia $(\Sigma, \leq)$ un *poset*, ovvero un insieme Σ parzialmente ordinato da una relazione di ordine $\leq$.

T. 150. Le seguenti condizioni sono equivalenti:

1. ogni catena $s_1 \leq s_2 \leq \ldots \leq s_k \leq \ldots$ di elementi di Σ si *stabilizza*, o è *stazionaria*, cioè esiste un intero h tale che, per ogni $k \geq h$, si ha che $s_k = s_h$;
2. ogni sottoinsieme non vuoto di Σ ammette elementi massimali rispetto a $\leq$.

Dimostrazione T. 150 $1 \Rightarrow 2$. Sia S un sottoinsieme non vuoto di Σ ed $s_1 \in S$. Se S non ammette elementi massimali, esiste $s_2 \in S$ con $s_1 \leq s_2$. Ripetendo il ragionamento, si costruisce una catena ascendente infinita di elementi di Σ, negando dunque l'ipotesi.
$2 \Rightarrow 1$. Sia $s_0 \leq s_1 \leq \ldots \leq s_k \leq \ldots$ una catena ascendente di elementi di Σ. L'insieme $\{s_i\}_{i \in \mathbb{N}}$ è un sottoinsieme non vuoto di Σ, che quindi ammette un elemento s_h massimale, cioè tale che $s_k = s_h$ per ogni $k \geq h$.

Come fondamentale esempio consideriamo la famiglia Σ di tutti gli ideali di un anello A. Come relazione d'ordine $\leq$ su Σ si possono considerare sia la relazione $\subseteq$ sia la relazione $\supseteq$. Nel primo caso, la condizione 1 si chiama *condizione della catena ascendente*, in breve, dall'inglese *ascending chain condition*, a.c.c.; nel secondo caso si chiama invece *condizione della catena discendente*, in breve, dall'inglese *descending chain condition*, d.c.c.. Nel primo

caso diremo che A soddisfa a.c.c., nel secondo che soddisfa d.c.c. Similmente possiamo fare per i moduli: dato un A-modulo M consideriamo il poset $(\Sigma, \subseteq)$, rispettivamente $(\Sigma, \supseteq)$, di tutti i sottomoduli di M. Come prima si dirà che M soddisfa a.c.c., rispettivamente d.c.c..

7.1 Anelli e moduli noetheriani

Generalizziamo ora alla classe degli anelli e dei moduli la nozione di noetherianità che abbiamo già incontrato nello studio dell'anello dei polinomi, cf. **T.**40 e **T.**41. Sia dunque M un A-modulo e sia Σ la famiglia dei sottomoduli di M. Il modulo M si dice *noetheriano*, rispettivamente *artiniano*, se Σ soddisfa a.c.c., rispettivamente d.c.c.. In particolare, un anello A è noetheriano, rispettivamente artiniano, se lo è come A-modulo.

Un anello A è noetheriano se e solo se l'anello dei polinomi $A[x_1, \ldots, x_n]$ è noetheriano. L'implicazione non banale viene fornita dal seguente fondamentale risultato; per l'altra si veda **T.**152.2.

Teorema della base di Hilbert

T. 151. Sia A un anello noetheriano; allora $A[x_1, \ldots, x_n]$ è noetheriano.

Dimostrazione T. *151* Forniamo una dimostrazione non costruttiva, alternativa al teorema della base di Hilbert visto quando $A = K$ è un campo, cf. **T.**40, e più generale.

È chiaro che è sufficiente trattare il caso $n = 1$, dato che $A[x_1, \ldots, x_n] \simeq A[x_1, \ldots, x_{n-1}][x_n]$.

Supponiamo dunque per assurdo che esista un ideale I di $A[x]$ che non sia finitamente generato, e definiamo ricorsivamente una successione di elementi di I ponendo $f_0 = 0$ e scegliendo f_i tra gli elementi di grado minimo di $I \setminus (f_0, \ldots, f_{i-1})$. Questo è sempre possibile, altrimenti I risulterebbe finitamente generato. Se poniamo $\deg f_i = d_i$ per ogni $i \geq 1$ avremo per costruzione che $d_1 \leq d_2 \leq \ldots \leq d_i \leq \ldots$. Sia $a_i = \mathrm{lc}(f_i)$, per ogni $i \geq 1$, e consideriamo la catena di ideali di A $(a_1) \subseteq (a_1, a_2) \subseteq \ldots$. Essa si stabilizza per ipotesi e dunque esiste un intero k per cui $a_{k+1} \in (a_1, \ldots, a_k)$, ovvero $a_{k+1} = \sum_{i=1}^{k} b_i a_i$, per certi $b_i \in A$. Sia allora $g \in A[x]$ il polinomio

$$g = f_{k+1} - \sum_{i=1}^{k} b_i x^{d_{k+1}-d_i} f_i;$$

avremo che $g \in I \setminus (f_1, \ldots, f_k)$, e per costruzione $\deg g < d_{k+1} = \deg f_{k+1}$, ma questo contraddice la minimalità di f_{k+1}.

Come esempi di anelli noetheriani abbiamo i campi, i domini ad ideali principali, e gli anelli di polinomi a coefficienti in anelli noetheriani. Vedremo ora, tra le altre cose, che la noetherianità si preserva passando ai quozienti e alla localizzazione.

Moduli noetheriani: prime proprietà

T. 152. Siano A un anello, I un ideale di A, $S \subset A$ un insieme moltiplicativo, M, N, P, M_i A-moduli.

1. M è noetheriano se e solo se ogni suo sottomodulo è finitamente generato.
2. Sia $0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$ una successione esatta; allora, M è noetheriano se e solo se N e P sono noetheriani.
3. Sia $M = \bigoplus_{i=1}^{n} M_i$; allora, M è noetheriano se e solo se M_i è noetheriano per ogni i.
4. Sia A noetheriano; allora A/I è noetheriano sia come A-modulo che come A/I-modulo.
5. Sia A noetheriano; allora M è noetheriano se e solo se M è finitamente generato.
6. Sia $I \subseteq \operatorname{Ann} M$; allora M è noetheriano come A-modulo se e solo se è noetheriano come A/I-modulo.
7. Sia M noetheriano; allora $S^{-1}M$ è noetheriano come $S^{-1}A$-modulo.

Dimostrazione T. 152 1. Sia M noetheriano e N un suo sottomodulo; consideriamo l'insieme Σ dei sottomoduli di N finitamente generati ordinato con $\subseteq$. Chiaramente $0 \in \Sigma$, quindi Σ è non vuoto e pertanto esiste $N_0 \in \Sigma$ elemento massimale. Basta dunque mostrare che $N = N_0$ e avremo che N

è finitamente generato. Se così non fosse, preso $n \in N \setminus N_0$, avremmo che $N_0 \subsetneq N_0 + \langle n \rangle \subseteq N$, con $N_0 + \langle n \rangle$ finitamente generato, ma ciò contraddice la massimalità di N_0.
Viceversa, sia $M_0 \subseteq M_1 \subseteq \cdots \subseteq M_k \subseteq \cdots$ una catena ascendente di sottomoduli di M. Allora, $\widetilde{M} = \cup_i M_i$ è un sottomodulo di M, e quindi finitamente generato, diciamo da $m_1, \ldots, m_n$. Pertanto esiste un intero $h \in \mathbb{N}$ tale che $m_1, \ldots, m_n \in M_h$ e $M_h \subseteq \widetilde{M} = \langle m_1, \ldots, m_n \rangle \subseteq M_h$. Da ciò segue che la catena si stabilizza in M_h.
2. Sia M noetheriano e sia $N_0 \subseteq N_1 \subseteq \cdots$ una catena ascendente di sottomoduli di N. Allora $f(N_0) \subseteq f(N_1) \subseteq \cdots$ è una catena ascendente in M, e dunque stazionaria. Per l'iniettività di f, la catena è stazionaria anche in N, che quindi è noetheriano.

Sia ora $P_0 \subseteq P_1 \subseteq \cdots$ una catena ascendente in P. La catena $g^{-1}(P_0) \subseteq g^{-1}(P_1) \subseteq \cdots$ è ascendente in M e quindi stazionaria. Allora la catena $P_0 = g(g^{-1}(P_0)) \subseteq P_1 = g(g^{-1}(P_1)) \subseteq \cdots$ è stazionaria in P, dato che g è surgettiva.

Viceversa, supponiamo che N e P siano noetheriani. Data una catena ascendente $M_0 \subseteq M_1 \subseteq \cdots$ in M definiamo $N_i = f^{-1}(M_i)$ e $P_i = g(M_i)$. La catena degli N_i è stazionaria in N, e quindi esiste n_1 tale che, per ogni $n \geq n_1$, $N_n = N_{n_1}$. La catena dei P_i è stazionaria in P, e quindi esiste n_2 tale che, per ogni $n \geq n_2$, $P_n = P_{n_2}$. Sia $m = \max\{n_1, n_2\}$ e sia $i \geq m$. Consideriamo la successione

$$0 \longrightarrow N_i \xrightarrow{f_i} M_i \xrightarrow{g_i} P_i \longrightarrow 0,$$

ove $f_i = f|_{N_i}$ e $g_i = g|_{M_i}$, e dimostriamo che è esatta per ogni i. Sicuramente f_i è iniettiva e g_i è surgettiva; proviamo allora che la successione è esatta in M_i. Chiaramente $g_i \circ f_i = 0$ dato che $g \circ f = 0$, e quindi $\operatorname{Im} f_i \subseteq \operatorname{Ker} g_i$. Sia ora $m_i \in \operatorname{Ker} g_i \subseteq \operatorname{Ker} g = \operatorname{Im} f$. Allora esiste $n \in N$ tale che $f(n) = m_i$ e quindi $n \in N_i$, come volevamo. Adesso, per ogni $i \geq m$, basta considerare il diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N_m & \xrightarrow{f_m} & M_m & \xrightarrow{g_m} & P_m & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{Nm}} & & \downarrow{\scriptstyle j_m} & & \downarrow{\scriptstyle \mathrm{id}_{Pm}} & & \\ 0 & \longrightarrow & N_i & \xrightarrow{f_i} & M_i & \xrightarrow{g_i} & P_i & \longrightarrow & 0, \end{array}$$

ove j_m è l'omomorfismo di inclusione, ed applicare **T.**104 per ottenere la tesi.

3. Entrambe le implicazioni seguono dal punto precedente. Se $M = \oplus_{i=1}^{n} M_i$ è noetheriano, ogni sottomodulo M_i di M è noetheriano. Il viceversa si dimostra per induzione su n, osservando che $0 \longrightarrow M_1 \longrightarrow M \longrightarrow \oplus_{i=2}^{n} M_i \longrightarrow 0$ è una successione esatta.

4. Basta considerare la successione esatta $0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0$. Poiché A è Noetheriano, A/I è un A-modulo noetheriano per il punto 2; visto poi che gli A/I-sottomoduli di A/I sono in corrispondenza biunivoca con gli ideali di A che contengono I, avremo che le catene si stabilizzano e quindi che A/I è noetheriano anche come A/I-modulo.

5. Una implicazione discende immediatamente dal punto 1. Viceversa, sia $M = \langle m_1, \ldots, m_n \rangle$ finitamente generato e consideriamo la successione esatta $0 \longrightarrow \operatorname{Ker} \varphi \longrightarrow A^n \xrightarrow{\varphi} M \longrightarrow 0$, con $\varphi(e_i) = m_i$. Dato che A è noetheriano, anche A^n è noetheriano, e così pure M, per il punto 2.

6. Basta osservare che $N \subseteq M$ implica che $I \subseteq \operatorname{Ann} M \subseteq \operatorname{Ann} N$ e che N è un A-sottomodulo di M se e solo se N è un A/I-sottomodulo di M.

7. Sia $N = \langle n_1, \ldots, n_r \rangle$ un sottomodulo di M; allora $S^{-1}N = \langle \frac{n_1}{1}, \ldots, \frac{n_r}{1} \rangle$.

T. 153. [Primo teorema di finitezza] Siano A un anello noetheriano e I un ideale di A. Allora esiste un intero k tale che $\sqrt{I}^{\,k} \subseteq I$.

Dimostrazione T. 153 Per **T.**152.1, $\sqrt{I}$ è finitamente generato, diciamo da $f_1, \ldots, f_r$; esistono allora interi $k_1, \ldots, k_r$ tali che $f_i^{k_i} \in I$, per ogni $i = 1, \ldots, r$. Un qualsiasi intero $k \geq \sum_{i=1}^{r} k_i$ fa allora al caso nostro.

7.2 Decomposizione primaria

Negli anelli noetheriani possiamo finalizzare il nostro studio degli ideali: riusciremo a decomporli come intersezione finita di ideali primari, ovvero dimostreremo che ogni ideale proprio in un anello noetheriano è *decomponibile*. Lo

stesso fatto si generalizza facilmente ai sottomoduli di un modulo noetheriano su un anello noetheriano. In questa sezione conclusiva studiamo però tale decomposizione nel caso degli ideali e il problema della sua unicità.

Ricordiamo che, alla luce di **T.**7.1, un ideale I di un anello A si dice $\mathfrak{p}$-primario se è primario e $\sqrt{I} = \mathfrak{p}$. Il prossimo risultato dimostra che ogni ideale in un anello noetheriano è decomponibile.

T. 154. Siano A un anello noetheriano e $I \subsetneq A$ un ideale.

1. Se I è irriducibile allora I è primario.
2. Ogni ideale proprio di A è intersezione di un numero finito di ideali irriducibili.
3. Per ogni ideale proprio I esistono $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ ideali primari tali che $I = \cap_{i=1}^{n} \mathfrak{q}_i$.

Dimostrazione T. *154* 1. Supponiamo che I sia un ideale irriducibile e per contraddizione non sia primario: esistono allora $a, b \in A$ tali che $ab \in I$ con $a^n \notin I$ per ogni intero n e $b \notin I$. Consideriamo la catena ascendente di ideali $I \subseteq I : a \subseteq I : a^2 \subseteq \cdots$; essa per ipotesi è stazionaria. Sia dunque $I : a^n = I : a^{n+1}$ per un certo intero n. Mostriamo allora che $I = (I, b) \cap (I, a^n)$, e troveremo una contraddizione perché $I \subsetneq (I, b), (I, a^n)$ è irriducibile per ipotesi.

Chiaramente I è contenuto in tale intersezione. Per concludere ci basta allora mostrare che se $c \in (I, b) \cap (a^n, I)$ allora c è un elemento di I. Sia allora $c = da^n + i \in (I, b)$, per qualche $d \in A$ e $i \in I$. Avremo dunque che $ca = da^{n+1} + ai \in (aI, ab) \subseteq I$; quindi $d \in I : a^{n+1} = I : a^n$, da cui discende che $c \in I$.

2. Consideriamo la famiglia $\mathcal{F}$ di ideali propri di A che sono controesempi all'affermazione, e supponiamo per assurdo che essa sia non vuota. Allora, visto che A è noetheriano, esistono in $\mathcal{F}$ elementi massimali, che dunque sicuramente non sono irriducibili. Sia J un tale elemento: possiamo dunque scriverlo come $J_1 \cap J_2$, ove $J \subsetneq J_1, J_2$. Per la massimalità di J, avremo che J_1 e J_2 non sono elementi di $\mathcal{F}$, e si scrivono entrambi, e dunque anche J,

come intersezione finita di ideali irriducibili; una tale scrittura di J fornisce la contraddizione cercata.

3. Segue direttamente da 1 e 2.

La decomposizione di un ideale I come intersezione finita di ideali primari si chiama, come dicevamo sopra, *decomposizione primaria*. Essa non è unica, ma usando alcuni accorgimenti, come vedremo nel seguito, ci si può ridurre ad una decomposizione primaria *minimale*, ossia tale che

i) per ogni $i \neq j$, $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j} = \mathfrak{p}_j$;

ii) per ogni i, $\mathfrak{q}_i \not\supseteq \cap_{j\neq i}\mathfrak{q}_j$.

Chiaramente, data una decomposizione primaria di I possiamo da essa eliminare quegli ideali primari che contengono l'intersezione degli altri, in quanto ridondanti, e avere ancora una decomposizione primaria di I che verifica la seconda condizione. Per verificare anche la prima condizione, possiamo accorpare ideali con lo stesso radicale in un unico ideale intersezione; che questo sia lecito è garantito dal seguente semplice fatto.

T. 155. Siano $\mathfrak{q}_1$ e $\mathfrak{q}_2$ ideali $\mathfrak{p}$-primari di A; allora $\mathfrak{q} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ è $\mathfrak{p}$-primario.

Dimostrazione T. 155 L'ideale $\mathfrak{q}$ è primario: sia $ab \in \mathfrak{q} \subseteq \mathfrak{q}_1$ con $a \notin \mathfrak{q}_1$, e dunque anche $a \notin \mathfrak{q}$. Allora $b^n \in \mathfrak{q}_1$, da cui $b \in \sqrt{\mathfrak{q}_1} = \mathfrak{p} = \sqrt{\mathfrak{q}_2}$. Pertanto avremo anche che $b^m \in \mathfrak{q}_2$ per qualche intero m; da ciò segue allora che $b^{n+m} \in \mathfrak{q}_1\mathfrak{q}_2 \subseteq \mathfrak{q}$. (E se $a \in \mathfrak{q}_1 \setminus \mathfrak{q}$?)

Inoltre, $\sqrt{\mathfrak{q}} = \sqrt{\mathfrak{q}_1 \cap \mathfrak{q}_2} = \sqrt{\mathfrak{q}_1} \cap \sqrt{\mathfrak{q}_2} = \mathfrak{p}$.

T. 156. Siano $a \in A$ e $\mathfrak{q}$ un ideale $\mathfrak{p}$-primario di A.

1. Se $a \in \mathfrak{q}$, allora $\mathfrak{q} : a = A$.
2. Se $a \notin \mathfrak{q}$, allora $\mathfrak{q} : a$ è $\mathfrak{p}$-primario.
3. Se $a \notin \mathfrak{p}$, allora $\mathfrak{q} : a = \mathfrak{q}$.

Dimostrazione T. 156 1. Segue subito dal fatto che $1 \in \mathfrak{q} : a$.

2. Osserviamo innanzitutto che è sempre vero che $\mathfrak{q} : a \supseteq \mathfrak{q}$. Dimostriamo dapprima che $\sqrt{\mathfrak{q} : a} = \mathfrak{p}$ e poi che $\mathfrak{q} : a$ è primario.

Sia $b \in \mathfrak{q} : a$, i.e. $ab \in \mathfrak{q}$. Dato che $a \notin \mathfrak{q}$ e $\mathfrak{q}$ è primario, avremo che $b^n \in \mathfrak{q}$ per qualche intero positivo n, e dunque che $b \in \mathfrak{p}$. Pertanto $\mathfrak{q} \subseteq \mathfrak{q} : a \subseteq \mathfrak{p}$.

Passando ai radicali, otteniamo $\mathfrak{p} = \sqrt{\mathfrak{q}} \subseteq \sqrt{\mathfrak{q} : a} \subseteq \mathfrak{p}$, e la prima affermazione è provata.

Sia ora $bc \in \mathfrak{q} : a$, con $b \notin \mathfrak{p}$, e dunque $b^n \notin \mathfrak{q}$ per ogni intero n. Verifichiamo dunque che $c \in \mathfrak{q} : a$. Dato che $\mathfrak{q}$ è primario, $bca \in \mathfrak{q}$ implica che $ca \in \mathfrak{q}$, come volevamo.

3. Sia $b \in \mathfrak{q} : a$, i.e. $ab \in \mathfrak{q}$. Per ipotesi $a \notin \mathfrak{p}$, e dunque $a^n \notin \mathfrak{q}$ per ogni n. Dato che $\mathfrak{q}$ è primario, si deve allora avere che $b \in \mathfrak{q}$, e abbiamo verificato l'inclusione $\mathfrak{q} : a \subseteq \mathfrak{q}$.

Data una decomposizione primaria minimale di un ideale $I = \bigcap_{i=1}^n \mathfrak{q}_i$, con $\mathfrak{q}_i$ ideali $\mathfrak{p}_i$-primari, possiamo provare che gli ideali primi $\mathfrak{p}_i$ sono indipendenti dalla decomposizione data e caratterizzarli nel modo seguente. Osserviamo che il risultato vale senza che A sia noetheriano, basta che I sia decomponibile.

Teorema di unicità /I

T. 157. Sia $I = \bigcap_{i=1}^n \mathfrak{q}_i$ una decomposizione primaria minimale dell'ideale $I \subseteq A$. Allora

$$\{\mathfrak{p}_i \in \operatorname{Spec} A \mid \mathfrak{p}_i = \sqrt{\mathfrak{q}_i}\} = \{\sqrt{I : a} \mid a \in A,\ \sqrt{I : a} \in \operatorname{Spec} A\}.$$

Dimostrazione T. 157 Osserviamo in primo luogo che

$$I : a = \bigcap_{i=1}^n \mathfrak{q}_i : a = \bigcap_{i=1}^n (\mathfrak{q}_i : a)$$

e che se $a \in \bigcap_{i=1}^n \mathfrak{q}_i$ allora $\sqrt{I : a} = A$ non è primo.
Mostriamo ora le due inclusioni: sia $a \in A$ tale che $\sqrt{I : a}$ è primo. Possiamo scrivere $\sqrt{I : a} = \sqrt{\bigcap_{i=1}^n (\mathfrak{q}_i : a)} = \bigcap_{i=1}^n \sqrt{\mathfrak{q}_i : a} = \bigcap_{i\colon a \notin \mathfrak{q}_i} \mathfrak{p}_i$, ove l'ultima uguaglianza è garantita da **T.**156. Dato che $\sqrt{I : a}$ è primo, dovrà necessariamente esistere un indice j tale che $\sqrt{I : a} = \mathfrak{p}_j$.

Per ogni $\mathfrak{p}_i$ troviamo ora un elemento $a_i \in A$ tale che $\mathfrak{p}_i = \sqrt{I : a_i}$. Scegliamo tale $a_i \in \bigcap_{j \neq i} \mathfrak{q}_j \setminus \mathfrak{q}_i$; ciò è lecito poiché la decomposizione di I è minimale. Avremo allora che

$$\sqrt{I : a_i} = \bigcap_{j=1}^{n} \sqrt{\mathfrak{q}_j : a_i} = \bigcap_{j \neq i} \sqrt{\mathfrak{q}_j : a_i} \cap \sqrt{\mathfrak{q}_i : a_i} = \mathfrak{p}_i,$$

ove l'ultima uguaglianza discende nuovamente da **T.**156.

T. 158. Con le stesse notazioni di **T.**157, se A è noetheriano avremo

$$\{\mathfrak{p}_i \in \operatorname{Spec} A \mid \mathfrak{p}_i = \sqrt{\mathfrak{q}_i}\} = \{I : a \mid a \in A,\ I : a \in \operatorname{Spec} A\}.$$

Dimostrazione T. 158 Per **T.**153 esiste un intero k tale che $\mathfrak{p}_i^k \subseteq \mathfrak{q}_i$; avremo allora che $(\bigcap_{j \neq i} \mathfrak{q}_j)\mathfrak{p}_i^k \subseteq \bigcap_{j \neq i} \mathfrak{q}_j \cap \mathfrak{q}_i = I$. Scegliamo allora il più piccolo k per cui $(\bigcap_{j \neq i} \mathfrak{q}_j)\mathfrak{p}_i^k \subseteq I$ e sia $0 \neq a \in (\bigcap_{j \neq i} \mathfrak{q}_j)\mathfrak{p}_i^{k-1} \setminus I$. Allora $a\mathfrak{p}_i \subseteq I$, e dunque $\mathfrak{p}_i \subseteq I : a$; inoltre $a \in \bigcap_{j \neq i} \mathfrak{q}_j \setminus \mathfrak{q}_i$ e dalla dimostrazione di **T.**156 discende che $I : a \subseteq \sqrt{I : a} = \mathfrak{p}_i$. La prova è ora completa.

Chiameremo i primi $\mathfrak{p}_i$ del precedente teorema *primi associati di* I e denotiamo l'insieme di tali primi con $\operatorname{Ass} I$. Gli elementi minimali di $\operatorname{Ass} I$ si dicono *primi minimali di* I e l'insieme di tali primi si denota con $\operatorname{Min} I$; infine, i primi associati non minimali si chiamano *primi immersi* di I.

T. 159. 1. Sia I un ideale decomponibile; allora $\operatorname{Min} I$ è costituito esattamente dagli elementi minimali dell'insieme dei primi che contengono I.

2. Sia $0 = \bigcap_{i=1}^{n} \mathfrak{q}_i$ una decomposizione primaria minimale dell'ideale 0 di A, con $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$. Allora,

$$\mathcal{N}(A) = \bigcap_{\mathfrak{p}_i \in \operatorname{Min}(0)} \mathfrak{p}_i\,, \qquad \mathcal{D}(A) = \bigcup_{p_i \in \operatorname{Ass}(0)} \mathfrak{p}_i.$$

In virtù del punto 1 del precedente risultato, la notazione $\operatorname{Min} I$ è coerente, perché i primi minimali che contengono I sono sotto queste ipotesi i primi più piccoli di $\operatorname{Ass} I$. Come corollario, abbiamo dunque il *secondo teorema di finitezza*: in un anello noetheriano i primi minimali sono in numero finito e

sono proprio i primi minimali con cui decomponiamo $\sqrt{0}$. In questo senso possiamo scrivere $\operatorname{Min} A = \operatorname{Min}(0)$.

Dimostrazione T. 159 1. Vogliamo mostrare che

$$\operatorname{Min} I = \{\mathfrak{p}_i \in \operatorname{Ass} I : \mathfrak{p}_i \text{ minimale in } \operatorname{Ass} I\} = \{\mathfrak{p} \in \operatorname{Spec} A : \mathfrak{p} \supseteq I \text{ minimale}\}.$$

"$\supseteq$". Sia $\mathfrak{p}$ un primo che contiene $I = \bigcap_{i=1}^n \mathfrak{q}_i$; allora $\mathfrak{p} \supseteq \bigcap_{i=1}^n \mathfrak{p}_i$; quindi $\mathfrak{p} \supseteq \bigcap_{\mathfrak{p}_i \in \operatorname{Min} I} \mathfrak{p}_i$, e dunque, dato che è primo, per **T.**12.2 contiene un certo $\mathfrak{p}_{i_0} \in \operatorname{Min} I$; allora $\mathfrak{p} \supseteq \mathfrak{p}_{i_0} \supseteq I$, e se $\mathfrak{p}$ è minimale tra i primi che contengono I deve essere necessariamente $\mathfrak{p} = \mathfrak{p}_{i_0}$. In particolare, l'insieme dei primi che contengono I e sono minimali è finito.
"$\subseteq$". Sia $\sqrt{I} = \mathfrak{p}_{i_1} \cap \ldots \cap \mathfrak{p}_{i_k}$, con $\mathfrak{p}_{i_j} \in \operatorname{Min} I$ per $j \in \{1, \ldots, k\}$ e mostriamo ad esempio che $\mathfrak{p}_{i_1}$ è minimale rispetto all'inclusione. Visto che $\mathfrak{p}_{i_1}$ è primo, esiste un ideale primo $\mathfrak{p}'$ minimale tale che $\mathfrak{p}_{i_1} \supseteq \mathfrak{p}' \supseteq I$. Quindi $\mathfrak{p}_{i_1} \cap \ldots \cap \mathfrak{p}_{i_k} = \sqrt{I} \subseteq \mathfrak{p}'$. Allora, dato che $\mathfrak{p}'$ è primo, esiste i_j tale che $\mathfrak{p}_{i_1} \supseteq \mathfrak{p}' \supseteq \mathfrak{p}_{i_j}$, applicando nuovamente **T.**12.2. Per la minimalità, non si può avere $i_j \neq i_1$; da ciò segue che $\mathfrak{p}_{i_1} = \mathfrak{p}'$, come volevamo.

2. La prima uguaglianza discende subito dal punto 1, dato che $\mathcal{N}(A) = \sqrt{0}$. Dimostriamo allora la seconda.

Da **E.**30, sappiamo che $\mathcal{D}(A) = \bigcup_{0 \neq a \in A} \sqrt{0 : a}$. Preso $\mathfrak{p}_i \in \operatorname{Ass}(0)$, abbiamo che $\mathfrak{p}_i = \sqrt{0 : a_i}$ per qualche $a_i \in A$, per ogni $i = 1, \ldots, n$. Abbiamo pertanto dimostrato "$\supseteq$".

Sia ora $0 \neq a \in \mathcal{D}(A)$; ciò vuol dire che $a \notin \bigcap_{i=1}^n \mathfrak{q}_i$. Avremo dunque, grazie a **T.**156, che $\sqrt{0 : a} = \bigcap_{i=1}^n \sqrt{\mathfrak{q}_i : a} = \bigcap_{i \,:\, a \notin \mathfrak{q}_i} \mathfrak{p}_i$, che è contenuto in qualche $\mathfrak{p}_i$, per come abbiamo scelto a. Dunque anche l'altra inclusione è provata.

Vediamo ora il comportamento degli ideali primari rispetto alla localizzazione.

T. 160. Sia $\mathfrak{q}$ un ideale $\mathfrak{p}$-primario di A.

1. Sia $S \subseteq A$ un sottoinsieme moltiplicativo. Se $S \cap \mathfrak{p} = \emptyset$, allora $S^{-1}\mathfrak{q}$ è $S^{-1}\mathfrak{p}$-primario e $(S^{-1}\mathfrak{q})^c = \mathfrak{q}$; se invece $S \cap \mathfrak{p} \neq \emptyset$ allora $S^{-1}\mathfrak{q} = S^{-1}A$.

2. Sia $I = \cap_{i=1}^{n} \mathfrak{q}_i$ una decomposizione primaria minimale di I, con $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$. Sia inoltre $k \in \mathbb{N}$, con $k \leq n$, tale che $\mathfrak{p}_i \cap S = \emptyset$ per ogni $i = 1, \ldots, k$ e $\mathfrak{p}_i \cap S \neq \emptyset$ altrimenti. Allora

$$(S^{-1}I)^c = \bigcap_{i=1}^{k} \mathfrak{q}_i \,.$$

3. Sia $S = A \setminus \bigcup_{\mathfrak{p} \in \operatorname{Min} I} \mathfrak{p}$, allora S è un sottoinsieme moltiplicativo e

$$(S^{-1}I)^c = \bigcap_{\sqrt{\mathfrak{q}} \in \operatorname{Min} I} \mathfrak{q} \,.$$

Dimostrazione T. *160* 1. È sufficiente dimostrare che $S^{-1}\mathfrak{q}$ è primario in $S^{-1}A$ quando $S \cap \mathfrak{p} = \emptyset$, le altre affermazioni seguono da **T.**138 e da $S^{-1}\sqrt{\mathfrak{q}} = \sqrt{S^{-1}\mathfrak{q}}$, cf. **T.**140.4.

Supponiamo allora $S \cap \mathfrak{p} = \emptyset$ e sia $\frac{a}{s}\frac{b}{t} = \frac{q}{u} \in S^{-1}\mathfrak{q}$ con $\frac{a}{s} \notin S^{-1}\mathfrak{q}$, cioè tale che $wa \notin \mathfrak{q}$ per ogni $w \in S$. Esiste allora $w \in S$ tale che $wuab = wstq \in \mathfrak{q}$ e, dato che $uwa \notin \mathfrak{q}$ si ha $b \in \sqrt{\mathfrak{q}}$ e $\frac{b}{t} \in S^{-1}\sqrt{\mathfrak{q}} = \sqrt{S^{-1}\mathfrak{q}}$, come volevamo.

2. Segue direttamente da **T.**138.2 e **T.**140.3.

3. È un caso particolare del punto 2.

Come corollario del precedente risultato otteniamo il secondo teorema di unicità.

Dato un ideale I decomponibile in un anello A, e una sua decomposizione primaria minimale $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$, eventualmente riordinando gli indici, possiamo assumere la convenzione di scrivere

$$I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_k \cap \mathfrak{q}_{k+1} \cap \ldots \cap \mathfrak{q}_n,$$

con $\operatorname{Ass} I = \{\mathfrak{p}_i = \sqrt{\mathfrak{q}_i} \colon i = 1, \ldots n\}$, $\operatorname{Min} I = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ e $k \leq n$.

Teorema di unicità /II

T. 161. Sia $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$ una decomposizione primaria minimale dell'ideale $I \subseteq A$ scritta come sopra; allora, gli ideali primari $\mathfrak{q}_1, \ldots, \mathfrak{q}_k$ associati ai primi minimali sono univocamente determinati.

In particolare, per ogni $i = 1, \dots, k$,

$$\mathfrak{q}_i = (IA_{\mathfrak{p}_i})^c.$$

Dimostrazione ***T.*** *161* Sia $S_i = A \setminus \mathfrak{p}_i$, per un i fissato tra 1 e k; allora, per ogni $j \neq i$, $S_i \cap \mathfrak{p}_j \neq \emptyset$, altrimenti $\mathfrak{p}_j \subset \mathfrak{p}_i$ negherebbe la minimalità di $\mathfrak{p}_i$. Da **T.**160.1 segue allora che $IA_{\mathfrak{p}_i} = S_i^{-1}I = S_i^{-1}\mathfrak{q}_i$ e $(IA_{\mathfrak{p}_i})^c = \mathfrak{q}_i$.

Rivisitiamo la definizione di primo associato, generalizzando quanto visto in precedenza alla situazione di un A-modulo M. Un primo associato ad M è per definizione un elemento dell'insieme

$$\operatorname{Ass} M = \{\mathfrak{p} \in \operatorname{Spec} A \ : \ \exists\, 0 \neq m \in M \ \text{ tale che } \ \mathfrak{p} = \operatorname{Ann} m = 0 : m\}\,.$$

T. 162. 1. Gli elementi massimali dell'insieme $\Sigma = \{\operatorname{Ann} m \ : \ 0 \neq m \in M\}$ sono ideali primi, e quindi appartengono ad $\operatorname{Ass} M$.

2. Se A è noetheriano e $M \neq 0$ allora $\operatorname{Ass} M \neq \emptyset$.

Dimostrazione ***T.*** *162* 1. Sia $0 \neq m \in M$ tale che $\operatorname{Ann} m$ è massimale in Σ. Sia $ab \in \operatorname{Ann} m$; allora $abm = 0$. Se $bm = 0$, allora $b \in \operatorname{Ann} m$; altrimenti $a \in \operatorname{Ann}(bm) \supseteq \operatorname{Ann} m$. Per l'ipotesi di massimalità si deve avere $\operatorname{Ann}(bm) = \operatorname{Ann} m$ e quindi $a \in \operatorname{Ann} m$.

2. Siano A noetheriano e $M \neq 0$; allora l'insieme $\Sigma = \{\operatorname{Ann} m \ : \ 0 \neq m \in M\}$, che è non vuoto, ha elementi massimali che, per il punto precedente, sono elementi di $\operatorname{Ass} M$.

T. 163. Siano M un A-modulo e $\mathfrak{p} \in \operatorname{Spec} A$; allora $\mathfrak{p} \in \operatorname{Ass} M$ se e solo se esiste un omomorfismo iniettivo $A/\mathfrak{p} \longrightarrow M$, e dunque M contiene un sottomodulo isomorfo a $A/\mathfrak{p}$.

Dimostrazione ***T.*** *163* Sia $\mathfrak{p} = \operatorname{Ann} m$ e $f\colon A \xrightarrow{\cdot m} M$ definita da $f(1) = m$. Allora $\operatorname{Ker} f = \operatorname{Ann} m = \mathfrak{p}$ e dal primo teorema di omomorfismo si ha la tesi.

Viceversa, supponiamo che esista $j\colon A/\mathfrak{p} \longrightarrow M$ iniettiva con $m = j(\overline{1})$. Sia $a \in \mathfrak{p}$; allora $am = aj(\overline{1}) = j(\overline{a}) = 0$, da cui segue che $\mathfrak{p} \subset \operatorname{Ann} m$. Sia ora $a \in \operatorname{Ann} m$; allora $0 = am = aj(\overline{1}) = j(\overline{a})$ e dall'iniettività di j segue che $a \in \mathfrak{p}$. Perciò $\operatorname{Ann} m \subseteq \mathfrak{p}$, come volevamo.

T. 164. 1. Sia $0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$ una successione esatta di A-moduli. Allora

$$\operatorname{Ass} N \subseteq \operatorname{Ass} M \subseteq \operatorname{Ass} N \cup \operatorname{Ass} P.$$

2. Siano A ed M rispettivamente un anello e un A-modulo non nulli, entrambi noetheriani; allora esiste una catena di sottomoduli $M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ e un insieme di ideali primi $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ tali che $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$, per $i = 1, \ldots, n$.
3. [Terzo teorema di finitezza] Siano A un anello noetheriano e M un A-modulo finitamente generato. Allora $\operatorname{Ass} M$ è finito.

Dimostrazione T. 164 1. Sia $\mathfrak{p} \in \operatorname{Ass} N$ allora esiste $j\colon A/\mathfrak{p} \longrightarrow N$ iniettiva, per **T.**163.1. Dato che $f \circ j\colon A/\mathfrak{p} \longrightarrow M$ è ancora iniettiva $\mathfrak{p} \in \operatorname{Ass} M$, sempre per **T.**163.1.

Se $\mathfrak{p} = 0 : m \in \operatorname{Ass} M$, allora esiste $j\colon A/\mathfrak{p} \longrightarrow M$, $\overline{1} \mapsto m$, iniettiva. Ci sono due casi: $j(A/\mathfrak{p}) \cap \operatorname{Ker} g = 0$, allora $g \circ j\colon A/\mathfrak{p} \longrightarrow P$ rimane iniettiva e $\mathfrak{p} \in \operatorname{Ass} P$. Altrimenti $j(A/\mathfrak{p}) \cap \operatorname{Im} f \neq 0$; allora esiste $0 \neq m_1 \in \operatorname{Im} f \cap j(A/\mathfrak{p})$. Sia $m_1 = f(n) = j(\overline{a}) = am$, per qualche $0 \neq n \in N$ e $a \notin \mathfrak{p}$, allora $\mathfrak{p} = 0 : m = 0 : am$. Infatti certamente $0 : m \subseteq 0 : am$. Sia ora b tale che $bam = 0$; pertanto $ba \in 0 : m$ che è primo e dunque, visto che $a \notin 0 : m$, $b \in 0 : m$.
Per l'iniettività di f, possiamo allora concludere che $\operatorname{Ann} n = \operatorname{Ann} f(n) = \operatorname{Ann}(am) = \operatorname{Ann} m = \mathfrak{p}$ e quindi $\mathfrak{p} \in \operatorname{Ass} N$.

2. Dato che $M \neq 0$, avremo $\operatorname{Ass} M \neq \emptyset$ per **T.**162.2; sia $\mathfrak{p}_1 = 0 : m_1 \in \operatorname{Ass} M$, allora esiste $j\colon A/\mathfrak{p}_1 \longrightarrow M$ iniettiva, per **T.**163.1. Se j è anche surgettiva allora $A/\mathfrak{p}_1 \simeq M$, altrimenti $j(A/\mathfrak{p}_1) = M_1 = \langle m_1 \rangle \subset M$. Indichiamo con $M_0 = 0$. Allora $M_1 \simeq M_1/M_0 \simeq A/\mathfrak{p}_1$. Quindi se $M_1 = M$ abbiamo concluso; altrimenti $\operatorname{Ass}(M/M_1) \neq \emptyset$; sia dunque $\mathfrak{p}_2 = 0 : \overline{m_2} \in \operatorname{Ass}(M/M_1)$ e $j\colon A/\mathfrak{p}_2 \longrightarrow M/M_1$ iniettiva. Se è surgettiva allora $M_2 = M$ e abbiamo concluso; altrimenti sia $M_2 = \langle m_1, m_2 \rangle \supsetneq \langle m_1 \rangle = M_1$. Così procedendo troviamo una catena di sottomoduli con la proprietà richiesta e il processo termina perché M è noetheriano.

3. Siano $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ come nel punto precedente e mostriamo la tesi per induzione su n. Se $n = 1$ allora $M \cong A/\mathfrak{p}$, con $\mathfrak{p} \in \operatorname{Spec} A$ e quindi $\operatorname{Ass} M = \{\mathfrak{p}\}$, perché $\operatorname{Ass}(A/\mathfrak{p}) = \{\mathfrak{p}\}$, se consideriamo $A/\mathfrak{p}$ come A-modulo. Vediamo il passo induttivo: sappiamo che $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$ e quindi la successione $0 \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow A/\mathfrak{p}_i \longrightarrow 0$ è esatta. Dal punto 1 allora segue che $\operatorname{Ass} M_i \subseteq \operatorname{Ass} M_{i-1} \cup \{\mathfrak{p}_i\}$. Pertanto, dall'ipotesi induttiva segue che $\operatorname{Ass} M_i$ è finito.

7.3 Anelli e moduli artiniani

Alcune delle proprietà che valgono per gli anelli e moduli noetheriani hanno analoghi per gli anelli e moduli artiniani, anche se vedremo nel seguito che una vera e propria simmetria non c'è, cf. **T.**171.

T. 165. Siano A un anello, I un ideale di A e M, N, P A-moduli.
Sia $0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$ una successione esatta; allora M è artiniano se e solo se N e P sono artiniani.

In particolare, se A è artiniano e I è un ideale di A, allora A/I è artiniano.

***Dimostrazione* T. 165** La dimostrazione è del tutto analoga a quella di **T.**152.2.

T. 166. Sia A un anello artiniano. Allora

1. $\operatorname{Spec} A = \operatorname{Max} A$, ovvero gli ideali primi di A sono massimali;
2. esistono solo un numero finito di ideali massimali in A;
3. il nilradicale $\mathcal{N}(A)$ è nilpotente, ossia esiste $n \in \mathbb{N}$ tale che $\mathcal{N}(A)^n = 0$.

***Dimostrazione* T. 166** 1. Sia $\mathfrak{p} \subset A$ un ideale primo e $B = A/\mathfrak{p}$; B è un dominio di integrità e dimostriamo che è un campo. Sia $b \in B$ un elemento non nullo e consideriamo la catena discendente di ideali $B \supseteq (b) \supseteq (b^2) \supseteq \cdots$; per ipotesi la catena si stabilizza ed esiste k tale che $(b^k) = (b^{k+1})$. Pertanto $b^k \in (b^{k+1})$ ed esiste $c \in B$ tale che $b^k = cb^{k+1}$. Da ciò segue che $b^k(1-cb) = 0$ e, poiché B è un dominio, $cb = 1$ come volevamo.

2. Consideriamo la famiglia $\mathcal{F}$ degli ideali di A che si possono scrivere come intersezione di un numero finito di ideali massimali. Tale famiglia è non vuota

(perché?) e dunque esiste un elemento minimale $I_0 = \cap_{i=1}^{k} \mathfrak{m}_i \in \mathcal{F}$, cf. **T.**150. Per ogni ideale massimale $\mathfrak{m}$ di A avremo che $I_0 \cap \mathfrak{m} = I_0$ per la minimalità di I_0. Allora $\mathfrak{m} \supseteq \cap_{i=1}^{k} \mathfrak{m}_i$ e pertanto $\mathfrak{m} \supseteq \mathfrak{m}_i$ per qualche i, cf. **T.** 12.2. Per la massimalità di $\mathfrak{m}_i$, deve essere allora che $\mathfrak{m} = \mathfrak{m}_i$ e abbiamo concluso.

3. Per d.c.c., esiste k tale che la catena discendente $\mathcal{N}(A) \supseteq \cdots \supseteq \mathcal{N}(A)^k = \mathcal{N}(A)^{k+1} = I$. Supponiamo per assurdo che $I \neq 0$; allora la famiglia $\mathcal{F}$ di tutti gli ideali J tali che $JI \neq 0$ è non vuota (perché?); ne segue che $\mathcal{F}$ possiede un elemento minimale J_0. Allora esiste $b \in J_0$ tale che $bI \neq 0$ e $(b) \subseteq J_0$, e quindi deduciamo che $J_0 = (b)$ per la minimalità di J_0, con $b \neq 0$. Dato che $bI \in \mathcal{F}$ e $(bI)I = bI^2 = bI \neq 0$, ancora per la minimalità osserviamo che $bI = (b)$. Avremo dunque che $b = bc$, con $c \in I$, da cui $b = bc = bc^2 = \cdots = bc^h = \cdots$. Dato che $c \in I$ è nilpotente, cioè esiste un intero positivo s tale che $c^s = 0$, possiamo concludere che $b = bc^s = 0$, trovando la contraddizione cercata.

T. 167. Sia $(A, \mathfrak{m})$ un anello artiniano locale; allora ogni elemento di A è invertibile o nilpotente.

Dimostrazione T. *167* In un anello locale ogni elemento di $A \setminus \mathfrak{m}$ è invertibile, dunque basta mostrare che ogni elemento di $\mathfrak{m}$ è nilpotente. Dato che A è artiniano, ogni ideale primo è massimale per **T.**166.1. Di conseguenza, $\mathcal{N}(A) = \mathfrak{m}$ e la tesi segue da **T.**166.3.

Il prossimo enunciato generalizza quanto avevamo visto nella discussione che seguiva la dimostrazione di **T.**72.

T. 168. [Teorema di struttura degli anelli artiniani] Sia A un anello artiniano; allora A è isomorfo ad una somma diretta finita di anelli artiniani locali.

Dimostrazione T. *168* Per **T.**166, A possiede solo un numero finito di ideali primi $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ che sono massimali. Inoltre, esiste k tale che $0 = \mathcal{N}(A)^k = (\bigcap_{i=1}^{s} \mathfrak{m}_i)^k \supseteq \prod_{i=1}^{s} \mathfrak{m}_i^k$. Allora, visto che gli ideali $\mathfrak{m}_i^k$ sono a coppie comassimali, per il teorema cinese del resto **T.**20 avremo che

$$A \simeq {}^{A}\!/_{0} \simeq {}^{A}\!/_{\prod_{i=1}^{s} \mathfrak{m}_i^k} \simeq \prod_{i=1}^{s} A/\mathfrak{m}_i^k,$$

ove gli anelli $A/\mathfrak{m}_i^k$ sono anelli artiniani locali.

T. 169. Sia K un campo e V un K-spazio vettoriale. I seguenti fatti sono equivalenti:

1. $\dim_K V < \infty$;
2. V è un K-modulo noetheriano;
3. V è un K-modulo artiniano.

Dimostrazione T. *169* È ovvio che $1 \Rightarrow 2$ e $1 \Rightarrow 3$, dato che $V \simeq K^n$. Vediamo che $2 \Rightarrow 1$ e $3 \Rightarrow 1$. Se la dimensione di V non fosse finita, esisterebbe un insieme infinito $\{v_i\}$ di vettori linearmente indipendenti di V. Al variare di $n \in \mathbb{N}$, i sottospazi $V_n = \langle v_1, \ldots, v_n \rangle_K$ e $W_n = \langle v_n, v_{n+1}, \ldots \rangle_K$, definiscono rispettivamente una catena ascendente e una catena discendente infinita di sottospazi di V.

T. 170. Siano A un anello e $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ ideali massimali di A non necessariamente distinti; allora

$$A/\prod_{i=1}^{n} \mathfrak{m}_i \quad \text{è artiniano se e solo se è noetheriano}\,.$$

In particolare, se $\prod_{i=1}^{n} \mathfrak{m}_i = 0$, allora A è artiniano se e solo se è noetheriano.

Dimostrazione T. *170* Dimostriamo l'enunciato per induzione su n. Se $n = 1$, allora $A/\mathfrak{m}_1$ è un campo, che è artiniano e noetheriano. Sia ora $n > 1$. Consideriamo $N = \left(\prod_{i=1}^{n-1} \mathfrak{m}_i\right) / \left(\prod_{i=1}^{n} \mathfrak{m}_i\right)$ e la successione esatta

$$0 \longrightarrow N \longrightarrow A/\prod_{i=1}^{n} \mathfrak{m}_i \longrightarrow A/\prod_{i=1}^{n-1} \mathfrak{m}_i \longrightarrow 0\,.$$

Si ha che N è un $(A/\mathfrak{m}_n)$-spazio vettoriale, cf. **T.**85; per **T.**169 è dunque artiniano se e solo se noetheriano. Inoltre $A/\prod_{i=1}^{n-1} \mathfrak{m}_i$ è artiniano se e solo se noetheriano per ipotesi induttiva, quindi la tesi segue da **T.**152.2 e **T.**165.

T. 171. [Caratterizzazione degli anelli artiniani]
Un anello è artiniano se e solo se è noetheriano di dimensione 0.

***Dimostrazione T.** 171* Sia A è un anello artiniano; allora ogni ideale primo è massimale e dunque $\dim A = 0$. Inoltre, vale che un prodotto $\prod_{i=1}^{s} \mathfrak{m}_i^k$ degli ideali massimali di A, è nullo, come abbiamo visto ad esempio nella dimostrazione di **T.**168. Per **T.**170, A è dunque noetheriano.

Viceversa, se $\dim A = 0$, si avrà che $\sqrt{0} = \bigcap_{i=1}^{s} \mathfrak{m}_i$ poiché in A gli ideali primi sono massimali; se inoltre A è noetheriano, esiste un intero k tale che $\prod_{i=1}^{s} \mathfrak{m}_i^k \subseteq \sqrt{0}^{\,k} \subseteq 0$. Quindi, ancora per **T.**170, A è artiniano.

Parte II

Esercizi

8

Esercizi su anelli e ideali

E. 1. (→ p. 255) Sia S un sottoinsieme di un anello A; mostrare che (S) è l'intersezione di tutti gli ideali che contengono S.

E. 2. (→ p. 255) Sia A un anello. Provare che i seguenti fatti sono equivalenti:

1. A è un dominio;
2. [Legge di cancellazione] per ogni $a, b, c \in A$, con $a \neq 0$, si ha $ab = ac \iff b = c$;
3. $A \setminus \{0\}$ è chiuso rispetto alla moltiplicazione.

E. 3. (→ p. 255) Sia $A = \mathbb{Z}/(n)$.

1. Determinare $\mathcal{D}(A)$, A^* e gli ideali primi e gli ideali massimali di A, quando $n = 24$.
2. Stesso esercizio per $n = 17$.
3. Determinare per quali valori di n l'anello A è un dominio e per quali è un campo.

E. 4. (→ p. 256) Sia a un elemento nilpotente di A. Provare che $1 + a$ è un'unità di A. Dedurre che la somma di un elemento nilpotente e di un'unità è un'unità.

E. 5. (→ p. 256) Sia $f(x) = \sum_{i=0}^{n} a_i x^i$ un polinomio di $A[x]$. Provare che:

1. f è invertibile se e solo se a_0 è invertibile e $a_1, \ldots, a_n$ sono nilpotenti;
2. f è nilpotente se e solo se $a_0, \ldots, a_n$ sono nilpotenti;
3. f è un divisore di zero se e solo se esiste $0 \neq a \in A$ tale che $af = 0$;

E. 6. (→ p. 256) Provare che, per ogni anello A, il radicale di Jacobson e il nilradicale di $A[x]$ coincidono.

E. 7. (→ p. 257) Sia $I \subset A$ un ideale. Provare che, se $\bigcap_{n\in\mathbb{N}} I^n = 0$, allora $1 + a \notin \mathcal{D}(A)$ per ogni $a \in I$.

E. 8. (→ p. 257) Siano A un anello e I un ideale di A. Provare che l'insieme $I[x] = \{f(x) = \sum_i a_i x^i \in A[x] \colon a_i \in I \text{ per ogni } i\}$ dei polinomi di $A[x]$ che hanno tutti i coefficienti in I è un ideale di $A[x]$.
Provare inoltre che $A[x]/I[x] \simeq \left(A/I\right)[x]$.

E. 9. (→ p. 257) [Lemma di Gauss] Dato un polinomio $f = \sum_{i=0}^{n} f_i x^i \in A[x]$, diciamo che f è *primitivo* se e solo se $(f_0, \ldots, f_n) = (1)$.
Provare che se f e g sono primitivi, allora anche fg è tale.

E. 10. (→ p. 257) Provare che $f, g \in A[x]$ sono primitivi se e solo se fg è primitivo.

E. 11. (→ p. 257) Sia A un anello per cui valgono le seguenti condizioni:
(i) il radicale di Jacobson $\mathcal{J}(A)$ è un ideale primo e non nullo;
(ii) ogni ideale $I \supseteq \mathcal{J}(A)$ è principale;
(iii) $\mathcal{D}(A) \subseteq \mathcal{J}(A)$.
Provare che A è un anello locale con ideale massimale $\mathcal{J}(A)$.

E. 12. (→ p. 258) Sia A un anello locale con ideale massimale $\mathfrak{m} = (m)$ principale. Provare che:

1. per ogni $0 \neq a, b \in \mathfrak{m}$ si ha che: $(a) = (b) \iff a = bu$, con $u \in A^*$;
2. se $\mathfrak{m} \neq (0)$, allora m è un elemento irriducibile di A.

E. 13. (→ p. 258) Siano A un anello e I, J ideali di A. Provare che se $I \subseteq \mathcal{J}(A)$ e $(I, J) = 1$, allora $J = (1)$.

E. 14. (→ p. 258) Un anello locale A non contiene idempotenti diversi da $0, 1$.

E. 15. (→ p. 258) Sia A un anello booleano. Provare che

1. $2a = 0$ per ogni $a \in A$;
2. ogni ideale primo $\mathfrak{p}$ è massimale e $A/\mathfrak{p}$ è un campo con due elementi;
3. ogni ideale finitamente generato è principale.

E. 16. (→ p. 258) Provare che, se ogni ideale di A è primo, allora A è un campo.

E. 17. (→ p. 258) [Operazioni in $\mathbb{Z}$] Sia $A = \mathbb{Z}$ e siano $I = (m)$, $J = (n)$, $H = (h)$ ideali di A. Provare che:

1. $I + J = (\gcd(m, n))$;
2. $I \cap J = (\operatorname{lcm}(m, n))$;
3. $IJ = (mn)$;
4. $I : J = (m/\gcd(m, n))$;
5. $I \cap (J + H) = (I \cap J) + (I \cap H)$;
6. $(I + J)(I \cap J) = IJ$.

E. 18. (→ p. 259) [Proprietà del quoziente di ideali] Siano $I, J, H, I_\alpha, J_\beta$ ideali di un anello A, con α e β che variano in insiemi di indici Λ e Δ rispettivamente. Verificare che:

1. $I \subseteq I : J$;
2. $(I : J)J \subseteq I$;
3. $(I : J) : H = I : JH = (I : H) : J$;
4. $\left(\bigcap_{\alpha\in\Lambda} I_\alpha\right) : J = \bigcap_{\alpha\in\Lambda}(I_\alpha : J)$;
5. $I : \sum_{\beta\in\Delta} J_\beta = \bigcap_{\beta\in\Delta} I : J_\beta$.

E. 19. (→ p. 260) Provare con un esempio che, relativamente alle operazioni tra ideali, in generale non vale la proprietà distributiva della somma rispetto all'intersezione.

E. 20. (→ p. 260) Siano $I \subset R = K[x_1, \ldots, x_n]$ un ideale e $f \in R$; provare che

$$I : (f) = \frac{1}{f}(I \cap (f)).$$

E. 21. (→ p. 260) Siano I, J, H ideali di un anello A. Provare che:

1. se $I + H = A$ e $J + H = A$, allora $I \cap J + H^n = A$ per ogni $n \in \mathbb{N}$;
2. se $I \subseteq H$, $I \cap J = H \cap J$, e $I/(I \cap J) = H/(H \cap J)$, allora $I = H$.

E. 22. (→ p. 260) Siano I, $H_1, \ldots, H_n \subseteq A$ ideali. Provare che se $I + H_i = A$ per ogni i, allora $I + H_1 H_2 \cdots H_n = A$.

E. 23. (→ p. 260) Siano I e J ideali di A. Provare che

1. se $\sqrt{IJ} = A$, allora $I = A$ e $J = A$;
2. se $\mathfrak{p} \subset A$ è un ideale primo tale che $IJ = \mathfrak{p}$, allora $I = \mathfrak{p}$ o $J = \mathfrak{p}$.

E. 24. (→ p. 260) Siano $I, J \subseteq A$ ideali. Provare che

1. $I + J = (1)$ se e solo se $\sqrt{I} + \sqrt{J} = (1)$;
2. $\sqrt{I + \sqrt{J}} = \sqrt{I + J}$.

E. 25. (→ p. 261) Mostrare con un esempio che, in generale, $\sqrt{I} + \sqrt{J} \neq \sqrt{I + J}$.

E. 26. (→ p. 261) Siano $A = K[x, y]$ e $I = (x^2, xy)$. Provare che $\sqrt{I}$ è primo e I non è un primario.

E. 27. (→ p. 261) Sia A un anello dotato della seguente proprietà: ogni ideale $I \not\subseteq \mathcal{N}(A)$ possiede un elemento idempotente diverso da zero. Provare che $\mathcal{J}(A) = \mathcal{N}(A)$.

E. 28. (→ p. 261) Siano A un anello e $\mathcal{N}(A)$ il suo nilradicale. Provare che i seguenti fatti sono equivalenti.

1. A possiede un unico ideale primo.
2. Ogni elemento di A è invertibile oppure nilpotente.
3. $A/\mathcal{N}(A)$ è un campo.

E. 29. (→ p. 261) Sia $\{E_\alpha\}_{\alpha \in \Lambda}$ una famiglia di sottoinsiemi di un anello A. Mostrare che $\sqrt{\cup_\alpha E_\alpha} = \cup_\alpha \sqrt{E_\alpha}$.

E. 30. (→ p. 262) Provare che, in un anello A, si ha $\mathcal{D}(A) = \bigcup_{0 \neq a \in A} \sqrt{\operatorname{Ann} a}$.

E. 31. (→ p. 262) Siano A un anello e $\mathcal{J}(A)$ il suo radicale di Jacobson. Provare che:

1. $a \in A$ è invertibile se e solo se $\overline{a}$ è invertibile in $A/\mathcal{J}(A)$;
2. se $a \in \mathcal{J}(A)$ è idempotente, allora $a = 0$.

E. 32. (→ p. 262) Sia A un anello e $a \in A$. Provare che se $a \in \mathcal{J}(A)$ ed è idempotente modulo un ideale I di A, allora $a \in I$.

E. 33. (→ p. 262) Sia A un dominio infinito con un numero finito di elementi invertibili. Dimostrare che A possiede un numero infinito di ideali massimali.

E. 34. (→ p. 262) Siano A e B anelli. Descrivere gli ideali, gli ideali primi e gli ideali massimali di $A \times B$.

E. 35. (→ p. 263) Provare che ogni ideale di $A = \prod_{i=1}^{n} A_i$ è della forma $I = \prod_{i=1}^{n} I_i$, con I_i ideale dell'anello A_i, per ogni i; descrivere inoltre gli ideali primi e massimali di A.

E. 36. (→ p. 263) 1. Provare che un anello A è prodotto diretto di un numero finito di campi se e solo contiene solo un numero finito di ideali e $\mathcal{J}(A) = (0)$.

2. Provare che un anello finito è prodotto diretto di campi se e solo se non contiene nilpotenti diversi da zero.

E. 37. (→ p. 264) Si consideri l'anello $A = \mathbb{Z} \times \mathbb{Z}/(36) \times \mathbb{Q}$. Determinare:

1. il nilradicale di A;
2. gli elementi idempotenti di A;
3. gli ideali di A e dire se sono tutti principali;
4. gli ideali primi e gli ideali massimali di A.

E. 38. (→ p. 264) Siano $p, p_1, \ldots, p_n$ primi distinti di $\mathbb{Z}$.

1. Verificare che l'anello $A_p = \left\{ \frac{a}{b} \in \mathbb{Q} \colon\ b \not\equiv 0 \mod p \right\}$ è locale e descriverne l'ideale massimale ed il campo residuo.
2. Verificare che l'anello $A_{p_1,\ldots,p_n} = \left\{ \frac{a}{b} \in \mathbb{Q} \colon\ b \not\equiv 0 \mod p_j\,,\ 1 \leq j \leq n \right\}$ è semilocale e descriverne gli ideali massimali.

E. 39. (→ p. 265) Provare che il prodotto di un numero finito di anelli semilocali è semilocale, ma non è vero il viceversa.

E. 40. (→ p. 265) Sia A un anello tale che, per ogni $a \in A$, si ha $a^n = a$ per qualche $n > 1$. Provare che ogni ideale primo di A è massimale.

E. 41. (→ p. 265) Siano A un anello e $\Sigma = \{I \subset A\colon I \text{ ideale},\ I \subseteq \mathcal{D}(A)\}$ parzialmente ordinato rispetto a $\subseteq$. Provare che:

1. Σ possiede elementi massimali e ogni elemento massimale è un ideale primo;
2. $\mathcal{D}(A)$ è unione di ideali primi.

E. 42. (→ p. 266) Sia A un anello tale che ogni ideale primo è principale. Allora A è PIR.

E. 43. (→ p. 266) Sia A un anello tale che ogni ideale primo è finitamente generato. Allora ogni ideale di A è finitamente generato, ovvero A è noetheriano.

E. 44. (→ p. 267) Sia $f : A \longrightarrow B$ un omomorfismo di anelli. Mostrare che:

1. $\operatorname{Ker} f$ è un ideale di A;
2. f è iniettiva se e solo se $\operatorname{Ker} f = 0$;
3. $\operatorname{Im} f$ è un sottoanello di B.

E. 45. (→ p. 267) Se $A = B = \mathbb{Z}$ esiste un unico omomorfismo di anelli $f : A \longrightarrow B$.

E. 46. (→ p. 267) Siano A un anello, $I \subseteq A$ un ideale e $a \in A$ fissato. Si consideri l'insieme $J = \{f \in A[x]\colon\ f(a) \in I\}$. Provare che:

1. J è un ideale;
2. J è primo se e solo se I è primo.

Se $A = \mathbb{Q}[y],\ a = y - 1$ e $I = (y - 2)$, trovare J.

E. 47. (→ p. 267) Sia A un anello non banale. Provare che i seguenti fatti sono equivalenti:

1. A è un campo;
2. gli unici ideali di A sono (0) e (1);
3. ogni omomorfismo di A in un anello $B \neq 0$ è iniettivo.

E. 48. (→ p. 268) Si consideri l'omomorfismo di immersione $A \xrightarrow{j} A[x]$ e sia $I[x] = \{f(x) = \sum_i a_i x^i \in A[x]\colon a_i \in I \text{ per ogni } i\}$, cf. **E.**8. Provare che:

1. $I[x]$ è l'ideale esteso I^e rispetto ad j;
2. se I è primo allora $I[x]$ è primo.

È vero che se I è massimale allora $I[x]$ è massimale?

E. 49. (→ p. 268) Siano $f : A \longrightarrow B$ un omomorfismo di anelli e $I \subset A$ un ideale tale che $\operatorname{Ker} f \subseteq I$. Provare che:

1. $(f(\sqrt{I})) \subseteq \sqrt{(f(I))}$, i.e. $(\sqrt{I})^e \subseteq \sqrt{I^e}$;
2. se f è surgettivo allora $(\sqrt{I})^e = \sqrt{I^e}$;
3. se $J \subset B$ è un ideale di B allora $\sqrt{J^c} = (\sqrt{J})^c$.

E. 50. (→ p. 268) Sia i una radice quarta primitiva dell'unità e, per ogni primo dispari p, sia ζ_p una radice primitiva p-esima dell'unità. Consideriamo gli omomorfismi di inclusione $\mathbb{Z} \longrightarrow \mathbb{Z}[i]$ e $\mathbb{Z} \longrightarrow \mathbb{Z}[\zeta_p]$.

1. Mostrare che in $\mathbb{Z}[i]$ si ha:
$$(p)^e = \begin{cases} (1+i)^2 & \text{se } p = 2 \\ (a+ib)(a-ib) & \text{se } p \equiv 1 \mod 4 \\ (p) & \text{se } p \equiv 3 \mod 4. \end{cases}$$
2. Mostrare che per ogni $a \in (\mathbb{Z}/(p))^*$ si ha $\dfrac{1-\zeta_p^a}{1-\zeta_p} \in \mathbb{Z}[\zeta_p]^*$ e dedurre che in $\mathbb{Z}[\zeta_p]$ si ha $(p)^e = (1-\zeta_p)^{p-1}$.

E. 51. (→ p. 269) Siano A e B anelli commutativi con identità e sia $f\colon A \longrightarrow B$ un omomorfismo di anelli. Provare che:

1. $f(\mathcal{N}(A)) \subseteq \mathcal{N}(B)$;
2. se f è surgettivo allora $f(\mathcal{J}(A)) \subseteq \mathcal{J}(B)$;
3. se f non è surgettivo la conclusione del punto precedente non vale;
4. il contenimento del punto 2 può essere stretto;
5. se f è surgettivo e A è semilocale allora $f(\mathcal{J}(A)) = \mathcal{J}(B)$.

E. 52. (→ p. 270) Siano A e $I \subset A$ un ideale contenuto in $\mathcal{N}(A)$. Provare che A è locale se e solo se A/I è locale.

E. 53. (→ p. 270) Sia A un PID e siano $I, J \subset A$ ideali di A. Provare che $(I+J)^2 = I^2 + J^2$.

E. 54. (→ p. 270) Sia A un anello tale che $\mathcal{D}(A) \subseteq \mathcal{J}(A)$. Provare che due elementi $a, b \in A$ per cui $(a) = (b)$ sono associati.

E. 55. (→ p. 270) Sia A un PIR. Provare che, se $\mathcal{J}(A) = \mathcal{D}(A) \neq (0)$, allora A è un anello locale.

E. 56. (→ p. 270) Sia A un PID. Provare che:

1. a è irriducibile se e solo se $A/(a)$ è un campo;
2. gli ideali massimali di A sono gli ideali generati da elementi irriducibili.
3. Sia $A = K[x]$, con K campo, e sia $f \in A$ di grado positivo. Allora (f) è primo se e solo se f è irriducibile.

E. 57. (→ p. 271) Sia A un PID; provare che gli ideali primari di A sono generati da potenze di elementi primi.

E. 58. (→ p. 271) Sia A un anello. Provare che $A[x]$ è un PID se e solo se A è un campo.

E. 59. (→ p. 271) Sia A un PID. Provare che se d è massimo comun divisore di a e b allora esistono $u, v \in A$ tali che $ua + vb = d$.
Costruire poi un esempio di anello A per cui la proprietà precedente non è vera.

E. 60. (→ p. 271) Provare che nell'anello $\mathbb{Z}[\sqrt{-5}]$ l'elemento 3 è irriducibile, ma l' ideale (3) non è irriducibile.

E. 61. (→ p. 272) Sia A un dominio di integrità. Provare che se ogni catena ascendente di ideali principali di A è stazionaria allora A ha (UFD1).

E. 62. (→ p. 272) Provare che un dominio che è quoziente di un UFD non è necessariamente UFD.

E. 63. (→ p. 272) Siano A un anello e $a \in A$. Definiamo $I_a = \{ax - x\colon\ x \in A\}$ e diciamo che a è un elemento *quasi-regolare* se $I_a = A$. Provare che:

1. I_a è un ideale per ogni $a \in A$;
2. a è quasi-regolare se e solo se esiste $c \in A$ tale che $a + c - ac = 0$;
3. ogni elemento nilpotente di A è quasi-regolare;

4. se ogni elemento di A diverso da 1 è quasi-regolare allora A è un campo.

E. 64. (→ p. 273) Sia A un dominio d'integrità, che non è campo, e con la proprietà che ogni ideale proprio di A è prodotto di un numero finito di ideali massimali. Provare che:

1. se $\mathfrak{m} \subset A$ è un ideale massimale, allora per ogni $a \in \mathfrak{m} \setminus \{0\}$ esiste un ideale I tale che $I\mathfrak{m} = (a)$;
2. se J, H e $\mathfrak{m}$ sono ideali di A, con $\mathfrak{m}$ massimale, allora $J\mathfrak{m} = H\mathfrak{m}$ implica $J = H$.

E. 65. (→ p. 273) Sia A un anello e siano I, J ideali di A. Provare che:

1. se I è primario e $J \not\subseteq \sqrt{I}$, allora $\sqrt{I : J^m} = \sqrt{I}$ per ogni $m \geqslant 1$;
2. se $I = \sqrt{I}$ e $h \notin I$, allora $I : h$ è radicale.

E. 66. (→ p. 273) Sia $p = p(x) = \sum_{i\in\mathbb{N}} a_i x^i \in A[[x]]$. Mostrare che:

1. p è invertibile se e solo se a_0 è invertibile;
2. se p è nilpotente allora a_i è nilpotente, per ogni i. È vero il viceversa?
3. $p \in \mathcal{J}(A[[x]])$ se solo se $a_0 \in \mathcal{J}(A)$;
4. la contrazione ad A di un ideale massimale $\mathfrak{m}$ di $A[[x]]$ è un ideale massimale di A; mostrare inoltre che $\mathfrak{m}$ è generato da $\mathfrak{m}^c$ e x.

E. 67. (→ p. 274) Sia A un anello commutativo con identità e sia $I \subset A$ un ideale. Provare che, se un elemento $g \in A$ verifica $I : g^m = I : g^{m+1}$ per qualche $m \in \mathbb{N}$, allora:

1. per ogni $s \in \mathbb{N}_+$, $I : g^{m+s} = I : g^m$;
2. $I = (I : g^m) \cap (I, g^m)$.

E. 68. (→ p. 274) [Esistenza dei primi minimali] Dimostrare che l'insieme degli ideali primi di un anello $A \neq 0$ contiene elementi minimali rispetto all'inclusione. Dedurre che, dato un ideale I, l'insieme $\mathcal{V}(I) = \{\mathfrak{p} : \mathfrak{p} \in \operatorname{Spec} A, \mathfrak{p} \supseteq I\}$ contiene elementi minimali rispetto all'inclusione.

L'insieme degli elementi minimali di $\mathcal{V}(I)$ si denota con $\operatorname{Min} I$; se $I = 0$ si usa anche la notazione $\operatorname{Min} A$.

E. 69. (→ p. 275) Siano A un anello ridotto e $a \in A$ un divisore di zero; allora a appartiene a uno dei primi minimali di A.

E. 70. (→ p. 275) Si consideri l'anello $A = \mathbb{Z}[x, y]$ e l'ideale $I = (9x^2 - y, 7y^2 + 2x + y, 63)$ di A.

1. Provare che ogni ideale primo di A/I è massimale.
2. Provare che $A/I \simeq \mathbb{Z}/(9) \times (\mathbb{Z}/7)^2$.
3. Scrivere I come intersezione di ideali primari.
4. Se B è un dominio ed esiste un omomorfismo di anelli $f\colon B \longrightarrow A/I$ iniettivo, allora B è un campo.

E. 71. (→ p. 276) Provare che

$$\operatorname{Spec} \mathbb{Z}[x] = \{(0), (p), (f(x)), (p, g(x))\} \quad \text{e} \quad \operatorname{Max} \mathbb{Z}[x] = \{(p, g(x))\},$$

al variare di p primo in $\mathbb{Z}$, $f(x) \in \mathbb{Z}[x]$ irriducibile e $g(x) \in \mathbb{Z}[x]$ irriducibile modulo p.

re

9

Esercizi su anello di polinomi, basi di Gröbner, risultante e varietà

E. 72. (→ p. 276) $>$ è un buon ordinamento su $\mathbb{N}^n$ se e solo se ogni catena discendente in $\mathbb{N}^n$ è stazionaria.

E. 73. (→ p. 277) Provare che gli ordinamenti lex, deglex, degrevlex sono ordinamenti monomiali.

E. 74. (→ p. 277) Sia $>$ un ordinamento totale su $\mathbb{N}^n$ tale che se $\alpha > \beta$ allora $\alpha + \gamma > \beta + \gamma$ per ogni $\alpha, \beta, \gamma \in \mathbb{N}^n$. Dimostrare che $>$ è un ordinamento monomiale se e solo se $\alpha \geq 0$ per ogni $\alpha \in \mathbb{N}^n$.

E. 75. (→ p. 278) Sia $K \subset K'$ un'estensione di campi e $I \subset K[x_1, \ldots, x_n]$ un ideale; sia inoltre $I^e \subset K'[x_1, \ldots, x_n]$ l'ideale generato da I in $K'[x_1, \ldots, x_n]$. Allora, ogni base di Gröbner di I rispetto ad un ordinamento monomiale fissato è anche una base di Gröbner di I^e rispetto a tale ordinamento. In particolare, per ogni ordinamento, $E(I) = E(I^e)$.

E. 76. (→ p. 279) Siano $A = K[x_1, x_2]$ dotato dell'ordinamento lessicografico con $x_1 > x_2$, $f = x_1^4 x_2$, e $F = \{f_1 = x_1^3, f_2 = x_1^2 x_2 - x_2^2\}$. Mostrare che il resto della divisione di f per F non è unico.

E. 77. (→ p. 279) Siano $g_1 = z + x, g_2 = y - x \in \mathbb{Q}[x, y, z]$, $G = \{g_1, g_2\}$ e $I = (g_1, g_2)$; siano inoltre $>_1$ l'ordinamento lex dato da $x < y < z$ e $>_2$ l'ordinamento lex dato da $x > y > z$. Mostrare che G è una base di Gröbner di I rispetto a $>_1$ ma non rispetto a $>_2$.

E. 78. (→ p. 279) [Test di monomialità] Provare che I è monomiale se e solo se la sua base di Gröbner ridotta, rispetto ad un qualsiasi ordinamento monomiale, è costituita da monomi.

E. 79. (→ p. 280) Sia $I = (x^2 - xy, xz - y^2, yz^2 - z^4) \subseteq \mathbb{R}[x, y, z]$. Calcolare una base di Gröbner di I, rispetto all'ordinamento lessicografico con $x > y > z$. Dire se la base trovata è minimale e ridotta.

E. 80. (→ p. 281) Siano $I = (yz - y, xy + 2z^2, y - z) \subset \mathbb{Q}[x, y, z]$ e $f = x^3z - y^2$. Determinare se $f \in I$.

E. 81. (→ p. 281) Siano $I = (x^2 + xy + y^2, xy^2 + 1) \subset A = (\mathbb{Z}/(2))[x, y]$, $f_1 = x^3 + y^5 + xy^2$, $f_2 = y(x^2 + x + y)$; determinare se $\overline{f_1} = \overline{f_2}$ in A/I.

E. 82. (→ p. 281) Siano $I = (x^2y - y + x, y^2 - yx - x^2, x^3 + y - 2x) \subset \mathbb{Q}[x, y]$ e $f = y + x + 1$. Calcolare l'inverso di $\overline{f}$ in $A = \mathbb{Q}[x, y]/I$.

E. 83. (→ p. 282) Sia $I = (x^2y + z, xz + y) \subset \mathbb{Q}[x, y, z]$.

1. Calcolare la base di Gröbner ridotta G di I rispetto all'ordinamento deglex con $x > y > z$.
2. Calcolare la matrice di passaggio da G ai generatori dati.
3. Verificare che $f = xy^2z + y^3 \in I$; esprimere f come combinazione lineare degli elementi di G e dei generatori dati.

E. 84. (→ p. 282) Sia $I = (x^2 + 2y^2 - 3, x^2 + xy + y^2 - 3) \subset \mathbb{C}[x, y]$; calcolare $I \cap \mathbb{C}[y]$.

E. 85. (→ p. 283) Siano $I, J \subset K[x, y]$, con $I = (x(x + y)^2, y)$ e $J = (x^2, x + y)$; calcolare $I : J$.

E. 86. (→ p. 283) Siano K un campo di caratteristica 0, $I = (x^2 + y^2, x^3y^3 + y^4) \subset K[x, y]$ e $f = x^2 + 5x$. Determinare se $f \in \sqrt{I}$.

E. 87. (→ p. 283) Sia $I = (x^2y^2z^4,\ x^2 + y^2 + z^2 - 1,\ 2 - xy) \subset \mathbb{C}[x, y, z]$. Provare che:

1. $\dim_{\mathbb{C}} \mathbb{C}[x, y, z]/I$ è finita, e calcolarla;
2. se $J = (3x^3 + xz - 2,\ xy + z^2 - 2) \subset \mathbb{C}[x, y, z]$, allora $I + J = (1)$.

E. 88. (→ p. 284) Dato il sistema di equazioni polinomiali

$$\begin{cases} x + y = a \\ x^2 + y^2 = a^2 \\ x^3 + y^3 = a^5 \end{cases}$$

determinare per quali valori del parametro $a \in \mathbb{C}$ esistono soluzioni in $\mathbb{C}^2$ e in tal caso calcolarle.

E. 89. (→ p. 285) Siano $I = (x^2y + xz + yz, y^2z) \subset \mathbb{R}[x, y, z]$ e $A = \mathbb{R}[x, y, z]/I$.

1. Calcolare la base di Gröbner ridotta di I rispetto all'ordinamento lessicografico con $x > y > z$.
2. Trovare gli elementi nilpotenti di A.
3. Provare che $(x^2y^3, y^3z) \subset I \subset (x^2, z)$.

E. 90. (→ p. 285) Siano $f, g_1, g_2 \in K[x]$, e $a_m = \mathrm{lc}(f)$; allora

1. $\mathrm{Ris}(f, g_1\, g_2) = \mathrm{Ris}(f, g_1)\ \mathrm{Ris}(f, g_2)$;
2. sia $N = \deg(g_1 f + g_2)$; allora

$$\mathrm{Ris}(f, g_1\, f\ +\ g_2) = a_m^{N-\deg(g_2)}\ \mathrm{Ris}(f, g_2).$$

E. 91. (→ p. 285) [Costruzione di polinomi con radici assegnate]
Siano $f, g \in K[x]$ di gradi $m, n > 0$ rispettivamente. Siano $\alpha_1, \ldots, \alpha_m$ e $\beta_1, \ldots, \beta_n$ le radici in $\overline{K}$ di f e g rispettivamente; allora

1. il polinomio $r(x) = \mathrm{Ris}_y(f(x - y), g(y))$ ha radici $\alpha_i + \beta_j$;
2. il polinomio $r(x) = \mathrm{Ris}_y(f(x + y), g(y))$ ha radici $\alpha_i - \beta_j$;
3. il polinomio $r(x) = \mathrm{Ris}_y\left(y^m f(\frac{x}{y}), g(y)\right)$ ha radici $\alpha_i\beta_j$;
4. se $g(0) \neq 0$, il polinomio $r(x) = \mathrm{Ris}_y(f(xy), g(y))$ ha radici $\frac{\alpha_i}{\beta_j}$.

E. 92. (→ p. 286) Siano $f, g \in \mathbb{Q}[x]$ di grado positivo. Provare che, se $f(0) = 1$, allora per ogni intero pari k si ha che $\mathrm{Ris}(f, x^k g) = \mathrm{Ris}(f, g)$.

E. 93. (→ p. 287) Sia $A = \mathbb{Z}[x]$.

1. Siano $f, g \in A$ polinomi monici tali che $\mathrm{Ris}(f, g) = p$, con p primo in $\mathbb{Z}$. Provare che $(f, g) \cap \mathbb{Z} = (p)$.
2. Sia $I = (x^2 - 4x + 1, x^2 - x) \subset A$. Calcolare $I \cap \mathbb{Z}$ e descrivere A/I.

E. 94. (→ p. 287) 1. Siano K un campo perfetto, $0 \neq f \in K[x]$ e f' la sua derivata prima. Provare che l'anello $A = K[x]/(f)$ è ridotto se e solo se $\gcd(f, f') = 1$.
2. Sia $f \in \mathbb{Z}[x]$ un polinomio che verifica $\gcd(f, f') = 1$. Provare che l'insieme dei primi $p \in \mathbb{Z}$ per cui l'anello $(\mathbb{Z}/(p))[x]/(\overline{f})$ non è ridotto è un insieme finito.

E. 95. (→ p. 288) Siano $A = K[x, y, z]$, con K campo, e $I = (xz-y, yz-x) \subset A$. Decomporre $\mathbf{V}(I)$ come unione di varietà irriducibili.

E. 96. (→ p. 288) Sia $I = (x^2 - yzt, t - yt, zt - y)$ un ideale di $\mathbb{C}[x, y, z, t]$.

1. Trovare le componenti irriducibili di $\mathbf{V}(I)$.
2. Determinare se $f = xt + y \in I$.

E. 97. (→ p. 288) Sia $I = (x^2 + y^2 + z^2 - 1, x + y + z - 1) \subset \mathbb{C}[x, y, z]$. Calcolare

1. $\dim_{\mathbb{C}} \mathbb{C}[x, y, z]/I$;
2. $\mathbf{V}(I) \cap \mathbf{V}(z - 1)$.

E. 98. (→ p. 289) Siano $A = \mathbb{C}[x, y, z]$ e $I = (xy^3, xy + y^2, y^2 - z^2)$.

1. Calcolare $I_1 = I \cap \mathbb{C}[y, z]$ e $I_2 = I \cap \mathbb{C}[z]$.
2. Sia $\pi_1 : \mathbb{C}^3 \longrightarrow \mathbb{C}^2$ la proiezione sulle ultime due componenti data da $\pi_1(a_1, a_2, a_3) = (a_2, a_3)$. Determinare se $\pi_1(\mathbf{V}(I)) = \mathbf{V}(I_1)$.

E. 99. (→ p. 289) Sia $I = (t^2 - x, t^3 - y, t^4 - z) \subset \mathbb{C}[x, y, z, t]$. Calcolare $J = I \cap \mathbb{C}[x, y]$. Determinare inoltre se ogni elemento di $\mathbf{V}(J) \subset \mathbb{C}^2$ si estende ad un elemento di $\mathbf{V}(I) \subset \mathbb{C}^4$.

E. 100. (→ p. 289) Siano $I = (x^2 - y^2 - yz, xy - y^2z)$ e $J = (x^2 - y^2 - yz, xy - y^2z, y^3z^2 - y^3 - y^2z)$ ideali in $\mathbb{C}[x, y, z]$. Determinare se $I = J$ e se $\mathbf{I}(\mathbf{V}(I)) = I$.

E. 101. (→ p. 289) Sia $I = (x + y + z, xy + yz + zx, xyz - 1) \subseteq \mathbb{C}[x, y, z]$. Mostrare che:

1. $\mathbf{V}(I)$ è l'insieme costituito dall'elemento $(1, \alpha, \alpha^2)$, con $\alpha = \frac{1}{2}(-1 + i\sqrt{3})$, e dagli elementi di $\mathbb{C}^3$ ottenuti permutando le sue coordinate;

2. I è radicale.

E. 102. (→ p. 290) Sia $I = (x^3+y^3+z^3+1, x^2+y^2+z^2+1, x+y+z+1) \subset \mathbb{Z}/(2)[x,y,z]$.

1. $\mathbf{V}(I) \subset \overline{\mathbb{Z}/(2)}^3$ è finita?
2. Decomporre $\mathbf{V}(I)$ come unione di varietà irriducibili.

E. 103. (→ p. 290) Sia $I = (x^2 - yz + y^2, xyz - x) \subset \mathbb{Q}[x,y,z]$.

1. Trovare una base di Gröbner ridotta di I.
2. Calcolare la contrazione di I rispetto all'omomorfismo di immersione $\mathbb{Q}[y,z] \longrightarrow \mathbb{Q}[x,y,z]$.
3. Determinare se $\mathbf{V}(I) \subset \mathbb{Q}^3$ è finita.
4. Determinare $\mathrm{Min}(I)$.

E. 104. (→ p. 291) Siano $I = (yt^2 + x^3z^2t^3, z^2 + yt^2, x^2t^2) \subset K[x,y,z,t]$ e A il suo anello quoziente.

1. Verificare che I è un ideale monomiale.
2. Decomporre I come intersezione irridondante di ideali primari.
3. Trovare $\mathcal{N}(A)$ ed esprimerlo come intersezione irridondante di ideali primi.
4. Stabilire se $\mathbf{V}(I)$ è finita.

E. 105. (→ p. 291) Siano $I = (y^2 - xz, x^2 - y^2, x^2 - yz) \subset \mathbb{Q}[x,y,z]$.

1. Trovare le componenti irriducibili di $\mathbf{V}(I)$ e stabilire se $\mathbf{V}(I)$ è finita.
2. Determinare se $f = y(x^2 + x + y) \in \sqrt{I}$.

E. 106. (→ p. 291) Sia $I = (x^2z, y^2z^2 - yz, y^2 - z^2) \subset \mathbb{C}[x,y,z]$. Stabilire se $\mathbf{V}(I)$ è finita e $I \subset (x^2, y+1, z-1)$.

E. 107. (→ p. 291) Sia $I = (xyz - 2, y^2z - x, 3x^2z^2 - y) \subset K[x,y,z]$.

1. Provare che, se $K = \mathbb{C}$, allora $\mathbf{V}(I)$ è finita.
2. Trovare, se esistono, primi $p \in \mathbb{Z}$ tali che se $K = \overline{\mathbb{Z}/(p)}$, $\mathbf{V}(I)$ è vuota oppure infinita.

E. 108. (→ p. 292) Siano $I = (x^2+y^2+z^2-2, y^2-z^2+1, xz-1) \subset \mathbb{Q}[x,y,z]$ e A il suo anello quoziente.

1. Provare che A è un $\mathbb{Q}$-spazio vettoriale di dimensione finita e trovarne una base.
2. Determinare le coordinate di $p = x^2+y^2z+2y+1$ rispetto alla base trovata sopra.
3. Stabilire se $\dim_{\mathbb{Q}} A = |\,\mathbf{V}_{\mathbb{C}}(I)|$.
4. Decomporre $\sqrt{I}$ come intersezione di ideali massimali in $\mathbb{Q}[x, y, z]$.

E. 109. (→ p. 293) Dato il sistema

$$\Sigma = \begin{cases} f_1 = x^2 - 3xy + y^2 = 0 \\ f_2 = x^3 - 8x + 3y = 0 \\ f_3 = x^2y - 3x + y = 0, \end{cases}$$

1. provare che Σ ha un numero finito di soluzioni in $\mathbb{C}^2$;
2. trovare tutte le soluzioni β di Σ tali che $\beta \in \mathbb{Q}^2$;
3. decomporre la varietà $V = \mathbf{V}_{\mathbb{R}}(f_1, f_2, f_3)$ come unione di varietà irriducibili.

E. 110. (→ p. 293) Sia $I = (xz - yz, y^2 - z, xyz - 1) \subset \mathbb{Q}[x, y, z]$.

1. Trovare, se esiste, un polinomio univariato $p(y) \in I$.
2. Determinare l'insieme $\Sigma = \{q(y) \in \mathbb{Q}[y] \colon \mathbf{V}_{\mathbb{Q}}((q, I)) \neq \emptyset\}$, e dire se è un ideale.

E. 111. (→ p. 293) Siano $V = \{\alpha_1, \ldots, \alpha_m\} \subset \mathbb{C}^n$, con $\alpha_i \neq \alpha_j$ per $i \neq j$, e sia $A = \mathbb{C}[x_1, \ldots, x_n]/\mathbf{I}(V)$ l'anello delle coordinate di V.

1. Provare che esistono m elementi non nulli $a_1, \ldots, a_m \in A$, tali che $a_i^2 = a_i$, $a_i a_j = 0$ per $i \neq j$ e tali che $\sum_{i=1}^{m} a_i = 1$.
2. Determinare quanti e quali sono gli elementi idempotenti di A.

10

Esercizi sui moduli

10.1 Moduli, sottomoduli e omomorfismi

E. 112. (→ p. 294) Dati un ideale $I \subset A$ e un A-modulo M, provare che, ponendo $\bar{a}\overline{m} = \overline{am}$, per ogni $\bar{a} \in A/I$ e $\overline{m} \in M/IM$, si definisce su M/IM una struttura di A/I-modulo.

E. 113. (→ p. 294) Verificare che l'operazione di restrizione di scalari induce effettivamente una struttura di modulo.

E. 114. (→ p. 294) Sia $f\colon A \longrightarrow B$ un omomorfismo surgettivo di anelli e consideriamo B come A-modulo per restrizione di scalari tramite f. Provare che gli ideali di B coincidono con gli A-sottomoduli di B.

E. 115. (→ p. 294) Sia M un A-modulo, e siano N e P sottomoduli di M; sia inoltre $N\colon P = \{a \in A\colon aP \subseteq N\}$. Allora $N\colon P$ e, in particolare, $\operatorname{Ann} P = 0\colon P$ sono ideali di A.

E. 116. (→ p. 294) Siano $I, J_1, J_2 \subset A$ ideali e sia $M = {}^{A}\!/_{J_1} \oplus {}^{A}\!/_{J_2}$; verificare che

$$ {}^{M}\!/_{IM} \simeq {}^{A}\!/_{(J_1 + I)} \oplus {}^{A}\!/_{(J_2 + I)}. $$

E. 117. (→ p. 294) Siano $J \subset A$ un ideale, $M = A/J$ e $a \in A$; verificare che

$$ aM \simeq {}^{A}\!/_{(J\,:\,a)}. $$

E. 118. (→ p. 295) Sia A un anello e sia $f : A^m \longrightarrow A^n$ un omomorfismo surgettivo di A-moduli; mostrare che se $n > m$, allora $A = 0$.

E. 119. (→ p. 295) Sia M un A-modulo libero di rango r. Allora ogni insieme di generatori ha cardinalità maggiore o uguale a r.

E. 120. (→ p. 295) Siano A un anello commutativo, $I \subset A$ un ideale nilpotente e $\varphi\colon M \longrightarrow N$ un omomorfismo di A-moduli. Provare che se l'omomorfismo indotto $\overline{\varphi} : M/IM \longrightarrow N/IN$ è surgettivo allora anche φ è surgettivo.

E. 121. (→ p. 295) Siano $m, n \in \mathbb{N}$, $A \neq 0$ un anello e $f : A^m \longrightarrow A^n$ un omomorfismo di A-moduli. Provare che:

1. se f è surgettivo allora $m \geq n$;
2. se f è iniettivo allora $m \leq n$;
3. se f è un isomorfismo allora $m = n$.

E. 122. (→ p. 295) Siano M un A-modulo finitamente generato e $0 \neq N \subseteq M$ un sottomodulo.

1. Provare che $M \not\simeq M/N$.
2. Trovare un controesempio al punto precedente nel caso in cui M non sia finitamente generato.

E. 123. (→ p. 296) Siano A un anello e M, N due A-moduli. Provare che:

1. $M \neq 0$ è semplice se e solo se è $M \simeq A/\mathfrak{m}$, con $\mathfrak{m}$ ideale massimale;
2. se $M, N \neq 0$ sono semplici e $\varphi\colon M \longrightarrow N$ è un omomorfismo, allora φ è l'omomorfismo nullo o un isomorfismo.
3. se M è semplice allora $\mathcal{J}(A)M = 0$.

E. 124. (→ p. 296) Provare che un A-modulo $M \neq 0$ è semplice se e solo se per ogni $0 \neq m \in M$ si ha $\langle m \rangle = M$. Determinare poi tutti gli $\mathbb{Z}$-moduli semplici.

E. 125. (→ p. 296) Sia M uno $\mathbb{Z}$-modulo ciclico e siano N e P sottomoduli di M. Provare che, se esistono $p, q \in \mathbb{Z}$ coprimi e tali che $\operatorname{Ann} N = (p)$, $\operatorname{Ann} P = (q)$ e $\operatorname{Ann} M = (pq)$, allora $M = N \oplus P$.

E. 126. (→ p. 297) Siano M, N, P degli A-moduli; dimostrare che

$$\operatorname{Hom}_A(M, P) \oplus \operatorname{Hom}_A(N, P) \simeq \operatorname{Hom}_A(M \oplus N, P),$$
$$\operatorname{Hom}_A(P, M) \oplus \operatorname{Hom}_A(P, N) \simeq \operatorname{Hom}_A(P, M \oplus N).$$

E. 127. (→ p. 297) Provare che:

1. $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}) = 0$;
2. $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n),\mathbb{Z}) = 0$;
3. $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n),\mathbb{Q}/\mathbb{Z}) \neq 0$.

E. 128. (→ p. 297) Siano A un anello, $I, J \subsetneq A$ ideali e $0 \neq M$ un A-modulo. Provare che:

1. $\mathrm{Hom}_A(A/I, M) \simeq 0 :_M I = \{m \in M : Im = 0\}$;
2. $\mathrm{Hom}_A(A/I, M)$ ha una struttura di A/I-modulo;
3. se $M = A/J$, allora $\mathrm{Hom}_A(A/I, M) \simeq (J : I)/J$.

E. 129. (→ p. 298) Siano $A = K[x,y,z]$, $I = (x^3, x^2y, yz)$ e $J = (x^2, yz)$; calcolare la dimensione di $\mathrm{Hom}_A(A/I, A/J)$ come K-spazio vettoriale.

E. 130. (→ p. 298) Siano $(A, \mathfrak{m})$ un anello locale e sia $M \neq 0$ un A-modulo finitamente generato. Provare che $\mathrm{Hom}_A(M, A/\mathfrak{m}) \neq 0$.

E. 131. (→ p. 298) Siano K un campo e $B \subset K$ un anello locale che non è un campo. Provare che K non è un B-modulo finitamente generato.

E. 132. (→ p. 299) Siano M un A-modulo finitamente generato e $I \subset A$ un ideale; allora:

$$\sqrt{\mathrm{Ann}(M/IM)} = \sqrt{\mathrm{Ann}\, M + I}.$$

E. 133. (→ p. 299) Siano A un anello e M un A-modulo non necessariamente finitamente generato. Provare che, se $\mathcal{N}(A)$ è finitamente generato e $\mathcal{N}(A)M = M$, allora $M = 0$.

E. 134. (→ p. 299) Fornire un controesempio all'enunciato del lemma di Nakayama nel caso in cui il modulo M non sia finitamente generato.

10.2 Successioni esatte e moduli proiettivi

E. 135. (→ p. 299) [Lemma dei 5] Dato il seguente diagramma commutativo di A-moduli con righe esatte

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5, \end{array}$$

dimostrare che

1. se α_1 è surgettivo, e $\alpha_2,\ \alpha_4$ sono iniettivi, allora α_3 è iniettivo;
2. se α_5 è iniettivo, e $\alpha_2,\ \alpha_4$ sono surgettivi, allora α_3 è surgettivo.

In particolare, se α_1 è surgettivo, α_5 è iniettivo, α_2 e α_4 sono isomorfismi, allora α_3 è un isomorfismo.

E. 136. (→ p. 300) Siano M, N, P tre $\mathbb{Z}$-moduli. Provare che, se $pN = qP = 0$, con p, q primi distinti di $\mathbb{Z}$, allora la successione

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$$

spezza.

E. 137. (→ p. 300) Siano $A = \mathbb{Z}$, $M = \mathbb{Z}/(2)$, $N = \mathbb{Z}/(4)$, $P = \mathbb{Z}/(8)$. Trovare, se possibile, successioni esatte corte di A-moduli

1. $0 \longrightarrow M \longrightarrow N \longrightarrow M \longrightarrow 0$;
2. $0 \longrightarrow M \longrightarrow N \oplus M \longrightarrow M \oplus M \longrightarrow 0$;
3. $0 \longrightarrow M \longrightarrow P \longrightarrow M \oplus M \longrightarrow 0$.

E. 138. (→ p. 301) Sia $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ una successione esatta corta di A-moduli. Dimostrare che, se M e P sono generati rispettivamente da m e p elementi, allora N può essere generato da $m + p$ elementi.
Esistono casi in cui N può essere generato da meno di $m + p$ elementi?

E. 139. (→ p. 301) Siano M, N A-moduli e siano $f\colon M \longrightarrow N$ e $g\colon N \longrightarrow M$ omomorfismi tali che $g \circ f = \mathrm{id}_M$. Provare che $N = \operatorname{Ker} g \oplus \operatorname{Im} f$.

E. 140. (→ p. 302) Siano

$$0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{f} P \longrightarrow 0$$

$$0 \longrightarrow P \xrightarrow{g} T \xrightarrow{\psi} W \longrightarrow 0$$

due successioni esatte di A-moduli. Provare che

$$0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{g\circ f} T \xrightarrow{\psi} W \longrightarrow 0$$

è esatta.

E. 141. (→ p. 302) Provare che $\mathbb{Z}/(n)$ non è proiettivo come $\mathbb{Z}$-modulo ma lo è come $\mathbb{Z}/(n)$-modulo.

E. 142. (→ p. 302) Sia $A = \mathbb{Z}/(12)$. Allora $\mathbb{Z}/(4)$ è un A-modulo proiettivo non libero.

E. 143. (→ p. 302) Siano $A = \mathbb{Z}/(4)$ e $B = \mathbb{Z}/(6)$. Trovare i sottomoduli non banali di A e B e dire quali di essi sono proiettivi come A e B-moduli rispettivamente.

E. 144. (→ p. 302) Siano I, J ideali comassimali di un anello A. Provare che:

1. $I \oplus J \simeq IJ \oplus A$;
2. se A è un dominio e IJ è principale, allora I e J sono proiettivi.

E. 145. (→ p. 303) Sia $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ una successione esatta di A-moduli.

1. Se $A = \mathbb{Z}$, e due dei tre moduli della successione sono isomorfi a $\mathbb{Z}$, cosa possiamo dire del terzo, in ognuno dei casi possibili?
2. Se $A = \mathbb{Z}$, e uno dei tre moduli della successione è isomorfo a $\mathbb{Z}$, cosa possiamo dire degli altri due, in ognuno dei casi possibili?
3. Le conclusioni dei punti precedenti, opportunamente riformulate, valgono per un qualsiasi PID A?

E. 146. (→ p. 303) Siano A un anello e $0 \neq M$ un A-modulo. Provare che:

1. se $\varphi \in \mathrm{End}_A(M)$ e $\varphi^2 = \varphi$, allora $M \simeq \varphi(M) \oplus (\mathrm{id}_M - \varphi)(M)$;
2. se M è finitamente generato, allora M è proiettivo se e solo se esistono $n \in \mathbb{N}$ e $f \in \mathrm{End}_A(A^n)$ tali che $f^2 = f$ e $M \simeq f(A^n)$.

E. 147. (→ p. 304) Provare che un dominio A è un campo se e solo se ogni A-modulo è proiettivo.

E. 148. (→ p. 304) Siano $N \subset M$, $N' \subset M'$ A-moduli tali che $M/N \simeq A \simeq M'/N'$. Provare che:

1. le successioni $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$ e $0 \longrightarrow N' \longrightarrow M' \longrightarrow M'/N' \longrightarrow 0$ spezzano;
2. se $N \simeq N'$ allora $M \simeq M'$.

E. 149. (→ p. 304) Sia $A = \mathbb{Z}[\sqrt{-5}]$ e siano $I = (3, 1 - \sqrt{-5})$ e $J = (3, 1 + \sqrt{-5})$ ideali di A. Provare che:

1. I e J sono ideali massimali distinti e non principali, quindi A non è PID;
2. $I \cap J = IJ = (3)$. Inoltre I e J sono A-moduli proiettivi non liberi.

E. 150. (→ p. 304) [Criterio di Baer] Dimostrare che un A-modulo E è iniettivo se e solo se ogni omomorfismo $f\colon I \longrightarrow E$, con I ideale A, si estende ad un omomorfismo $\tilde{f}\colon A \longrightarrow E$.

E. 151. (→ p. 305) Dimostrare che le seguenti condizioni sono equivalenti.

1. E è iniettivo.
2. $\mathrm{Hom}_A(\bullet, E)$ è un funtore esatto.
3. Ogni successione esatta
$$0 \longrightarrow E \longrightarrow M \longrightarrow N \longrightarrow 0$$
spezza.
4. Se E è isomorfo ad un sottomodulo di M allora E è un addendo diretto di M, i.e. esiste L sottomodulo di M tale che $M \simeq E \oplus L$.

E. 152. (→ p. 307) Sia A un anello e F un A-modulo libero.

1. Se A è un campo, allora F è iniettivo.
2. L'affermazione precedente è ancora valida per un anello qualsiasi?

11

Esercizi su moduli su PID e forma normale di Smith

E. 153. (→ p. 307) Sia A PID; provare che ogni sottomodulo di un modulo proiettivo è proiettivo.

E. 154. (→ p. 308) Siano A un anello, $p \in A$, M un A-modulo e M_p la p-componente di M. Provare che M_p è un sottomodulo di M.

E. 155. (→ p. 308) Siano A PID, M un A-modulo finitamente generato e $a, b \in A$ tali che $\gcd(a, b) = 1$. Provare che:

1. $M_a \oplus M_b \simeq M_{ab}$;
2. siano π_a e π_b le proiezioni di M_{ab} su M_a e M_b rispettivamente; allora, esistono elementi $c, d \in A$ tali che, per ogni $m \in M_{ab}$ si ha $\pi_a(m) = cm$ e $\pi_b(m) = dm$;
3. M_{ab} è ciclico se e solo se M_a e M_b sono ciclici.

E. 156. (→ p. 308) Sia $M \neq 0$ un A-modulo ciclico, con A PID e $M \not\simeq A$. Provare che esistono primi $p_1, \ldots, p_h \in A$ e sottomoduli cicici p_i-primari $M_i \subseteq M$ tali che $M \simeq \oplus_{i=1}^{h} M_i$.

E. 157. (→ p. 309) Sia A un dominio e M un A-modulo. Provare che:

1. ogni A-modulo libero è libero da torsione;
2. se A è un PID, M è finitamente generato e libero da torsione allora M è libero;
3. il risultato precedente è vero se A non è PID? E se A è PID ma M non è finitamente generato?

E. 158. (→ p. 309) Sia M uno $\mathbb{Z}$-modulo tale che la successione

$$0 \longrightarrow \mathbb{Z}^3 \xrightarrow{f} \mathbb{Z}^4 \longrightarrow M \longrightarrow 0,$$

con $f(x,y,z) = (x+y+z, -3x+y+z, x-3y-3z, x+3y+z)$, è esatta. Esprimere M come somma diretta di $\mathbb{Z}$-moduli ciclici.

E. 159. (→ p. 309) Sia $\varphi\colon \mathbb{Q}[x]^4 \to \mathbb{Q}[x]^4$ l'omomorfismo dato da

$$\varphi(a,b,c,d) = (a+3c, b+2xc+3d, (x^2-x)(a+3c)+2xd, (x^2-x)(b+3d)).$$

Trovare la dimensione su $\mathbb{Q}$ di $\operatorname{Coker}\varphi$.

E. 160. (→ p. 309) Siano $a \in \mathbb{Z}$ e $\varphi\colon \mathbb{Z}^3 \to \mathbb{Z}^3$ l'omomorfismo dato da

$$\varphi(x,y,z) = (6x+2y+4z, ay+4z, 2x+2y+2z).$$

Determinare la classe di isomorfismo di $\operatorname{Coker}\varphi$ in funzione di a.
Esistono valori di a per cui $\operatorname{Coker}\varphi$ ha infiniti elementi?

E. 161. (→ p. 310) Sia $\varphi\colon \mathbb{Z}^3 \to \mathbb{Z}^3$ l'omomorfismo definito dalla matrice $\begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix}$, con $a,b,c \in \mathbb{Z}$. Provare che:

1. $\operatorname{Coker}\varphi$ ha al più due generatori se e solo se $\gcd(a,b,c) = 1$;
2. $\operatorname{Coker}\varphi$ è ciclico se e solo se $\gcd(a,b) = 1$.

E. 162. (→ p. 310) Sia $\varphi\colon \mathbb{Z}^3 \to \mathbb{Z}^3$ l'omomorfismo definito dalla matrice $\begin{pmatrix} a & 6 & 6 \\ -3 & 6 & 0 \\ a & 3 & 3 \end{pmatrix}$, con $a \in \mathbb{Z}$. Trovare, se esistono, i valori di a per cui:

1. $\operatorname{Coker}\varphi$ è finito;
2. $\operatorname{Coker}\varphi$ non è ciclico.

E. 163. (→ p. 311) Sia $M = \mathbb{Z}^3/N$, ove N è il sottomodulo generato da $m_1 = (0,a,b)$, $m_2 = (3,3,0)$ e $m_3 = (3,-1,0)$, con $a,b \in \mathbb{Z}$.
Trovare i valori di a,b per cui M è finito e quelli per cui M è ciclico.

E. 164. (→ p. 311) Sia $M = \mathbb{Z}^3/N$, ove N è il sottomodulo generato da $m_1 = (2, 4, -4)$, $m_2 = (4, 12, -12)$ e $m_3 = (2, -4, -4)$. Trovare l'annullatore di M.

E. 165. (→ p. 311) Siano A, B, C matrici intere 3×3 e sia $D = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$. Sapendo che $\det A = 28$ e $\det B = 7$, trovare le possibili forme di Smith di D, esibendo un esempio di ciascuna.

E. 166. (→ p. 311) Sia M il gruppo abeliano generato da elementi m_1, m_2 e m_3 che soddisfano le relazioni $3m_1 + m_3 = 0$, $2m_1 - 2m_2 + m_3 = 0$ e $m_1 + 4m_2 + 2m_3 = 0$. Trovare i possibili ordini degli elementi di M.

E. 167. (→ p. 312) Siano $A \in M_n(\mathbb{Z})$ e M lo $\mathbb{Z}$-modulo $\mathbb{Z}^n/A\mathbb{Z}^n$. Supponiamo che per ogni $m \in M$ esista un primo $p_m \in \mathbb{Z}$ tale che $p_m m = 0$.
Dimostrare che il rango di A è n e che esiste $p \in \mathbb{Z}$ primo tale che $\det A = \pm p^k$ con $k \leq n$.

E. 168. (→ p. 312) Sia $A = K[x, y]/(y^3 - xy^2 - y + x, x^2 - xy + x - y)$.

1. Provare che A è finitamente generato come $K[x]$-modulo.
2. Rappresentare A come il conucleo di un omomorfismo di $K[x]$-moduli e decomporlo come somma diretta di moduli ciclici.

E. 169. (→ p. 313) Sia M lo $\mathbb{Z}$-modulo generato da elementi m_1, m_2, m_3 che soddisfano le seguenti relazioni

$$\begin{cases} 2m_1 - 4m_2 - 2m_3 = 0 \\ 10m_1 - 6m_2 + 4m_3 = 0 \\ 6m_1 - 12m_2 + am_3 = 0\,. \end{cases}$$

1. Rappresentare M come somma diretta di moduli ciclici al variare di $a \in \mathbb{Z}$.
2. Trovare, se esistono, i valori di a per cui $\operatorname{Ann} M = 0$.

E. 170. (→ p. 314) Siano $G_1 = \langle a, b, c, d \rangle$ ove gli elementi a, b, c, d soddisfano le relazioni

$$\begin{cases} 2a+2b+c+3d=0 \\ -2b+c+3d=0 \\ -4a+4b-3c-15d=0 \\ 6a+4b+c+9d=0 \\ 12a+4b+c+21d=0 \end{cases}$$

e $G_2(\alpha) = \operatorname{Coker}\varphi_\alpha$, ove $\varphi_\alpha\colon \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ è l'omomorfismo di $\mathbb{Z}$-moduli definito da

$$\varphi_\alpha(x,y,z) = (2x+8y-4z, \alpha x+6y+\alpha z, -2x-2y+4z),$$

al variare di $\alpha \in \mathbb{Z}$.
Determinare, se esistono, i valori di α per cui G_1 e $G_2(\alpha)$ sono isomorfi.

E. 171. (→ p. 315) Siano $\alpha, \beta \in \mathbb{N}$, $A = A_{\alpha,\beta}$ una matrice 6×6 ad entrate reali, con polinomio caratteristico $p_A(x) = (x-1)^\alpha (x-2)^\beta (x^2+1)$. Determinare, se esistono, valori di α e β per cui le possibili forme di Smith della matrice caratteristica $A - xI$ siano esattamente 4.

E. 172. (→ p. 316) Sia M lo $\mathbb{Z}$-modulo generato da elementi v_1, v_2, v_3, v_4 che soddisfano le relazioni $3v_1 = 0$, $av_1 + 3v_2 = 0$, $bv_2 + 3v_3 = 0$, con $a, b \in \mathbb{Z}$ tali che $\gcd(a,b) = 1$.
Descrivere il sottomodulo di torsione $T(M)$ di M al variare di a, b.

E. 173. (→ p. 316) Siano $N \subset \mathbb{Z}^3$ il sottomodulo di $\mathbb{Z}^3$ generato da $m_1 = (2,2,a)$, $m_2 = (2,a,0)$, $m_3 = (0,4,2)$ e $M = \mathbb{Z}^3/N$, con $a \in \mathbb{Z}$.

1. Determinare M a meno di isomorfismo, al variare di a.
2. Trovare, se esistono, i valori di a per cui $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(7), M) \neq 0$.

E. 174. (→ p. 317) Sia $M = \langle v_1, v_2, v_3 \rangle_{\mathbb{Z}}$, ove $2v_1 = v_2$, $v_1 = 3v_2$, $v_1 + v_2 = av_3$, al variare di $a \in \mathbb{Z}$.

1. Per $a = 3$, costruire, se possibile, un omomorfismo non banale $\varphi\colon \mathbb{Z}/(20) \longrightarrow M$.
2. Descrivere $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(20), M)$, al variare di a.

E. 175. (→ p. 317) Sia $\psi\colon \mathbb{Z}^3 \longrightarrow M$ un omomorfismo surgettivo di $\mathbb{Z}$-moduli tale che $\operatorname{Ker}\psi = \langle m_1, m_2, m_3 \rangle$, con $m_1 = (2,4,6)$, $m_2 = (0,a,2a)$, $m_3 = (b,4,6)$, al variare di $a, b \in \mathbb{Z}$. Trovare, se esistono, i valori di a, b per cui M è semplice.

E. 176. (→ p. 317) Siano $A = K[x, y, z]$ e $I = (x^2 + y^2 - z, xy - 1)$.

1. Dimostrare che A/I è un $K[z]$-modulo finitamente generato e determinarne un insieme di generatori finito.
2. Decomporre A/I come somma diretta di $K[z]$-moduli ciclici.

E. 177. (→ p. 318) Sia $I = (z^2+xy, x^2y-y^2z+z^2, x^2+xy+2yz, x^2-yz) \subset K[x, y, z]$.

1. Provare che I è un ideale monomiale.
2. Determinare un insieme di generatori del $K[y]$-modulo $M = K[x, y, z]/I$.
3. M è libero?
4. Rappresentare M come conucleo di un omomorfismo di $K[y]$-moduli e decomporlo come somma diretta di moduli ciclici.

E. 178. (→ p. 318) Sia K un campo. In ognuno dei seguenti casi, dimostrare che l'anello A è finitamente generato come $K[x]$-modulo e scriverlo come somma diretta di moduli ciclici.

1. $A = K[x, y, z]/(x^3 - y^2 + z, x^2 - y^2)$;
2. $A = K[x, y, z]/(zy - 1, y^2 - z + x^2)$;
3. $A = K[x, y]/(x^2 - y^2, x^4 - x^3y + y)$.

12

Esercizi sul prodotto tensoriale

E. 179. (→ p. 319) Siano A un anello e M, N e P degli A-moduli. Per ogni $f, g \in \mathrm{Bil}(M, N; P)$ e $a \in A$ definiamo

$$(f+g)(m,n) = f(m,n) + g(m,n) \quad \text{e} \quad (af)(m,n) = af(m,n),$$

per ogni $m \in M, n \in N$. Mostrare che $\mathrm{Bil}(M, N; P)$ dotato di tali operazioni è un A-modulo.

E. 180. (→ p. 320) Calcolare $\mathbb{Z}/(a) \otimes \mathbb{Z}/(b)$ quando $\gcd(a, b) = 1$.

E. 181. (→ p. 320) È possibile ripercorrere la dimostrazione dell'esempio 5.1.2 per dimostrare che $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C}$?

E. 182. (→ p. 320) Siano A un anello e M, N due A-moduli liberi. Dimostrare che $M \otimes N$ è libero.

E. 183. (→ p. 321) Siano I, J ideali di un anello A; dimostrare che $A/I \otimes_A A/J \simeq A/I + J$.

E. 184. (→ p. 322) Siano A un anello, M, M', N, N' degli A-moduli e $f\colon M \longrightarrow M'$, $g\colon N \longrightarrow N'$ omomorfismi di A-moduli. Mostrare che

$$f \otimes g\colon M \otimes N \longrightarrow M' \otimes N' \qquad (f \otimes g)(m \otimes n) = f(m) \otimes g(n)$$

è un omomorfismo di A-moduli ben definito.

E. 185. (→ p. 322) Siano A un anello, M, M', M'', N, N', N'' degli A-moduli e $f\colon M \longrightarrow M'$, $f'\colon M' \longrightarrow M''$, $g\colon N \longrightarrow N'$ e $g'\colon N' \longrightarrow N''$ omomorfismi di A-moduli. Allora $(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$.

E. 186. (→ p. 323) 1. Mostrare che $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/(n) = 0$ per ogni $n \in \mathbb{N}_+$.
2. Provare che in generale il prodotto diretto e il prodotto tensoriale non commutano.

E. 187. (→ p. 323) Siano N_1, N_2 due A-moduli. Provare che:

1. N_1 e N_2 sono proiettivi $\iff$ $N_1 \oplus N_2$ è proiettivo;
2. N_1 e N_2 sono proiettivi $\Rightarrow$ $N_1 \otimes N_2$ è proiettivo;
3. il viceversa dell'affermazione precedente in generale non vale;
4. N_1 e N_2 sono piatti $\iff$ $N_1 \oplus N_2$ è piatto;
5. N_1 e N_2 sono piatti $\Rightarrow$ $N_1 \otimes N_2$ è piatto;
6. il viceversa dell'affermazione precedente in generale non vale.

E. 188. (→ p. 324) Siano $(A, \mathfrak{m}, K)$ un anello locale e M, N A-moduli finitamente generati. Provare che $\mu(M \otimes_A N) = \mu(M)\mu(N)$.

E. 189. (→ p. 324) Siano $(A, \mathfrak{m}, K)$ un anello locale e M, N A-moduli finitamente generati; allora $M \otimes_A N = 0$ implica $M = 0$ oppure $N = 0$.

E. 190. (→ p. 325) Siano $p \in \mathbb{Z}$ primo e $M = \{\frac{a}{p^n} \ : \ a \in \mathbb{Z}\,,\, n \in \mathbb{N}\}$. Dopo aver verificato che M è uno $\mathbb{Z}$-modulo, provare che $M \otimes_{\mathbb{Z}} (M/\mathbb{Z}) = 0$.

E. 191. (→ p. 325) 1. Calcolare la dimensione dello spazio vettoriale

$$\mathbb{Q}[x]/(x) \otimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/(x^2+1).$$

2. Sia $\alpha = \sqrt[5]{3}$; provare che $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}[\alpha] \simeq \mathbb{C}^5$.

E. 192. (→ p. 325) Sia $(A, \mathfrak{m}, K)$ un anello locale. Provare che ogni A-modulo proiettivo finitamente generato è libero.

E. 193. (→ p. 326) Siano A e B anelli e $f\colon A \longrightarrow B$ un omomorfismo *piatto*, cioè tale che la restrizione di scalari tramite f rende B un A-modulo piatto. Dati I, J ideali di A, provare che $(I \cap J)B = IB \cap JB$.

E. 194. (→ p. 326) Siano A un anello e $a \in A$. Provare che i seguenti fatti sono equivalenti:

1. $(a) = (a^2)$;
2. (a) è addendo diretto di A;

3. $A/(a)$ è un A-modulo piatto.

E. 195. (→ p. 327) Sia M un A-modulo tale che $\mathfrak{m}M \neq M$ per ogni $\mathfrak{m} \in \operatorname{Max} A$.

1. Provare che $M/IM \neq 0$ per ogni ideale proprio I di A.
2. Sia M un A-modulo piatto; provare che allora per ogni A-modulo $N \neq 0$, si ha $M \otimes N \neq 0$.

E. 196. (→ p. 327) Siano A un anello e a un elemento di $A \setminus \mathcal{D}(A)$. Provare che se N è un A-modulo piatto, allora $an \neq 0$ per ogni $0 \neq n \in N$.

E. 197. (→ p. 327) Siano $A = K[x, y]$, $I = (x)$ e $J = (y)$. Provare che:

1. I, J e $I \cap J$ sono A-moduli liberi;
2. $I + J$ è privo di torsione, ma non è piatto.

E. 198. (→ p. 328) Siano M e N due A-moduli liberi di rango finito; allora

$$\operatorname{End}_A(M) \otimes \operatorname{End}_A(N) \simeq \operatorname{End}_A(M \otimes N).$$

E. 199. (→ p. 328) Sia $M = \mathbb{Z}/(15)$ e sia $\varphi : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^3$ l'omomorfismo dato da $\varphi(x, y) = (4x + 8y, 4x - 4y, 16x + 20y)$. Determinare $M \otimes_{\mathbb{Z}} T(\operatorname{Coker} \varphi)$.

E. 200. (→ p. 328) Siano $a \in \mathbb{N}_+$ e M_a lo $\mathbb{Z}$-modulo generato da elementi m_1, m_2, m_3 che soddisfano le relazioni $2m_1 - m_2 = 0$, $m_1 + m_2 + m_3 = 0$, $m_1 + am_2 = 0$. Al variare di a determinare, se esistono, i valori $n \in \mathbb{N}$ per cui $M_a \otimes_{\mathbb{Z}} \mathbb{Z}/(n) \neq 0$.

13

Esercizi sulla localizzazione

E. 201. (→ p. 328) Sia $a \notin \mathcal{N}(A)$; dimostrare che esiste un ideale primo $\mathfrak{p}$ di A che non contiene a.

E. 202. (→ p. 329) Siano A un anello e S un insieme moltiplicativo di A; provare che σ_S è un isomorfismo se e solo se $S \subseteq A^*$.

E. 203. (→ p. 329) Siano A un anello finito e $S \subset A$ un insieme moltiplicativo tale che l'omomorfismo canonico è iniettivo; provare che $A \simeq S^{-1}A$.

E. 204. (→ p. 329) Descrivere l'anello $S^{-1}A$ quando

1. $A = \mathbb{Z}$ e $S = A \setminus (p)$ con p primo;
2. $A = \mathbb{Z}$ e $S = A \setminus \cup_{i=1}^{n}(p_i)$ con p_i primi distinti;
3. $A = \mathbb{Z}/(12)$ e $S = \{\overline{2}^n \ : \ n \in \mathbb{N}\}$;
4. $A = \mathbb{Z}/(12)$ e $S = A \setminus (\overline{2})$;
5. $A = \mathbb{Z}/(12)$ e $S = A \setminus (\overline{3})$.

E. 205. (→ p. 330) Sia A un anello finito e $S \subset A$ un insieme moltiplicativamente chiuso.

1. Provare che σ_S è un omomorfismo surgettivo, in particolare se σ_S è iniettivo allora $A \simeq S^{-1}A$.
2. Siano $A = \mathbb{Z}/(24)$ e $S = \{s \equiv 2^n \mod 24 \ : \ n \in \mathbb{N}\}$. Trovare $\operatorname{Ker} \sigma_S$ e $S^{-1}A$.

E. 206. (→ p. 330) Sia A un anello e $I \subset A$ un ideale.

1. Mostrare che l'insieme $S = 1 + I = \{1 + i \,:\, i \in I\}$ è moltiplicativo e che $S^{-1}I$ è contenuto nel radicale di Jacobson di $S^{-1}A$.
2. Sia $A = \mathbb{Z}/(60)$ e $S = 1 + 4A$. Trovare tutti gli ideali (distinti) di $S^{-1}A$. $S^{-1}A$ è un anello locale?
3. Sia ancora $A = \mathbb{Z}/(60)$: esiste $0 \neq m \in \mathbb{N}$, $m \neq 4$ e $T = 1 + mA$ tale che $T^{-1}A$ non sia locale?

E. 207. (→ p. 331) Dati sottoinsiemi $I, S \subset A$, definiamo la *saturazione* di I rispetto a S come l'insieme

$$I^S = \{a \in A \,:\, \exists s \in S, \text{ t.c. } as \in I\} = \bigcup_{s \in S} I : s$$

e diciamo che I è *saturato rispetto ad* S se $I = I^S$.

1. Provare che, se I è un ideale e S è un insieme moltiplicativo, allora I^S è un ideale.
2. Siano $I, J \subset A$ ideali e $\sigma = \sigma_S \colon A \longrightarrow S^{-1}A$ l'omomorfismo canonico. Provare che:
   a) $\operatorname{Ker} \sigma_S = (0)^S$;
   b) $I \subseteq I^S$;
   c) se $I \subseteq J$, allora $I^S \subseteq J^S$;
   d) $(I^S)^S = I^S$;
   e) $(I^S J^S)^S = (IJ)^S$.

E. 208. (→ p. 331) Siano A un anello, $S \subset A$ un insieme moltiplicativo e M un A-modulo. Dato un sottomodulo $N \subseteq M$, definiamo la *saturazione* di N rispetto ad S come l'insieme $N^S = \{m \in M \,:\, \exists s \in S \text{ t.c. } sm \in N\}$ e diciamo che N è *saturato rispetto ad* S se $N = N^S$.

1. Provare che N^S è un sottomodulo di M.
2. Siano $\sigma_S \colon M \longrightarrow S^{-1}M$ l'omomorfismo canonico, P un sottomodulo di M e Q un sottomodulo di $S^{-1}M$.
   a) $N \subseteq N^S$ e se $N \subseteq P$ allora $N^S \subseteq P^S$;
   b) $\sigma_S^{-1}(Q) = \sigma_S^{-1}(Q)^S$;
   c) $\sigma_S^{-1}(S^{-1}N) = N^S$; in particolare $\operatorname{Ker} \sigma_S = (0)^S$;

d) $(N^S)^S = N^S$;
e) $(N \cap P)^S = N^S \cap P^S$;
f) $(N + P)^S \supseteq N^S + P^S$.

E. 209. (→ p. 331) Siano A e B anelli commutativi con identità, $B \neq 0$ e sia C l'anello $C = A \times B$.

1. Sia $S = \{1\} \times B \subset C$; provare che $S^{-1}C \simeq A$.
2. Sia $T = \{(1,0),(1,1)\} \subset C$, provare che $T^{-1}C \simeq A$.
3. Si consideri su $C \times T$ la relazione $(x,s) \sim (y,t)$ se e solo se $xt = ys$. Provare che non è una relazione di equivalenza.

E. 210. (→ p. 332) Sia A un anello e $f \in A$. Provare che $A_f \simeq A[x]/(1-fx)$.

E. 211. (→ p. 332) Sia $\mathbb{Z}\left[\frac{2}{3}\right] = \left\{p\left(\frac{2}{3}\right) \,:\, p(x) \in \mathbb{Z}[x]\right\} \simeq \mathbb{Z}[x]/(3x-2)$.

1. Provare che $\mathbb{Z}\left[\frac{2}{3}\right] \simeq \mathbb{Z}_3$.
2. Trovare tutti gli anelli A tali che $\mathbb{Z} \subset A \subset \mathbb{Q}$ e descrivere ogni A come localizzazione di $\mathbb{Z}$.

E. 212. (→ p. 333) Siano p un primo di $\mathbb{Z}$ e $A = \mathbb{Z}_2$. Provare che $A_{(p)A} \simeq A \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ se e solo se $p \neq 2$.

E. 213. (→ p. 333) [Anello totale dei quozienti] Siano A un anello, $\mathcal{D}(A)$ l'insieme dei divisori di zero di A e $S = A \setminus \mathcal{D}(A)$. L'anello $S^{-1}A$ si chiama *anello totale dei quozienti* o *delle frazioni di* A e si denota con $Q(A)$ o $\mathrm{Quot}(A)$. Provare che:

1. S è il più grande sistema moltiplicativo tale che $\sigma_S : A \longrightarrow S^{-1}A$ è iniettivo;
2. ogni elemento di $Q(A)$ è invertibile oppure è un divisore di zero;
3. se $A = A^* \sqcup \mathcal{D}(A)$, allora σ_S è un isomorfismo;
4. se A è un dominio, allora $Q(A)$ è il più piccolo campo che contiene A, e si chiama *campo dei quozienti* o *delle frazioni di* A.

E. 214. (→ p. 334) Sia $\mathfrak{p} \subset A$ un ideale primo di un anello A; provare che $Q(A/\mathfrak{p}) \simeq A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$.

E. 215. (→ p. 335) Sia $A = B/\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$, con B dominio e $\mathfrak{p}_i \subset B$ ideali primi tali che $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ se $i \neq j$, e sia $Q(A)$ l'anello totale dei quozienti di A.

1. Provare che $Q(A) \simeq \bigoplus_{i=1}^{n} Q(B/\mathfrak{p}_i)$.
2. Siano $A = \mathbb{C}[x,y]/(xy)$ e $S = A \setminus \mathcal{D}(A)$; trovare $S^{-1}A$.
3. Siano $A = \mathbb{C}[x,y]/(x^2 - y^3)$ e $S = A \setminus \mathcal{D}(A)$; trovare $S^{-1}A$.

E. 216. (→ p. 335) Siano A un dominio con un numero finito di ideali primi e $Q(A)$ il suo campo delle frazioni. Provare che esiste un elemento $a \in A$ tale che $Q(A) \simeq A_a$.

E. 217. (→ p. 336) Sia p un primo di $\mathbb{Z}$; provare che $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}_p/\mathbb{Z} = 0$.

E. 218. (→ p. 336) Nelle ipotesi di **E.**80, sia $J = I\mathbb{Q}[x,y,z]_{(x,y,z)}$. Stabilire se l'immagine di f in $\mathbb{Q}[x,y,z]_{(x,y,z)}$ è un elemento di J.

E. 219. (→ p. 336) Nelle ipotesi di **E.**84, siano $\mathfrak{p}_1 = (x-1, y-1)$ e $\mathfrak{p}_2 = (x,y)$; descrivere $I_{\mathfrak{p}_1} \cap \mathbb{C}[x,y]$ e $I_{\mathfrak{p}_2} \cap \mathbb{C}[x,y]$.

E. 220. (→ p. 336) Nelle ipotesi di **E.**86, verificare se l'immagine di f in $K[x,y]_{(x,y)}$ è un elemento di $\sqrt{I_{(x,y)}}$.

E. 221. (→ p. 337) Nelle ipotesi di **E.**89, sia $\mathfrak{p} = (x,z)A$; determinare $A_{\mathfrak{p}}$.

E. 222. (→ p. 337) Nelle stesse ipotesi di **E.**95, sia $S = A \setminus (x,y)$. Descrivere $S^{-1}(A/I)$.

E. 223. (→ p. 337) Nelle ipotesi di **E.**105, sia $S = A \setminus (x,y)A$. Calcolare $S^{-1}A$.

E. 224. (→ p. 337) Siano K un campo e $B \subset K$ un anello che non è un campo. Provare che K non è un B-modulo finitamente generato.

E. 225. (→ p. 337) Sia K un campo, $A = K[x]_{(x)}$ e M il campo delle frazioni di A. Provare che:

1. $M/(x)M$ è un A-modulo finitamente generato;
2. M non è un A-modulo finitamente generato.

E. 226. (→ p. 337) Siano A un anello, $S \subset A$ un insieme moltiplicativamente chiuso e M un A-modulo.

1. Provare che, se $\operatorname{Ann} M \cap S \neq \emptyset$, allora $S^{-1}M = 0$.

2. Provare che, se M è finitamente generato, vale anche il viceversa dell'affermazione precedente.
3. Dare un esempio di un A-modulo M tale che $S^{-1}M = 0$ e $\operatorname{Ann} M \cap S = \emptyset$.

E. 227. (→ p. 338) Siano A un anello e $\{f_h\}_{h\in H}$ un insieme di generatori di A. Siano inoltre M un A-modulo e $m \in M$. Provare che se l'immagine di m è zero in M_{f_h} per ogni $h \in H$, allora $m = 0$.

E. 228. (→ p. 338) Sia M un A-modulo e definiamo *supporto* di M l'insieme

$$\operatorname{Supp} M = \{\mathfrak{p} \in \operatorname{Spec} A \,:\, M_\mathfrak{p} \neq 0\}.$$

Provare che:

1. se M è finitamente generato allora $\mathfrak{p} \in \operatorname{Supp} M$ se e solo $\mathfrak{p} \supseteq \operatorname{Ann} M$;
2. se $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ è una successione esatta allora $\operatorname{Supp} M = \operatorname{Supp} M' \cup \operatorname{Supp} M''$;
3. se M e N sono A-moduli finitamente generati allora $\operatorname{Supp}(M \otimes_A N) = \operatorname{Supp} M \cap \operatorname{Supp} N$.

E. 229. (→ p. 338) Sia $M = \mathbb{Z}/(10) \oplus \mathbb{Z}/(12)$.

1. Trovare i primi $p \in \mathbb{Z}$ tali che $M_{(p)} \neq 0$.
2. Descrivere $M_{(3)}$.

E. 230. (→ p. 339) Sia $A = \mathbb{Q}[x, y, z]$ e sia M l'A-modulo $A/(xyz - z^2, xy^2 - 4) \otimes_A A/(yz, x - y^2)$.

1. Calcolare la dimensione di M come spazio vettoriale su $\mathbb{Q}$.
2. Trovare il supporto di M.

E. 231. (→ p. 339) Siano A un anello e $0 \neq I \subset A$ un ideale finitamente generato. Provare che, se per ogni ideale massimale $\mathfrak{m} \subset A$ si ha $I_\mathfrak{m} = 0$ oppure $I_\mathfrak{m} = A_\mathfrak{m}$, allora I è principale ed è generato da un elemento idempotente.

E. 232. (→ p. 339) Siano $p(x) = (x-1)^2(x^2+2) \in \mathbb{Q}[x]$, $S = \{q(x) \in \mathbb{Q}[x] \,:\, (q(x), p(x)) = 1\}$ e $A = S^{-1}\mathbb{Q}[x]$.

1. Provare che S è moltiplicativamente chiuso.
2. Provare che $|\operatorname{Spec} A| = 3$.

3. Descrivere $A/\mathfrak{p}$ per ogni $\mathfrak{p} \in \operatorname{Spec} A$.
4. Calcolare $A/\mathfrak{p}_1 \otimes_A A/\mathfrak{p}_2$ per ogni coppia di ideali $\mathfrak{p}_1 \neq \mathfrak{p}_2 \in \operatorname{Spec} A$.

E. 233. (→ p. 340) Siano M un A-modulo e $I \subset A$ un ideale tali che $M_{\mathfrak{m}} = 0$ per ogni ideale massimale $\mathfrak{m}$ che contiene I. Provare che $M = IM$.

E. 234. (→ p. 340) Siano A un anello commutativo con identità e $\mathfrak{p} \in \operatorname{Min} A$. Provare che:

1. ogni elemento di $\mathfrak{p}A_{\mathfrak{p}}$ è nilpotente;
2. ogni elemento di $\mathfrak{p}$ è un divisore di zero in A;
3. se A è ridotto, allora $A_{\mathfrak{p}}$ è un campo.

E. 235. (→ p. 340) Sia S un sottoinsieme moltiplicativo di un anello A. Dimostrare che la sua saturazione $\overline{S}$ è un insieme moltiplicativo saturato.

E. 236. (→ p. 341) Siano $A = (\mathbb{Z}/(200))_{18}$, $B = (\mathbb{Z}/(200))_6$, $C = (\mathbb{Z}/25) \otimes_{\mathbb{Z}} (\mathbb{Z}/40)$ e $D = \mathbb{Z}_{(3)}[x]/(6x - 1)$. Stabilire quali di questi anelli sono isomorfi tra loro.

E. 237. (→ p. 341) Siano A e B anelli, $T \subset B$ un insieme moltiplicativo e $f\colon A \longrightarrow B$ un omomorfismo. Provare che:

1. $f^{-1}(T)$ è un insieme moltiplicativo. Il viceversa vale se f è surgettivo;
2. se $T \subset B$ è saturato, allora anche $f^{-1}(T)$ è saturato. Il viceversa vale se f è surgettivo.

E. 238. (→ p. 342) Siano A un anello e $S, T \subseteq A$ insiemi moltiplicativi. Provare che:

1. se $S \subseteq T$ e $T_1 = \sigma_S(T)$, allora
$$T^{-1}A \simeq T_1^{-1}(S^{-1}A) \simeq T^{-1}(S^{-1}A);$$
2. se $U = \{st \in A\colon s \in S \text{ e } t \in T\}$, allora
$$T^{-1}(S^{-1}A) \simeq S^{-1}(T^{-1}A) \simeq U^{-1}A.$$

E. 239. (→ p. 343) Siano A un anello e $S \subset A$ un insieme moltiplicativo. Provare che S è massimale rispetto all'inclusione nell'insieme degli insiemi moltiplicativi di A se e solo se $A \setminus S$ è un primo minimale.

E. 240. (→ p. 343) Sia A un anello.

1. Sia $I \subset A$ un ideale e $S = 1 + I$; provare che $\overline{S} = A \setminus \bigcup_{\mathfrak{p} \in \mathcal{V}(I)} \mathfrak{p}$, dove $\mathcal{V}(I) = \{\mathfrak{p} \in \operatorname{Spec} A \,:\, I \subseteq \mathfrak{p}\}$.
2. Siano $f, g \in A$; provare che $\overline{S}_f \subseteq \overline{S}_g$ se e solo se $\sqrt{(f)} \supseteq \sqrt{(g)}$.

E. 241. (→ p. 344) Siano K un campo di caratteristica diversa da 2, $A = K[x, y]/(x^2 - y^2)$, $\mathfrak{p} = (x + y)A$ e $\mathfrak{q} = (x, y)A$.

1. Quali sono gli ideali primi di $A_{\mathfrak{q}}$?
2. Descrivere $(A_{\mathfrak{q}})_{\mathfrak{p}A_{\mathfrak{q}}}$.

14

Esercizi su moduli noetheriani e artiniani

E. 242. (→ p. 344) Sia Σ la famiglia degli ideali di un anello A. Provare che:

1. se $A = \mathbb{Z}$, allora Σ, e dunque A, soddisfa a.c.c. ma non d.c.c.;
2. se $A = \mathbb{R}[x]/(x^2 + 2)$, allora Σ, e dunque A, soddisfa sia a.c.c. sia d.c.c..

E. 243. (→ p. 344) Siano A un anello noetheriano e $\varphi\colon A \longrightarrow A$ un omomorfismo surgettivo. Provare che:

1. φ è iniettivo;
2. $\varphi(I \cap J) = \varphi(I) \cap \varphi(J)$, per ogni coppia di ideali $I, J \subset A$.
3. Le precedenti affermazioni sono vere anche se A non è noetheriano?

E. 244. (→ p. 345) Siano A un anello noetheriano e $I \subset A$ un ideale tale che $I = I^2$; provare che I è principale ed è generato da un elemento idempotente.

E. 245. (→ p. 345) Siano $N_1, N_2 \subseteq M$ sottomoduli tali che M/N_1 e M/N_2 sono noetheriani. Provare che $M/(N_1 \cap N_2)$ è noetheriano.

E. 246. (→ p. 345) Sia $A = K[x]/(fg^2)$, ove $(f, g) = 1$. Allora un A-modulo M è noetheriano se e solo se M/fM e M/g^2M sono noetheriani.

E. 247. (→ p. 346) Sia A un dominio di integrità tale che per ogni ideale non nullo I esistono un ideale $J \neq 0$ e un elemento $d \in A$ tali che $IJ = (d)$. Provare che:

1. esiste un ideale finitamente generato $\bar{J} = (g_1, \ldots, g_k)$ tale che $I\bar{J} = (d)$;
2. per ogni $f \in I$ e per ogni $i = 1, \ldots, k$, esiste $h_i \in A$ tale che $fg_i = h_i d$;

3. A è noetheriano.

E. 248. (→ p. 346) Siano A, B, C anelli e $f\colon A \longrightarrow C$ e $g\colon B \longrightarrow C$ omomorfismi surgettivi. Definiamo $A \times_C B = \{(a,b) \in A \times B \,:\, f(a) = g(b)\}$.

1. Verificare che $A \times_C B$ è un sottoanello di $A \times B$.
2. Provare che se A e B sono noetheriani allora $A \times_C B$ è un anello noetheriano.

E. 249. (→ p. 346) Sia A un anello locale, con ideale massimale $\mathfrak{m} = (m)$ principale. Provare che:

1. ogni elemento $0 \neq a \in \mathfrak{m}$ ha una fattorizzazione della forma $a = um^k$, con u invertibile se e solo se $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = 0$;
2. se $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = 0$ e $I \subsetneq A$ è un ideale di A allora $I = \mathfrak{m}^h$ per qualche h;
3. se A è noetheriano allora A è PIR.

E. 250. (→ p. 347) Sia A un anello noetheriano. Provare che:

1. se A è locale e il suo ideale massimale $\mathfrak{m} = (m)$ è principale allora ogni ideale di A è principale;
2. se ogni ideale massimale di A è principale allora $\dim A \leq 1$.

E. 251. (→ p. 347) Sia M un A-modulo noetheriano e sia $I = 0 : M = \mathrm{Ann}_A M$. Provare che A/I è noetheriano.

E. 252. (→ p. 348) Siano A un anello noetheriano e I, J ideali di A tali che ogni ideale primo di A contiene o I o J ma non entrambi. Provare che:

1. $A = I + J$;
2. esiste $n \in \mathbb{N}$ tale che $(IJ)^n = 0$.

E. 253. (→ p. 348) Sia $(A, \mathfrak{m}, K)$ un anello locale noetheriano. Provare che:

1. se $I \subseteq A$ è un ideale e $\mu(I) > 1$, allora $\mu(I^2) < \mu(I)^2$;
2. se ogni ideale di A è un A-modulo piatto, allora A è PID.

E. 254. (→ p. 349) Dato un ideale primo $\mathfrak{p} \in \operatorname{Spec} A$ si definisce la sua *altezza* $\operatorname{ht} \mathfrak{p}$ come l'estremo superiore delle lunghezze delle catene ascendenti di ideali primi contenuti in $\mathfrak{p}$:

$$\operatorname{ht} \mathfrak{p} = \sup\{l \colon \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_l = \mathfrak{p},\ \mathfrak{p}_i \in \operatorname{Spec} A\}.$$

Dato un qualsiasi ideale $I \subset A$ si definisce la sua *altezza* $\operatorname{ht} I$ come l'estremo inferiore delle altezze dei primi che lo contengono

$$\operatorname{ht} I = \inf\{\operatorname{ht}(\mathfrak{p}) \colon \mathfrak{p} \in \mathcal{V}(I)\}.$$

Sia A un anello noetheriano e I, J ideali di A. Provare che:

1. $\sqrt{I} = \sqrt{J}$ se e solo se I e J hanno gli stessi primi minimali;
2. se $\sqrt{I} = \sqrt{J}$, allora $\operatorname{ht} I = \operatorname{ht} J$ e $\dim A/I = \dim A/J$.

E. 255. (→ p. 349) Siano A un anello noetheriano e M un A-modulo tale che $0 \neq \operatorname{Ann} M$ è un ideale 0-dimensionale; provare che allora M contiene un sottomodulo semplice non banale.

E. 256. (→ p. 349) Siano A un anello noetheriano e $\mathfrak{p} \in \operatorname{Spec} A$. Provare che $\mathfrak{p}$ è un primo minimale di A se e solo se esiste un elemento $a \in A$ non nilpotente e $n \in \mathbb{N}$ tale che $a\mathfrak{p}^n = 0$.

E. 257. (→ p. 350) Sia A un anello noetheriano. Provare che ogni ideale $J \subseteq A$ che contiene un ideale radicale Q di dimensione 0 è radicale di dimensione 0 oppure $J = (1)$.

E. 258. (→ p. 350) Nell'anello $K[x, y, z, t]$, trovare i primi minimali associati all'ideale $I = (x^2zt, yt^3, xyzt, x^5z^6)$.

E. 259. (→ p. 350) Sia $I = (x^2z - x^2t^3, x^2y^4t + x^2y^3 - x^3z, xt^2) \subset \mathbb{Q}[x, y, z, t] = A$.

1. Dire se I è un ideale monomiale.
2. Trovare una decomposizione di I come intersezione di ideali primari, individuando i primi associati e i primi minimali.
3. Determinare i nilpotenti e i divisori di zero di A/I.

E. 260. (→ p. 351) Sia $A = \mathbb{Q}[x]/(x^5 - 3x^2) \oplus \mathbb{Z}/(12)$. Trovare

1. gli elementi nilpotenti e i divisori di zero in A;
2. gli ideali primi $\mathfrak{p}$ di A per cui $A_\mathfrak{p}$ è un campo, se esistono.

E. 261. (→ p. 351) Siano $I = (3x^2 + 10y - 2, (x + y)^3, 45) \subset \mathbb{Z}[x, y]$, e $A = \mathbb{Z}[x, y]/I$. Trovare

1. i divisori di zero di A;
2. un ideale primo $\mathfrak{p} \subset A$ per cui $A_\mathfrak{p}$ non è un dominio, se esiste.

E. 262. (→ p. 352) Siano M un A-modulo e $I \subseteq \operatorname{Ann} M$. Allora M è artiniano come A-modulo se e solo se è artiniano come A/I-modulo.

E. 263. (→ p. 352) Siano M un A-modulo artiniano e $u\colon M \longrightarrow M$ un omomorfismo iniettivo. Dimostrare che u è un isomorfismo.

E. 264. (→ p. 352) Sia A un anello artiniano. Provare che:

1. $A = A^* \cup \mathcal{D}(A)$;
2. se A è locale, dato un qualsiasi insieme moltiplicativo $S \subseteq A$, l'omomorfismo canonico $\sigma_S : A \longrightarrow S^{-1}A$ è surgettivo.

E. 265. (→ p. 353) Siano M un A-modulo e $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ ideali massimali di A non necessariamente distinti tali che $\prod_{i=1}^{n} \mathfrak{m}_i\, M = 0$. Provare che allora M è noetheriano se e solo se M è artiniano.

15

Vero o Falso?

Dire quali delle seguenti affermazioni sono vere e quali false. Giustificare le risposte con una dimostrazione o un controesempio.

E. 266. (→ p. 353) Sia A un anello e $I \subset A$ un ideale. Un elemento $a \in A$ non è divisore di zero in A/I se e solo se $I : a = I$.

E. 267. (→ p. 353) Siano A un dominio e Q il suo campo dei quozienti; allora

$$Q[x] \otimes_{A[x]} Q[x] \simeq Q[x].$$

E. 268. (→ p. 353) Siano A un PID, B un dominio e $\varphi\colon A \longrightarrow B$ un omomorfismo surgettivo; allora B è un campo oppure φ è un isomorfismo.

E. 269. (→ p. 354) Siano $I, J, K \subset A$ ideali; allora

1. $\sqrt{I + JK} = \sqrt{I + J} \cap \sqrt{I + K}$;
2. $\sqrt{I + \sqrt{J}} = \sqrt{I + J}$;
3. $\sqrt{I} + \sqrt{J} = \sqrt{I + J}$.

E. 270. (→ p. 354) Siano A un anello e $I \subset A$ un ideale tali che $\mathcal{N}(A/I) = 0$; allora I è primo.

E. 271. (→ p. 354) $\mathbb{Q}[x]/(x^2 - 1) \otimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/(x^2 + 1)$ è il $\mathbb{Q}[x]$-modulo nullo.

E. 272. (→ p. 354) Sia $A[X]$ noetheriano; allora A è noetheriano.

E. 273. (→ p. 354) Siano $<$ un ordinamento monomiale e $0 \neq I \subset K[X]$ un ideale; se $\mathrm{Lt}_<(I)$ è primo allora I è primo.

E. 274. (→ p. 354) Siano $I, J \subset A$ ideali; allora $\sqrt{I : J} \subseteq \sqrt{I} : \sqrt{J}$.

E. 275. (→ p. 354) Siano $I, J \subset A$ ideali massimali tali che $I \cap J = 0$; allora A è artiniano.

E. 276. (→ p. 355) Siano A un dominio e M, N A-moduli; allora $T(M \otimes N) \simeq T(M) \otimes T(N)$.

E. 277. (→ p. 355) Siano $f, g \in \mathbb{C}[x, y] \setminus \mathbb{C}$ e $I = (f, g)$; allora

$$\mathbf{V}_{\mathbb{C}}(I) \text{ è infinita} \iff \gcd(f, g) \neq 1.$$

E. 278. (→ p. 355) Siano A un anello e $I \subset A$ un ideale; allora $A^n/IA^n \simeq \prod_{i=1}^{n} A/IA$.

E. 279. (→ p. 355) Sia $p(x) \in K[x]$, con K campo, un polinomio irriducibile; allora l'ideale $(p(x), p(y))$ è primo in $K[x, y]$.

E. 280. (→ p. 355) Siano M un A-modulo proiettivo e $N \subseteq M$ un sottomodulo; allora N è proiettivo.

E. 281. (→ p. 355) Sia $I \subset A$ un ideale proprio; allora I è massimale se e solo se per ogni ideale $J \subseteq A$ si ha $J \subseteq I$ oppure $I + J = A$.

E. 282. (→ p. 355) Sia $\mathfrak{p} \subset A$ un ideale primo tale che $A/\mathfrak{p}$ è finito; allora $\mathfrak{p}$ è massimale.

E. 283. (→ p. 356) Siano A un anello e $I, J \subset A$ ideali; allora

1. $I + J = A$ se e solo se $I^n + J^n = A$ per ogni $n \in \mathbb{N}$.
2. $\sqrt{I : J} \subseteq \sqrt{I} : J$.
3. $\sqrt{I : J} = \sqrt{I} : J$.
4. $I : J = I : \sqrt{J}$.

E. 284. (→ p. 356) Siano $I = (x^2 + 1, y^2 - 1)$ e $J = (x^2 + xy, y^2 + xy + 1)$ ideali di $\mathbb{Q}[x, y]$; allora $\mathbb{Q}[x, y]/I \simeq \mathbb{Q}[x, y]/J$.

E. 285. (→ p. 356) Sia $I \subset K[x, y]$, con K campo, un ideale tale che $I \cap K[x] = 0$. Sia inoltre $\varphi\colon K[x, y] \longrightarrow K(x)[y]$; allora I è primo se e solo se I^e è primo e $I^{ec} = I$.

E. 286. (→ p. 356) Siano $f, g \in K[x, y]$, con K campo; allora $\sqrt{(f, g)} = \sqrt{(f^2, g^3)}$.

E. 287. (→ p. 357) Siano $(A, \mathfrak{m})$ un anello locale e $\pi\colon A \longrightarrow A/\mathfrak{m}$ la proiezione canonica; allora $a \in A^*$ se e solo se $\pi(a) \in (A/\mathfrak{m})^*$.

E. 288. (→ p. 357) Sia $(A, \mathfrak{m})$ un anello noetheriano locale; se le immagini di certi elementi $a_1, \ldots, a_n \in A$ in $\mathfrak{m}/\mathfrak{m}^2$ lo generano come spazio vettoriale, allora $\mathfrak{m} = (a_1, \ldots, a_n)$.

E. 289. (→ p. 357) Un sottoanello di un anello noetheriano è noetheriano.

E. 290. (→ p. 357) Siano $B = \mathbb{Z}/(18)$ e M_1, M_2 i B-moduli $(2)\mathbb{Z}/(18)$ e $(3)\mathbb{Z}/(18)$ rispettivamente; allora

1. M_1 è proiettivo;
2. M_2 è proiettivo;
3. M_1 è libero;
4. M_2 è libero.

E. 291. (→ p. 357) Sia K un campo; allora la successione di $K[x]$-moduli $0 \longrightarrow (x) \longrightarrow K[x] \longrightarrow K \longrightarrow 0$ spezza.

E. 292. (→ p. 357) Sia $M = \mathbb{Z}/(12) \otimes_{\mathbb{Z}} \mathbb{Z}/(30)$; allora $\operatorname{Supp} M = \{\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}\colon M_{\mathfrak{p}} \neq (0)\} = \{(2), (3)\}$.

E. 293. (→ p. 357) Sia $A = K[x, y]/(xy)$; allora $a \notin \mathcal{D}(A)$ se e solo se $a \in K$.

E. 294. (→ p. 357) Siano K un campo algebricamente chiuso e $f, g \in K[X]$ tali che f è irriducibile e $\mathbf{V}(f) \subseteq \mathbf{V}(g)$; allora f divide g.

E. 295. (→ p. 357) Siano P e Q A-moduli proiettivi e $\varphi \in \operatorname{Hom}_A(P, Q)$ un omomorfismo di A-moduli surgettivo; allora $\operatorname{Ker} \varphi$ è proiettivo.

E. 296. (→ p. 358) Sia $f \in \mathbb{Q}[x]$ tale che $\gcd(f, f') = 1$; allora in $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}[x]/(f)$ esistono elementi nilpotenti diversi da zero.

E. 297. (→ p. 358) Un A-modulo M si dice *finitamente presentato* se esiste una successione esatta $A^m \longrightarrow A^n \longrightarrow M \longrightarrow 0$ per qualche $m, n \in \mathbb{N}$. Dimostrare che un A-modulo proiettivo è finitamente presentato se e solo se è finitamente generato.

E. 298. (→ p. 358) Siano $S \subset A$ un insieme moltiplicativo e M un A-modulo noetheriano; allora $S^{-1}M$ è un A-modulo noetheriano.

E. 299. (→ p. 358) Siano $\mathfrak{m}, \mathfrak{n} \subset A$ ideali massimali distinti e M un A-modulo; allora $M/\mathfrak{m}M \otimes_A M/\mathfrak{n}M = 0$.

E. 300. (→ p. 358) Siano $S = \{24^n\}_{n\in\mathbb{N}}$ e $T = \{4^n 6^m\}_{n,m\in\mathbb{N}}$; allora $S^{-1}\mathbb{Z} \simeq T^{-1}\mathbb{Z}$.

E. 301. (→ p. 358) Siano $<$ un ordinamento monomiale e $I \subset K[X]$ un ideale; se $\mathrm{Lt}_<(I)$ è primario allora I è primario.

E. 302. (→ p. 358) Sia $\varphi\colon \mathbb{Q}[x]^3 \longrightarrow \mathbb{Q}[x]^3$ l'omomorfismo definito dalla matrice

$$\begin{pmatrix} (x-1) & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x(x-1)^3 \end{pmatrix};$$

allora $\dim_{\mathbb{Q}} \operatorname{Coker} \varphi = 6$.

E. 303. (→ p. 359) Sia $A \neq 0$ un anello; ogni A-modulo M è libero se e solo se A è un campo.

E. 304. (→ p. 359) Sia $M \neq 0$ un A-modulo; se per ogni primo $\mathfrak{p} \subset A$ il modulo $M_\mathfrak{p}$ è privo di torsione allora M è privo di torsione.

E. 305. (→ p. 359) Siano A e B due anelli e $f : A \longrightarrow B$ un omomorfismo; se M è un A-modulo libero di rango k, allora $M \otimes_A B$ è un B-modulo libero di rango k.

E. 306. (→ p. 359) Siano A un anello, $f \in A \setminus \mathcal{N}(A)$, e $I \subset A$ un ideale; allora $\sqrt{I} = \sqrt{IA_f \cap A} \cap \sqrt{(I, f)}$.

E. 307. (→ p. 359) Ogni dominio artiniano è un campo.

E. 308. (→ p. 359) Il radicale di Jacobson di un PID è sempre nullo.

E. 309. (→ p. 359) Gli $\mathbb{Z}$-moduli $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{R}$ e $\mathbb{R}$ sono isomorfi.

E. 310. (→ p. 360) Siano N e N' sottomoduli di un A-modulo M; se per ogni ideale massimale $\mathfrak{m} \subset A$ vale $N'_\mathfrak{m} \subseteq N_\mathfrak{m}$, allora $N' \subseteq N$.

E. 311. (→ p. 360) Sia A un anello tale che $A_{\mathfrak{m}}$ è un dominio per ogni $\mathfrak{m} \in \operatorname{Max} A$; allora A è un dominio.

E. 312. (→ p. 360) Siano $A = \mathbb{C}[t]$ e $M = A[x]/(x^2 - t)$; allora M è un A-modulo piatto.

E. 313. (→ p. 360) Sia A un PID e M un A-modulo privo di torsione; allora M è libero.

E. 314. (→ p. 360) Siano $A = \mathbb{Z}$, $S = \{3^n 5^m : m, n \in \mathbb{N})$ e $T = \{15^n : n \in \mathbb{N}\}$; allora $S^{-1}\mathbb{Z} \simeq T^{-1}\mathbb{Z}$.

E. 315. (→ p. 360) Siano M, N A-moduli finitamente generati tali che $M \otimes_A N = 0$; allora $\operatorname{Ann} M + \operatorname{Ann} N = A$.

E. 316. (→ p. 360) Siano $(A, \mathfrak{m}, K)$ un anello locale e $M \neq 0$ un A-modulo finitamente generato; allora $\mathcal{V}(\operatorname{Ann}(M/\mathfrak{m}M)) = \{\mathfrak{m}\}$.

E. 317. (→ p. 361) Sia M un A-modulo piatto; allora per ogni ideale $I \subset A$ si ha $I \otimes_A M \simeq IM$.

E. 318. (→ p. 361) Siano $I, J \subset A$ ideali; allora $I \subset J$ se e solo se $I_{\mathfrak{m}} \subset J_{\mathfrak{m}}$ per ogni $\mathfrak{m} \in \operatorname{Max} A$.

E. 319. (→ p. 361) Sia A un anello noetheriano; allora ogni endomorfismo di A surgettivo è un isomorfismo.

E. 320. (→ p. 361) Sia A un anello tale che ogni sottomodulo di un A-modulo libero è libero; allora A è PID.

E. 321. (→ p. 361) Sia A un anello locale; allora esistono un anello B e un ideale primo $\mathfrak{p}$ di B tali che $A \simeq B_{\mathfrak{p}}$.

E. 322. (→ p. 361) Il polinomio $p(x) = 30x^5 + 60x^3 + 90x + 7$ è un'unità di $\mathbb{Z}/(540)[x]$.

E. 323. (→ p. 361) Ogni ideale massimale in $\mathbb{Z}_{(2)}[x]$ ha non meno di due generatori.

E. 324. (→ p. 361) Sia $M = (\mathbb{Z}/(15) \oplus \mathbb{Z}/(18))_{(3)}$; allora M è ciclico.

E. 325. (→ p. 361) Siano $a \in \mathbb{Z}$ e $M = M(a)$ uno $\mathbb{Z}$-modulo generato da elementi m_1, m_2, m_3 che soddisfano le relazioni $2m_1 - m_2 = 0, m_1 + m_2 + m_3 = 0, m_1 + am_2 = 0$; allora per ogni a positivo esiste un intero n per cui $M \otimes_{\mathbb{Z}} \mathbb{Z}/(n) \neq 0$.

E. 326. (→ p. 361) Siano $I \subset \mathfrak{p} \subset A$, con I ideale e $\mathfrak{p} \in \operatorname{Spec} A$; se $I_{\mathfrak{p}}$ è primario allora I è primario.

E. 327. (→ p. 362) Siano $f(x, y) \in K[x, y]$, con K campo, un polinomio di grado n, $\mathcal{C} = \mathbf{V}(f)$ la curva piana di K^2 definita da f, e ℓ una retta non contenuta in $\mathcal{C}$; allora $|\mathcal{C} \cap \ell| \leq n$.

E. 328. (→ p. 362) Siano A un PID, $Q(A)$ il suo campo delle frazioni e $M \simeq A^n \oplus \bigoplus_{i=1}^{k} A/(a_i^{n_i})$; allora $\dim_{Q(A)} Q(A) \otimes_A M = n$.

E. 329. (→ p. 362) Siano A un anello e M un A-modulo tali che $\mathcal{J}(A)$ è finitamente generato e $\mathcal{J}(A)M = M$; allora $M = 0$.

Parte III

Soluzioni

16

Soluzioni degli esercizi proposti

16.1 Soluzioni del capitolo 8

Soluzione E. *1* Dato $I \supset S$, avremo che $as_1 + bs_2 \in I$, per ogni $s_1, s_2 \in S$ e $a, b \in A$, visto che I è un ideale. Pertanto $I \supseteq (S)$, e l'intersezione di tutti questi ideali contiene S. Per ottenere l'altra inclusione basta osservare che, per costruzione, (S) è un ideale che contiene S.

Soluzione E. *2* $1 \Rightarrow 2$. Se $b = c$ allora $ab = ac$ per ogni $a \in A$. Sia ora $ab = ac$, con $a \neq 0$: allora $a(b - c) = 0$ implica che $b - c$ è uguale a 0, poiché $a \neq 0$ e A è un dominio, come richiesto.

$2 \Rightarrow 3$. Siano $b, c \in A \setminus \{0\}$ e supponiamo per assurdo che $bc \notin A \setminus \{0\}$, ovvero $bc = 0$. Allora, o $b = 0$ oppure dall'ipotesi discende che $c = 0$, essendo $bc = 0 = b0$ con $b \neq 0$; in entrambi casi abbiamo una contraddizione.

$3 \Rightarrow 1$. Dire che, per ogni $b, c \in A$ con $b, c \neq 0$, $bc \neq 0$ è equivalente a dire che se $bc = 0$ allora $b = 0$ oppure $c = 0$, che è la definizione di dominio.

Soluzione E. *3* 1. A è un anello finito e dunque, da **T.**1, sappiamo che $A = \mathcal{D}(A) \sqcup A^*$. Un elemento $\overline{h} \in A$ è invertibile se e solo se esiste $k \in \mathbb{Z}$ tale che $hk \equiv 1 \mod 24$, ovvero se e solo se $(h, 24) = 1$. Pertanto $A^* = \{\overline{h} : h \in \mathbb{Z}\,, (h, 24) = 1\}$ e $\mathcal{D}(A) = \{\overline{h} : h \in \mathbb{Z}, (h, 24) \neq 1\}$. Gli ideali di $\mathbb{Z}/(24)$ corrispondono agli ideali (a) di $\mathbb{Z}$ tali che $(a) \supseteq (24)$, ossia tali che $a|24 = 4 \cdot 3$. Gli ideali primi sono (2) e (3) che sono anche massimali.

2. Ragionando come al punto precedente, troviamo che $A^* = \{\overline{h} : h \in \mathbb{Z}\,, (h, 17) = 1\} = A \setminus \{0\}$, dato che 17 è primo in $\mathbb{Z}$, e $\mathcal{D}(A) = \{0\}$. Quindi (0) è l'unico ideale primo che è anche massimale.

3. Abbiamo che $A = \mathbb{Z}/(n)$ è un dominio se e solo se $\mathcal{D}(A) = \{0\}$ se e solo se $A^* = A \setminus \{0\}$ se e solo se A è un campo. Questo si verifica se e solo se n è primo in $\mathbb{Z}$, poiché in questo caso $(m, n) = 1$ per ogni $m \in \mathbb{N}_+$, $m \leq n - 1$.

Soluzione E. *4* Poiché a è nilpotente, esiste $n > 0$ tale che $a^n = 0$. Da questo segue che $1 = 1 - a^n = (1 - a)\sum_{i=0}^{n-1} a^i$, ossia la prima parte della tesi. Se poi $b \in A$ è un elemento invertibile, basta osservare che $a + b = b(ab^{-1} + 1)$. Dato che ab^{-1} è nilpotente, la conclusione segue dalla prima parte dell'esercizio, poiché il prodotto di invertibili è invertibile.

Soluzione E. *5* 1. Supponiamo che $f = \sum_{i=0}^{n} a_i x^i$ sia invertibile e sia $g(x) = \sum_{i=0}^{m} b_i x^i$ il suo inverso, i.e. tale che $fg = \sum_{i=0}^{n+m} c_i x^i = 1$. Otteniamo subito che $c_0 = a_0 b_0 = 1$ quindi a_0 e b_0 sono invertibili. Inoltre, da $c_{n+m} = a_n b_m = 0$ e $c_{n+m-1} = a_n b_{m-1} + a_{n-1} b_m = 0$, moltiplicando per a_n, otteniamo che $a_n^2 b_{m-1} = -a_n a_{n-1} b_m = 0$. Iterando il ragionamento, da $c_{n+m-r} = 0$ si ricava la relazione $a_n^{r+1} b_{m-r} = 0$ che, per $r = m$, diviene $a_n^{m+1} b_0 = 0$. Poiché b_0 è invertibile questo implica che a_n è nilpotente. Considerando $f - a_n x^n$, che ha grado $< n$ ed è anch'esso invertibile per **E.**4, argomentando nello stesso modo si ottiene la tesi.

Il viceversa discende immediatamente da **E.**4, visto che $f = a_0 + (a_1 x + \ldots a_n x^n)$, a_0 è invertibile e la somma per $i = 1, \ldots, n$ dei nilpotenti $a_i x^i$ è nilpotente.

2. Per quanto detto sopra, se $a_0, \ldots, a_n$ sono nilpotenti, è immediato vedere che f è nilpotente. Viceversa, se f è nilpotente, xf è nilpotente e $1 + xf$ è invertibile. Allora la tesi seguente dal punto precedente.

3. Una direzione è ovvia. Sia dunque $f = \sum_{i=0}^{n} a_i x^i$ un divisore di zero e sia $0 \neq g = \sum_{i=0}^{m} b_i x^i$ un polinomio di grado minimo m tale che $fg = 0$. Dato che $a_n b_m = 0$ e $(a_n g) f = 0$, la minimalità di deg g implica che $a_n g = 0$ e quindi che $a_n b_i = 0$ per ogni i. Considerando il coefficiente del termine di grado $n + m - 1$ di fg, si ha che $a_n b_{m-1} + a_{n-1} b_m = 0$ e dunque $a_{n-1} b_m = 0$. Ripetendo il ragionamento sui coefficienti di fg di grado $< n+m-1$ otteniamo anche che $a_i b_m = 0$ per ogni i; allora la tesi vale prendendo per $a = b_m$.

Soluzione E. *6* È sempre vero che il radicale di Jacobson contiene il nilradicale. Sia dunque $f \in \mathcal{J}(A[x])$; allora, per la caratterizzazione degli elementi

nel radicale di Jacobson **T.** 15, $1+xf$ è invertibile e, quindi, i coefficienti di f sono nilpotenti; pertanto, da **E.**5.1, segue che f è nilpotente, come volevamo.

Soluzione E. *7* Supponiamo che, per qualche $b \in A$, si abbia $b(1+a) = 0$. Allora $b = -ba$ e anche b è un elemento di I. Moltiplicando per $-a$ ambo i membri otteniamo $b = -ba = ba^2 \in I^2$. Induttivamente, avremo che $b \in I^n$ per ogni n e quindi $b = 0$, cioè la tesi.

Soluzione E. *8* La verifica del fatto che $I[x]$ è un ideale di $A[x]$ è immediata, usando il fatto che I è un ideale di A.
Consideriamo la funzione $\varphi\colon A[x] \longrightarrow \left(A/I\right)[x]$ definita da $\varphi\left(\sum_i a_i x^i\right) = \sum_i \overline{a_i} x^i$. È facile verificare φ che è un omomorfismo surgettivo; inoltre $f(x) \in \operatorname{Ker}\varphi$ se e solo se $\sum_i \overline{a_i} x^i = 0$, cioè, per il principio di identità dei polinomi, se e solo se $\overline{a_i} = \overline{0}$ per ogni i, i.e. se e solo se $a_i \in I$ per ogni i e quindi se e solo se $f(x) \in I[x]$; la tesi segue ora dal I teorema di omomorfismo di anelli.

Soluzione E. *9* Siano $f = \sum_{i=0}^n f_i x^i$, $g = \sum_{j=0}^m g_j x^j$ e $h = fg = \sum_{l=0}^t h_l x^l$. Se $(h_0, \ldots, h_t)$ fosse un ideale proprio di A esisterebbe un ideale massimale $\mathfrak{m} \supseteq (h_0, \ldots, h_t)$; d'altra parte, per ipotesi, esistono f_i e g_j che non appartengono ad $\mathfrak{m}$. Siano r, s i più piccoli indici per cui $f_r, g_s \notin \mathfrak{m}$. Allora, da $h_{r+s} = \sum_{i=0}^{r+s} f_i g_{r+s-i} = \sum_{i=0}^{r-1} f_i g_{r+s-i} + f_r g_s + \sum_{i=r+1}^{r+s} f_i g_{r+s-i}$, si otterrebbe $f_r g_s \in \mathfrak{m}$, che è assurdo.
Alternativamente, si può argomentare nel seguente modo: se $\mathfrak{m} \supseteq (h_0, \ldots, h_t)$, allora $\overline{fg} = \overline{h} = 0$ in $A[x]/\mathfrak{m}[x]$, che è un dominio, perché isomorfo a $(A/\mathfrak{m})[x]$, cf. **E.**8. Pertanto si dovrebbe avere che $\mathfrak{m} \supseteq (f_0, \ldots, f_n)$ oppure $\mathfrak{m} \supseteq (g_0, \ldots, g_m)$, che è contro l'ipotesi.

Soluzione E. *10* Dato un polinomio $f = \sum_{i=0}^n f_i x^i \in A[x]$, denotiamo con $I(f) = (f_0, \ldots, f_n)$ l'ideale di A generato dai coefficienti di f.
Se fg è primitivo, si ha che $(1) = I(fg) \subseteq I(f)I(g)$, da cui $I(f) = I(g) = (1)$. Il viceversa è fornito da **E.**9.

Soluzione E. *11* Per la caratterizzazione degli anelli locali **T.** 16, basta dimostrare che ogni elemento $a \notin \mathcal{J}(A)$ è invertibile. Per (ii), esiste $0 \neq x \in A$ tale che $\mathcal{J}(A) = (x)$; inoltre, se $a \notin \mathcal{J}(A)$, allora $(\mathcal{J}(A), a) = (b)$ ove $b \notin \mathcal{J}(A)$. Da questo segue che $x = by$ per qualche y. Poiché $\mathcal{J}(A)$ è un

ideale primo e $b \notin \mathcal{J}(A)$, si deve avere $y \in \mathcal{J}(A)$; quindi $y = cx$ con $c \in A$. Otteniamo dunque $x = by = bcx$, e pertanto $x(1 - bc) = 0$. Da questo, usando (iii), deduciamo che $1 - bc \in \mathcal{J}(A)$; di conseguenza $1 - (1 - bc) = bc$ è invertibile per **T.** 15 e quindi b lo è. Da ciò segue che $(\mathcal{J}(A), a) = (1)$ ed esiste dunque $s \in A$ tale che $1 - sa \in \mathcal{J}(A)$; ragionando come prima, otteniamo allora che a è invertibile, come volevamo.

Soluzione E. *12* 1. Se $(a) = (b)$ esistono $r, s \in A$ tali che $a = bs = ars$. Supponiamo per assurdo che s non sia invertibile; allora $s \in \mathfrak{m}$ e dunque $1 - rs$ è invertibile. Dalla relazione $a(1 - rs) = 0$, si ottiene allora che $a = 0$, contro l'ipotesi. Il viceversa è ovvio.

2. Sia $m = ab$ e supponiamo che a non sia invertibile. Allora, per il punto precedente $(m) \subsetneq (b)$. Dalla massimalità di (m) segue che $(b) = A$, e abbiamo quindi mostrato che b è invertibile e m è irriducibile.

Soluzione E. *13* Siano $a \in I$, $b \in J$ tali che $a + b = 1$. Dato che $I \subseteq \mathcal{J}(A)$, si ha che $1 - a = b \in J$ è invertibile, da cui la tesi.

Soluzione E. *14* Sia a un elemento idempotente, ossia tale che $a(1-a) = 0$. Se a non è invertibile, allora è contenuto nell'ideale massimale di A e $1 - a$ è invertibile, quindi $a = 0$; altrimenti a è invertibile e $a = 1$.

Soluzione E. *15* 1. Possiamo scrivere $2a = a + a = (a + a)^2 = 4a$, da cui $2a = 0$.

2. Sia $A/\mathfrak{p}$ un dominio e $\overline{a} \neq 0$ in $A/\mathfrak{p}$. Allora, dato che $\overline{a}^2 = \overline{a^2} = \overline{a}$, avremo che $\overline{a} = \overline{1}$ e $A/\mathfrak{p}$ è un campo con due elementi. In particolare, $\mathfrak{p}$ è anche massimale.

3. Basta osservare che, dati due qualsiasi elementi $a, b \in A$, si ha $a = a(a + b - ab)$ e $b = b(a + b - ab)$ e quindi $(a, b) = (a + b - ab)$.

Soluzione E. *16* A è un dominio perché (0) è primo. Sia $b \in A$ un elemento non invertibile; dato che (b^2) è primo, si ha $b \in (b^2)$ e quindi $(b) = (b^2)$ cio $b = ab^2$ per qualche $a \in A$. Dato che b non è invertibile, e dunque $ab \neq 1$, da $b(1 - ab) = 0$ segue che $b = 0$, e ciò mostra che A è un campo.

Soluzione E. *17* 1. Per ogni $m, n \in \mathbb{Z}$ sappiamo che esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha m + \beta n = \gcd(m, n)$, che mostra che $(m, n) \supseteq (\gcd(m, n))$. Per l'altra inclusione basta osservare che $\gcd(m, n) | m, n$ e dunque $(\gcd(m, n)) \supseteq (m, n)$.

2. Sia $a \in I \cap J$. Allora esistono $\alpha, \beta \in \mathbb{Z}$ tali che $a = \alpha m = \beta n$. Da ciò si deduce che $\operatorname{lcm}(m, n) | a$. Viceversa, se h è il minimo comune multiplo di m e n, e questo divide un certo $a \in A$, allora $m | a$ e $n | a$, per cui si ha anche l'altra inclusione.

3. Dato che $IJ = (ij \colon i \in I, j \in J)$ è l'ideale *generato* dai prodotti, avremo sicuramente che $mn \in IJ$. D'altra parte, se $a \in IJ$, allora $a = \sum_{h=1}^{r} a_h(\alpha_h m)(\beta_h n)$, per un certo intero r e $a_h, \alpha_h, \beta_h \in \mathbb{Z}$. Pertanto possiamo scrivere a come $(\sum_{h=1}^{r} a_h \alpha_h \beta_h) mn$, che mostra l'altra inclusione.

4. Osserviamo intanto che $I : J = (m) \colon (n)$ è l'insieme degli elementi $a \in A$ tali che $an \in (m)$. Chiaramente $n \cdot m / \gcd(m, n)$ è multiplo di m, per cui vale $\supseteq$. Inoltre, se scriviamo $m = m' \gcd(m, n)$ e $n = n' \gcd(m, n)$, e $a \in I \colon J$ allora an' è multiplo di m', ovvero anche l'altra inclusione è dimostrata.

5. Per il teorema fondamentale dell'aritmetica possiamo scrivere ogni $d \in \mathbb{Z}$ come $d = \pm \prod_{p \in \mathbb{N} \text{ primo}} p^{d_p}$, ove $d_p = 0$ per quasi ogni p. Usando i punti precedenti, si vede che la tesi è equivalente a mostrare che $\operatorname{lcm}(m, \gcd(n, h)) = \gcd(\operatorname{lcm}(m, n), \operatorname{lcm}(m, h))$, ovvero che, per ogni primo positivo p si ha

$$\max\{m_p, \min\{n_p, h_p\}\} = \min\{\max\{m_p, n_p\}, \max\{m_p, h_p\}\},$$

la cui verifica è immediata.

6. Usando i punti precedenti abbiamo che

$$(I + J)(I \cap J) = (\gcd(m, n) \operatorname{lcm}(m, n)) = (mn) = IJ.$$

Soluzione E. *18* I punti 1 e 2 seguono immediatamente dalla definizione di ideale quoziente.

3. Si ha che $a \in (I \colon J) \colon H$ se e solo se $aH \subseteq I \colon J$, dunque se e solo se $aHJ \subseteq I$, cioè se e solo se $aJH \subseteq I$, e ciò dimostra le due uguaglianze.

4. Basta osservare che $aJ \subseteq I_\alpha$ per ogni α se e solo se $a \in I_\alpha : J$ per ogni α.

5. Se $a \sum_\beta J_\beta \subseteq I$, allora $aJ_\beta \subseteq a \sum_\beta J_\beta \subseteq I$ per ogni β, il che prova $\subseteq$.

Ora, se $aJ_\beta \subseteq I$ per ogni β, dato un qualsiasi $b = \sum_\beta j_\beta$, ove la somma è finita e $j_\beta \in J_\beta$ per ogni β, avremo che $ab = \sum_\beta aj_\beta \subseteq I$, cioè abbiamo verificato anche l'altra inclusione.

Soluzione E. *19* È sempre vero che $I + (J \cap H) \subseteq (I + J) \cap (I + H)$, ma il contenimento può essere stretto. Si considerino ad esempio $A = K[x, y]$, con K campo, e gli ideali $I = (x + y)$, $J = (x)$ e $H = (y)$. Si ottiene

$$I+(J\cap H) = (x+y, xy) \quad \text{e} \quad (I+J)\cap(I+H) = (x+y, x)\cap(x+y, y) = (x, y)\ .$$

Soluzione E. *20* Sia $g \in \frac{1}{f}(I \cap (f))$; allora $gf \in I$ ossia $g \in I : (f)$.

Viceversa, se $g \in I : (f)$ allora $gf \in I$ e quindi $gf \in (I \cap (f))$, e allora $g \in \frac{1}{f}(I \cap (f))$.

Soluzione E. *21* 1. Per ipotesi esistono $a \in I$, $b \in J$ e $h_1, h_2 \in H$ tali che $a + h_1 = b + h_2 = 1$. Possiamo scrivere $1 = (a + h_1)(b + h_2) = ab + q$, con $q = ah_2 + bh_1 + h_1h_2 \in H$. Allora, per ogni $n \in \mathbb{N}$, avremo $1 = (ab + q)^n = abp + q^n \in I \cap J + H^n$, con $p = \sum_{i=1}^{n} \binom{n}{i}(ab)^{i-1}q^{n-i} \in A$.

2. Basta provare che $H \subseteq I$. Sia $h \in H$; per ipotesi esistono $j_1 \in H \cap J$, $j_2 \in I \cap J$ e $i \in I$ tali che $i + j_2 = h + j_1$, da cui deduciamo che $h = i - j_1 + j_2 \in I$, come volevamo.

Soluzione E. *22* Per induzione su n. L'affermazione è ovvia per $n = 1$. Sia $n = 2$; per $i = 1, 2$, siano $a_i \in I$, $b_i \in H_i$ tali che $1 = a_i + b_i$. Allora $1 = (a_1 + b_1)(a_2 + b_2) = a_1a_2 + a_1b_2 + a_2b_1 + b_1b_2 \in I + H_1H_2$. Sia ora $n \geq 3$. Per ipotesi induttiva si ha che $I + H_1 \cdots H_{n-1} = A$ e per ipotesi $I + H_n = A$; la conclusione discende allora dal caso $n = 2$.

Soluzione E. *23* 1. Sappiamo che $\sqrt{I} = (1)$ se e solo se $I = (1)$, cf **T.**6.5., dunque $\sqrt{IJ} = A$ se e solo se $IJ = A$. Dato che $IJ \subset I, J$ la conclusione è immediata.

2. Si ha sicuramente che $\mathfrak{p} \subseteq I, J$. Se $\mathfrak{p}$ non contenesse né I né J allora esisterebbero elementi $i \in I \setminus \mathfrak{p}$ e $j \in J \setminus \mathfrak{p}$ tali che $ij \in IJ = \mathfrak{p}$, contraddicendo la primalità di $\mathfrak{p}$. Pertanto $I = \mathfrak{p}$ oppure $J = \mathfrak{p}$.

Soluzione E. *24* 1. Dato che ogni ideale I è contenuto nel suo radicale, se $I + J = (1)$ allora anche l'altra uguaglianza è vera.

Viceversa, se a, b sono elementi tali che $a+b=1$, con $a^m \in I$, $b^n \in J$, allora $1=(a+b)^{m+n}=a^m\sum_{i=0}^{n-1}\binom{m+n-i}{i}a^{n-i}b^i+b^n\sum_{i=n}^{m+n}\binom{m+n-i}{i}a^{m+n-i}b^{i-n} \in I+J$, e abbiamo concluso.

2. Dato che $\sqrt{I+\sqrt{J}} \supseteq I+\sqrt{J} \supseteq I+J$, basta provare la relazione $\subseteq$. Sia $a \in \sqrt{I+\sqrt{J}}$; allora esiste $m \in \mathbb{N}$ tale che $a^m = i+j$, con $i \in I, j \in \sqrt{J}$. Se $n \in \mathbb{N}$ è tale che $j^n \in J$, troviamo che $a^{nm}=(i+j)^n = c+j^n$, con $c \in I$ e $j^n \in J$, e la conclusione segue subito.

Soluzione E. *25* Consideriamo in $\mathbb{Q}[x,y]$ gli ideali $I=(x^2+y)$ e $J=(x^2-y)$. Dato che x^2+y e x^2-y sono irriducibili in $\mathbb{Q}[x,y]$, si ha $\sqrt{I}=I$ e $\sqrt{J}=J$, cosicché $\sqrt{I}+\sqrt{J}=(x^2,y)$, mentre $\sqrt{I+J}=(x,y)$.

Soluzione E. *26* Proviamo che $\sqrt{I}=(x)$, che è un ideale primo di A. Infatti, $x^2 \in I$ e dunque $(x) \subseteq \sqrt{I}$. D'altra parte, se $a \in A$ è tale che $a^k \in I$, avremo che $a^k = \alpha x^2 + \beta xy \in (x)$, per qualche $\alpha, \beta \in A$. Dalla primalità di (x) discende allora che $a \in (x)$, e l'altra inclusione è verificata. Rimane da mostrare che I non è primario; a tal scopo basta osservare che $x \notin I$, $y^n \notin (x)$ per ogni $n \in \mathbb{N}$, mentre $xy \in I$.

Soluzione E. *27* Poiché $\mathcal{N}(A) \subseteq \mathcal{J}(A)$, è sufficiente provare l'inclusione opposta. Supponiamo allora per assurdo che $\mathcal{J}(A) \not\subseteq \mathcal{N}(A)$. In tal caso, per ipotesi esisterebbe un elemento $0 \neq a \in \mathcal{J}(A)$ idempotente, i.e. tale che $a(a-1)=0$. Dato che $a \in \mathcal{J}(A)$, $a-1$ risulterebbe invertibile e si avrebbe pertanto $a=0$, che fornisce la contraddizione cercata.

Soluzione E. *28* $1 \Rightarrow 2$. Per ipotesi, A è un anello locale e $\mathcal{N}(A)$ è il suo ideale massimale. Allora, se a vi appartiene è nilpotente, altrimenti è invertibile.

$2 \Rightarrow 3$. Se a è nilpotente allora $\overline{a}=0$ in $A/\mathcal{N}(A)$; altrimenti a è invertibile in A e quindi $\overline{a}$ è invertibile in $A/\mathcal{N}(A)$.

$3 \Rightarrow 1$. Sia $\mathfrak{p} \subset A$ un ideale primo, allora $\mathcal{N}(A) \subseteq \mathfrak{p}$. Poiché $\mathcal{N}(A)$ è massimale, si deve avere necessariamente che $\mathcal{N}(A)=\mathfrak{p}$, ossia A possiede un solo ideale primo.

Soluzione E. *29* L'elemento $a \in \sqrt{\cup_\alpha E_\alpha}$ se e solo se esistono $n \in \mathbb{N}$ e un indice $\alpha_0 \in \Lambda$ tali che $a^n \in E_{\alpha_0}$, quindi se e solo se $a \in \sqrt{E_{\alpha_0}} \subseteq \bigcup_\alpha \sqrt{E_\alpha}$. L'altra inclusione segue immediatamente da $E_\alpha \subseteq \bigcup_\alpha E_\alpha$ per ogni α.

Soluzione E. *30* Dalle definizioni di divisore di zero e annullatore di un elemento si ha che $\mathcal{D}(A) = \bigcup_{0 \neq a \in A} \operatorname{Ann} a$. Visto che le operazioni di radicale e unione commutano per **E.**29, basta mostrare che $\mathcal{D}(A) = \sqrt{\mathcal{D}(A)}$. Se $0 \neq a \in \sqrt{\mathcal{D}(A)}$ allora siano n il minimo intero tale che $a^n \in \mathcal{D}(A)$ e $b \neq 0$ tale che $a^n b = 0$. Dato che $a^{n-1} b \neq 0$, a è uno zero divisore e abbiamo concluso.

Soluzione E. *31* 1. Indichiamo con π la proiezione $A \to A/\mathcal{J}(A)$. Se $a \in A$ è invertibile e b è il suo inverso, $ab = 1$ e quindi $\overline{a}\overline{b} = \pi(a)\pi(b) = \pi(1) = 1$. Viceversa, se esiste $b \in A$ tale che $\overline{a}\overline{b} = 1$ si ha che $1 - ab \in \mathcal{J}(A)$ e quindi $ab = 1 - (1 - ab)$ è invertibile in A; quindi a è invertibile, come richiesto.

2. Sia $a \in \mathcal{J}(A)$ tale che $a^2 = a$. Si ha che $1 - a$ è invertibile e quindi $a(1 - a) = 0$ implica che $a = 0$.

Soluzione E. *32* Per ipotesi, $\overline{a}^2 = \overline{a}$, ovvero $a(1-a) \in I$. Poiché $a \in \mathcal{J}(A)$, $1 - a$ è invertibile e quindi $a \in I$.

Soluzione E. *33* Osserviamo che, per ipotesi, A non è un campo. Supponiamo per assurdo che A possegga solo un numero finito di ideali massimali $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ e, per ogni $i = 1, \ldots, k$, sia a_i un elemento di $\mathfrak{m}_i$ non nullo. Allora, $0 \neq a = \prod_i a_i \in \bigcap_i \mathfrak{m}_i = \mathcal{J}(A)$; per ogni $b \in A$ avremo allora che $1 - ab$ è invertibile. Ora, poiché A ha infiniti elementi tra cui solo un numero finito di questi è invertibile, esiste $b_1 \neq b$ tale che $1 - ab = 1 - ab_1$. Essendo A un dominio, questo implica che $b = b_1$, che è la contraddizione cercata.

Soluzione E. *34* Ricordiamo che le operazioni sono definite componente per componente. Pertanto, dati I, J ideali di A e B rispettivamente, per ogni $(a, b) \in A \times B$ e per ogni $(i, j) \in I \times J$, $(a, b)(i, j) = (ai, bj) \in I \times J$. Questo implica che $I \times J$ è ideale di $A \times B$.
Viceversa, sia $H \subseteq A \times B$ un ideale. Mostriamo che esistono ideali I di A e J di B tali che $H = I \times J$. A tal scopo consideriamo le proiezioni $\pi_1 \colon A \times B \longrightarrow A$, e $\pi_2 \colon A \times B \longrightarrow B$, definite da $(a, b) \mapsto a$, $(a, b) \mapsto b$ rispettivamente; è facile verificare che si tratta di omomorfismi surgettivi di anelli. Pertanto $\pi_1(H)$ e

$\pi_2(H)$ sono ideali di A e B rispettivamente. Inoltre, se $(a,b) \in H$, avremo $a = \pi_1(a,b) \in \pi_1(H)$ e $b = \pi_2(a,b) \in \pi_2(H)$, per cui $H \subseteq \pi_1(H) \times \pi_2(H)$. Sia ora $(a,b) \in \pi_1(H) \times \pi_2(H)$; dunque esistono un $b_1 \in B$ tale che $(a,b_1) \in H$ e un $a_1 \in A$ tale che $(a_1,b) \in H$, da cui segue che $(a,0) = (1,0)(a,b_1)$ e $(0,b) = (0,1)(a_1,b)$, e quindi anche $(a,b) = (a,0) + (0,b)$, sono elementi di H.

Osserviamo che, se $A, B \neq 0$, $A \times B$ non è un dominio, in quanto, ad esempio $(1,0)(0,1) = (0,0)$.

Sia $H = I \times J$ un ideale di $A \times B$ e consideriamo l'omomorfismo $f : A \times B \longrightarrow A/I \times B/J$ definito da $(a,b) \mapsto (\overline{a}, \overline{\overline{b}})$; esso è chiaramente surgettivo, poiché le singole mappe di proiezione lo sono, e il suo nucleo è $I \times J = H$. Dunque, per il primo teorema d'omomorfismo, $(A \times B)/H = (A \times B)/(I \times J) \simeq A/I \times B/J$.

Dalle osservazioni precedenti possiamo concludere che, per essere primo, rispettivamente massimale, H deve essere della forma $I \times 1$ oppure $1 \times J$, con I ideale primo, risp. massimale, di A e J ideale primo, risp. massimale, di B.

Soluzione E. *35* È una semplice generalizzazione del caso $n = 2$, cf. **E.**34. Inoltre, un ideale $H = I_1 \times \cdots \times I_n$ è primo, rispettivamente massimale, se e solo se $H = (1) \times \cdots \times (1) \times I_j \times (1) \times \cdots \times (1)$, con $j \in \{1, \ldots, n\}$ e I_j ideale primo, risp. massimale, di A_j.

Soluzione E. *36* 1. Sia $A \simeq \prod_{i=1}^n K_i$, con K_i campo per ogni i, e $n \in \mathbb{N}_+$. Allora, per **E.**35, gli ideali di A sono tutti del tipo $I_1 \times \cdots \times I_n$ con $I_j = (0)$ oppure $I_j = K_j$, quindi sono in numero finito. Inoltre gli ideali massimali sono quelli con un unico $I_j = (0)$ e dunque $\mathcal{J}(A) = \bigcap_{i=1}^n J_i = (0)$.

Viceversa, se A ha solo un numero finito di ideali massimali, e dunque a due a due comassimali, e $\mathcal{J}(A) = (0)$, per il Teorema Cinese del Resto si ha che $A \simeq A/\mathcal{J}(A) \simeq \prod_{i=1}^n A/\mathfrak{m}_i$ è una somma diretta di campi.

2. Se $A \simeq \prod_{i=1}^n K_i$ con K_i campo per ogni i e $n \in \mathbb{N}_+$, allora un elemento nilpotente è del tipo $(a_1, \ldots, a_n)$ con $a_i \in K_i$ nilpotente per ogni i. Dato che K_i campo, ciò implica $a_i = 0$ per ogni i.

Viceversa in un anello finito ci sono solo un numero finito di ideali; inoltre per ogni ideale primo $\mathfrak{p}$ il quoziente $A/\mathfrak{p}$ è un dominio finito, quindi un campo.

Di conseguenza ogni ideale primo è massimale, $\mathcal{J}(A) = \mathcal{N}(A) = (0)$ e la tesi segue dal punto 1.

Soluzione E. *37* Ricordiamo che la somma e il prodotto in una somma diretta di anelli sono definiti componente per componente, e gli ideali sono tutti e soli prodotti di ideali nelle singole componenti, cf. **E.**35.

1. Poiché $\mathbb{Z}$ e $\mathbb{Q}$ non hanno elementi nilpotenti diversi da zero, il nilradicale di A è costituito dagli elementi della forma $(0, \overline{a}, 0)$ con $\overline{a} \in \mathbb{Z}/(36)$ nilpotente; pertanto $\mathcal{N}(A) = (0) \times (\overline{6}) \times (0)$.

2. Un elemento è idempotente se e solo se $(a^2, \overline{b}^2, c^2) = (a, \overline{b}, c)$, quindi si deve avere $a, c = 0, 1$ e $b^2 \equiv b \mod 36$. Dato che $\mathbb{Z}/(36) \simeq \mathbb{Z}/(4) \times \mathbb{Z}/(9)$ e gli unici elementi idempotenti in $\mathbb{Z}/(4)$ e $\mathbb{Z}/(9)$ sono 0 e 1, otteniamo che $b \equiv 0, 1, 9, 28 \mod 36$, e abbiamo concluso.

3. Come osservato all'inizio, gli ideali di A sono della forma $I \times J \times H$ con I, J, H ideali di $\mathbb{Z}$, $\mathbb{Z}/(36)$, $\mathbb{Q}$ rispettivamente e sono quindi tutti principali, cosicché A è a ideali principali, i.e. A è PIR, ma A non è un dominio e quindi non è PID.

4. Un ideale è primo se e solo se $A/\mathfrak{p}$ è un dominio e quindi si deve avere $\mathfrak{p} = (p, \overline{1}, 1)$, con p primo in $\mathbb{Z}$ o $p = 0$, oppure $(1, \mathfrak{q}, 1)$, con $\mathfrak{q}$ ideale primo di $\mathbb{Z}/(36)$, ossia $\mathfrak{q} = (\overline{q})$ con $(q, 36) \neq 1$ e q primo in $\mathbb{Z}$, e $\mathfrak{p} = (1, \overline{1}, 0)$.
È immediato verificare che l'unico primo non massimale è quello generato da $(0, \overline{1}, 1)$.

Soluzione E. *38* 1. Consideriamo solo numeri razionali $\frac{a}{b}$ ridotti, i.e. tali che $\gcd(a, b) = 1$ e sia $I = \left\{ \frac{a}{b} \in A_p \colon a \equiv 0 \mod p \right\}$. Allora, per ogni $\frac{a}{b}, \frac{c}{d} \in I$ e $\frac{\alpha}{\beta} \in A_p$ si ha che $0 \in I$, $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd} \in I$ e $\frac{\alpha}{\beta}\frac{a}{b} = \frac{\alpha a}{\beta b} \in I$; dunque I è un ideale di A_p. Inoltre $\frac{\alpha}{\beta} \notin I$ implica $\alpha \not\equiv 0 \mod p$, quindi $\frac{\beta}{\alpha} \in A_p$ e ogni elemento fuori da I è invertibile; pertanto A_p è locale con ideale massimale I, cf. **T.**16. Infine la mappa $f : A_p \longrightarrow \mathbb{Z}/(p)$ definita da $f\left(\frac{a}{b}\right) = \overline{a}\overline{b^{-1}}$ è un omomorfismo surgettivo: infatti, per ogni $\frac{a}{b}, \frac{c}{d} \in A_p$

$$f\left(\frac{a}{b} + \frac{c}{d}\right) = f\left(\frac{ad + bc}{bd}\right) = (\overline{ad + bc})\overline{b^{-1}d^{-1}} = \overline{a}\overline{b^{-1}} + \overline{c}\overline{d^{-1}} = f\left(\frac{a}{b}\right) + f\left(\frac{c}{d}\right)$$

$$f\left(\frac{a}{b}\cdot\frac{c}{d}\right)=f\left(\frac{ac}{bd}\right)=\overline{ac}\,\overline{(bd)^{-1}}=\overline{a}\overline{b^{-1}}\,\overline{c}\overline{d^{-1}}=f\left(\frac{a}{b}\right)f\left(\frac{c}{d}\right)$$

e, per ogni $\overline{a}\in\mathbb{Z}/(p)$, si ha $f\left(\frac{a}{1}\right)=\overline{a}$. Ovviamente $f\left(\frac{a}{b}\right)=\overline{0}$ se e solo se $a\equiv 0 \mod p$, dunque $\operatorname{Ker} f=I$ e f induce un isomorfismo $A_p/I\simeq\mathbb{Z}/(p)$.

2. Analogamente al punto precedente si dimostra che tutti gli insiemi $I_j=\left\{\frac{a}{b}\in A_{p_1,\dots,p_n}\colon a\equiv 0 \mod p_j\right\}$ per $j\in\{1,\dots,n\}$, sono ideali di $A_{p_1,\dots,p_n}$ e che gli omomorfismi $f_j : A_{p_1,\dots,p_n}\longrightarrow\mathbb{Z}/(p_j)$, definiti da $f\left(\frac{a}{b}\right)=\overline{a}\overline{b^{-1}}$, inducono isomorfismi $\widetilde{f}_j : A_{p_1,\dots,p_n}/I_j\longrightarrow\mathbb{Z}/(p_j)$. Dunque tutti gli I_j sono ideali massimali di $A_{p_1,\dots,p_n}$.
Sia adesso $0\neq J$ un ideale di $A_{p_1,\dots,p_n}$; se $J\not\subseteq I_j$ per ogni j, allora esiste $\frac{a}{b}\in J$ tale che $a\not\equiv 0 \mod p_j$ per ogni j, i.e. $\frac{b}{a}\in A_{p_1,\dots,p_n}$ e $J=A_{p_1,\dots,p_n}$. Dunque gli I_j sono tutti e soli gli ideali massimali di $A_{p_1,\dots,p_n}$.

Soluzione E. *39* Sia $A=\prod_{i=1}^n A_i$ con A_i anello semilocale per ogni i. Dato che gli ideali di A sono somme dirette di ideali degli A_i e, se $I=\prod_{i=1}^n I_i$, si ha $A/I=\prod_i A_i/I_i$, gli ideali massimali di A sono tutti e soli quelli del tipo $A_1\times\cdots\times A_{i-1}\times\mathfrak{m}_i\times A_{i+1}\cdots\times A_n$ con $\mathfrak{m}_i$ massimale in A_i e sono dunque in numero finito.
L'anello $A_{p_1,\dots,p_n}$ definito in **E.**38 è semilocale ma, essendo un dominio, non può essere una somma diretta non banale di anelli.

Soluzione E. *40* Proviamo la tesi dimostrando che se I è un ideale primo, allora in A/I ogni elemento diverso da zero è invertibile. Sia dunque $0\neq\overline{a}\in A/I$. Per ipotesi si ha che $\overline{a}(\overline{a}^{n-1}-1)=0$; poiché A/I è un dominio d'integrità si ha la tesi.

Soluzione E. *41* 1. L'insieme Σ è non vuoto, dato che $(0)\in\Sigma$, e le catene $I_1\subset I_2\subset\dots$ in Σ sono superiormente limitate dall'ideale $\bigcup_j I_j$ che è un ideale contenuto in $\mathcal{D}(A)$, quindi per il Lemma di Zorn esiste in Σ almeno un elemento massimale P. Proviamo che P è primo: siano $a,b\notin P$ e proviamo che anche $ab\notin P$. Consideriamo gli ideali (P,a) e (P,b); essi per ipotesi contengono propriamente P e quindi esistono $\alpha=p+ka\in(P,a)$ e $\beta=q+hb\in(P,b)$ che non sono divisori di zero. Allora l'elemento $\alpha\beta\in(P,ab)$ non è un divisore di zero, da questo segue che $P\subsetneq(P,ab)$ e quindi $ab\notin P$.

2. Osservando che, se $a \neq 0$ allora $\operatorname{Ann} a \in \Sigma$ e $\mathcal{D}(A) = \bigcup_{0 \neq a \in A} \operatorname{Ann} a$, possiamo scrivere $\mathcal{D}(A) \subseteq \cup_\alpha \mathfrak{p}_\alpha$, ove $\mathfrak{p}_\alpha$ è un elemento massimale di Σ e quindi, per il punto precedente, è un ideale primo. D'altro lato, tali $\mathfrak{p}_\alpha$ sono ideali di zero divisori, e dunque ciascuno di essi è contenuto in $\mathcal{D}(A)$, e vale pertanto $\mathcal{D}(A) = \bigcup_\alpha \mathfrak{p}_\alpha$

Soluzione E. *42* Sia $\Sigma = \{J \subset A \colon J \text{ non è principale}\}$ e supponiamo per assurdo che $\Sigma \neq \emptyset$. Per ogni catena ascendente di elementi di Σ, l'unione degli elementi di tale catena è un ideale non principale (verificare!), pertanto dal lemma di Zorn discende che Σ possiede almeno un elemento massimale I. Poiché I non è principale, per ipotesi non è primo ed esistono dunque $a, b \notin I$ con $ab \in I$. Inoltre, per la massimalità di I, l'ideale (I, a) è principale; sia dunque $(I, a) = (c)$. Osserviamo anche che $b \in I \colon c$, perché $bI \subseteq I$ e $ab \in I$; dunque $I \subsetneq I \colon c$. Di conseguenza, ancora per la massimalità di I, anche $I \colon c = (d)$ è principale. Troviamo ora una contraddizione dimostrando che $I = (cd)$. Si ha subito che $(cd) \subseteq I$; per l'inclusione opposta, se $j \in I \subset (I, a) = (c)$, allora $j = ck$ con $k \in I \colon c = (d)$, i.e. $k = hd$ e $j = hcd \in (cd)$.

Soluzione E. *43* Sia $\Sigma = \{I \subset A \colon I \text{ ideale non finitamente generato}\}$, e supponiamo per assurdo che $\Sigma \neq \emptyset$. Per ogni catena ascendente di elementi di Σ, l'unione degli elementi di tale catena è un ideale non finitamente generato. Pertanto, dal lemma di Zorn discende che Σ possiede almeno un elemento massimale P.

Poiché P non è finitamente generato, è un ideale proprio e non primo. Esistono dunque $a, b \notin P$ con $ab \in P$ e, per la massimalità di P, (P, a) è finitamente generato. Esistono dunque un intero k ed elementi $d_1 = p_1 + s_1 a, \ldots, d_k = p_k + s_k a$, con $p_i \in P$ e $s_i \in A$ per ogni i tali che $(P, a) = (d_1, \ldots, d_k)$.
Consideriamo anche l'ideale $P : a$, che contiene P propriamente, dato che $b \in P : a$ ma $b \notin P$. Di nuovo per massimalità di P, $J = P : a$ è finitamente generato, e dunque anche aJ lo è.

Proviamo ora che $P = (p_1, \ldots, p_k) + aJ$: in questo modo P risulterà finitamente generato, che è la contraddizione cercata. Certamente vale l'inclusione $\supseteq$. Sia dunque $c \in P \subseteq (P, a)$, con $c = \sum_i c_i d_i = \sum_i c_i (p_i + s_i a) = \sum_i c_i p_i + ja$,

per certi $c_i, j \in A$. Allora $c - \sum_i c_i p_i \in P$, per cui $j \in P : a = J$ e $c \in (p_1, \ldots, p_k) + aJ$, come volevamo.

Soluzione E. *44* 1. Se $a, b \in \operatorname{Ker} f$ allora $f(a) = f(b) = 0$; inoltre $f(a+b) = f(a)+f(b) = 0$, i.e. $a+b \in \operatorname{Ker} f$; se poi $c \in A$, allora $f(ca) = f(c)f(a) = 0$, quindi $ca \in \operatorname{Ker} f$.

2. Sia $\operatorname{Ker} f = (0)$ e siano $a, b \in A$ tali che $f(a) = f(b)$. Allora, $f(a-b) = 0$, ovvero $a - b \in (0)$, cioè $a = b$.
Viceversa, se $\operatorname{Ker} f \neq (0)$, esiste $0 \neq a \in A$ tale che $f(a) = 0 = f(0)$, negando l'iniettività di f.

3. Bisogna verificare che la somma di due elementi dell'immagine è ancora un elemento dell'immagine, che è vero per la linearità di f, e che lo stesso vale per il prodotto, e questo discende dal fatto che, per ogni $a, b \in A$, $f(a)f(b) = f(ab)$. Infine $1_B = f(1_A)$.

Soluzione E. *45* Per definizione di omomorfismo dobbiamo avere $f(0) = 0$ e $f(1) = 1$. Se $n \in \mathbb{Z}_+$, avremo $f(n) = \underbrace{f(1) + \cdots + f(1)}_{n \text{ volte}} = nf(1) = n$, e se $n \in \mathbb{Z}_-$, allora $f(n) = f(-(-n)) = -f(-n) = -(-n) = n$. In conclusione, per ogni $n \in \mathbb{Z}$ dobbiamo avere $f(n) = n$, ovvero l'unico omomorfismo è l'identità.

Soluzione E. *46* 1. Consideriamo $\phi_a \colon A[x] \longrightarrow A$, l'omomorfismo di sostituzione definito da $\phi_a(f) = f(a)$; allora $J = \phi_a^{-1}(I)$ ed è quindi un ideale di $A[x]$.

2. ϕ_a induce un omomorfismo surgettivo $\pi \circ \phi_a \colon A[x] \longrightarrow A/I$ il cui nucleo è J. Allora $A[x]/J \cong A/I$, da cui segue che J è primo se e solo se I lo è.

Si ha che $\phi_a(x-1) = \phi_a(y-2) = y-2 \in I$ e quindi che $(x-1, y-2) \subseteq J$. Dal momento che J è un ideale proprio, poiché ad esempio $x \notin J$, e $(x-1, y-2)$ è un ideale massimale, avremo che $J = (x-1, y-2)$.

Soluzione E. *47* $1 \Rightarrow 2$. Sia A un campo e I un suo ideale. Se $I \neq 0$, allora esiste $0 \neq a \in I$ e tale elemento è invertibile. Pertanto $I = (a) = 1$.

$2 \Rightarrow 3$. Sia $f \colon A \longrightarrow B$ un omomorfismo di anelli. Per $\operatorname{Ker} f$ ci sono per ipotesi solo due possibilità: se $\operatorname{Ker} f = (1)$, allora f è l'omomorfismo nullo e

la condizione che $f(1_A) = 1_B$ implica che $B = 0$, che abbiamo escluso; deve quindi essere $\operatorname{Ker} f = (0)$.

$3 \Rightarrow 2$. Osserviamo che, dato che A è non banale, possiede un ideale massimale $\mathfrak{m}$. Consideriamo allora la proiezione $\pi\colon A \longrightarrow A/\mathfrak{m} \neq 0$; per ipotesi sappiamo che essa è iniettiva e dunque $\mathfrak{m} = \operatorname{Ker} \pi = 0$. Da ciò segue che (0) e (1) sono gli unici ideali di A.

$2 \Rightarrow 1$. Se A non ha ideali non banali, allora per ogni $0 \neq a \in A$, l'ideale generato da a è (1), cioè ogni elemento non nullo di A è invertibile.

Soluzione E. *48* 1. Sia $f \in I[x]$, con $f = \sum_i a_i x^i$ e $a_i \in I$ per ogni i. Dato che $I \subseteq I[x] \subseteq A[x]$, avremo $I[x] \subseteq I^e$.
Per **E.**8, $I[x]$ è un ideale, allora I^e, che è il più piccolo ideale di $A[x]$ che contiene I, è contenuto in $I[x]$.

2. Consideriamo l'omomorfismo $\varphi\colon A[x] \longrightarrow (A/I)[x]$ definito da $\sum_i a_i x^i \mapsto \sum_i \overline{a_i} x^i$; allora $\operatorname{Ker} \varphi = I[x]$. Infatti, $\varphi(\sum_i a_i x^i) = \sum_i \overline{a_i} x^i = 0$ se e solo se $\overline{a_i} = 0$ per ogni i se e solo se $a_i \in I$ per ogni i, ossia se e solo se $\sum_i a_i x^i \in I[x]$. Quindi $A[x]/I[x] \simeq (A/I)[x]$ e $A[x]/I[x]$ è un dominio se e solo se A/I lo è, ossia se e solo se I è primo.

Sia $A = \mathbb{Z}$. Allora per ogni primo p l'ideale (p) è massimale in A, mentre l'ideale $(p)[x] = (p)^e \subsetneq (p, x) \subsetneq A[x]$ non è massimale.

Soluzione E. *49* 1. Sia $b \in f(\sqrt{I})$; dunque $b = f(c)$ con $c^m \in I$ per qualche m. Allora $b^m = f(c)^m = f(c^m) \in f(I)$ da cui $b \in \sqrt{f(I)}$. Quindi $(f(\sqrt{I})) \subseteq \sqrt{f(I)} \subseteq \sqrt{(f(I))}$, come volevamo.
2. Per la surgettività di f, per ogni ideale I si ha che $f(I) = (f(I)) = I^e$.
Abbiamo provato un'inclusione nel punto precedente; verifichiamo allora l'altra: siano $b \in \sqrt{f(I)}$ e m tale che $b^m = f(c)$, con $c \in I$. Per la surgettività di f, si ha anche che $b = f(a)$ per qualche $a \in A$, e dunque $f(a^m - c) = f(a^m) - f(c) = f(a)^m - f(c) = 0$, cioè $a^m - c \in \operatorname{Ker} f \subseteq I$. Si ha allora che $a^m \in I$, $a \in \sqrt{I}$, e dunque $b \in f(\sqrt{I})$.
3. Si ha che $a \in \sqrt{f^{-1}(J)} \iff a^m \in f^{-1}(J)$ per qualche $m \iff f(a)^m = f(a^m) \in J$ per qualche $m \iff f(a) \in \sqrt{J} \iff a \in f^{-1}(\sqrt{J})$.

Soluzione E. *50* 1. Sappiamo che $p = a^2 + b^2$ se e solo se $p \equiv 1 \mod 4$ e che $\mathbb{Z}[i]$ è un anello euclideo e quindi un PID. Allora $p \equiv 3 \mod 4$ implica che p è irriducibile in $\mathbb{Z}[i]$, mentre $p \equiv 1 \mod 4$ implica $p = (a+ib)(a-ib)$ per qualche $a, b \in \mathbb{Z}$; le formule per p dispari seguono immediatamente.
Per $p = 2$ basta osservare che $2 = (1+i)(1-i)$ e che gli ideali $(1+i)$ e $(1-i)$ sono uguali perché $1 + i = (1 - i)i$, ovvero i loro generatori sono associati.
2. Ovviamente $\frac{1-\zeta_p^a}{1-\zeta_p} = 1 + \zeta_p + \cdots + \zeta_p^{a-1} \in \mathbb{Z}[\zeta_p]$. Cerchiamo il suo eventuale inverso: sia b tale che $ab \equiv 1 \mod p$, allora

$$\frac{1-\zeta_p}{1-\zeta_p^a} = \frac{1-\zeta_p^{ab}}{1-\zeta_p^a} = 1 + \zeta_p^a + \cdots + \zeta_p^{a(b-1)} \in \mathbb{Z}[\zeta_p].$$

Ricordiamo che gli elementi ζ_p^a con $a \neq 0$ sono tutte e sole le radici del polinomio $1 + x + \cdots + x^{p-1}$, dunque $1 + x + \cdots + x^{p-1} = \prod_{a\neq 0}(x - \zeta_p^a)$ e, valutando in $x = 1$ si ha $p = \prod_{a\neq 0}(1 - \zeta_p^a)$. Per quanto visto prima $(1 - \zeta_p) = (1 - \zeta_p^a)$ per ogni $a \neq 0$, dunque

$$(p)^e = p\mathbb{Z}[\zeta_p] = \left(\prod_{a\neq 0}(1-\zeta_p^a)\right) = \prod_{a\neq 0}(1-\zeta_p^a) = \prod_{a\neq 0}(1-\zeta_p) = (1-\zeta_p)^{p-1}.$$

Soluzione E. *51* 1. Sia $a \in \mathcal{N}(A)$; allora esiste $n \in \mathbb{N}$ tale che $a^n = 0$ e quindi $f(a)^n = f(a^n) = 0$. Pertanto $f(a) \in \mathcal{N}(B)$ e ciò mostra che $f(\mathcal{N}(A)) \subseteq \mathcal{N}(B)$.
2. Sia $a \in \mathcal{J}(A)$; allora, per ogni $b \in A$, avremo che $1 - ba$ è invertibile. Ne consegue che $f(1 - ba) = 1 - f(b)f(a)$ è invertibile in B. La surgettività di f implica allora che $f(a) \in \mathcal{J}(B)$.
3. Sia $A = \left\{\frac{a}{b} \in \mathbb{Q} \colon \ b \not\equiv 0 \mod 2\right\}$: è facile verificare che è un sottoanello di $\mathbb{Q}$, inoltre notiamo che l'ideale $(2) = \left\{\frac{a}{b} \in A \colon \ a \equiv 0 \mod 2\right\}$ è l'unico ideale massimale, quindi A è un anello locale, cf **E.**38.1. Consideriamo l'omomorfismo di inclusione di A in $\mathbb{Q}$, che sicuramente è iniettivo e non surgettivo; chiaramente $\mathcal{J}(\mathbb{Q}) = 0$ e sappiamo che $\mathcal{J}(A) = (2)$.
4. Consideriamo $f \colon \mathbb{Z} \longrightarrow \mathbb{Z}/(4)$; in questo caso $f(\mathcal{J}(\mathbb{Z})) = (0) \subsetneq \mathcal{J}(\mathbb{Z}/(4)) = (2)$.

5. Sia A semilocale e siano $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ i suoi ideali massimali. Osserviamo che, per **T.**18.3, $f(\mathfrak{m}_i)$ è un ideale massimale di B se $\mathfrak{m}_i \supseteq \operatorname{Ker} f$, oppure è tutto B. Si ha inoltre che $\mathcal{J}(A) = \bigcap_{i=1}^k \mathfrak{m}_i = \prod_{i=1}^k \mathfrak{m}_i$, quindi $f(\mathcal{J}(A)) = f(\prod_{i=1}^k \mathfrak{m}_i) = \prod_{i=1}^k f(\mathfrak{m}_i) = \bigcap_{i=1}^k f(\mathfrak{m}_i) \supseteq \mathcal{J}(B)$.

Soluzione E. *52* Per la corrispondenza tra gli ideali di A e quelli di A/I, è immediato vedere che se A è locale anche A/I è locale per ogni ideale I. Supponiamo quindi che A/I sia locale con ideale massimale $\overline{\mathfrak{m}}$, e sia $\mathfrak{m}$ la sua controimmagine in A. Provando che ogni elemento $a \notin \mathfrak{m}$ è invertibile, avremo che A è locale con massimale $\mathfrak{m}$. Per un tale a si ha che $\overline{a} \notin \overline{\mathfrak{m}}$ e pertanto $\overline{a}$ è invertibile poiché A/I è locale. Esistono allora $b \in A$, $i \in I$ tali che $ab = 1 + i$. Poiché $I \subseteq \mathcal{N}(A)$, da **E.**4 segue che $1 + i$ è invertibile, da cui otteniamo la tesi.

Soluzione E. *53* È sempre vero che $I^2 + J^2 \subseteq (I + J)^2$; mostriamo dunque l'inclusione opposta. Sia $I = (a)$, $J = (b)$ e $I + J = (d)$; abbiamo allora che $(a, b) = (d)$, e possiamo scrivere $a = da_1$ e $b = db_1$ con $\gcd(a_1, b_1) = 1 = \gcd(a_1^2, b_1^2)$. Esistono pertanto $\alpha, \beta \in A$ tali che $1 = \alpha a_1^2 + \beta b_1^2$ e quindi $d^2 = d^2 \cdot 1 = \alpha a^2 + \beta b^2 \in I^2 + J^2$.

Soluzione E. *54* Possiamo supporre $a, b \neq 0$. Se $(a) = (b)$ allora esistono $c, d \in A$ tali che $a = bd = acd$, da cui segue che $a(1 - cd) = 0$, e quindi che $1 - cd \in \mathcal{D}(A) \subseteq \mathcal{J}(A)$. Possiamo allora dedurre che cd è invertibile, da cui discende ad esempio che d è invertibile, come volevamo.

Soluzione E. *55* Osserviamo dapprima che l'ideale $\mathcal{J}(A) = (j)$, ove $j \neq 0$, è primo. Infatti, se $ab \in \mathcal{J}(A) = \mathcal{D}(A)$, allora esiste $c \neq 0$ tale che $cab = 0$ da cui segue che a oppure b è un elemento di $\mathcal{D}(A) = \mathcal{J}(A)$.

Per provare la tesi, dimostriamo che $\mathcal{J}(A)$ è massimale, e al tal scopo basta provare che se $a \notin \mathcal{J}(A)$ allora $(a) + \mathcal{J}(A) = A$. Sia dunque $(a) + \mathcal{J}(A) = (a, j) = (b)$, dove $b \notin \mathcal{J}(A)$; allora $j = bc$ con $c \in \mathcal{J}(A)$, poiché $\mathcal{J}(A)$ è primo. Possiamo scrivere $c = jd$, per qualche d, e da ciò segue che $j(1 - bd) = bc - bc = 0$ e quindi che $1 - bd \in \mathcal{D}(A) = \mathcal{J}(A)$. Allora bd è invertibile e quindi b lo è, che era quello che volevamo.

Soluzione E. *56* Dato che un ideale $\mathfrak{m}$ è massimale se e solo se $A/\mathfrak{m}$ è un campo le affermazioni 1 e 2 sono equivalenti. Proviamo quindi 2. Se a è

irriducibile i suoi soli divisori sono unità o elementi associati ad a, quindi gli unici ideali che contengono (a) sono (1) e (a); dato che ogni ideale di Aè principale, questo prova che ogni elemento irriducibile genera un ideale massimale. Viceversa, sia $b \in A$ riducibile, $b = ac$, con $a, c \notin A^*$; allora $(b) \subsetneq (a) \subsetneq (1)$ e quindi (b) non è massimale.

3. Dato che un ideale non nullo in un PID è primo se e solo se è massimale, la tesi segue dal punto 2.

Soluzione E. *57* Sia $I = (a)$ un ideale primario con $\sqrt{I} = \mathfrak{p} = (p)$; allora esiste $k \in \mathbb{N}$ tale che $p^k \in I$. Quindi $a|p^k$ e, dato che A è un UFD, p è l'unico irriducibile che divide a. Dunque $a = up^t$ per qualche $u \in A^*$ e $t \in \mathbb{N}$, cioè $(a) = (p^t)$.

Soluzione E. *58* Se A è un campo, allora $A[x]$ è un anello euclideo, che è un PID per **T.**28. Viceversa, consideriamo l'omomorfismo di sostituzione $\phi_0 \colon A[x] \longrightarrow A$ dato dalla valutazione di un polinomio $f(x) \in A[x]$ in 0, i.e. $\varphi_0(f) = f(0)$. È facile verificare che $\operatorname{Ker} \varphi_0 = (x)$, da cui discende che $A[x]/(x) \simeq A$. Dato che A è un dominio, poiché $A[x]$ lo è per ipotesi, l'ideale (x) è primo; dato che $A[x]$ è un PID e x è irriducibile, si ha che (x) è massimale o, equivalentemente, che A è un campo.

Soluzione E. *59* Sia $(a, b) = (c)$, allora $c|a$, $c|b$ ed esistono $u, v \in A$ tali che $ua + vb = c$. Inoltre per ogni $d \in A$ che divide sia a che b si ha $d|(ua + vb) = c$. Dunque, per definizione, $d = c$.

Sia $A = \mathbb{Z}[x]$, che è un UFD ma non PID; allora $\gcd(3, x) = 1$ ma per ogni $f, g \in A$ si ha $3f + xg \neq 1$, perché il termine noto a sinistra appartiene a $(3) \subsetneq (1)$.

Soluzione E. *60* Ricordiamo che la norma del numero complesso $\alpha = a + b\sqrt{-5}$ è data da $N(\alpha) = a^2 + 5b^2$; inoltre, dati α, β si ha che $N(\alpha\beta) = N(\alpha)N(\beta)$. Non è difficile verificare che α è invertibile se e solo se $N(\alpha) = 1$ e che nessun elemento di $\mathbb{Z}[\sqrt{-5}]$ ha norma 3.

Siano dunque $a + b\sqrt{-5}, c + d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ tali che $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 3$; allora, passando alle norme, segue che $(a^2 + 5b^2)(c^2 + 5d^2) = 9$, che è possibile se e solo se uno dei due fattori è 1, cioè se e solo se uno

tra $a+b\sqrt{-5}$ e $c+d\sqrt{-5}$ è invertibile. Questo prova che 3 è un elemento irriducibile.
Gli ideali $(3,1+\sqrt{-5})$ e $(3,1-\sqrt{-5})$ sono comassimali e quindi $(3,1+\sqrt{-5})\cap(3,1-\sqrt{-5})=(3,1+\sqrt{-5})(3,1-\sqrt{-5})=(3)$, mentre $(3)\subsetneq(3,1+\sqrt{-5})$ e $(3)\subsetneq(3,1-\sqrt{-5})$, dal momento che la norma di 3 non divide la norma di $1+\sqrt{-5}$ e di $1-\sqrt{-5}$; da questo segue che (3) non è irriducibile.

Soluzione E. *61* Supponiamo per assurdo che esista un elemento $a_1\in A$ non invertibile e che non ammette una decomposizione come prodotto di un numero finito di irriducibili. Allora a_1 non è irriducibile e si può dunque scrivere come prodotto a_2b_1, con a_2 e b_1 entrambi non invertibili e con almeno uno dei due che non ammette una decomposizione come prodotto di un numero finito di irriducibili, sia esso a_2. Possiamo dunque ripetere il ragionamento su a_2 e proseguendo in questo modo ottenere una catena ascendente infinita di ideali $(a_1)\subsetneq(a_2)\subsetneq\ldots$, assurdo.

Soluzione E. *62* Cerchiamo un anello UFD A e un ideale I di A tali che A/I sia un dominio ma senza fattorizzazione unica. Consideriamo $A=\mathbb{Q}[x,y,z,t]/(xy-zt)$. Allora A è un dominio (perché?) e non è UFD. Chiaramente A eredita (UFD1) da $\mathbb{Q}[x,y,z,t]$ e, intuitivamente abbiamo "rovinato" ad hoc l'unicità della fattorizzazione dell'elemento $\overline{xy}$, ovvero abbiamo costruito un anello dove non vale (UFD2). Con i conti si può verificare che $\overline{x},\overline{y},\overline{z},\overline{t}$ sono elementi irriducibili non associati e dedurre che le fattorizzazioni di $\overline{xy}=\overline{zt}$ sono effettivamente distinte.

Osserviamo anche che $\overline{x}$ è irriducibile ma $(\overline{x})$ non è primo, cf. **T.**26 - e lo stesso vale per $\overline{y},\overline{z},\overline{t}$; ci sono infine coppie di elementi di A che non ammettono massimo comun divisore, ad esempio $\overline{xy}$ e $\overline{xz}$.

Soluzione E. *63* 1. Siano $b_1=ax_1-x_1$, $b_2=ax_2-x_2\in I_a$ e $c\in A$; allora $0\in I_a$ e $b_1+b_2=a(x_1+x_2)-(x_1+x_2)$ e $cb_1=a(cx_1)-(cx_1)$ sono elementi di I_a, dunque I_a è un ideale.
Alternativamente, basta osservare che I_a è l'ideale di A generato dall'elemento $a-1$, quindi, in particolare, a è quasi-regolare se e solo se $a-1$ è invertibile.
2. Se a è quasi-regolare allora $a\in I_a$, ed esiste dunque $c\in A$ tale che $a=ac-c$.

Per verificare il viceversa, dobbiamo mostrare che per ogni $d \in A$ si ha che $d \in I_a$ sapendo che, per ipotesi, $a = ac - c$ e quindi che $a \in I_a$. Avremo allora che $ad \in I_a$ e, per definizione di I_a, anche $ad - d \in I_a$; ne segue che $d = ad - (ad - d) \in I_a$.

3. Se a è nilpotente allora $1 - a$ è invertibile e quindi a è quasi-regolare.

4. Sia $0, 1 \neq a \in A$ e proviamo che a è invertibile. Dato che a è un elemento quasi-regolare, $1 - a$ è invertibile per quanto detto sopra. Allora esiste $0 \neq b \in A$ tale che $b - ab = b(1 - a) = 1$, e quindi $ab = b - 1$. Poiché $b \neq 1$ è quasi-regolare, $b - 1$ è invertibile, e da ciò discende subito la tesi.

Soluzione E. *64* 1. Dato che A non è un campo esiste un ideale massimale $\mathfrak{m} \neq (0)$ e sia $0 \neq a \in \mathfrak{m}$. Per ipotesi, $(a) = \prod_{i=1}^{k} \mathfrak{m}_i = \bigcap_{i=1}^{k} \mathfrak{m}_i$ e, dunque, $\bigcap_{i=1}^{k} \mathfrak{m}_i \subseteq \mathfrak{m}$; esiste allora i tale che $\mathfrak{m}_i \subseteq \mathfrak{m}$ e, per la massimalità di $\mathfrak{m}_i$, vale l'uguaglianza. Ora basta porre $I = \mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}\mathfrak{m}_{i+1} \cdots \mathfrak{m}_k$ per ottenere la tesi.

2. Per il punto precedente, sia $I\mathfrak{m} = (a)$, con $a \neq 0$. Moltiplicando per J l'uguaglianza precedente, si ottiene che $J(a) = J\mathfrak{m}I = H\mathfrak{m}I = H(a)$, da cui segue che, per ogni $j \in J$, esiste $h \in H$ tale che $ja = ha$, ossia $a(j - h) = 0$. Poiché $a \neq 0$ e A è un dominio, si ha $j = h$ e da ciò discende che $J \subseteq H$. Scambiando i ruoli di J ed H si ottiene la tesi.

Soluzione E. *65* 1. Dato che $\sqrt{I} \subseteq \sqrt{I \colon J^m}$, basta provare l'altra inclusione.
Per ipotesi $J \not\subseteq \sqrt{I}$, e pertanto esiste $j \in J$ tale che $j^n \notin I$ per ogni $n \in \mathbb{N}$. Sia ora $a \in \sqrt{I \colon J^m}$; allora $a^n j^m \in I$ per qualche $n \geq 1$. Visto che che I è primario e $j^m \notin I$, si avrà che $a \in \sqrt{I}$, e la dimostrazione è completa.

2. Basta mostrare che $\sqrt{I \colon h} \subseteq I \colon h$. Sia dunque $a \in \sqrt{I \colon h}$; allora $a^n h \in I$ per qualche intero n e, di conseguenza, $(ah)^n \in I$. Ne deduciamo che $ah \in \sqrt{I} = I$, e dunque che $a \in I \colon h$.

Soluzione E. *66* 1. Se p è invertibile, esiste q tale che $pq = 1$ quindi a_0 è invertibile. Viceversa, supponiamo che a_0 sia invertibile e costruiamo l'elemento $q = \sum_{i \geq 0} b_i x^i \in A[[x]]$ inverso di p. Dalla condizione $pq = 1$ otteniamo $a_0 b_0 = 1$, $a_0 b_1 + a_1 b_0 = 0$, $\ldots$, $\sum_{i=0}^{k} a_i b_{k-i} = 0, \ldots$, da cui deduciamo che $b_0 = {a_0}^{-1}$, $b_1 = -{a_0}^{-1} a_1 b_0$, $\ldots$, $b_k = -{a_0}^{-1} \sum_{i=1}^{k} a_i b_{k-i}$, ovvero abbiamo

ottenuto una formula ricorsiva per il calcolo dei b_i in funzione dei coefficienti a_j, cioè abbiamo determinato l'inverso di p.

2. Se p è nilpotente allora $p^n = 0$ per un certo intero n, da cui si ha subito che a_0 è nilpotente. Inoltre $p - a_0 = x \sum_{i\geq 1} a_i x^{i-1}$ è nilpotente perché somma di nilpotenti; ne deduciamo che a_1 è nilpotente e, iterando il ragionamento, che a_i è nilpotente per ogni i.
Il viceversa è falso in generale. Consideriamo per esempio l'anello $A = \prod_{n\in\mathbb{N}_+} \mathbb{Z}/(2^n)$, con le operazioni definite componente per componente, e ricordiamo che (2) è l'unico ideale massimale di $\mathbb{Z}/(2^n)$. Sia $p = (0,0,\ldots) + (0,2,0,\ldots)x + (0,0,2,\ldots)x^2 + \cdots \in A[[x]]$; allora tutti i coefficienti di p sono nilpotenti e non è difficile verificare che p non è nilpotente.

3. L'elemento $p \in \mathcal{J}(A[[x]])$ se e solo se $1-pq$ è invertibile per ogni $q \in A[[x]]$. Per il punto 1 questo equivale a dire che $1 - a_0 b_0$ è invertibile per ogni $b_0 \in A$ e questo accade se e solo se $a_0 \in \mathcal{J}(A)$.

4. Sia $\mathfrak{m} \subset A[[x]]$ un ideale massimale. Osserviamo innanzitutto che $x \in \mathfrak{m}$; infatti, se $x \notin \mathfrak{m}$, per la massimalità di $\mathfrak{m}$ si avrebbe che $(\mathfrak{m}, x) = (1)$ ed esisterebbero quindi $f \in \mathfrak{m}$ e $h \in A[[x]]$ tali che $1 = f + xh = f_0$, ove f_0 indica il termine noto di f. Ne segue che f_0 è invertibile e, per il punto 1, f è invertibile in $A[[x]]$, contraddizione.
Consideriamo ora $\mathfrak{n} = \{a \in A\colon\ a$ termine noto di un elemento di $\mathfrak{m}\}$. È immediato verificare che $\mathfrak{n}$ è un ideale di A e che $(\mathfrak{n}, x) \subseteq \mathfrak{m}$. Per definizione di $\mathfrak{n}$ si ha subito anche l'altra inclusione, e dunque $\mathfrak{m} = (\mathfrak{n}, x)$. Da questo segue che $\mathfrak{m}^c = \mathfrak{n}$. Infine $\mathfrak{n} = \mathfrak{m}^c$ è massimale poiché $A[[x]]/\mathfrak{m} \cong A/\mathfrak{n}$ è un campo.

Soluzione E. *67* 1. Per ipotesi l'uguaglianza è vera per $s = 1$. Supponiamo dunque che sia vera per $s \geq 1$ e proviamola per $s+1$.
Basta mostrare un'inclusione, essendo l'altra sempre vera. Se $b \in I\colon g^{m+s+1}$ allora $bg \in I\colon g^{m+s} = I\colon g^m$ e quindi $bg^{m+1} \in I$; da ciò discende che $b \in I\colon g^{m+1} = I\colon g^m$, come desiderato.

2. Basta provare che, se $a \in (I\colon g^m) \cap (I, g^m)$, allora $a \in I$. Scriviamo $a = i + hg^m$, con $i \in I, h \in A$. Visto che $ig^m + hg^{2m} = ag^m \in I$, avremo che $h \in I\colon g^{2m}$. Per il punto precedente $h \in I\colon g^m$, e dunque $a \in I$.

Soluzione E. *68* Sia Σ l'insieme degli ideali primi di A, ordinato parzialmente con $\supseteq$. L'insieme Σ è non vuoto poiché $A \neq 0$ possiede un ideale massimale. Sia $\mathfrak{p}_0 \supseteq \mathfrak{p}_1 \supseteq \cdots$ una catena discendente di ideali primi. Proveremo che $\mathfrak{p} = \cap_i \mathfrak{p}_i$ è un ideale primo, e la prima conclusione discenderà direttamente dal Lemma di Zorn. L'intersezione di una qualsiasi famiglia di ideali è un ideale. Siano dunque $a, b \in A$ tali che $ab \in \mathfrak{p}$. Quindi $ab \in \mathfrak{p}_i$ per ogni i e supponiamo che $a, b \notin \mathfrak{p}$. Esistono allora interi m, n tali che $a \notin \mathfrak{p}_m$ e $b \notin \mathfrak{p}_n$; supponiamo pure che $m \leq n$, cosicché $\mathfrak{p}_m \supseteq \mathfrak{p}_n$ e $ab \notin \mathfrak{p}_n$, che è assurdo, poiché $ab \in \mathfrak{p}$.
Per l'affermazione sugli ideali contenenti I è sufficiente ripetere la dimostrazione considerando l'insieme Σ_I degli ideali primi di A contenenti I ordinato parzialmente con $\supseteq$. Infine osserviamo che, per quanto appena dimostrato $\mathcal{N}(A)$ è intersezione dei primi minimali di A.

Soluzione E. *69* Sia $b \in A$, $b \neq 0$, tale che $ab = 0$. Dato che $\mathcal{N}(A) = (0)$, esiste un primo minimale $\mathfrak{p}$ che non contiene b; da ciò segue che $ab = 0 \in \mathfrak{p}$ implica che $a \in \mathfrak{p}$, come richiesto.

Soluzione E. *70* Dato che $63 = 3^2 7$, per **T.**6.7, possiamo scrivere $\sqrt{I} = \sqrt{(I,9)} \cap \sqrt{(I,7)}$. Avremo che $(I,9) = (9x^2 - y, 7y^2 + 2x + y, 9) = (y, 2x, 9) = (x, y, 9)$, che è primario per **T.**7.2 poiché $\sqrt{(I,9)} = (x, y, 3)$. Dato che $(I,7) = (2x^2 - y, 2x + y, 7) = (2x^2 + 2x, 2x + y, 7) = (x^2 + x, 2x + y, 7)$, da **T.**6.3 e 7, avremo anche che

$$\begin{aligned}\sqrt{(I,7)} &= \sqrt{(x, 2x+y, 7) \cap (x+1, 2x+y, 7)} \\ &= \sqrt{(x, y, 7)} \cap \sqrt{(x+1, y-2, 7)} \\ &= (x, y, 7) \cap (x+1, y-2, 7),\end{aligned}$$

ove l'ultima uguaglianza segue dal fatto che gli ideali sotto il segno di radicale sono entrambi massimali, e quindi primi.

1. Dalla discussione precedente, **T.**14 ed **E.**68 deduciamo che i primi minimali di I sono anche massimali e la conclusione segue dalla corrispondenza tra gli ideali di A/I e gli ideali di A che contengono I.

2. Dato che $(9,7) = (1)$, $(I,7)$ e $(I,9)$ sono comassimali e, per il teorema cinese del resto, si ha

$$A/I \simeq A/(I,9) \times A/(I,7) = A/(x,y,9) \times A/(x^2+x, 2x+y, 7).$$

Notiamo ora che (x) e $(x+1)$ sono comassimali, dunque $(x^2+x) = (x) \cap (x+1)$, e per la legge modulare, cf. **T.**5.4, avremo $(x^2+x, 2x+y, 7) = (x, 2x+y, 7) \cap (x+1, 2x+y, 7)$; nuovamente per il teorema cinese del resto

$$\begin{aligned} A/I &\simeq A/(x,y,9) \times A/(x+1, 2x+y, 7) \times A/(x, 2x+y, 7) \\ &\simeq \mathbb{Z}/(9) \times (\mathbb{Z}/(7))^2 . \end{aligned}$$

3. Per quanto abbiamo visto nella discussione iniziale, $I \subseteq (x,y,9) \cap (x,y,7) \cap (x+1, y-2, 7)$, ove questi tre ideali sono primari e anche a due a due comassimali. Dal momento che $(x,y,9) \cap (x,y,7) \cap (x+1, y-2, 7) = (x,y,9)(x,y,7)(x+1, y-2, 7) \subseteq I$, otteniamo l'uguaglianza.
4. Dato che A/I ha un numero finito di elementi, se tale f esiste, allora B è un dominio finito e quindi un campo.

Soluzione E. *71* Poniamo $A = \mathbb{Z}[x]$. Ovviamente (0) è un ideale primo di A. Sia $P \neq (0)$ un ideale primo di A. Considerando l'immersione $\mathbb{Z} \longrightarrow A$, si ha che $P^c = P \cap \mathbb{Z}$ è ancora un ideale primo, dunque $P^c = (0)$ o (p) per qualche primo p di $\mathbb{Z}$. Se $P^c = (0)$, allora sia $0 \neq f \in P$ di grado minimo. La primalità di P implica che f è irriducibile. Se esiste $g \in P \setminus (f)$ allora in $\mathbb{Q}[x]$ si ha $\gcd(f,g) = 1$ quindi esistono $r, s \in \mathbb{Q}[x]$ tali che $rf + sg = 1$; moltiplicando per il minimo comune multiplo m dei denominatori dei coefficienti si ottiene $\tilde{r}f + \tilde{s}g = m$ per qualche $m \in \mathbb{Z} \setminus \{0\}$, $\tilde{s}, \tilde{r} \in A$, ma questo implica $m \in P \cap \mathbb{Z} = (0)$, contraddizione. Dunque, in questo caso, $P = (f)$ con f irriducibile in A. Se invece $P^c = (p)$ allora $P = (p)$ oppure esiste $f \in P \setminus (p)$ di grado minimo. Notiamo che $A/P \simeq (\mathbb{Z}/(p))[x]/(\overline{f})$ dove $\overline{f}$ è la riduzione di f modulo p. Dato che $\mathbb{Z}/(p)$ è un campo si ha che A/P è un dominio se e solo se $\overline{f}$ è irriducibile, i.e. f è irriducibile modulo p. Notiamo che questo è l'unico caso in cui si ottiene P massimale.

16.2 Soluzioni del capitolo 9

Soluzione E. *72* Sia $\mathbf{a}_1 > \mathbf{a}_2 > \cdots$ una catena discendente; se non fosse stazionaria, allora $\{\mathbf{a}_1, \mathbf{a}_2, \dots, \}$ sarebbe un sottoinsieme non vuoto di $\mathbb{N}^n$ che non ha minimo, e quindi $>$ non sarebbe un buon ordinamento.

Viceversa, se $>$ non fosse un buon ordinamento, esisterebbe un sottoinsieme non vuoto di $V \subset \mathbb{N}^n$ che non ha minimo elemento. Quindi, dato un elemento $\mathbf{a}_1 \in V$, esiste $\mathbf{a}_2 \in V$ tale che $\mathbf{a}_1 > \mathbf{a}_2$ e, ripetendo il procedimento, costruiremmo una catena discendente infinita di elementi di $\mathbb{N}^n$.

Soluzione E. *73* È chiaro che si tratta in tutti e tre i casi di ordinamenti totali su $\mathbb{N}^n$, perché se $\mathbf{a} \neq \mathbf{b}$ allora o $|\mathbf{a}| \neq |\mathbf{b}|$, e dunque chi è più piccolo tra $\mathbf{a}$ e $\mathbf{b}$ viene deciso dal grado per deglex e degrevlex, oppure $|\mathbf{a}| = |\mathbf{b}|$, ma comunque esistono coordinate $a_i \neq b_i$; quindi esiste una prima coordinata, partendo da sinistra per lex, o partendo da destra per degrevlex, diversa da zero che determina se $\mathbf{a} > \mathbf{b}$ o viceversa.

Sia adesso S un sottoinsieme non vuoto di $\mathbb{N}^n$ e dimostriamo che ha minimo. Iniziamo da lex: dato che in $\mathbb{N}$ vale il principio del buon ordinamento, esiste $\alpha_1 = \min\{a_1 \,:\, \mathbf{a} \in S\}$, cioè il minimo tra tutte le prime coordinate dei vettori di S. Definiamo $S_1 = \{\mathbf{a} \in S \,:\, a_1 = \alpha_1\}$ e consideriamo $\alpha_2 = \min\{a_2 \,:\, \mathbf{a} \in S_1\}$. Iterando il procedimento si arriva a trovare $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in S$ che è il minimo di S rispetto a lex.
Per deglex basta seguire lo stesso procedimento, con una riduzione preliminare da S a $S_0 = \{\mathbf{a} \in S \,:\, |\mathbf{a}| = \min\{|\mathbf{b}| \,:\, \mathbf{b} \in S\}\}$.
Per degrevlex usiamo la stessa riduzione precedente da S a S_0; definiamo poi $\beta_n = \max\{c_n \,:\, \mathbf{c} \in S_0\}$, cioè il massimo tra le ultime coordinate dei vettori di S_0: tale massimo esiste perché il grado degli elementi di S_0 è fissato. Adesso si definisce $S_1' = \{\mathbf{a} \in S_0 \,:\, a_n = \beta_n\}$ e si itera il procedimento fino ad ottenere $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ che è il minimo di S rispetto a degrevlex.

Infine siano $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n$ tali che $\mathbf{a} > \mathbf{b}$ rispetto a uno qualsiasi degli ordinamenti lex, deglex, degrevlex. Dato che $|\mathbf{a}+\mathbf{c}| = |\mathbf{a}|+|\mathbf{c}|$, $|\mathbf{b}+\mathbf{c}| = |\mathbf{b}|+|\mathbf{c}|$ e $(\mathbf{a}+\mathbf{c}) - (\mathbf{b}+\mathbf{c}) = \mathbf{a} - \mathbf{b}$, sommare non altera l'ordine tra $\mathbf{a}$ e $\mathbf{b}$.

Soluzione E. *74* Per definizione di ordinamento monomiale, dobbiamo solo provare che $>$ è un buon ordinamento se e solo se $\alpha \geq 0$ per ogni $\alpha \in \mathbb{N}^n$. Se $>$ è un buon ordinamento allora esiste $\overline{\alpha}$ elemento minimo di $\mathbb{N}^n$. Se fosse $0 > \overline{\alpha}$, allora avremmo una catena discendente $0 > \overline{\alpha} > 2\overline{\alpha} > 3\overline{\alpha} > \ldots$ infinita, contro l' ipotesi che $>$ è un buon ordinamento, cf. **E.** 72.

Viceversa, supponiamo che per ogni $\alpha \in \mathbb{N}^n$ valga $\alpha \geq 0$. Siano $X \subset \mathbb{N}^n$ un sottoinsieme non vuoto ed $E = (X)$ l'$\mathcal{E}$-sottoinsieme generato dagli elementi di X. Dal lemma di Dickson **T.** 31 segue che E ha una frontiera finita minimale $F = \{\alpha_1, \ldots, \alpha_m\}$. Eventualmente riordinando gli elementi di F possiamo supporre che $\alpha_1 > \ldots > \alpha_m$. Dimostriamo ora che α_m è l'elemento minimo di X. Infatti, per ogni $\beta \in X \subseteq E$ esistono $i \in \{1, \ldots, m\}$ e $\gamma \in \mathbb{N}^n$ tali che $\beta = \alpha_i + \gamma$; per ipotesi $\gamma \geq 0$, e dunque si ha $\beta = \alpha_i + \gamma \geq \alpha_i > \alpha_m$, come volevamo.

Soluzione E. *75* Fissiamo un ordinamento monomiale sull'insieme dei monomi nelle variabili $x_1, \ldots, x_n$ e sia $G = \{g_1, \ldots, g_s\}$ una base di Gröbner di $I \subseteq K[x_1, \ldots, x_n]$ rispetto a tale ordinamento. Osserviamo preliminarmente che, per **T.**37, $g_1, \ldots, g_s$ sono un insieme di generatori di I e, ovviamente, anche di I^e.

Vogliamo mostrare che $\mathrm{Lt}(I)^e = \mathrm{Lt}(G)^e = \mathrm{Lt}(I^e)$.
È immediato convincersi che $\mathrm{Lt}(I)^e \subseteq \mathrm{Lt}(I^e)$, dato che ogni monomio di $\mathrm{Lt}(G)$ è certamente anche un elemento di $\mathrm{Lt}(I^e)$.

Fissiamo ora una base $\{e_\lambda\}_{\lambda \in \Lambda}$ di K' su K. Per ogni $f \in K'[x_1, \ldots, x_n]$ possiamo scrivere $f = \sum_{\mathbf{a} \in \mathbb{N}^n} c_{\mathbf{a}} X^{\mathbf{a}}$, dove, come al solito, $X^{\mathbf{a}} = x_1^{a_1} \cdots x_n^{a_n}$ e $c_{\mathbf{a}} \neq 0$ solo per un numero finito di $\mathbf{a}$. Dato che $c_{\mathbf{a}} \in K'$ possiamo scrivere $c_{\mathbf{a}} = \sum_{\lambda \in \Lambda} c_{\mathbf{a},\lambda} e_\lambda$, con $c_{\mathbf{a},\lambda} \in K$, e $c_{\mathbf{a},\lambda} \neq 0$ solo per un numero finito di λ; quindi

$$f = \sum_{\mathbf{a} \in \mathbb{N}^n} c_{\mathbf{a}} X^{\mathbf{a}} = \sum_{\mathbf{a} \in \mathbb{N}^n} \sum_{\lambda \in \Lambda} c_{\mathbf{a},\lambda} e_\lambda X^{\mathbf{a}} = \sum_{\lambda \in \Lambda} e_\lambda \sum_{\mathbf{a} \in \mathbb{N}^n} c_{\mathbf{a},\lambda} X^{\mathbf{a}} = \sum_{\lambda \in \Lambda} e_\lambda f_\lambda$$

per certi $f_\lambda \in K[x_1, \ldots, x_n]$. Allora, un elemento di I^e si può scrivere come

$$f = \sum_{i=1}^{s} f_i g_i = \sum_i \left(\sum_\lambda e_\lambda f_{i,\lambda} \right) g_i = \sum_\lambda e_\lambda \sum_i f_{i,\lambda} g_i$$

con $f_i \in K'[x_1, \ldots, x_n]$ e $f_{i,\lambda} \in K[x_1, \ldots, x_n]$; pertanto, per un certo λ_0, avremo $\mathrm{lt}(f) = \alpha h$, con $\alpha \in K'$ e $h = \mathrm{lm}(\sum_i f_{i,\lambda_0} g_i) \in \mathrm{Lt}(I)$. Infatti, $\mathrm{lm}(f)$ sarà dato dal massimo dei leading monomial dei polinomi $\sum_i f_{i,\lambda} g_i$, e in caso più di un polinomio avesse leading monomial massimo, siamo sicuri che non

ci possono essere cancellazioni, in quanto gli e_λ sono linearmente indipendenti su K. Abbiamo dunque provato anche l'altra inclusione.

In alternativa, per il Criterio di Buchberger tutti gli S-polinomi di $g_1, \ldots, g_s$ riducono a 0; senz'altro anche gli S-polinomi di $g_1, \ldots, g_s$ visti come elementi di $K'[x_1, \ldots, x_n]$ riducono a 0; ancora per il Criterio di Buchberger, questo implica che $\{g_1, \ldots, g_s\}$ è una base di Gröbner di I^e.

L'ultima affermazione discende immediatamente dalla precedente e dalla definizione di escalier di un ideale.

Soluzione E. *76* Dividendo f per $\{f_1, f_2\}$ si ottiene $f = x_1x_2f_1 + 0$ mentre dividendo per $\{f_2, f_1\}$ si ottiene $f = (x_1^2 + x_2)f_2 + x_2^3$ in particolare il resto della divisione non è univocamente determinato.

Soluzione E. *77* Risolviamo l'esercizio senza utilizzare il criterio di Buchberger.
Mostriamo che G è base di Gröbner di I rispetto a $>_1$. Supponiamo per assurdo che esista $f \in I$ tale che $\mathrm{lt}_{>_1}(f) \notin \mathrm{Lt}_{>_1}(G) = (\mathrm{lt}_{>_1}(g_1), \mathrm{lt}_{>_1}(g_2)) = (z, y)$. Allora $z, y \nmid \mathrm{lt}_{>_1}(f)$. Visto che $>_1$ è un ordinamento lex, allora z e y non appaiono neanche come divisori degli altri termini di f, ovvero $f = f(x)$. Allora, dato che $f = u_1(z+x)+u_2(y-x)$ per certi $u_1, u_2 \in \mathbb{Q}[x, y, z]$, operando la sostituzione $y = x$ troviamo che $f = f(x) = u_1(x, x, z)(z+x)$, da cui segue che $z + x$ divide f, che non è possibile, poiché f non contiene termini in cui è presente la z.
Per il secondo punto, riscriviamo $g_1 = x + z$ e $g_2 = -x + y$. Allora $y + z = (x + z) + (-x + y) = g_1 + g_2 \in I$ e $y \in \mathrm{Lt}_{>_2}(I)$. D'altra parte $\mathrm{lm}_{>_2}(g_1) = \mathrm{lm}_{>_2}(g_2) = x$, per cui $\mathrm{Lt}_{>_2}(I) \supseteq (x, y) \supsetneq (x) = (\mathrm{lt}_{>_2}(g_1), \mathrm{lt}_{>_2}(g_2)) = \mathrm{Lt}_{>_2}(G)$.

Soluzione E. *78* Supponiamo che I sia monomiale; allora, $f = \sum_{\mathbf{a}} c_{\mathbf{a}} X^{\mathbf{a}} \in I$ se e solo se $X^{\mathbf{a}} \in I$ per ogni $\mathbf{a}$ tale che $c_{\mathbf{a}} \neq 0$, cf. **T.**30. Allora, per ogni ordinamento dato, $I = \mathrm{Lt}(I)$ è monomiale. Il suo insieme minimale di generatori $G(I)$ è dunque una base di Gröbner minimale di I. Essendo $G(I)$ costituito da monomi, essa è chiaramente ridotta - e dunque unica.

Viceversa, se vi è una base di Gröbner di I costituita da monomi, in particolare I possiede un insieme di generatori monomiale.

Soluzione E. *79* La base di Gröbner ridotta rispetto all'ordinamento assegnato è:

$$G = \{x^2 - xy, xz - y^2, yz^2 - z^4, xy^2 - y^3, y^4 - z^7, y^3z - z^7, z^9 - z^8\}.$$

Siano $f_1 = x^2 - xy$, $f_2 = xz - y^2$ e $f_3 = yz^2 - z^4$ e $G_0 = \{f_1, f_2, f_3\}$. Nel seguito indichiamo con S_{ij} l'S-polinomio di f_i e f_j.

$S_{12} = zf_1 - xf_2 = xy^2 - xyz \xrightarrow{f_2} xy^2 - y^3 = f_4$, che è ridotto rispetto a G_0. Poniamo pertanto $G_1 = G_0 \cup \{f_4\}$.

$S_{14} = y^2f_1 - xf_4 = xy^3 - xy^3 = 0$.

$S_{24} = y^2f_2 - zf_4 = -y^4 + y^3z$; pertanto poniamo $f_5 = y^4 - y^3z$ e dato che $y^4 \notin \{x^2, xz, yz^2, xy^2\}$ consideriamo $G_2 = G_1 \cup \{f_5\}$.

$S_{35} = y^3f_3 - z^2f_5 = y^3z^3 - y^3z^4$ e $y^3z^4 - y^3z^3 \xrightarrow{f_3}_* z^{10} - z^9$; poniamo $f_6 = z^{10} - z^9$ e $G_3 = G_2 \cup \{f_6\}$.

$S_{23} = yzf_2 - xf_3 = xz^4 - y^3z \xrightarrow{f_2,f_3} yz^5 - y^3z$, e $y^3z - yz^5 \xrightarrow{f_3}_* y^3z - z^7$.
Dato che $y^3z \notin \{\mathrm{lt}(f) : f \in G_3\} = \{x^2, xz, yz^2, xy^2, y^4, z^{10}\}$, poniamo $f_7 = y^3z - z^7$ e $G_4 = G_3 \cup \{f_7\}$. A questo punto ci accorgiamo che possiamo ridurre f_5 rispetto a G_4 usando f_7 per ottenere $f_{5'} = y^4 - z^7$ e porre $G_5 = (G_4 \cup \{f_{5'}\}) \setminus \{f_5\}$.
Potremmo pensare di avere finito il calcolo; controlliamo dunque che l'insieme G_5 sia una base di Gröbner usando il criterio degli S-polinomi.

$S_{12} \xrightarrow{f_4} 0$, $S_{14} = 0$, $S_{24} \xrightarrow{f_3,f_{5'},f_7}_* 0$, $S_{23} \xrightarrow{f_3,f_7}_* 0$, $S_{26} = z^9f_2 - xf_6 = xz^9 - y^2z^9 \xrightarrow{f_2,f_3,f_6}_* 0$, e $S_{27} = y^3f_2 - xf_7 \xrightarrow{f_2,f_3,f_{5'},f_3,f_6}_* 0$.

A questo punto calcoliamo $S_{34} = xyf_3 - z^2f_4 = -xyz^4 + y^3z^2 \xrightarrow{f_2,f_3}_* z^9 - z^8 = f_{6'}$ e consideriamo $G_6 = (G_5 \cup \{f_{6'}\}) \setminus \{f_6\}$.
Dovremmo ripartire daccapo con il controllo degli S-polinomi: sicuramente $S_{12}, S_{14}, S_{23}, S_{24}, S_{34} \xrightarrow{G_6}_* 0$, ma anche $S_{27} = y^3f_2 - xf_7 \xrightarrow{f_2,f_3,f_{5'},f_3,f_{6'}}_* 0$.
Avremo poi che $S_{26'} \xrightarrow{f_2,f_3,f_{6'}}_* 0$, $S_{35'} \xrightarrow{f_3,f_{6'}}_* 0$, $S_{36'} \xrightarrow{f_3,f_{6'}}_* 0$, $S_{37} \xrightarrow{f_3}_* 0$, $S_{45'} \xrightarrow{f_2,f_{5'},f_3,f_{6'}}_* 0$, $S_{47} \xrightarrow{f_2,f_{5'},f_3,f_{6'}}_* 0$, $S_{5'7} \xrightarrow{f_3,f_{6'}}_* 0$, e infine $S_{6'7} \xrightarrow{f_3,f_{6'}}_* 0$.

Dalla teoria sappiamo che se due polinomi hanno monomi di testa privi di fattori comuni allora tali polinomi costituiscono una base di Gröbner per l'ideale che generano, cf. **T.**43. In particolare, il loro S-polinomio riduce completamente a 0. Da questo possiamo concludere che certamente

$$S_{13}, S_{15'}, S_{16'}, S_{17}, S_{25'}, S_{46'}, S_{5'6'} \xrightarrow{G_6}_* 0.$$

Pertanto G è la base cercata, che per costruzione risulta già essere ridotta.

Soluzione E. *80* La base di Gröbner ridotta di I rispetto all'ordinamento lex con $x > y > z$ è $G = \{xz + 2z, y - z, z^2 - z\}$. Dato che $f \xrightarrow{G}_* -9z \neq 0$, $f \notin I$.
Alternativamente, si può osservare che $(-2, 1, 1) \in \mathbf{V}(I)$ ma $f(-2, 1, 1) = -9 \neq 0$.

Soluzione E. *81* La base di Gröbner ridotta di I rispetto all'ordinamento lex con $x > y$ è $G = \{x + y^4 + y, y^6 + y^3 + 1\}$. Riducendo $f_1 - f_2 = x^3 - x^2y + xy^2 - xy + y^5 - y^2$ modulo G si ottiene resto 0, quindi $\overline{f_1} = \overline{f_2}$.

Soluzione E. *82* L'insieme dei generatori $G = \{f_1 = yx^2 - y + x, f_2 = y^2 - yx - x^2, f_3 = x^3 + y - 2x\}$ di I è una base di Gröbner rispetto all'ordinamento deglex con $y > x$, ed f è ridotto rispetto a tale base.

Per verificare se $\overline{f}$ è invertibile in $\mathbb{Q}[x, y]/I$ è sufficiente applicare quanto visto in **T.**51. Sia dunque $H = G \cup \{f\}$; dato che
$S(f_1, f) \xrightarrow{G} x^2 + x = -(f_1 - x^2 f + f_3) = g_1$
$S(f_2, f) \xrightarrow{G\cup\{g_1\}} 2x+1 = f_2 - yf + 2xf - g_1 + f = f_2 - (y - 2x - 1)f - g_1 = g_2$
$S(g_1, g_2) \xrightarrow{G\cup\{g_1,g_2\}} -\frac{1}{2} = 2g_1 - xg_2 - \frac{1}{2}g_2 = 2g_1 - (x + \frac{1}{2})g_2,$
possiamo concludere che $1 \in (I, f)$, f è invertibile in $\mathbb{Q}[x, y]/I$ e per calcolare il suo inverso procediamo a ritroso, ottenendo

$$\begin{aligned}
1 &= (-2) \cdot \left(-\tfrac{1}{2}\right) = -2\left(2g_1 - \left(x + \tfrac{1}{2}\right) g_2\right) \\
&= -2\left[2\left(x^2 f - f_1 - f_3\right) - \left(x + \tfrac{1}{2}\right)\left((2x - y + 1)f + f_2 - g_1\right)\right] = \\
&= -2\left[f\left(2x^2 - \left(x + \tfrac{1}{2}\right)(2x - y + 1)\right) + \left(x + \tfrac{1}{2}\right)\left(x^2 f - f_1 - f_3\right) + h_1\right] \\
&= f(-2x^3 - 2yx - x^2 - y + 4x + 1) + h_2 \\
&= f(-2xy - x^2 + y + 1) + h_3,
\end{aligned}$$

dove, nell'ultima uguaglianza, abbiamo ridotto il coefficiente di f modulo I sommandogli $2f_3$, e $h_1, h_2, h_3 \in I$. Dunque $f^{-1} = \overline{-2xy - x^2 + y + 1} \in \mathbb{Q}[x,y]/I$.

Soluzione E. *83* 1. La base di Gröbner richiesta è $G = \{f_1 = x^2y + z, f_2 = xz + y, f_3 = xy^2 - z^2, f_4 = y^3 + z^3\}$.
2. Dal calcolo della base di Gröbner si ricavano in particolare le seguenti relazioni:

$$S(f_1, f_2) = zf_1 - xyf_2 = -f_3$$
$$S(f_2, f_3) = y^2f_2 - zf_3 = f_4 = y^2f_2 + z^2f_1 - xyzf_2) = z^2f_1 + (-xyz + y^2)f_2\,.$$

Dunque la matrice associata al passaggio tra i due insiemi di generatori è

$$M = \begin{pmatrix} 1 & 0 & -z & z^2 \\ 0 & 1 & xy & -xyz + y^2 \end{pmatrix}.$$

3. Come è ben noto i coefficienti della divisione di f per G non sono unici. Osserviamo subito che $f = y^2f_2 = 0f_1 + y^2f_2 + 0f_3 + 0f_4 = 0f_1 + y^2f_2$, che fornisce le scritture di f richieste.

D'altra parte, possiamo anche scrivere $f = 0f_1 + 0f_2 + zf_3 + f_4$, e per risalire ai coefficienti da dare a f_1, f_2 basta usare la matrice di passaggio trovata al punto precedente:

$$M \begin{pmatrix} 0 \\ 0 \\ z \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ y^2 \end{pmatrix}.$$

Una terza scrittura possibile (perché, ne esistono infinite?) è $f = yf_1 - zf_2 - (x - z)f_3 + f_4$, che fornisce coordinate rispetto ai generatori iniziali

$$M \begin{pmatrix} y \\ -z \\ -x + z \\ 1 \end{pmatrix} = \begin{pmatrix} xz + y \\ -x^2y + y^2 - z \end{pmatrix}.$$

Soluzione E. *84* La base di Gröbner ridotta di I rispetto all'ordinamento lessicografico con $x > y$ è $\{x^2 + 2y^2 - 3, xy - y^2, y^3 - y\}$, quindi da **T.**52 segue che $I \cap \mathbb{C}[y] = (y^3 - y)$.

Soluzione E. *85* Abbiamo delineato una strategia per procedere nell'Osservazione 2.8: per brevità scriviamo $g_1 = x(x+y)^2$, $g_2 = y$, $f_1 = x^2$ e $f_2 = x+y$. Per **E.**18.5 abbiamo che $I : J = (I : (f_1)) \cap (I : (f_2))$; inoltre $I = (x^3, y)$ e quindi $I : (x^2) = (x, y)$, cf. **T.**33.3.
Per determinare $I : (f_2)$, grazie a **E.**20 possiamo calcolare $\frac{1}{f_2}(I \cap (f_2))$, e a tal scopo utilizzare **T.**53. Una base di Gröbner di $(tI, (1-t)f_2)$ rispetto all'ordinamento lessicografico con $t > x > y$ è

$$\{tx - x - y, ty, x^3 + y^3, xy + y^2\},$$

da cui si ottiene che $\frac{1}{x+y}(I \cap (f_1)) = \frac{1}{x+y}(x^3+y^3, xy+y^2) = (x^2-xy+y^2, y) = (x^2, y)$. Pertanto $I : J = (x, y) \cap (x^2, y) = (x^2, y)$.

Soluzione E. *86* Usando due volte **T.**6.7 si ottiene

$$\begin{aligned}\sqrt{I} &= \sqrt{(x^2+y^2, y^3)} \cap \sqrt{(x^2+y^2, x^3+y)} = (x, y) \cap \sqrt{(x^6+x^2, x^3+y)} \\ &= (x, y) \cap \sqrt{(x^4+1, x^3+y)}.\end{aligned}$$

L'ideale (x^4+1, x^3+y) è radicale. Infatti $K[x, y]/(x^4+1, x^3+y) \simeq K[x]/(x^4+1)$ non ha nilpotenti diversi da zero, dato che x^4+1 è libero da quadrati.
Allora $\sqrt{I} = (x, y) \cap (x^4+1, x^3+y)$ e $f \notin \sqrt{I}$ perchè non appartiene a (x^4+1, x^3+y); infatti i polinomi x^4+1, x^3+y sono base di Gröbner per l'ideale che generano rispetto all'ordinamento lex con $y > x$, e $0 \neq f$ è ridotto rispetto a tale base.

Soluzione E. *87* Prima di calcolare una base di Gröbner di I, osserviamo che usando la relazione $xy - 2$ possiamo ridurre $x^2y^2z^4$ e ottenere che $z^4 \in I$; in questo modo possiamo semplificare i generatori ed ottenere $I = (f_1, f_2, f_3)$, con $f_1 = z^4$, $f_2 = x^2 + y^2 + z^2 - 1$, $f_3 = xy - 2$.
Rispetto all'ordinamento lessicografico $x > y > z$ basta allora calcolare i seguenti S-polinomi.

$$S(f_2, f_3) = yf_2 - xf_3 = 2x + y^3 + yz^2 - y = f_4;$$

$$S(f_2, f_4) = 2f_2 - xf_4 \xrightarrow{f_3} 0;$$

$$S(f_3, f_4) = 2yf_4 - 2f_3 = y^4 + y^2z^2 - y^2 + 4 = f_5.$$

Dato che i termini di testa di f_1, f_4, f_5 sono a coppie coprimi, $G = \{f_1, \frac{1}{2}f_4, f_5\}$ è la base di Gröbner ridotta di I e si ha $\dim_{\mathbb{C}} \mathbb{C}[x,y,z]/I = 16$, la base come spazio vettoriale è formata dagli elementi

$$\{1, y, z, y^2, yz, z^2, y^3, y^2z, yz^2, z^3, y^3z, y^2z^2, yz^3, y^3z^2, y^2z^3, y^3z^3\} .$$

2. Per verificare che $I + J = 1$ si può dimostrare che $\mathbf{V}(I + J) = \emptyset$ risolvendo il sistema triangolare calcolato nel primo punto e verificando che nessuna soluzione soddisfa le equazioni di J.

In alternativa, si può osservare che $z \in \sqrt{I + J}$ quindi il polinomio $g_1 = 3x^3 - 2 \in \sqrt{I + J}$. Ma allora anche $y^3 g_1 = 3x^3y^3 - 2y^3 \in \sqrt{I + J}$. Usando il polinomio $xy - 2$ si ottiene che $2y^3 - 24 \in \sqrt{I + J}$. Poichè $\gcd(y^3 - 12, f_5) = 1$ si ha la tesi.

Soluzione E. *88* Scriviamo $f_1 = x+y-a$, $f_2 = x^2+y^2-a^2$ e $f_3 = x^3+y^3-a^5$. La base di Gröbner ridotta dell'ideale $I = (f_1, f_2, f_3)$ rispetto all'ordinamento lessicografico con $x > y > a$ è $\{f_1, f_4 = y^2 - ay, f_5 = a^5 - a^3\}$; quindi esistono soluzioni se $a^5 - a^3 = a^3(a + 1)(a - 1) = 0$. Sostituendo nel sistema triangolare superiore, equivalente a quello originario, dato dalle equazioni $f_1 = f_4 = f_5 = 0$ si ottiene che

1. se $a = 0$ esiste solo la soluzione $(0, 0)$.
2. se $a = -1$ esistono due soluzioni, $(-1, 0)$ e $(0, -1)$
3. se $a = 1$ esistono due soluzioni, $(1, 0)$ e $(0, 1)$.

Osserviamo che la base di Gröbner in questo caso si ottiene tramite il mero processo di riduzione dei polinomi. Riducendo f_2 tramite f_1 otteniamo che $f_2 \xrightarrow{f_1}_* 2y^2 - 2ya$; ponendo $f_4 = y^2 - ya$, abbiamo $f_2 = (x - y + a)(x + y - a) + 2f_4$ e $I = (f_1, f_4, f_3)$. Riducendo poi $f_3 \xrightarrow{f_1, f_4}_* -a^5 + a^3$, poniamo $f_5 = a^5 - a^3$. Avremo che $I = (f_1, f_4, f_5)$; ora questi generatori formano una base di Gröbner perché i loro leading monomials x, y^2, a^5, sono coprimi, cf. **T.**43.

Osserviamo che da questo discende che il nostro sistema ha certamente soluzione, poiché $I \neq (1)$, e ne ha un numero finito, perché $\mathrm{Lt}(I)$ contiene le potenze pure di tutte le variabili, cf. **T.**71.

Soluzione E. *89* 1. La base di Gröbner ridotta è

$$G = \{x^2y + xz + yz, xyz^2, xz^3 + yz^3, y^2z\}.$$

2. Gli elementi nilpotenti di A sono le immagini in A degli elementi di $\sqrt{I} = \sqrt{(x^2y, z)} \cap \sqrt{(x^2y + xz + yz, xyz^2, xz^3 + yz^3, y^2)} = (xy, z) \cap (xz, y) = (xy, xz, yz)$.

3. Dato che $x^2y^3, y^3z \xrightarrow{G}_* 0$ avremo che $J = (x^2y^3, y^3z) \subseteq I$; analogamente, per ogni $g \in G$ abbiamo che $g \xrightarrow{x^2,z}_* 0$ e dunque $I \subseteq (x^2, z)$. Dato che $\mathrm{Lt}(J) = (x^2y^3, y^3z) \subsetneq \mathrm{Lt}(I) = \mathrm{Lt}(G) = (x^2y, xyz^2, xz^3, y^2z) \subsetneq (x^2, z) = \mathrm{Lt}(x^2, z)$, avremo inclusioni strette $J \subsetneq I \subsetneq (x^2, z)$.

Soluzione E. *90* Siano $\alpha_1, \ldots, \alpha_m \in \overline{K}$ le radici di f. Da **T.**63 segue subito che

$$\begin{aligned}
\mathrm{Ris}(f, g_1\, g_2) &= a_m^{\deg g_1 + \deg g_2} \prod_{i=1}^{m} g_1(\alpha_i) g_2(\alpha_i) \\
&= \left(a_m^{\deg g_1} \prod_{i=1}^{m} g_1(\alpha_i) \right) \left(a_m^{\deg g_2} \prod_{i=1}^{m} g_2(\alpha_i) \right) \\
&= \mathrm{Ris}(f, g_1)\, \mathrm{Ris}(f, g_2);
\end{aligned}$$

$$\begin{aligned}
\mathrm{Ris}(f, g_1 f + g_2) &= a_m^N \prod_{i=1}^{m} (g_1 f + g_2)(\alpha_i) \\
&= a_m^N \prod_{i=1}^{m} g_2(\alpha_i) = a_m^{N - \deg(g_2)}\, \mathrm{Ris}(f, g_2).
\end{aligned}$$

Soluzione E. *91* Gli enunciati sono conseguenze di **T.**63. Siano $f = a_m \hat{f}$, e $g = b_n \hat{g}$, con $\hat{f} = \prod_{i=1}^{m} (x - \alpha_i)$, e $\hat{g} = \prod_{j=1}^{n} (x - \beta_j)$. Allora,

$$\begin{aligned}\mathrm{Ris}_y(f(x-y),g(y)) &= (-1)^{mn}b_n^m\prod_j f(x-\beta_j)\\ &= (-1)^{mn}a_m^n b_n^m\prod_j \hat{f}(x-\beta_j)\\ &= (-1)^{mn}a_m^n b_n^m\prod_{i,j}(x-(\alpha_i+\beta_j));\end{aligned}$$

$$\begin{aligned}\mathrm{Ris}_y(f(x+y),g(y)) &= (-1)^{mn}a_m^n b_n^m\prod_j \hat{f}(x+\beta_j)\\ &= (-1)^{mn}a_m^n b_n^m\prod_{i,j}(x-(\alpha_i-\beta_j));\end{aligned}$$

$$\begin{aligned}\mathrm{Ris}_y\left(y^m f\left(\frac{x}{y}\right),g(y)\right) &= (-1)^{mn}b_n^m\prod_j \beta_j^m f\left(\frac{x}{\beta_j}\right)\\ &= (-1)^{mn}a_m^n b_n^m\prod_i\prod_j \beta_j\left(\frac{x}{\beta_j}-\alpha_i\right)\\ &= (-1)^{mn}a_m^n b_n^m\prod_{i,j}(x-\alpha_i\beta_j),\end{aligned}$$

e infine

$$\begin{aligned}\mathrm{Ris}_y(f(xy),g(y)) &= (-1)^{mn}b_n^m\prod_j f(x\beta_j)\\ &= (-1)^{mn}a_m^n b_n^m\prod_i\prod_j (x\beta_j-\alpha_i)\\ &= (-1)^{mn}a_m^n b_n^m\prod_{i,j}\beta_j(x-\frac{\alpha_i}{\beta_j}),\end{aligned}$$

poiché $g(0)\neq 0$ implica $\beta_j\neq 0$ per ogni j.

Soluzione E. *92* Per **E.** 90.1 si ha che

$$\mathrm{Ris}(f,x^k g) = \mathrm{Ris}(f,x^k)\,\mathrm{Ris}(f,g) = (\mathrm{Ris}(f,x))^k\ \mathrm{Ris}(f,g).$$

D'altra parte, per **T.** 63.1, vale che $\operatorname{Ris}(f,x) = (-1)^{\deg f} f(0)$ e dunque possiamo concludere che $\operatorname{Ris}(f,x^k g) = (-1)^{k\deg f} f(0)^k \operatorname{Ris}(f,g) = \operatorname{Ris}(f,g)$, poiché k è pari.

Soluzione E. *93* 1. Grazie a **T.**61 sappiamo che $(p) \subseteq (f,g) \cap \mathbb{Z}$. Dato che (p) è massimale basterà allora provare che $(f,g) \neq (1)$. Supponiamo per assurdo che esistano $a, b \in A$ tali che $af + bg = 1$, che implica che $\overline{a}\overline{f} + \overline{b}\overline{g} = \overline{1}$ in $(\mathbb{Z}/(p))[x]$. Osserviamo che essendo f e g monici, la matrice di Sylvester di $\overline{f}$ e $\overline{g}$ è esattamente la riduzione modulo p di $\operatorname{Syl}(f,g)$. Avremmo dunque che $\operatorname{Ris}(\overline{f},\overline{g}) = \overline{\operatorname{Ris}(f,g)} = \overline{0}$, e questo contraddice che $\gcd(\overline{f},\overline{g}) = \overline{1}$.

2. $\operatorname{Ris}(f,g) = \det \begin{pmatrix} 1 & -4 & 1 & 0 \\ 0 & 1 & -4 & 1 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix} = -2$. Per il punto precedente allora $I \cap \mathbb{Z} = (2)$; inoltre $I = I + (2) = (x-1, 2)$, dunque $A/I \simeq \mathbb{Z}/(2)$.

Soluzione E. *94* Proviamo innanzitutto che $\gcd(f,f') = 1$ se e solo se $f = \prod_i f_i$ con f_i irriducibili e distinti.

Se esiste i tale che $f = f_i^s h$ con $s > 1$, si ha che $f' = f_i^{s-1}(s f_i' h + f_i h')$ e quindi $\gcd(f,f') \neq 1$.

Viceversa, se g è un fattore irriducibile di $\gcd(f,f')$ allora $\deg(g) > 0$, $f = gh$ e $f' = g'h + gh' = gq$, per qualche $h, q \in K[x]$. Dall'unicità della fattorizzazione in irriducibili in $K[x]$ segue che $g | g'h$. Se $g' \neq 0$ allora $\deg g' < \deg g$, quindi $g|h$ e, di conseguenza $g^2|f$, che avrebbe un fattore multiplo. D'altra parte se g è irriducibile non si può avere $g' = 0$. In caratteristica 0 ciò è chiaro; se invece $\operatorname{char} K = p$, con K perfetto, ricordiamo che un polinomio $r \in K[x]$ ha derivata nulla se e solo se esiste $s \in K[x]$ tale che $r = s^p$.

1. Supponiamo ora che $\gcd(f,f') = 1$ e siano $A_i = K[x]/(f_i)$, per ogni i. Dato che i polinomi f_i sono irriducibili e distinti, generano ideali massimali e per il teorema cinese del resto si ha che $A = K[x]/\prod_i (f_i) \simeq \prod_i A_i$. L'anello A è dunque prodotto diretto di domini e pertanto $\mathcal{N}(A) \simeq \prod_i \mathcal{N}(A_i) = (0)$.

Viceversa, se $\gcd(f,f') \neq 1$, allora $f = \prod_j f_j^{s_j}$ con $s_j > 1$ per qualche j; quindi la classe dell'elemento $\prod_j f_j$ è un elemento non nullo di $\mathcal{N}(A)$ e dunque l'anello A non è ridotto.

2. Sia $r = \mathrm{Ris}(f, f') \in \mathbb{Z}$; dato che $\gcd(f, f') = 1$, da **T.**63.4 segue che $r \neq 0$, ed esistono polinomi $a, b \in \mathbb{Z}[x]$ tali che $af + bf' = r$, cf. **T.** 61. Rileggendo questa ultima uguaglianza modulo p, con p primo di $\mathbb{Z}$ che non divide r, otteniamo che $\overline{a}\,\overline{f} + \overline{b}\,\overline{f'} = \overline{r}$ in $(\mathbb{Z}/(p))[x]$, cioè $\gcd(\overline{f}, \overline{f}') = 1$ e quindi, per il punto 1, $(\mathbb{Z}/(p))[x]/(\overline{f})$ è ridotto.

Soluzione E. *95* La base di Gröbner ridotta rispetto all'ordinamento lessicografico con $x > y > z$ è $\{x - yz, yz^2 - y\}$ e quindi si ha $\sqrt{I} = (x, y) \cap (x + y, z + 1) \cap (x - y, z - 1)$ e

$$\mathbf{V}(I) = \mathbf{V}(\sqrt{I}) = \mathbf{V}(x, y) \cup \mathbf{V}(x + y, z + 1) \cup \mathbf{V}(x - y, z - 1).$$

Sia K infinito e sia $f \in \mathbf{I}(\mathbf{V}(x, y))$: allora possiamo scrivere $f = xg(x, y, z) + yh(x, y, z) + r(z)$ e $f(0, 0, a) = r(a) = 0$ per ogni a implica $r(z) = 0$, cioè $f \in (x, y)$. Dato che l'altra inclusione è ovvia, si ha che $\mathbf{I}(\mathbf{V}(x, y)) = (x, y)$ è primo e quindi $\mathbf{V}(x, y)$ è irriducibile per **T.** 57. Per le altre due componenti $\mathbf{V}(x \pm y, z \pm 1) = \{(a, \mp a, \mp 1) : a \in K\} \subset K^3$ la dimostrazione è analoga osservando che per ogni $f \in \mathbf{I}(\mathbf{V}(x \pm y, z \pm 1))$ si può scrivere $f = (z \pm 1)g(x, y, z) + (x \pm y)h(x, y) + r(y)$. Quindi $0 = f(x, \mp x, \mp 1) = r(\mp x)$ per infiniti valori di x, dunque $r = 0$.

Sia K finito: ovviamente $\mathbf{V}(x, y) = \{(0, 0, a) : a \in K\} \subset K^3$ si decompone ulteriormente come unione finita di $|K|$ punti che sono le sue componenti irriducibili; lo stesso vale per $\mathbf{V}(x \pm y, z \pm 1)$.

Soluzione E. *96* La base di Gröbner ridotta rispetto all'ordinamento lex con $x > y > z > t$ è $G = \{x^2 - zt, y - zt, zt^2 - t\}$.
1. Avremo allora $\sqrt{I} = \sqrt{(x^2 - zt, y - zt, t)} \cap \sqrt{(x^2 - zt, y - zt, zt - 1)} = (x, y, t) \cap (x + 1, y - 1, zt - 1) \cap (x - 1, y - 1, zt - 1)$ che, essendo primi, determinano le componenti irriducibili di $\mathbf{V}(I)$, dato che, con $\mathbb{C}$ algebricamente chiuso, $\mathbf{I}(\mathbf{V}(J)) = \sqrt{J}$.
2. Dato che, rispetto all'ordinamento fissato, $\mathrm{lt}(f) = xt \notin \mathrm{Lt}(I) = (x^2, y, zt^2)$, avremo che $f \notin I$.

Soluzione E. *97* La base di Gröbner ridotta di I rispetto all'ordinamento lessicografico con $x > y > z$ è $\{x + y + z - 1, y^2 + yz - y + z^2 - z\}$.

1. Per **T.**71, $\dim_{\mathbb{C}} \mathbb{C}[x,y,z]/I$ è infinita, dato che l'ideale iniziale di I non contiene una potenza pura della z.

2. Sappiamo che $\mathbf{V}(I) \cap \mathbf{V}(z-1) = \mathbf{V}(I, z-1)$; dato che $(x+y+z-1, y^2+yz-y+z^2-z, z-1) = (x+y, y^2, z-1)$, avremo che la varietà cercata è $\{(0,0,1)\}$.

Soluzione E. *98* La base di Gröbner ridotta di I rispetto all'ordinamento lessicografico con $x > y > z$ è $\{xy+z^2, xz^2+yz^2, y^2-z^2, z^4\}$.

1. Dal teorema di eliminazione **T.**52 discende subito che $I_1 = (y^2-z^2, z^4)$ e $I_2 = (z^4)$.

2. Dato che $\mathbf{V}(I) = \{(a,0,0), a \in \mathbb{C}\}$ e $\mathbf{V}(I_1) = \{(0,0)\}$ si ha che $\pi_1(\mathbf{V}(I)) = \mathbf{V}(I_1)$.

Soluzione E. *99* Per calcolare J usiamo l'ordinamento lessicografico con $z > t > x > y$. La base di Gröbner ridotta di I rispetto a questo ordinamento è

$$G = \{z - x^2, t^2 - x, tx - y, ty - x^2, x^3 - y^2\}$$

e quindi, per **T.**52, $J = (x^3 - y^2)$.
Dato che G contiene polinomi monici in t e z il teorema di estensione **T.**65 garantisce che ogni elemento di $\mathbf{V}(J)$ si estende ad un elemento di $\mathbf{V}(I)$.

Soluzione E. *100* Dato che $I \subset J$ è sufficiente vedere che $y^3z^2 - y^3 - y^2z \in I$. Calcolando la base di Gröbner di I rispetto all'ordinamento lessicografico con $x > y > z$ si trova che $I = (x^2 - y^2 - yz, xy - y^2z, y^3z^2 - y^3 - y^2z) = J$.
Dato che $\mathbb{C}$ è algebricamente chiuso, sappiamo dal Nullstellensatz **T.**68 che $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$; quindi è sufficiente verificare se I è radicale. Fattorizzando l'ultimo polinomio della base di Gröbner si ha $y^2(yz^2 - y - z) \in I$; dato che $y^2z^2 \notin \mathrm{Lt}(I)$ possiamo allora concludere che $y(yz^2 - y - z) \in \sqrt{I} \setminus I$, e che $I \subsetneq \mathbf{I}(\mathbf{V}(I))$.

Soluzione E. *101* La base di Gröbner ridotta di I rispetto all'ordinamento lessicografico dato da $x > y > z$ è

$$G = \{x + y + z, y^2 + yz + z^2, z^3 - 1\}.$$

1. Notiamo che α è una radice terza primitiva dell'unità, e dunque $\alpha \cdot \overline{\alpha} = \alpha \cdot \alpha^2 = \alpha^3 = 1$. Pertanto è immediato verificare che l'insieme delle 6 permutazioni di $(1, \alpha, \alpha^2)$ è contenuto in $\mathbf{V}(I)$.
Inoltre, dato che $\mathrm{Lt}(I) = (x, y^2, z^3)$, per **T.**71 I è zero-dimensionale e, per l'Osservazione 3.3, $|\mathbf{V}(I)| \leq \dim_{\mathbb{C}} \mathbb{C}[x,y,z]/I = 6$. Quindi $|\mathbf{V}(I)| = 6$ e $\mathbf{V}(I)$ è l'insieme delle permutazioni prima descritte.

2. Per il punto 1 e l'Osservazione 3.3, $\dim_K(A/\sqrt{I}) = \dim_K(A/I) = 6$, quindi $\mathrm{Lt}(\sqrt{I}) = \mathrm{Lt}(I)$ e I è radicale.

Soluzione E. *102* 1. La base di Gröbner ridotta di I rispetto all'ordinamento lex con $x > y > z$ è $\{x + y + z + 1, (z+1)(y+z)(y+1)\}$. Pertanto $\mathbf{V}(I)$ non è finita per **T.**71.

2. Dal momento che $\sqrt{I} = (x+y, z+1) \cap (x+1, y+z) \cap (x+z, y+1)$ e questi ideali sono primi, $\mathbf{V}(I) = \mathbf{V}(x+y, z+1) \cup \mathbf{V}(x+1, y+z) \cup \mathbf{V}(x+z, y+1)$ è una decomposizione in varietà irriducibili dato che il campo è algebricamente chiuso.

Soluzione E. *103* 1. Scegliamo l'ordinamento lessicografico con $x > y > z$; la base di Gröbner ridotta di I rispetto a questo ordinamento è

$$G = \{x^2 + y^2 - yz, xyz - x, y(y-z)(yz-1)\}.$$

2. I^c è il primo ideale di eliminazione di I, dunque $J = (y(y-z)(yz-1))$.

3. Si ha

$$\sqrt{I} = \sqrt{(I, y)} \cap \sqrt{(I, y-z)} \cap \sqrt{(I, yz-1)} =$$
$$(x, y) \cap \sqrt{(x^2, xz^2 - x, y-z)} \cap \sqrt{(x^2 + y^2 - 1, yz - 1)}$$

Quindi $\mathbf{V}_{\mathbb{Q}}(I) = \mathbf{V}_{\mathbb{Q}}(\sqrt{I}) \supset \mathbf{V}_{\mathbb{Q}}(x, y)$, dunque $\mathbf{V}_{\mathbb{Q}}(I)$ è infinita.

4. Gli ideali (x, y) e $\sqrt{(x^2, xz^2 - x, y-z)} = (x, y-z)$ sono ovviamente primi. Inoltre, si ha anche $\sqrt{(x^2 + y^2 - 1, yz - 1)} = (x^2 + y^2 - 1, yz - 1)$; infatti $\mathbb{Q}[x,y,z]/(x^2 + y^2 - 1, yz - 1) \simeq \mathbb{Q}[y, \frac{1}{y}][x]/(x^2 + y^2 - 1)$ è un dominio, e quindi l'ideale $(x^2 + y^2 - 1, yz - 1)$ è primo. Dunque

$$\mathrm{Min}(I) = \{(x, y), (x, y-z), (x^2 + y^2 - 1, yz - 1)\}.$$

Soluzione E. *104* 1. La base di Gröbner ridotta di I rispetto all'ordinamento lessicografico con $x > y > z > t$ è $G = \{x^2t^2, yt^2, z^2\}$, quindi I è monomiale.

2. Una tale decomposizione è data da $I = (x^2, y, z^2) \cap (z^2, t^2)$.

3. Si ha $\mathcal{N}(A) = \sqrt{I}/I$. Quindi, dal punto precedente otteniamo immediatamente che $\mathcal{N}(A) = (\overline{x}, \overline{y}, \overline{z}) \cap (\overline{z}, \overline{t})$.

4. Dalla forma della base G si ricava immediatamente che

$$\mathbf{V}(I) = \{(a, b, 0, 0) \,:\, a, b \in K\} \cup \{(0, 0, c, 0) \,:\, c \in K\}$$

dunque $|\mathbf{V}(I)|$ è finita se e solo se è finito il campo K.

Soluzione E. *105* La base di Gröbner ridotta di I rispetto all'ordinamento lessicografico con $x > y > z$ è $\{x^2 - yz, xz - yz, y^2 - yz\}$.

1. Sia A l'anello quoziente di I. Si ha $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$ e

$$\begin{aligned}\sqrt{I} &= \sqrt{(x^2 - yz, xz - yz, y)} \cap \sqrt{(x^2 - yz, xz - yz, y - z)} \\ &= (x, y) \cap (x - z, y - z)\ .\end{aligned}$$

Dato che $A/(x, y) \simeq A/(x-z, y-z) \simeq \mathbb{Q}[z]$, questi ideali sono primi (distinti) e quindi $\mathbf{V}(I)$ non è irriducibile. Infine $\mathbf{V}(I) = \mathbf{V}(x, y) \cup \mathbf{V}(x - z, y - z)$ è una decomposizione in componenti irriducibili, cf. **E.**95, e nessuna delle due componenti è finita.

2. Se $f \in \sqrt{I}$ allora $\mathbf{V}(f) \supseteq \mathbf{V}(\sqrt{I}) = \mathbf{V}(I)$, ma $P = (1, 1, 1) \in \mathbf{V}(I) \setminus \mathbf{V}(f)$, quindi $f \notin \sqrt{I}$.

Soluzione E. *106* Dato che $(a, 0, 0) \in \mathbf{V}(I)$ per ogni $a \in \mathbb{C}$, $\mathbf{V}(I)$ non è finita.
Se $I \subseteq (x^2, y + 1, z - 1)$ allora $P = (0, -1, 1) \in \mathbf{V}(x^2, y + 1, z - 1) \subseteq \mathbf{V}(I)$. Dato che P non è soluzione di $y^2z^2 - yz$, questo non è possibile.

Soluzione E. *107* Prima di calcolare una base di Gröbner G di I rispetto all'ordinamento lessicografico con $x > y > z$, osserviamo che l'ideale I contiene un polinomio monico in x; riducendo gli altri generatori dati mediante questo polinomio possiamo riscrivere $I = (f_1 = x - y^2z, f_2 = y^3z^2 - 2, f_3 = 3y^4z^4 - y)$.

Se $\operatorname{char} K = 3$, allora $y \in I$, quindi $2 \in I$ e $I = (1)$. Se invece $\operatorname{char} K \neq 3$, allora $S(f_2, f_3) = -(6yz^2 - y)$. Se $\operatorname{char} K = 2$ allora $y \in I$ e $I = (x, y)$. Infine, se $\operatorname{char} K \neq 2, 3$, si ottiene che $G = \{x - y^2 z, y^3 - 12, 6z^2 - 1\}$.

1. Dato che $\mathbb{C}$ è algebricamente chiuso, la conclusione segue direttamente da **T.**71.

2. Se $p = 3$ allora $\mathbf{V}(I) = \emptyset$, mentre se $p = 2$ chiaramente $\mathbf{V}(I)$ è infinita. Nei rimanenti casi, dato che $\emptyset \neq \mathbf{V}(I) \subset K^3$, allora certamente $\mathbf{V}(I)$ è finita di nuovo per **T.**71.

Soluzione E. *108* La base di Gröbner ridotta G di I rispetto all'ordinamento lex con $x > y > z$ è

$$G = \left\{x + 2z^3 - 3z, y^2 - z^2 + 1, z^4 - 3/2z^2 + 1/2\right\}.$$

1. Abbiamo che $\operatorname{Lt}(I) = \operatorname{Lt}(G) = (x, y^2, z^4)$ e $\mathcal{B} = \{1, y, yz, yz^2, yz^3, z, z^2, z^3\}$ è la base cercata, cf. **T.**50.1.

2. Riducendo p tramite G otteniamo $2y + z^3 - 2z^2 - z + 4$; pertanto il vettore delle coordinate cercato è

$$(4, 2, 0, 0, 0, -1, -2, 1).$$

3. L'uguaglianza non vale; infatti $z^4 - \frac{3}{2}z^2 + \frac{1}{2} = (z^2 - 1)(z^2 - \frac{1}{2})$ ma per $z = \pm 1$ si trovano solo 2 punti $(1, 0, 1)$ e $(-1, 0, -1)$ in $\mathbf{V}(I)$, mentre per $z = \pm\frac{1}{\sqrt{2}}$ si trovano i punti $\left(\sqrt{2}, \pm\frac{i}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$ e $\left(-\sqrt{2}, \pm\frac{i}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)$. Dunque $|\mathbf{V}_{\mathbb{C}}(I)| = 6 < \dim_{\mathbb{Q}} A = 8$.

4. Abbiamo che

$$\begin{aligned}\sqrt{I} &= \sqrt{(I, (z+1)(z-1)(z^2 - 1/2))} \\ &= \sqrt{(I, z+1)} \cap \sqrt{(I, z-1)} \cap \sqrt{(I, z^2 - 1/2)} \\ &= \sqrt{(x-1, y, z-1)} \cap \sqrt{(x+1, y, z+1)} \cap \sqrt{(x - 2z, y^2 + 1/2, z^2 - 1/2)}\end{aligned}$$

e gli ideali sotto il segno di radicale sono massimali in $\mathbb{Q}[x, y, z]$; ciò è immediato per i primi due ideali. Per vedere che il terzo ideale è massimale basta osservare che

$$\mathbb{Q}[x, y, z]/(x - 2z, y^2 + 1/2, z^2 - 1/2) \simeq \mathbb{Q}[y, z]/(y^2 + 1/2, z^2 - 1/2) \simeq \mathbb{Q}(\sqrt{2}, i).$$

Soluzione E. *109* 1. Sia $I = (f_1, f_2, f_3)$. Rispetto all'ordinamento deglex con $y > x$ si ha che $x^3, y^2 \in \mathrm{Lt}(I)$, quindi Σ ha un numero finito di soluzioni.

2. Usiamo ora l'ordinamento lex con $x > y$. Si ha $S(f_1, f_2) \xrightarrow{f_3} xy^2 - x = f \in I$. Pertanto

$$\begin{aligned}\mathbf{V}(I) &= \mathbf{V}(f_1, f_3, f) = \mathbf{V}(I, x) \cup \mathbf{V}(I, y^2 - 1)\\ &= \mathbf{V}(x, y) \cup \mathbf{V}(x^2 - 3x + 1, y - 1) \cup \mathbf{V}(x^2 + 3x + 1, y + 1),\end{aligned}$$

quindi l'unica soluzione razionale è $(0, 0)$.

3. Raffinando la decomposizione di $\mathbf{V}(I)$ ottenuta al punto precedente, si ha

$$\begin{aligned}\mathbf{V}(I) = \mathbf{V}(x, y) \cup \mathbf{V}\left(x - \frac{3 - \sqrt{5}}{2}, y - 1\right) \cup \mathbf{V}\left(x - \frac{3 + \sqrt{5}}{2}, y - 1\right)\\ \cup \mathbf{V}\left(x - \frac{-3 - \sqrt{5}}{2}, y + 1\right) \cup \mathbf{V}\left(x - \frac{-3 + \sqrt{5}}{2}, y + 1\right).\end{aligned}$$

Dato che gli ideali sono tutti massimali in $\mathbb{R}[x, y]$, le componenti della decomposizione di V corrispondono a punti di $\mathbb{R}^2$ e sono irriducibili.

Soluzione E. *110* La base di Gröbner ridotta di I rispetto all'ordinamento lex dato da $x > z > y$ è $\{x - y, z - y^2, y^4 - 1\}$.

1. Possiamo calcolare $I \cap \mathbb{Q}[y] = (y^4 - 1)$; pertanto $p(y) = y^4 - 1$ ha le proprietà richieste.

2. Per il teorema degli zeri, $\mathbf{V}_{\mathbb{C}}((q, I)) = \emptyset$ se e solo se $(q, I) = 1$, quindi una condizione necessaria per appartenere a Σ è che $\gcd(q(y), y^4 - 1) \neq 1$. Sicuramente $y + 1$ e $y - 1$ appartengono a Σ, mentre $y^2 + 1 \notin \Sigma$. Infine, $\Sigma = (y - 1) \cup (y + 1)$ non è un ideale.

Soluzione E. *111* 1. Per ogni $i = 1, \ldots, m$, sia $\mathfrak{m}_i$ l'ideale massimale associato ad α_i; allora $\mathbf{I}(V) = \bigcap_{i=1}^{m} \mathfrak{m}_i$. Dato che $\alpha_i \neq \alpha_j$ per $i \neq j$, tali ideali sono a due a due comassimali e dal teorema cinese del resto segue che $A \simeq \prod_i A/\mathfrak{m}_i \simeq \mathbb{C}^m$. Si verifica allora facilmente che le immagini $a_i \in A$ degli elementi e_i, $i = 1, \ldots, m$, della base canonica di $\mathbb{C}^m$ sono gli idempotenti cercati, cf. **T.**19.

2. Gli idempotenti di $\mathbb{C}^m$ sono tutti e soli i 2^m vettori con coordinate 0 o 1: per l'isomorfismo precedente essi corrispondono agli idempotenti di A che, quindi, sono tutti della forma $a = \sum_{i=1}^{m} b_i a_i$ con $b_i = 0$ o 1 per ogni i.

16.3 Soluzioni del capitolo 10

Soluzione E. *112* La verifica della definizione della struttura di A/I-modulo segue immediatamente dalla definizione della struttura di A-modulo su M, una volta provata la buona definizione del prodotto esterno: se $\overline{a} = \overline{b}$ in A/I, allora $a - b \in I$ e $\overline{am} - \overline{bm} = \overline{a}\overline{m} - \overline{b}\overline{m} = \overline{(a-b)}\overline{m} = 0$ in M/IM.

Soluzione E. *113* Segue immediatamente dalla definizione di B-modulo e dal fatto che f è un omomorfismo di anelli, quindi, in particolare, $f(1_A) = 1_B$.

Soluzione E. *114* Chiaramente per la somma non vi è nulla da verificare.
Sia I un ideale di B; allora per ogni $a \in A$ si ha $aI = f(a)I \subseteq I$, e dunque I è un A-sottomodulo di B.
Sia ora M un A-sottomodulo di B. Dato che per ogni $b \in B$ esiste $a \in A$ tale che $f(a) = b$, si ha $bM = f(a)M = a \cdot M \subseteq M$ ed M è un ideale di B.

Soluzione E. *115* Per ogni $a, b \in N : P$, $c \in A$ e $p \in P$, dalla definizione di $N : P$ e poiché N è un sottomodulo di M, segue immediatamente che $(a-b)p = ap - bp \in N$ e $(ca)p = c(ap) \in N$.

Soluzione E. *116* Il risultato è una conseguenza dei teoremi di omomorfismo. Osserviamo dapprima che

$$IM \simeq I(A/J_1 \oplus A/J_2) \simeq (I + J_1)/J_1 \oplus (I + J_2)/J_2;$$

inoltre l'omomorfismo di proiezione $M \longrightarrow A/(J_1 + I) \oplus A/(J_2 + I)$ è surgettivo ed è facile verificare che il suo nucleo è IM. Questo basta per concludere.

Soluzione E. *117* Consideriamo l'omomorfismo di A-moduli $f : A \longrightarrow aM$ definito da $1 \mapsto a\overline{1}$, che risulta surgettivo. Un elemento $b \in A$ è nel nucleo di f se e solo se $\overline{0} = f(b) = bf(1) = ba\overline{1}$, cioè se e solo se $ab \in J$, i.e. $b \in J : a$. La conclusione segue ora dal primo teorema di omomorfismo.

Soluzione E. *118* Se $n > m$ possiamo scrivere $A^n = A^m \oplus A^{n-m}$ e considerare l'omomorfismo surgettivo $f \circ \pi_1 \colon A^n = A^m \oplus A^{n-m} \longrightarrow A^m \longrightarrow A^n$. Per **T.**98, esso è un isomorfismo; dal momento che $0 = \mathrm{Ker}(f \circ \pi_1) \supseteq A^{n-m}$ si ha allora che A^{n-m}, e dunque A, è 0.

Soluzione E. *119* Siano $\{m_1, \dots, m_r\}$ e $\{n_1, \dots, n_s\}$ rispettivamente una base e un insieme di generatori di M, con $s < r$. L'assegnazione $m_i \mapsto n_i$ per ogni $i = 1, \dots, s$ e $m_i \mapsto 0$ se $i = s+1, \dots, r$, induce per **T.**91 un endomorfismo surgettivo $\tilde{f}$ di M. Per **T.**98 $\tilde{f}$ è un isomorfismo, che non è possibile dato che $m_{s+1} \mapsto 0$.

Soluzione E. *120* Dall'ipotesi discende che $N = \varphi(M) + IN$: infatti per ogni $n \in N$ esiste $m \in M$ tale che $\overline{\varphi}(\overline{m}) = \overline{n}$, dunque $n = \varphi(m) + h$, con $h \in IN$ e l'altra inclusione è ovvia. Allora vale anche $N = \varphi(M) + I(\varphi(M) + IN) = \varphi(M) + I^2N$, dato che $I\varphi(M) \subset \varphi(M)$. Iterando n volte, ove n è tale che $I^n = 0$, si ottiene $N = \varphi(M) + I^nN = \varphi(M)$ e quindi φ è surgettivo.

Soluzione E. *121* Sia $\mathcal{B} = \{e_1, \dots, e_m\}$ la base canonica di A^m.

1. È l'esercizio **E.**118. Equivalentemente si può osservare che f surgettivo implica che $f(\mathcal{B})$ è un insieme di generatori di A^n; da **E.**119 segue allora che $m \geq \mathrm{rank}\, A^n = n$.

2. Supponiamo per contraddizione che $m > n$ e consideriamo l'omomorfismo di inclusione $i \colon A^n \longrightarrow A^m$ dato da $(a_1, \dots, a_n) \mapsto (a_1, \dots, a_n, 0, \dots, 0)$. Allora $\varphi = i \circ f \in \mathrm{End}_A(A^m)$ e, per **T.**94, esistono $a_i \in A$ tali che $\varphi^k + a_{k-1}\varphi^{k-1} + \cdots + a_1\varphi + a_0 = 0$. Possiamo supporre che tale k sia minimo e in tal caso osserviamo che $a_0 \neq 0$, altrimenti $\varphi(\varphi^{k-1} + a_{k-1}\varphi^{k-2} + \cdots + a_1) = 0$ e l'iniettività di φ implica $\varphi^{k-1} + a_{k-1}\varphi^{k-2} + \cdots + a_1 = 0$ che contraddice la minimalità di k. Valutando in e_m otteniamo $(\varphi^k + a_{k-1}\varphi^{k-1} + \cdots + a_1\varphi)(e_m) = -a_0e_m$, ma, per come abbiamo definito φ, $(\varphi^k + a_{k-1}\varphi^{k-1} + \cdots + a_1\varphi)(e_m)$ deve avere ultima coordinata 0, contraddizione.

3. Segue direttamente da 1 e 2.

Soluzione E. *122* 1. Per assurdo, se esistesse un isomorfismo $\varphi : M/N \longrightarrow M$ allora $\varphi \circ \pi : M \longrightarrow M/N \longrightarrow M$ sarebbe un endomorfismo surgettivo e quindi iniettivo, e dunque $N \subseteq \mathrm{Ker}(\varphi \circ \pi) = 0$, che è contro le ipotesi.

2. Consideriamo $M = K[x_i \colon i \in \mathbb{N}]$, un anello di polinomi in infinite variabili a coefficienti in un campo K, come K-modulo, e sia $0 \neq N = (x_0) \subset M$; allora $\varphi \colon M \longrightarrow M/N \simeq K[x_i \colon i \in \mathbb{N}_+]$ definito da $\varphi(x_i) = x_{i+1}$ è un isomorfismo di K-moduli.

Soluzione E. *123* 1. Se $M \simeq A/\mathfrak{m}$, che è un campo, allora M è semplice. Viceversa, sia $0 \neq m \in M$ e sia $f \colon A \longrightarrow M$ l'omomorfismo definito da $1 \mapsto m$; allora $0 \neq f(A) \subseteq M$ è un sottomodulo di M diverso da 0, e quindi, dato che M è semplice, si ha $f(A) = M$, ovvero f è un omomorfismo surgettivo. Quindi $M \simeq A/\operatorname{Ker} f$. Infine, dato che a ogni ideale proprio che contiene strettamente $\operatorname{Ker} f$ corrisponderebbe un sottomodulo non banale di M, $\operatorname{Ker} f$ è necessariamente massimale.

2. Si ha $\operatorname{Ker} \varphi \subseteq M$ e $\operatorname{Im} \varphi \subseteq N$; dato che M è semplice, si ha $\operatorname{Ker} \varphi = M$ e in tal caso φ è l'omomorfismo nullo, oppure $\operatorname{Ker} \varphi = 0$ ossia φ è iniettivo. In questo caso $0 \neq \operatorname{Im} \varphi$ e quindi si deve avere $\operatorname{Im} \varphi = N$.

3. Dal punto 1 segue che o $M = 0$, e la tesi è banale, oppure $M \simeq A/\mathfrak{m}$, per qualche ideale $\mathfrak{m}$ massimale; quindi $\mathcal{J}(A) \subset \mathfrak{m} = \operatorname{Ann} M$, come richiesto.

Soluzione E. *124* Sia M un modulo semplice; allora, per ogni $m \in M$ il sottomodulo ciclico $\langle m \rangle \subseteq M$ è nullo o è tutto M. Viceversa, supponiamo che M sia ciclico generato da un qualunque elemento diverso da zero, e sia $0 \neq N \subseteq M$ un sottomodulo di M. Per ogni $0 \neq n \in N$ avremo per ipotesi che $\langle n \rangle = M$, e quindi $N = M$, come volevamo.

Per quanto appena visto, cerchiamo gli $\mathbb{Z}$-moduli ciclici per cui ogni elemento non nullo è un generatore; pertanto i moduli cercati sono tutti e soli della forma $\mathbb{Z}/(p)$, con p primo.

Soluzione E. *125* Proveremo dapprima che $M = pM \oplus qM$ e in secondo luogo che $N = qM$ e $P = pM$.

Siano dunque $x, y \in \mathbb{Z}$ tali che $xp + yq = 1$; allora, per ogni $m \in M$, si ha che $m = (xp + yq)m = p(xm) + q(ym) \in pM + qM$. Inoltre, vale che $pM \cap qM = 0$. Infatti, se $m \in pM \cap qM$, dato che $\operatorname{Ann} M = (pq)$, avremo $\operatorname{Ann} m \supseteq (q) + (p) = (1)$ e quindi $m = 0$.

Proviamo ora che $qM = N$. Dato che $M = \langle m \rangle$ è uno $\mathbb{Z}$-modulo ciclico e $N \subseteq M$, anche N è ciclico e $N = \langle n \rangle = \langle am \rangle$ per qualche $a \in A$. Dalle

relazioni $apm = pn = 0$ segue che $ap \in \operatorname{Ann} M = (pq)$; di conseguenza, $a = bq \in (q)$ per qualche $b \in A$. Per quanto appena detto avremo che $N \subseteq qM$. Dimostriamo l'inclusione opposta: dato che $\operatorname{Ann} N = (p)$, si deve avere che $(b, p) = 1$ (perché ?), e quindi esistono $c, d \in \mathbb{Z}$ tali che $cb + dp = 1$. Moltiplicando per qm, si ottiene $qm = cbqm = cam \in N$, come volevamo.

Ragionando in maniera analoga si dimostra anche che $P = pM$.

Soluzione E. *126* Dimostriamo il primo isomorfismo, il secondo si dimostra in maniera del tutto analoga. Definiamo

$$\Phi : \operatorname{Hom}_A(M, P) \oplus \operatorname{Hom}_A(N, P) \longrightarrow \operatorname{Hom}_A(M \oplus N, P)$$

come $\Phi(\varphi_1, \varphi_2) = \lambda_{\varphi_1,\varphi_2}$, con $\lambda_{\varphi_1,\varphi_2}(m, n) = (\varphi_1(m), \varphi_2(n))$; definiamo inoltre

$$\Psi : \operatorname{Hom}_A(M \oplus N, P) \longrightarrow \operatorname{Hom}_A(M, P) \oplus \operatorname{Hom}_A(N, P)$$

come $\Psi(\psi) = (\psi_{|M}, \psi_{|N})$. È facile verificare che sono due omomorfismi, uno inverso dell'altro.

Soluzione E. *127* 1. Per ogni $f \in \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$ e per ogni $\frac{a}{b} \in \mathbb{Q}$ si ha $f\left(\frac{a}{b}\right) = af\left(\frac{1}{b}\right)$; è quindi sufficiente controllare quali sono i possibili valori $f\left(\frac{1}{b}\right)$. Dato che $bf\left(\frac{1}{b}\right) = f(1)$ per ogni $b \in \mathbb{Z} \setminus \{0\}$, $f(1)$ è divisibile in $\mathbb{Z}$ per ogni $b \neq 0$, cioè $f(1) = 0$. Quindi $f\left(\frac{1}{b}\right) = 0$ per ogni $b \in \mathbb{Z} \setminus \{0\}$ e di conseguenza $f = 0$.

2. Sia $f \in \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z})$, allora $\operatorname{Im} f$ è generata da $f(\overline{1})$. Inoltre $nf(\overline{1}) = f(\overline{0}) = 0$ implica $f(\overline{1}) = 0$ e quindi $f = 0$.

3. Basta definire $f(\overline{1})$ come la classe di $\frac{1}{n}$ in $\mathbb{Q}/\mathbb{Z}$ per ottenere un elemento non banale di $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Q}/\mathbb{Z})$.

Soluzione E. *128* Osserviamo innanzitutto che, se $\pi : A \longrightarrow A/I$ è la proiezione canonica, risulta definita su A/I una struttura di A-modulo per restrizione di scalari, ponendo $a\overline{b} = \pi(a)\overline{b} = \overline{a}\overline{b} = \overline{ab}$, cf. **E.**113. Inoltre, con una dimostrazione simile a **E.**115, è facile verificare che $0 :_M I$ è un sottomodulo di M.

1. Si consideri ora la mappa $\Phi : 0 :_M I \longrightarrow \operatorname{Hom}_A(A/I, M)$ definita da $\Phi(m) = \varphi_m$, dove $\varphi_m(\overline{b}) = bm$.

Proviamo che Φ è ben definito, e cioè che $\varphi_m \in \mathrm{Hom}_A(A/I, M)$ per ogni $m \in 0 :_M I$. Infatti, se $\overline{b_1} = \overline{b_2} \in A/I$ allora $b_1 - b_2 \in I$ e quindi $(b_1 - b_2)m = 0$, da cui segue che $\varphi_m(\overline{b_1}) = \varphi_m(\overline{b_2})$, ovvero la buona definizione di φ_m.
Inoltre, $\varphi_m(\overline{b_1}) + \varphi_m(\overline{b_2}) = b_1 m + b_2 m = (b_1 + b_2)m = \varphi_m(\overline{b_1 + b_2}) = \varphi_m(\overline{b_1} + \overline{b_2})$ e $a\varphi_m(\overline{b_1}) = a(b_1 m) = (ab_1)m = \varphi_m(\overline{ab_1}) = \varphi_m(a\overline{b_1})$, per ogni $a, b_1, b_2 \in A$; questo mostra che per ogni tale m, φ_m è un omomorfismo di A-moduli, e dunque Φ è ben definito.
È facile verificare che Φ è un omomorfismo di A-moduli. Vediamo ora che Φ è un isomorfismo: è iniettivo poiché se $\Phi(m) = \varphi_m = 0$ allora $0 = \varphi_m(\overline{1}) = m$. È surgettivo poiché ogni $f \in \mathrm{Hom}_A(A/I, M)$ è determinato per A-linearità da $f(\overline{1})$, che, come prima, si verifica essere un elemento di $0 :_M I$; allora $\Phi(f(\overline{1})) = \varphi_{f(\overline{1})} = f$.
2. Usando il punto precedente, possiamo mostrare che l'A-modulo $0 :_M I$ è un A/I-modulo; a questo scopo basta notare che $I \subseteq 0 :_A (0 :_M I) = \mathrm{Ann}(0 :_M I)$ e concludere grazie a **T.**85.
3. Per il punto 1, basta osservare che $0 :_{A/J} I \simeq (J : I)/J$. Consideriamo la mappa $J : I \xrightarrow{\varphi} 0 :_{A/J} I \subseteq A/J$ definita da $a \mapsto \overline{a}$; essa è ben definita poiché, se $aI \subseteq J$, allora $\overline{a}I = 0_{A/J}$. Chiaramente φ è un omomorfismo di A-moduli; è surgettivo poiché se $0 = \overline{a}i = \overline{ai}$ per ogni $i \in I$, allora $aI \subseteq J$, i.e. $a \in J : I$. La conclusione segue ora dal fatto che $\mathrm{Ker}\,\varphi = J$.

Soluzione E. *129* Grazie all'esercizio precedente, e visto che $I \subset J$, deduciamo che $\mathrm{Hom}_A(A/I, A/J) \simeq (J : I)/J = A/J$, il quale è un K-spazio vettoriale di dimensione infinita dato che, ad esempio, gli elementi di $\{\overline{y}^n \mid n \in \mathbb{N}\}$ sono linearmente indipendenti.

Soluzione E. *130* Dato che A è locale, dal lemma di Nakayama discende che $\mathfrak{m}M \neq M$ dato che M è finitamente generato e $M \neq 0$. Da questo segue che $M/\mathfrak{m}M$ è un $A/\mathfrak{m}$-modulo, e quindi uno spazio vettoriale, non nullo di dimensione finita ed esiste certamente una applicazione lineare $f\colon M/\mathfrak{m}M \longrightarrow A/\mathfrak{m}$ non nulla. Sia $\pi\colon M \longrightarrow M/\mathfrak{m}M$ la proiezione canonica; allora $f \circ \pi$ è un elemento non nullo di $\mathrm{Hom}_A(M, A/\mathfrak{m})$.

Soluzione E. *131* Ogni elemento non zero di B è invertibile in K; pertanto, indicato con $\mathfrak{m}$ l'ideale massimale di B, avremo $\mathfrak{m}K = K$. Se K fosse un

B-modulo finitamente generato dal lemma di Nakayama discenderebbe che $K = 0$, che non è possibile poiché $B \neq 0$.

Soluzione E. *132* Sia $a \in \sqrt{\operatorname{Ann} M + I}$; allora esiste $n \in \mathbb{N}$ tale che $a^n = b + i$, con $b \in \operatorname{Ann} M$ e $i \in I$. Quindi si ha $a^n M = (b+i)M = 0 + iM \subset IM$, che implica $a^n \in \operatorname{Ann}(M/IM)$ e quindi che $a \in \sqrt{\operatorname{Ann}(M/IM)}$.

Viceversa, sia $a \in \sqrt{\operatorname{Ann}(M/IM)}$, e sia $k \in \mathbb{N}$ tale che $a^k \in \operatorname{Ann}(M/IM)$; pertanto $a^k M \subseteq IM$. Consideriamo allora l'endomorfismo $\varphi\colon M \longrightarrow M$, definito da $\varphi(m) = a^k m$. Abbiamo $\varphi(M) = a^k M \subseteq IM$ e quindi, dato che M è finitamente generato, possiamo applicare il teorema di Cayley-Hamilton, cf. **T.**94, per ottenere $n \in \mathbb{N}$ e $a_0, \ldots, a_{n-1} \in I$ tali che

$$\varphi^n + a_{n-1}\varphi^{n-1} + \ldots + a_0 = 0.$$

Se indichiamo con $b = a^{kn} + a_{n-1}a^{k(n-1)} + \ldots + a_1 a^k + a_0$, si ha allora che $bM = 0$, ossia che $b \in \operatorname{Ann} M$. Inoltre, $a^{kn} = b - \sum_{i=0}^{n-1} a_i a^{ki}$ e dato che l'ultima sommatoria è un elemento di I, otteniamo che $a \in \sqrt{\operatorname{Ann} M + I}$, come volevamo.

Soluzione E. *133* Sia $\{a_1, \ldots, a_n\}$ un insieme di generatori di $\mathcal{N}(A)$; allora esiste $r_i \in \mathbb{N}$ tale che $a_i^{r_i} = 0$ per ogni $i = 1, \ldots, n$. È facile verificare che esiste $s \in \mathbb{N}$ tale che $\mathcal{N}(A)^s = 0$. Ora, dato che $\mathcal{N}(A)M = M$, avremo anche che $0 = \mathcal{N}(A)^s M = M$, come volevamo.

Soluzione E. *134* Siano $A = K[x_i\colon i \in \mathbb{N}]$ un anello di polinomi in infinite variabili a coefficienti in un campo K e $I \subset A$ l'ideale $I = (x_0^2, x_1^2 - x_0, x_2^2 - x_1, \ldots, x_n^2 - x_{n-1}, \ldots)$.
È immediato verificare che $\mathcal{N}(A/I) \supseteq (\overline{x_i}\colon i \in \mathbb{N})$, dato che $\overline{x_0} \in \mathcal{N}(A/I)$ e $\overline{x_i}^{2^i} = \overline{x_0}$ per ogni i; inoltre K non ha nilpotenti non banali, e dunque vale anche l'altra inclusione.
Notiamo che $\mathcal{N}(A/I)^2 = \mathcal{N}(A/I)$ e ricordiamo che $\mathcal{N}(A/I) \subseteq \mathcal{J}(A/I)$: dunque l'$A/I$-modulo $M = \mathcal{N}(A/I) \neq 0$ fornisce il controesempio cercato a **T.**95, II forma.

Soluzione E. *135* Chiamiamo $f_i\colon M_i \longrightarrow M_{i+1}$ gli omomorfismi della prima riga e $g_i\colon N_i \longrightarrow N_{i+1}$ quelli della seconda.

1. Sia $m_3 \in M_3$ tale che $\alpha_3(m_3) = 0$ e verifichiamo che $m_3 = 0$. Avremo che $0 = \alpha_3(m_3) = g_3(\alpha_3(m_3)) = \alpha_4(f_3(m_3))$, e dall'iniettività di α_4 discende che $m_3 \in \operatorname{Ker} f_3 = \operatorname{Im} f_2$; pertanto esiste $m_2 \in M_2$ tale che $f_2(m_2) = m_3$ e $g_2(\alpha_2(m_2)) = \alpha_3(f_2(m_2)) = 0$. Ne segue che $\alpha_2(m_2) \in \operatorname{Ker} g_2 = \operatorname{Im} g_1$, pertanto esiste $n_1 \in N_1$ tale che $g_1(n_1) = \alpha_2(m_2)$. Poiché α_1 è surgettivo, esiste $m_1 \in M_1$ tale che $\alpha_1(m_1) = n_1$. Inoltre, $\alpha_2(f_1(m_1)) = g_1(\alpha_1(m_1)) = \alpha_2(m_2)$ e quindi per l'iniettività di α_2 avremo che $m_2 = f_1(m_1)$. Infine, $m_3 = f_2(m_2) = f_2(f_1(m_1)) = 0$, come volevamo.

2. Sia $n_3 \in N_3$; allora $g_3(n_3) \in N_4$ e, dato che α_4 è surgettiva, esiste $m_4 \in M_4$ tale che $\alpha_4(m_4) = g_3(n_3)$. Adesso $\alpha_5(f_4(m_4)) = g_4(\alpha_4(m_4)) = g_4(g_3(n_3)) = 0$, e α_5 iniettivo implica $f_4(m_4) = 0$. Quindi $m_4 \in \operatorname{Ker} f_4 = \operatorname{Im} f_3$ e possiamo scrivere $m_4 = f_3(m_3)$ per qualche $m_3 \in M_3$: da $\alpha_4(f_3(m_3)) = g_3(\alpha_3(m_3))$ otteniamo $g_3(\alpha_3(m_3) - n_3) = \alpha_4(m_4) - g_3(n_3) = 0$, cioè $\alpha_3(m_3) - n_3 \in \operatorname{Ker} g_3 = \operatorname{Im} g_2$ e $\alpha_3(m_3) - n_3 = g_2(n_2)$ per qualche $n_2 \in N_2$. Infine α_2 surgettiva implica $n_2 = \alpha_2(m_2)$ per qualche $m_2 \in M_2$ e $\alpha_3(f_2(m_2)) = g_2(\alpha_2(m_2)) = \alpha_3(m_3) - n_3$, quindi $\alpha_3(m_3 - f_2(m_2)) = n_3$ e α_3 è surgettiva.

Soluzione E. *136* Possiamo provare che esiste una retrazione di f, ossia un omomorfismo $\alpha : M \longrightarrow N$ tale che $\alpha \circ f = \mathrm{id}_N$. Dato che (p) e (q) sono comassimali, avremo che $p' + q' = 1$ per certi $p', q' \in \mathbb{Z}$ multipli di p e q rispettivamente. Per ogni $m \in M$, allora, $m = p'm + q'm$ e osserviamo che $g(m - p'm) = q'g(m) \in qP = 0$. Per l'esattezza della successione, $m - p'm \in \operatorname{Ker} g = \operatorname{Im} f$ ed esiste un unico $n \in N$ tale che $f(n) = m - p'm = q'm$. Possiamo ora definire $\alpha(m) = q'n$. Rimane da verificare che $\alpha \circ f = \mathrm{id}_N$; a tal scopo osserviamo che $\alpha(f(n)) = \alpha(q'm) = q'\alpha(m) = (1 - p')^2 n = n$, ove l'ultima uguaglianza discende dal fatto che $p'n \in pN = 0$.

Soluzione E. *137* 1. Consideriamo la successione

$$0 \longrightarrow \mathbb{Z}/(2) \xrightarrow{f} \mathbb{Z}/(4) \xrightarrow{g} \mathbb{Z}/(2) \longrightarrow 0,$$

ove f è definita da $f(1) = 2$, e $g = \pi$ la proiezione canonica di $\mathbb{Z}/(4)$ su $\mathbb{Z}/(2)$. Allora è chiaro che f è ben definita e iniettiva e g è ben definita e surgettiva. Il nucleo di g è dato da $(2)/(4)$, che è anche l'immagine di f.

2. Consideriamo la successione

$$0 \longrightarrow \mathbb{Z}/(2) \xrightarrow{f'} \mathbb{Z}/(2) \oplus \mathbb{Z}/(4) \xrightarrow{g'} \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \longrightarrow 0,$$

ove $f' = (0, f)$ e f è la moltiplicazione $\cdot 2$ come al punto precedente, e $g' = \mathrm{id}_{\mathbb{Z}/(2)} \oplus g$. Allora, g' è surgettiva perché le sue componenti lo sono, mentre f' è iniettiva perché f lo è. È altresì chiaro che $\operatorname{Im} f' = 0 \oplus (2)/(4) = \operatorname{Ker} g'$.

3. Consideriamo ora un omomorfismo $g : \mathbb{Z}/(8) \longrightarrow \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$: dato che $\operatorname{Im} g$ è generata da $g(\overline{1})$, deve essere uno $\mathbb{Z}$-modulo ciclico, quindi g non può essere surgettiva.

Alternativamente possiamo osservare che un omomorfismo $f : \mathbb{Z}/(2) \longrightarrow \mathbb{Z}/(8)$ è determinato da $f(\overline{1})$ e che deve essere $2f(\overline{1}) = \overline{0}$. Dunque l'unico omomorfismo iniettivo manda $\overline{1}$ in $\overline{4}$, ha per immagine $(4)/(8)$ e per conucleo $\mathbb{Z}/(4)$ e l'unica successione esatta possibile è

$$0 \longrightarrow M \longrightarrow P \longrightarrow N \longrightarrow 0\,.$$

Soluzione E. *138* Sia $n \in N$ e $g(n) = \sum_{i=1}^{p} a_i h_i$, ove $\{h_1, \ldots, h_p\}$ è un insieme di generatori di P, e $a_i \in A$ per ogni i. Essendo g surgettiva, possiamo scegliere $n_1, \ldots, n_p \in N$ tali che $g(n_i) = h_i$, per ogni i. Pertanto, $g\left(n - \sum_{i=1}^{p} a_i n_i\right) = 0$, ovvero $n - \sum_{i=1}^{p} a_i n_i \in \operatorname{Ker} g = \operatorname{Im} f$. Dato un insieme di generatori $\{k_1, \ldots, k_m\}$ di M , le immagini dei k_i formano un insieme di generatori per $\operatorname{Im} f$. Concludendo, possiamo dunque scrivere un qualsiasi elemento di N come combinazione lineare degli $m + p$ elementi $f(k_1), \ldots, f(k_m), n_1, \ldots, n_p$.

In generale N avrà sistemi di generatori con meno di $m + p$ elementi: basti pensare alla classica successione esatta corta con $M = I \subseteq A = N$, e $P = A/I$, con I ideale di un anello A.

Soluzione E. *139* Sia $n \in N$ e consideriamo $n = (n - f(g(n))) + f(g(n))$; ora, $f(g(n)) \in \operatorname{Im} f$ mentre $n - f(g(n)) \in \operatorname{Ker} g$, dato che per ipotesi $g \circ f = \mathrm{id}_M$. Inoltre se $n = f(m) \in \operatorname{Ker} g$, allora $0 = g(n) = g(f(m)) = m$. Questo prova che la somma è diretta e conclude la dimostrazione.

Alternativamente possiamo osservare che $g \circ f = \mathrm{id}_M$ implica f iniettiva e considerare la successione esatta

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{\pi} \operatorname{Coker} f \longrightarrow 0\,.$$

Per ipotesi la successione spezza quindi $N = M \oplus \operatorname{Coker} f \simeq \operatorname{Im} f \oplus \operatorname{Ker} g$: infatti una dimostrazione analoga alla precedente mostra che $\pi_{|\operatorname{Ker} g} : \operatorname{Ker} g \longrightarrow \operatorname{Coker} f$ è un isomorfismo.

Soluzione E. *140* La successione è sicuramente esatta in M e W, basta quindi provare l'esattezza in N e in T, ossia che $\operatorname{Ker}(g \circ f) = \operatorname{Im} \varphi$ e $\operatorname{Im}(g \circ f) = \operatorname{Ker} \psi$. Dato che g è iniettiva, avremo $\operatorname{Ker}(g \circ f) = \operatorname{Ker} f = \operatorname{Im} \varphi$, mentre dalla surgettività di f discende che $\operatorname{Im}(g \circ f) = \operatorname{Im} g = \operatorname{Ker} \psi$.

Soluzione E. *141* Se $\mathbb{Z}/(n)$ fosse uno $\mathbb{Z}$-modulo proiettivo, per **T.**106 la successione $0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/(n) \longrightarrow 0$ spezzerebbe. Per **T.**102, esisterebbe allora una sezione s di π ovvero un elemento non nullo di $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z})$, che non è possibile per via di **E.**127.2.

Chiaramente, come $\mathbb{Z}/(n)$-modulo, $\mathbb{Z}/(n)$ è libero e dunque proiettivo.

Soluzione E. *142* Per il teorema cinese del resto $A \simeq \mathbb{Z}/(4) \oplus \mathbb{Z}/(3)$ è libero come modulo su se stesso e quindi $\mathbb{Z}/(4)$ è un A-modulo proiettivo in quanto suo addendo diretto, cf. **T.**106. Per motivi di cardinalità $\mathbb{Z}/(4) \not\simeq A^n$, per ogni n; pertanto non può essere libero.

Soluzione E. *143* In A l'unico sottomodulo non banale è $(2)/(4) \simeq \mathbb{Z}/(2)$ e non è proiettivo perché se lo fosse allora sarebbe un fattore diretto di $\mathbb{Z}/(4)$ e quindi si dovrebbe avere $\mathbb{Z}/(4) \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$ che è assurdo. Per quanto riguarda B gli unici sottomoduli non banali sono $(3)/(6) \simeq \mathbb{Z}/(2)$ e $(2)/(6) \simeq \mathbb{Z}/(3)$. Dato che $\mathbb{Z}/(6) \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(3)$ entrambi i sottomoduli sono proiettivi.

Soluzione E. *144* 1. Consideriamo la successione

$$0 \longrightarrow I \cap J \xrightarrow{f} I \oplus J \xrightarrow{g} I + J \longrightarrow 0$$

dove $f(a) = (a, -a)$ e $g(a, b) = a + b$. È facile verificare che si tratta di una successione esatta. Dato che per ipotesi $I + J = A$ e dunque $I \cap J = IJ$, possiamo scrivere

$$0 \longrightarrow IJ \xrightarrow{f} I \oplus J \longrightarrow A \longrightarrow 0\,.$$

Dato che A è proiettivo la successione spezza e si ricava $I \oplus J \cong IJ \oplus A$, come volevamo.

2. Sia $IJ = (d)$. Se $d = 0$ allora $I \oplus J = A$; altrimenti $d \neq 0$ e $IJ = (d) \simeq A$ dato che A è un dominio, e dal punto precedente segue che $I \oplus J \simeq A^2$. In entrambi i casi, I e J sono addendi diretti di un modulo libero e dunque sono proiettivi.

Soluzione E. *145* 1. Se $M \simeq N \simeq \mathbb{Z}$, avremo $f(1) = n$, con $n \neq 0$. Se $n = \pm 1$, allora $P = 0$, altrimenti $P \simeq \mathbb{Z}/(n)$; in ogni caso $P \simeq \mathbb{Z}/(n)$.

Se invece $P \simeq \mathbb{Z}$, allora P è proiettivo e la successione spezza, e dunque avremo $0 \longrightarrow M \longrightarrow M \oplus \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow 0$. Se $M \simeq \mathbb{Z}$ allora $N \simeq \mathbb{Z}^2$, se invece $N \simeq \mathbb{Z}$ allora $N \simeq P$ e $M = 0$.

2. Se $N \simeq \mathbb{Z}$, avremo che $M = 0$ oppure $M \simeq \mathbb{Z}$, e possiamo utilizzare quanto visto nel punto precedente. Se $P \simeq \mathbb{Z}$, la successione spezza, e dunque avremo $0 \longrightarrow M \longrightarrow M \oplus \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow 0$, con M qualsiasi. Se infine $M \simeq \mathbb{Z}$, nulla di rilevante si può dire sulla successione senza ipotesi aggiuntive.

3. Nell'analogo della prima parte del punto 1, i.e. con $M \simeq N \simeq A$ si ha ancora $f(1_A) = a \neq 0$. Dunque $a \in A^*$ implica $P = 0$, altrimenti $P \simeq A/(a)$; in ogni caso $P \simeq A/(a)$. Nel resto delle dimostrazioni abbiamo utilizzato i seguenti fatti: $\mathbb{Z}$ è uno $\mathbb{Z}$-modulo proiettivo e un sottomodulo di $\mathbb{Z}$ è nullo o isomorfo a $\mathbb{Z}$. Entrambi questi fatti sono validi anche per un qualsiasi PID A, cf. **T.**108, quindi anche le dimostrazioni restano valide.

Soluzione E. *146* 1. Ogni elemento di M, si può scrivere come $m = (m - \varphi(m)) + \varphi(m)$, quindi $M = (\mathrm{id}_M - \varphi)(M) + \varphi(M)$, e questa somma è diretta; infatti se $n = \varphi(m_1) = m_2 - \varphi(m_2) \in \varphi(M) \cap (\mathrm{id}_M - \varphi)(M)$, allora si ha $n = \varphi^2(m_1) = \varphi(m_2) - \varphi(m_2) = 0$.

2. Dato che M è finitamente generato esiste $n \in \mathbb{N}$ e un omomorfismo $g : A^n \longrightarrow M$ surgettivo.

Se M è proiettivo allora esiste una sezione $\sigma\colon M \longrightarrow A^n$ tale che $g \circ \sigma = \mathrm{id}_M$. Definiamo $f : A^n \longrightarrow A^n$ come $f = \sigma \circ g$. Questo è un omomorfismo e $f^2 = \sigma \circ g \circ \sigma \circ g = f$. Inoltre $f(A^n) = \sigma(g(A^n)) = \sigma(M) \simeq M$, ove l'isomorfismo è dovuto al fatto che σ è iniettiva.

Viceversa, supponiamo che esista $f \in \mathrm{End}_A(A^n)$ tale che $f^2 = f$ e $f(A^n) \simeq M$; allora per il punto 1 $A^n \simeq f(A^n) \oplus (\mathrm{id}_{A^n} - f)(A^n) \simeq M \oplus (\mathrm{id}_{A^n} - f)(A^n)$. Allora M è addendo diretto di un modulo libero e quindi è proiettivo.

Soluzione E. *147* Sia A un campo; allora ogni A-modulo è uno spazio vettoriale e ogni successione esatta di spazi vettoriali spezza, quindi ogni A modulo è proiettivo.

Viceversa, sia $0 \neq a \in A$; consideriamo la successione esatta

$$0 \longrightarrow A \xrightarrow{f} A \longrightarrow A/(a) \longrightarrow 0$$

dove $f = \cdot a$ è iniettiva poiché A è un dominio. Per ipotesi la successione spezza quindi esiste $g\colon A \longrightarrow A$ tale che $g \circ f = \mathrm{id}_A$. Pertanto, $1 = g(f(1)) = g(a)$. Dato che g è un omomorfismo di A-moduli, $1 = g(a) = ag(1)$ e quindi a è invertibile in A e A è un campo.

Soluzione E. *148* 1. Dall'ipotesi discende subito che M/N e M'/N' sono liberi e dunque proiettivi. Pertanto le successioni in questione spezzano.

2. Dal punto 1 segue che $M \simeq N \oplus M/N$ e $M' \simeq N' \oplus M'/N'$. Dato che $N \simeq N'$ e $M/N \simeq M'/N'$, si ha anche $M \simeq M'$, come volevamo.

Soluzione E. *149* 1. È facile vedere che $A/I \simeq A/J \simeq \mathbb{Z}/(3)$, che è un campo. Pertanto I e J sono ideali massimali; se $I = J$, avremmo $1 \in I$, che non è possibile. Sia ora $\alpha = a + b\sqrt{-5} \in A$ un elemento che verifica $(\alpha) = I$; allora $\alpha | 3$ e $\alpha | 1 - \sqrt{-5}$: indicando con $\overline{\alpha}$ il complesso coniugato di α otteniamo $\alpha\overline{\alpha} | 9$ e $\alpha\overline{\alpha} | 6$, cioè $\alpha\overline{\alpha} = 1$ oppure 3. Dato che $\alpha\overline{\alpha} = a^2 + 5b^2$, si avrebbe che $\alpha\overline{\alpha} = 3$ non è possibile e $\alpha\overline{\alpha} = 1$ porta alla contraddizione $I = A$. Con una dimostrazione analoga si vede che lo stesso vale per J.

2. Gli ideali I e J sono comassimali, dunque $I \cap J = IJ$. Inoltre $(3) \in I \cap J$ e, d'altra parte, IJ è generato da 9, $3(1+\sqrt{-5})$, $3(1-\sqrt{-5})$ e 6, ed è quindi contenuto in (3).

Per **E.**144 I e J sono A-moduli proiettivi, inoltre $I \oplus J = A^2$ e abbiamo già verificato al punto 1 che non sono principali quindi non sono isomorfi ad A. Infine tra i generatori di I, risp. J, esiste la relazione $2 \cdot 3 - (1+\sqrt{-5})(1-\sqrt{-5}) = 0$, dunque I, risp. J, non è libero.

Soluzione E. *150* L'implicazione "$\Rightarrow$" è immediata dalla definizione di modulo iniettivo, dato che l'omomorfismo di inclusione $I \longrightarrow A$ è iniettivo.
Siano adesso M, N due A moduli con omomorfismi $f : M \longrightarrow N$ iniettivo e $g : M \longrightarrow E$ e definiamo

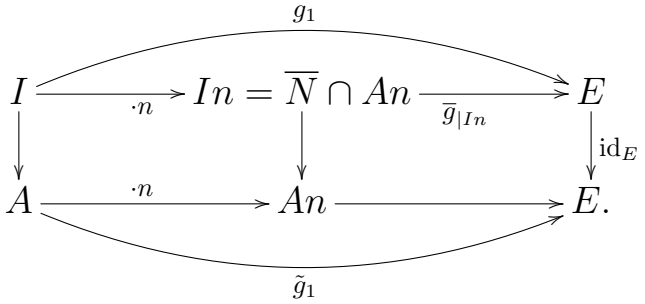
$$S = \{(N', g') \,:\, N' \subseteq N \text{ e } g' : N' \longrightarrow E \text{ tale che } g' \circ f = g\},$$

l'insieme delle coppie di sottomoduli N' di N e omomorfismi g' che estendono g. L'insieme S non è vuoto perché contiene la coppia $(f(M), \eta)$ dove $\eta(f(m)) = g(m)$ per ogni $m \in M$.

È facile vedere che S verifica le ipotesi del Lemma di Zorn rispetto all'ordinamento $(N', g') < (N'', g'') \iff N' \subseteq N''$ e $g''_{|N'} = g'$, e dunque ammette un elemento massimale $(\overline{N}, \overline{g})$. Se $\overline{N} = N$ abbiamo finito, altrimenti esiste $n \in N \setminus \overline{N}$ e possiamo considerare in A l'ideale $I = \overline{N} : n$. Abbiamo un omomorfismo $g_1 : I \longrightarrow E$ definito dalla composizione

$$I \xrightarrow{\cdot n} \overline{N} \xrightarrow{\overline{g}} E$$

che, per ipotesi, si estende a $\widetilde{g_1} : A \longrightarrow E$ e si inserisce nel seguente diagramma commutativo dove le due prime mappe verticali a sinistra sono le ovvie inclusioni



Possiamo allora definire $\tilde{g} : \overline{N} + An \longrightarrow E$ ponendo $\tilde{g}(\overline{n} + an) = \overline{g}(\overline{n}) + \widetilde{g_1}(a)$, per ogni $\overline{n} \in \overline{N}$ e per ogni $a \in A$. La mappa $\tilde{g}$ è ben definita perché se $\overline{n_1} + a_1 n = \overline{n_2} + a_2 n$ allora $a_1 - a_2 \in \overline{N} : n = I$ e

$$\begin{aligned}\tilde{g}(a_1 n - a_2 n) &= \widetilde{g_1}(a_1 - a_2) = g_1(a_1 - a_2) \\ &= \overline{g}(a_1 n - a_2 n) = \overline{g}(\overline{n_2} - \overline{n_1}) = \tilde{g}(\overline{n_2} - \overline{n_1}),\end{aligned}$$

quindi $\tilde{g}(\overline{n_1} + a_1 n) = \tilde{g}(\overline{n_2} + a_2 n)$. È facile vedere che $\tilde{g}$ è un omomorfismo e che $\tilde{g}_{|\overline{N}} = \overline{g}$, dunque abbiamo ottenuto la coppia $(\overline{N} + An, \tilde{g}) > (\overline{N}, \overline{g})$ appartenente ad S: contraddizione.

Soluzione E. *151* $1 \Leftrightarrow 2$. Dato che il funtore $\mathrm{Hom}_A(\bullet, E)$ è controvariante esatto a sinistra, dire che è esatto equivale al fatto che per ogni omomorfismo iniettivo $f\colon M \longrightarrow N$ l'omomorfismo indotto $f^*\colon \mathrm{Hom}_A(N, E) \longrightarrow$

$\mathrm{Hom}_A(M,E)$ è surgettivo, e cioè che per ogni omomorfismo $g\colon M \longrightarrow E$ esiste un omomorfismo $\tilde{g}\colon N \longrightarrow E$ tale che $f^*(\tilde{g}) = \tilde{g}\circ f = g$, ovvero E è iniettivo.

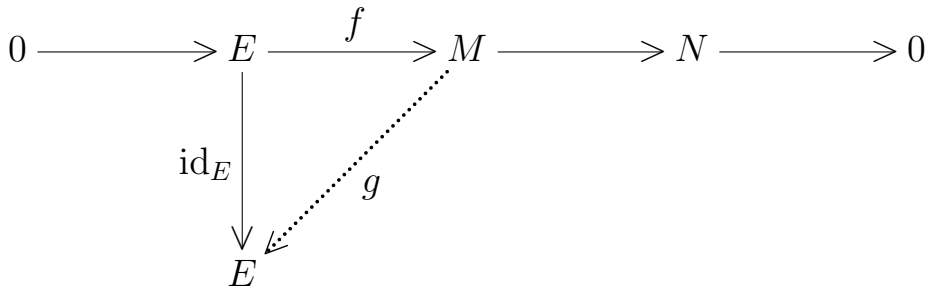
$3 \Leftrightarrow 4$. L'implicazione "$\Rightarrow$" è ovvia.

Per il viceversa, consideriamo una successione esatta

$$0 \longrightarrow E \xrightarrow{f} M \longrightarrow N \longrightarrow 0$$

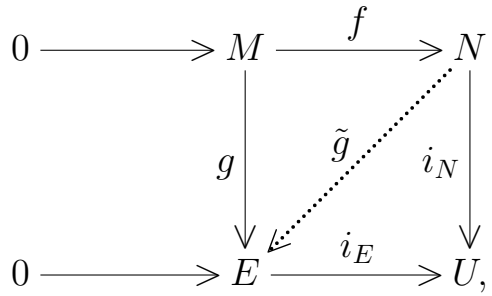
con $E \simeq f(E)$ sottomodulo di M e $N \simeq M/f(E)$. Per ipotesi esiste un sottomodulo L di M tale che $M \simeq E \oplus L$: dunque $L \simeq M/E \simeq M/f(E) \simeq N$ e $M \simeq E \oplus N$ che è una delle condizioni equivalenti per lo spezzamento della successione, cf. **T.**102.

$1 \Rightarrow 3$. Basta considerare il diagramma



ove per ipotesi esiste g tale che $g\circ f = \mathrm{id}_E$; tale g è dunque una retrazione di f, e la sua esistenza implica lo spezzamento della successione, cf. nuovamente **T.**102.

$3 \Rightarrow 1$. Siano $f\colon M \longrightarrow N$ e $g\colon M \longrightarrow E$ omomorfismi, con f iniettivo. Definiamo $U = (E\oplus N)/L$, ove L è il sottomodulo di U generato dalle coppie $(g(m), -f(m))$ al variare di $m \in M$, e consideriamo il diagramma



con $i_E(e) = \overline{(e,0)}$ e $i_N(n) = \overline{(0,n)}$. Per costruzione il quadrato commuta; inoltre i_E è iniettiva: infatti se $i_E(e) = 0$ allora esistono $m_i \in M$ e $a_i \in A$ tali

che $(e,0) = \sum_i a_i(g(m_i), -f(m_i)) = (g(m), -f(m))$, con $m = \sum_i a_i m_i \in M$. Dunque $0 = f(m)$, e l'iniettività di f implica $m = 0$ e, di conseguenza, $e = g(m) = 0$.
Per ipotesi allora esiste un omomorfismo $r\colon U \longrightarrow E$ tale che $r \circ i_E = \mathrm{id}_E$ e possiamo definire $\tilde{g}\colon N \longrightarrow E$ per composizione come $\tilde{g} = r \circ i_N$. Concludiamo mostrando che $\tilde{g}$ estende g, da cui discende che E è iniettivo: per ogni $m \in M$ si ha

$$(\tilde{g} \circ f)(m) = (r \circ (i_N \circ f))(m) = ((r \circ i_E) \circ g)(m) = g(m),$$

come volevamo.

Soluzione E. *152* 1. Se A è un campo, allora gli A-moduli sono spazi vettoriali e una successione esatta di spazi vettoriali verifica ovviamente la condizione 3 di **E.**151.

Alternativamente, possiamo osservare che se esiste un omomorfismo iniettivo $f : M \longrightarrow N$, allora estendendo una base di $f(M)$ ad una base di N possiamo scrivere $N = f(M) \oplus L$ per qualche sottospazio vettoriale L di N. È dunque facile estendere $g\colon M \longrightarrow F$ ad un omomorfismo $\tilde{g}\colon N \longrightarrow F$ tale che $g = \tilde{g} \circ f$ semplicemente definendo $\tilde{g}(f(m) + \ell) = g(m)$.
2. In generale un modulo libero non è iniettivo; consideriamo la successione esatta

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \longrightarrow \mathbb{Z}/(n) \longrightarrow 0$$

e applichiamo il funtore $\mathrm{Hom}_{\mathbb{Z}}(\bullet, \mathbb{Z})$ per ottenere la successione esatta

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \xrightarrow{(\cdot n)^*} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$$

in cui $(\cdot n)^*$ non è surgettiva; infatti basta osservare che $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \simeq \mathbb{Z}$ e $(\cdot n)^*$ corrisponde ancora alla moltiplicazione per n. Quindi $\mathrm{Hom}_{\mathbb{Z}}(\bullet, \mathbb{Z})$ non è esatto, e per il criterio **E.**151.2 abbiamo allora verificato che $\mathbb{Z}$ non è iniettivo.

16.4 Soluzioni del capitolo 11

Soluzione E. *153* Gli A-moduli proiettivi sono liberi, cf. **T.**109. Un sottomodulo N di M è libero anch'esso per **T.**108, quindi proiettivo per **T.**105.

Soluzione E. *154* Siano $m_1, m_2 \in M_p$ e $a \in A$; allora esistono $k_1, k_2 \in \mathbb{N}$ tali che $p^{k_1}m_1 = p^{k_2}m_2 = 0$. Dunque $p^{\max\{k_1,k_2\}}(m_1+m_2) = 0$ e $p^{k_1}(am_1) = 0$, cioè $m_1 + m_2, am_1 \in M_p$.

Soluzione E. *155* 1. Osserviamo che è sempre vero che $M_a + M_b \subseteq M_{ab}$: infatti, se $m_1 \in M_a$ e $m_2 \in M_b$, allora esistono k_1, k_2 tali che $a^{k_1}m_1 = b^{k_2}m_2 = 0$. Di conseguenza, $(ab)^{\max(k_1,k_2)}(m_1+m_2) = 0$. Visto che M_{ab} è finitamente generato per **T.**108, esiste un intero k tale che $(ab)^k M_{ab} = 0$, e dal fatto che $\gcd(a^k, b^k) = 1$, segue che esistono $s, t \in A$ tali che $sa^k + tb^k = 1$. Poniamo ora $c = tb^k$ e $d = sa^k$. È immediato verificare che:

- $cM_{ab} \subseteq M_a$ e $dM_{ab} \subseteq M_b$;
- $cM_b = 0$ e $dM_a = 0$;
- $cm_a = (c+d)m_a = m_a$ per ogni $m_a \in M_a$ e $dm_b = (c+d)m_b = m_b$ per ogni $m_b \in M_b$.

Quindi, se $m \in M_{ab}$ si ha $m = 1\cdot m = (c+d)m \in M_a + M_b$. Abbiamo pertanto concluso che $M_{ab} = M_a + M_b$. Inoltre, la somma è diretta: se $m \in M_a \cap M_b$ allora $m = (c+d)m = 0$.

2. Per quanto visto sopra la moltiplicazione per c, rispettivamente per d, è la proiezione di M_{ab} su M_a, rispettivamente su M_b.

3. Sia $M_{ab} = \langle m \rangle$; dal punto 2 discende allora che M_a è generato da cm e M_b da dm.

Viceversa, se $M_a = \langle m_a \rangle$ e $M_b = \langle m_b \rangle$, sia $m = m_a + m_b$; allora, $m_a = cm \in M_a$ e $m_b = dm \in M_b$ da cui segue che $M_{ab} \supseteq \langle m \rangle$. Preso poi $m' \in M_{ab}$, avremo che

$$\begin{aligned} m' &= cm' + dm' = fm_a + gm_b \\ &= fcm + gdm = (fc + gd)m\,, \end{aligned}$$

per qualche $f, g \in A$.

Soluzione E. *156* Per ipotesi $M \simeq A/(d)$, con $d \notin A^* \cup \{0\}$. Osserviamo che M coincide con la sua d-componente M_d. Sia dunque $d = \prod_{j=1}^{h} p_i^{e_i}$ la decomposizione di d in fattori irriducibili, ognuno contato con la sua molteplicità. Allora, per **E.** 155, $M = M_d = \oplus_{i=1}^{h} M_{p_i^{e_i}} = \oplus_{i=1}^{h} M_{p_i}$ e dato che M_{p_i} è ciclico e p_i-primario, per ottenere la conclusione basta porre $M_i = M_{p_i^{e_i}}$ per ogni i.

Soluzione E. *157* 1. Siano $\{m_\alpha : \alpha \in \Lambda\}$ una base di M, $0 \neq m = \sum_{\alpha\in\Lambda} a_\alpha m_\alpha \in M$ e $a \in A$ tali che $am = 0$; allora $\sum_{\alpha\in\Lambda} aa_\alpha m_\alpha = 0$, che implica $aa_\alpha = 0$ per ogni α. Dato che almeno un a_α è non nullo e A è un dominio, deve essere $a = 0$. Abbiamo perciò mostrato che in M non ci sono elementi di torsione non banali.

2. Segue immediatamente da **T.**118.2.

3. Consideriamo $A = K[x, y]$, con K campo, che è UFD ma non PID; l'ideale $I = (x, y)$ è finitamente generato e libero da torsione ma non libero.

Consideriamo poi $\mathbb{Q}$ che è uno $\mathbb{Z}$-modulo non finitamente generato e senza torsione; $\mathbb{Q}$ non è libero, perché ogni coppia di elementi di $\mathbb{Q}$ è linearmente dipendente su $\mathbb{Z}$.

Soluzione E. *158* Chiaramente $M \simeq \operatorname{Coker} f$; calcoliamo quindi la forma di Smith della matrice $\begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & -3 \\ 1 & 3 & 1 \end{pmatrix}$, che risulta $\begin{pmatrix} 1&0&0 \\ 0&2&0 \\ 0&0&4 \\ 0&0&0 \end{pmatrix}$; da questa deduciamo che $M \simeq \mathbb{Z} \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(4)$.

Soluzione E. *159* La forma di Smith della matrice associata a φ rispetto alle basi canoniche è

$$\begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&x&0 \\ 0&0&0&x^2(x-1) \end{pmatrix};$$

da ciò segue che $\operatorname{Coker}\varphi \simeq 0 \oplus 0 \oplus \mathbb{Q}[x]/(x) \oplus \mathbb{Q}[x]/(x^2) \oplus \mathbb{Q}[x]/(x-1)$, ove l'ultimo isomorfismo è dovuto al fatto che gli ideali (x^2) e $(x-1)$ sono comassimali. Pertanto, $\operatorname{Coker}\varphi \simeq \mathbb{Q} \oplus \langle 1, x\rangle_{\mathbb{Q}} \oplus \mathbb{Q}$ e $\dim_{\mathbb{Q}} \operatorname{Coker}\varphi = 4$.

Alternativamente, se d_1, d_2, d_3, d_4 sono i fattori invarianti nella forma di Smith della matrice M che rappresenta φ, si ha che $\operatorname{Coker}\varphi \simeq \bigoplus_{i=1}^{4} \mathbb{Q}[x]/(d_i)$; da ciò si desume che $\dim_{\mathbb{C}} \operatorname{Coker}\varphi = \sum \deg d_i = \deg(d_1 \cdots d_4) = 4$.

Soluzione E. *160* La matrice che rappresenta φ rispetto alle basi canoniche è $\begin{pmatrix} 6 & 2 & 4 \\ 0 & a & 4 \\ 2 & 2 & 2 \end{pmatrix}$. Dopo eventuali semplificazioni, calcolando gli ideali Δ_i dei determinanti dei minori $i \times i$ si ottiene:

- se $a = 2k+1$: $\Delta_1 = (1)$, $\Delta_2 = (2)$ e $\Delta_3 = (4(a-8))$, da cui segue che $d_1 = 1, d_2 = 2, d_3 = 2(a-8)$ e che $\operatorname{Coker}\varphi \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2a-16)$; quindi per ogni a dispari $\operatorname{Coker}\varphi$ è finito.

- se $a = 2k$: $\Delta_1 = (2)$, $\Delta_2 = (4)$ e $\Delta_3 = (4(a-8))$, da cui segue che $d_1 = d_2 = 2, d_3 = a-8$ e che $\operatorname{Coker}\varphi \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(a-8)$. In questo caso $\operatorname{Coker}\varphi$ è finito per ogni valore di $a \neq 8$.

In conclusione $\operatorname{Coker}\varphi$ è infinito solo se $a = 8$.

Soluzione E. *161* Avremo $\Delta_1 = (\gcd(a,b,c))$, $\Delta_2 = (\gcd(a^2, ab, b^2 - ac))$ e $\Delta_3 = (a^3)$.

1. $\operatorname{Coker}\varphi$ ha al più due generatori se e solo se $d_1 = 1$, e ciò accade se e solo se $\Delta_1 = (1)$.

2. $\operatorname{Coker}\varphi$ è ciclico se e solo se $d_1 = d_2 = 1$. Se $\gcd(a,b) = 1$ allora $\gcd(a,b,c) = 1$ e $\gcd(a^2, ab) = a$, e quindi $\Delta_1 = (1)$ e $\Delta_2 = (a, b^2) = (1)$, da cui $d_1 = d_2 = 1$.

Viceversa sia $k = \gcd(a,b)$; allora si ha che $k | \gcd(a^2, ab, b^2 - ac) = d_2 = 1$ e quindi $k = 1$.

Soluzione E. *162* Con alcune operazioni elementari possiamo ridurre la matrice e ottenere $\begin{pmatrix} a & 0 & 0 \\ -3 & 6 & 0 \\ 0 & 3 & 3 \end{pmatrix}$; avremo allora $\Delta_1 = (a,3)$, $\Delta_2 = (3a, 9)$ e $\Delta_3 = (18a)$.

1. Sicuramente affinché $\operatorname{Coker}\varphi$ sia finito si deve avere che $d_1, d_2, d_3 \neq 0$. Dato che $\Delta_1 \supseteq (3) \neq 0$ e $\Delta_2 \supseteq (9) \neq 0$ ciò equivale a $\Delta_3 \neq 0$ e questo accade se e solo se $a \neq 0$.

2. Abbiamo che $d_1 = 1$ se $\gcd(a,3) = 1$ e $d_1 = 3$ altrimenti. In questo ultimo caso, sicuramente $\operatorname{Coker}\varphi$ non è ciclico. Se invece $\gcd(a,3) = 1$ otteniamo

che $\Delta_2 = (3a, 9) = (3(a, 3)) = (3)$ e quindi anche in questo caso Coker φ non è ciclico.

Soluzione E. *163* Studiamo la forma di Smith della matrice A le cui colonne sono i vettori m_1, m_2, m_3, ossia $A = \begin{pmatrix} 0 & 3 & 3 \\ a & 3 & -1 \\ b & 0 & 0 \end{pmatrix}$. Abbiamo $\Delta_1 = (1)$, da cui $d_1 = 1$, $\Delta_2 = (b, 3a, 12), \Delta_3 = (12b)$. Quindi M è finito se e solo se $b \neq 0$.

Inoltre, M è ciclico se e solo se $\Delta_2 = (1)$. Dato che $\gcd(b, 3a, 12) = \gcd(b, 3\gcd(a, 4)) = \gcd(b, 3)\gcd(b, \gcd(a, 4))$ dovremo avere che $b \not\equiv 0 \mod 3$, e $\gcd(b, \gcd(a, 4)) = 1$; se a è dispari la condizione è verificata. Altrimenti $\gcd(a, 4) = (2)$ oppure $\gcd(a, 4) = 4$.
In conclusione M è ciclico se e solo se

- $b \not\equiv 0 \mod 3$ e a dispari, oppure
- $b \not\equiv 0 \mod 3$, a pari e b dispari.

Soluzione E. *164* La forma di Smith della matrice le cui colonne sono i vettori m_1, m_2 e m_3 è $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 8 \end{pmatrix}$.
Pertanto risulta $M \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(4) \oplus \mathbb{Z}/(8)$, e quindi $\operatorname{Ann} M = (8) \subset \mathbb{Z}$.

Soluzione E. *165* Dato che $\det A = 28$ le forme di Smith di A hanno sulla diagonale $1, 1, 28$ oppure $1, 2, 14$; analogamente, da $\det B = 7$, deduciamo che la forma di Smith di B è individuata dai valori diagonali $1, 1, 7$.
Analogamente, dal momento che il $\det D = \det A \det B = 196$ le possibili forme di Smith per D sono le seguenti. Le scriviamo insieme alle matrici A e C con le quali le realizziamo, con $B = \operatorname{diag}(1, 1, 7)$.

- $D_1 = \operatorname{diag}(1, 1, 1, 1, 1, 196)$, con $A = \operatorname{diag}(1, 1, 28)$, $C = \operatorname{diag}(0, 0, 1)$;
- $D_2 = \operatorname{diag}(1, 1, 1, 1, 7, 28)$, con $A = \operatorname{diag}(1, 1, 28)$, $C = 0$;
- $D_3 = \operatorname{diag}(1, 1, 1, 1, 2, 98)$, con $A = \operatorname{diag}(1, 2, 14)$, $C = \operatorname{diag}(0, 0, 2)$;
- $D_4 = \operatorname{diag}(1, 1, 1, 1, 14, 14)$, con $A = \operatorname{diag}(1, 2, 14)$, $C = 0$.

Soluzione E. *166* La matrice delle relazioni tra gli elementi di M è data da $\begin{pmatrix} 3 & 2 & 1 \\ 0 & -2 & 4 \\ 1 & 1 & 2 \end{pmatrix}$, che ha forma di Smith $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 14 \end{pmatrix}$. Quindi $M \simeq \mathbb{Z}/(14)$ e i possibili ordini degli elementi di M sono $1, 2, 7$ e 14.

Soluzione E. *167* Dato che M è uno $\mathbb{Z}$-modulo finitamente generato, segue da **T.**118.2 che $M \simeq \mathbb{Z}^r \oplus T(M)$, con $r \geq 0$ e $T(M)$ di torsione. L'ipotesi implica però che M è tutto di torsione, e dunque $r = 0$. Dal I teorema di struttura **T.**116 segue allora che $M = \oplus_{i=1}^{n} \mathbb{Z}/I_i$, ove $I_i \neq 0$ per ogni i e $I_i = 0 : m_i$, per certi elementi $m_i \in M$, si veda la dimostrazione di **T.**116. Supponiamo che $I_1 = \cdots = I_s = \mathbb{Z}$ e $I_{s+1} \subsetneq \mathbb{Z}$. Se $s = n$, allora $A\mathbb{Z}^n = \mathbb{Z}^n$, quindi A è invertibile con determinante ± 1 e $M = 0$. Se invece $s < n$ allora $(1) \neq I_i \supseteq (p_{m_i})$ per ogni $i = s+1, \ldots, n$. Dato che i p_{m_i} sono primi, essi generano ideali massimali, per cui $I_i = (p_{m_i})$, $i = s+1, \ldots, n$. Inoltre $I_h \subseteq I_k$ per ogni $h \geq k$, pertanto avremo necessariamente che $I_i = I_{s+1} = (p_{m_{s+1}})$ per ogni $i = s+1, \ldots, r$. Sia allora $p = p_{m_{s+1}}$.

Dimostriamo la seconda affermazione, che chiaramente implica la prima. A questo scopo basta ora osservare che la matrice A ha determinante associato a quello della sua forma di Smith D e che, per quanto discusso sopra, $\det D = p^{n-s} \neq 0$, con $n - s \leq n$.

Soluzione E. *168* Ricordiamo che $K[x, y]$ è un $K[x]$-modulo per restrizione di scalari tramite l'omomorfismo di immersione $K[x] \longrightarrow K[x, y]$. Questa struttura ne induce una naturale su A, che ne è quoziente.

Sia $g = y^3 - xy^2 - y + x$.

1. Si osserva che A è generato come $K[x]$-modulo da $\overline{1}, \overline{y}, \overline{y}^2$.

Se scriviamo un generico elemento $f(x, y)$ di $K[x, y] \simeq K[x][y]$ come $f(x, y) = p_0(x) + p_1(x)y + p_2(x)y^2 + p_3(x)y^3 + \ldots$, usando la relazione $\overline{g} = 0$ in A possiamo scrivere $\overline{f} = \sum_{i=0}^{2} p_i'(x)\overline{y}^i$, per certi $p_i' \in K[x]$ e ciò mostra l'affermazione.

Alternativamente possiamo argomentare dicendo che, dato che g è monico in y, effettuando la divisione di un generico polinomio f per g, otteniamo $f = qg + r$, con $\deg_y r < 3$. Pertanto, in A avremo che $\overline{f} = \overline{r} \in \langle 1, \overline{y}, \overline{y^2} \rangle_{K[x]}$.

2. Da ora in poi per semplificare le notazioni omettiamo le barre per le classi di equivalenza. Siano $B = K[x,y]/(g)$ e $h = x^2 - xy + x - y$; allora si ha che $A \simeq B/(h)$ e che B è un $K[x]$-modulo libero con base $\{1, y, y^2\}$. Sia $f\colon K[x]^3 \longrightarrow B$ l'omomorfismo di $K[x]$-moduli definito da $f(e_1) = h$, $f(e_2) = yh$ e $f(e_3) = y^2h$; allora $\operatorname{Im} f = \langle h, yh, y^2h\rangle_B$, quindi $\operatorname{Im} f \subseteq (h)$. D'altra parte se $s \in (h)$, allora $s = p(x,y)h$ per un certo $p(x,y) \in B$; dunque $p(x,y) = a_0(x) + a_1(x)y + a_2(x)y^2$ e di conseguenza $s \in \operatorname{Im} f$. Da questo deduciamo che $A \simeq B/(h) = \operatorname{Coker} f$.
La matrice che rappresenta f rispetto alla base $\{1, y, y^2\}$ è data da

$$\begin{pmatrix} x^2+x & 0 & x^2+x \\ -x-1 & x^2+x & -x-1 \\ 0 & -x-1 & 0 \end{pmatrix}.$$

Calcoliamo $\Delta_1 = (x+1)$, $\Delta_2 = (x+1)^2$ e $\Delta_3 = (0)$; possiamo concludere dunque che $d_1 = d_2 = x+1$, $d_3 = 0$ e di conseguenza $A \simeq K^2 \oplus K[x]$.

Soluzione E. *169* Consideriamo $\varphi\colon \mathbb{Z}^3 \longrightarrow M$ data da $\varphi(e_i) = m_i$, $i = 1,2,3$; allora $M \simeq \mathbb{Z}^3/\operatorname{Ker}\varphi$. Sia $\begin{pmatrix} 2 & 10 & 6 \\ -4 & -6 & -12 \\ -2 & 4 & a \end{pmatrix}$ la matrice delle relazioni tra i generatori di M; riducendola con alcune operazioni elementari di riga e di colonna consentite, cf. Osservazione 4.10, otteniamo la matrice $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 14 & 0 \\ 0 & 0 & 6+a \end{pmatrix}$.
Da questa deduciamo la forma di Smith associata e la rappresentazione di M come somma diretta di moduli ciclici, al variare di $a \in \mathbb{Z}$:

$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 14 & 0 \\ 0 & 0 & 6+a \end{pmatrix}$ $a \equiv 8 \mod 14$ $M \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(14) \oplus \mathbb{Z}/(a+6)$	$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 7(6+a) \end{pmatrix}$ $a \equiv 0 \mod 2$ $a \not\equiv 1 \mod 7$ $M \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/7(a+6)$
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 14 & 0 \\ 0 & 0 & 2(6+a) \end{pmatrix}$ $a \equiv 1 \mod 2$ $a \equiv 1 \mod 7$ $M \simeq \mathbb{Z}/(14) \oplus \mathbb{Z}/2(a+6)$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 14(6+a) \end{pmatrix}$ $a \equiv 1 \mod 2$ $a \not\equiv 1 \mod 7$ $M \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/14(a+6).$

L'unico caso in cui $\operatorname{Ann} M = 0$ si ha per $a = -6$.

Soluzione E. *170* G_1 e $G_2(\alpha)$ sono gruppi abeliani finitamente generati, quindi rappresentabili come somma diretta di gruppi ciclici, e sono isomorfi se e solo se tale rappresentazione è la stessa per entrambi. Consideriamo la matrice

$$A = \begin{pmatrix} 2 & 0 & -4 & 6 & 12 \\ 2 & -2 & 4 & 4 & 4 \\ 1 & 1 & -3 & 1 & 1 \\ 3 & 3 & -15 & 9 & 21 \end{pmatrix};$$

abbiamo allora che $G_1 \simeq \operatorname{Coker} \psi$, ove $\psi \colon \mathbb{Z}^5 \longrightarrow \mathbb{Z}^4$ è l'omomorfismo associato ad A rispetto alle basi canoniche. Calcolando la forma di Smith di A si ottiene la matrice

$$\begin{pmatrix} 1&0&0&0&0\\ 0&2&0&0&0\\ 0&0&6&0&0\\ 0&0&0&0&0 \end{pmatrix},$$

da cui discende che $G_1 \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/6 \oplus \mathbb{Z}$.
Calcoliamo ora la forma di Smith associata alla matrice

$$B = \begin{pmatrix} 2 & \alpha & -2\\ 8 & 6 & -2\\ -4 & \alpha & 4 \end{pmatrix},$$

che rappresenta φ_α e dunque $G_2(\alpha)$. I fattori invarianti di B devono essere $2, 6, 0$. Dato che $\Delta_3(B) = (\det B) = (36\alpha)$, l'unico valore possibile è $\alpha = 0$. Per $\alpha = 0$ si ha anche $\Delta_1(B) = 2$ e $\Delta_2(B) = 12$, da cui segue che $d_1 = 2, d_2 = 6$; pertanto $G_1 \simeq G_2(0)$.

Soluzione E. *171* Una forma di Smith della matrice $A - xI$ è una matrice diagonale $D = \mathrm{diag}(d_1, \ldots, d_6)$, ove $d_1|d_2|\cdots|d_6$ e $d_1 \cdots d_6 = (x-1)^\alpha (x-2)^\beta (x^2+1)$. Dalle condizioni di divisibilità e dal fatto che $\deg(p_A(x)) = 6$, segue che (x^2+1) deve essere un fattore solo di d_6, che $d_1 = d_2 = 1$, che $\alpha + \beta = 4$ e che le molteplicità γ_i di $(x-1)$ come fattore di d_i devono soddisfare le seguenti relazioni

$$\gamma_3 + \gamma_4 + \gamma_5 + \gamma_6 = \alpha \quad \text{e} \quad \gamma_3 \le \gamma_4 \le \gamma_5 \le \gamma_6\,;$$

quindi le possibili 4-uple $(\gamma_3, \gamma_4, \gamma_5, \gamma_6)_\alpha$ sono

$$(0,0,0,0)_0, (0,0,0,1)_1, (0,0,0,2)_2, (0,0,1,1)_2, (0,0,0,3)_3,$$
$$(0,0,1,2)_3, (0,1,1,1)_3, (0,0,0,4)_4, (0,0,1,3)_4, (0,0,2,2)_4,$$
$$(0,1,1,2)_4 \text{ e } (1,1,1,1)_4.$$

Le 4-uple per le molteplicità di $(x-2)$ sono analoghe. Per determinare la forma di Smith dobbiamo considerare tutte le coppie di 4-uple per cui $\alpha + \beta = 4$.
Se $\alpha = 0$ e $\beta = 4$ oppure $\alpha = 4$ e $\beta = 0$, abbiamo 5 possibili forme di Smith, tante quante le 4-uple con ultima coordinata 4.
Se $\alpha = 1$ e $\beta = 3$ oppure $\alpha = 3$ e $\beta = 1$, abbiamo 3 possibili forme di Smith.
Infine se $\alpha = \beta = 2$ abbiamo 4 forme di Smith, esattamente

- $\mathrm{diag}(1,1,1,1,1,(x-1)^2(x-2)^2(x^2+1))$;
- $\mathrm{diag}(1,1,1,1,(x-1),(x-1)(x-2)^2(x^2+1))$;
- $\mathrm{diag}(1,1,1,1,(x-2),(x-1)^2(x-2)(x^2+1))$;
- $\mathrm{diag}(1,1,1,1,(x-1)(x-2),(x-1)(x-2)(x^2+1))$.

Soluzione E. *172* Abbiamo $M \simeq \mathrm{Coker}\,\varphi$, dove $\varphi\colon \mathbb{Z}^3 \longrightarrow \mathbb{Z}^4$ è l'omomorfismo rappresentato dalla matrice

$$\begin{pmatrix} 3 & a & 0 \\ 0 & 3 & b \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}.$$

Per calcolare la forma di Smith di A consideriamo gli ideali $\Delta_1 = (3,a,b) = (1)$, $\Delta_2 = (9,3a,3b,ab)$, $\Delta_3 = (27)$.
Se $(3,ab) = 1$ allora $\Delta_2 = (1)$, $\Delta_3 = (27)$ quindi $M \cong \mathbb{Z} \oplus \mathbb{Z}/(27)$ e $T(M) \cong \mathbb{Z}/(27)$.
Se invece $(3,ab) = 3$ allora, $\Delta_2 = (3)$, $\Delta_3 = (27)$ quindi $M \cong \mathbb{Z}\oplus\mathbb{Z}/(3)\oplus\mathbb{Z}/(9)$ e $T(M) \cong \mathbb{Z}/(3) \oplus \mathbb{Z}/(9)$.

Soluzione E. *173* 1. Consideriamo la matrice $\begin{pmatrix} 2 & 2 & 0 \\ 2 & a & 4 \\ a & 0 & 2 \end{pmatrix}$ e calcoliamo $\Delta_1 = (\gcd(2,a))$, $\Delta_2 = (\gcd(4,2a,a^2))$ e $\Delta_3 = (4(2-3a))$. Otteniamo allora due casi:

i) se $\gcd(2,a) = 1$, la forma di Smith è $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4(2-3a) \end{pmatrix}$, quindi $M \simeq \mathbb{Z}/(4(2-3a))$;

ii) se $\gcd(2,a) \neq 1$, la forma di Smith è $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & (2-3a) \end{pmatrix}$, quindi $M \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2-3a)$.

2. Affinché esista $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(7), M)$ non nullo, in entrambi i casi, per **E.**126 ed **E.** 128.3, si deve avere $2-3a \equiv 0 \mod 7$, cioè $a \equiv 3 \mod 7$.

Soluzione E. *174* Si ha $M \simeq \operatorname{Coker} f$, dove l'omomorfismo $f : \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ è associato alla matrice $\begin{pmatrix} 2 & 1 & 1 \\ -1 & -3 & 1 \\ 0 & 0 & -a \end{pmatrix}$, la cui forma di Smith è $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5a \end{pmatrix}$. Da ciò segue che $M \simeq \mathbb{Z}/(5a)$.

1. Se $a = 3$ possiamo definire $\varphi : \mathbb{Z}/(20) \longrightarrow \mathbb{Z}/(15)$ ponendo $\varphi(n) = 3n$.
2. Si ha che $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(20), M) \simeq \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(20), \mathbb{Z}/(5a)) \simeq ((5a) : (20))/(5a)$. Pertanto, se $a = 0$ allora $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(20), \mathbb{Z}) = 0$; altrimenti $a \neq 0$ e

$$\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(20), M) \simeq \begin{cases} \mathbb{Z}/(5) & \text{se } \gcd(a,4) = 1; \\ \mathbb{Z}/(10) & \text{se } \gcd(a,4) = 2; \\ \mathbb{Z}/(20) & \text{se } \gcd(a,4) = 4. \end{cases}$$

Soluzione E. *175* Sia $\varphi\colon \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ l'omomorfismo definito da $\varphi(e_i) = m_i$, con $i = 1, 2, 3$; allora $M \simeq \mathbb{Z}^3/\operatorname{Ker}\psi \simeq \operatorname{Coker}\varphi$. La matrice che rappresenta φ rispetto alle basi canoniche è $\begin{pmatrix} 2 & 0 & b \\ 4 & a & 4 \\ 6 & 2a & 6 \end{pmatrix}$. Allora $\Delta_1 = (\gcd(2, a, b))$, $\Delta_2 = (\gcd(2a, ab, 4(b-2)))$ e $\Delta_3 = (2a(2-b))$. Per **E.**124, per avere M semplice è necessario e sufficiente che sia $d_1 = d_2 = 1$ e d_3 primo, cioè $\gcd(2, a, b) = 1$, $\gcd(2a, ab, 4(b-2)) = 1$ e $2a(b-2) = \pm 2$. Dunque $a = \pm 1$ e $b = 1$ o 3.

Alternativamente, riducendo con operazioni elementari consentite, cf. Osservazione 4.10, otteniamo $\begin{pmatrix} 2 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & b-2 \end{pmatrix}$; quindi, per **E.**124, M è semplice se e solo se $M \simeq \mathbb{Z}/(2)$ se e solo se $a = \pm 1$ e $b - 2 = \pm 1$.

Soluzione E. *176* Calcoliamo una base di Gröbner G, rispetto all'ordinamento lessicografico con $x > y > z$, di I, e otteniamo $G = \{x + y^3 - yz, y^4 - y^2z + 1\}$.

1. Risulta allora $A \simeq K[z][y]/(y^4 - y^2z + 1)$, che è generato come $K[z]$-modulo da $\langle \overline{1}, \overline{y}, \overline{y}^2, \overline{y}^3 \rangle$.
2. Dato che $\overline{1}, \overline{y}, \overline{y}^2, \overline{y}^3$ sono indipendenti modulo I, essi sono una base e quindi $A \simeq K[z]^4$.

Soluzione E. *177* 1. La base di Gröbner ridotta di I rispetto all'ordinamento lessicografico con $x > y > z$ è data da $\{x^2, xy, yz, z^2\}$ quindi I è monomiale, cf **E.**78.

2. È immediato verificare che $M = \langle 1, x, z, xz \rangle_{K[y]}$.

3. Dato che $yx = 0$ in M, M contiene un elemento di torsione diverso da zero e quindi non è libero.

4. Consideriamo l'omomorfismo $\varphi\colon K[y]^4 \longrightarrow M$ dato da $\varphi(e_1) = 1$, $\varphi(e_2) = x$, $\varphi(e_3) = z$ e $\varphi(e_4) = xz$. Supponiamo che $(a_1, a_2, a_3, a_4) \in \operatorname{Ker}\varphi$: allora $0 = \varphi(a_1, a_2, a_3, a_4) = a_1(y) + a_2(y)x + a_3(y)z + a_4(y)xz$ e dunque $a_1(y) + a_2(y)x + a_3(y)z + a_4(y)xz \in I$. Dato che I è monomiale segue allora che $a_1 = 0$, $a_2 = ya_2'$, $a_3 = ya_3'$ e $a_4 = ya_4'$. Pertanto otteniamo che

$$\operatorname{Ker}\varphi = \{(0, yb_2, yb_3, yb_4)\colon b_2, b_3, b_4 \in K[y]\}$$

è libero con base $\{v_1 = (0, y, 0, 0), v_2 = (0, 0, y, 0), v_3 = (0, 0, 0, y)\}$. Chiamati f_1, f_2, f_3 i vettori della base canonica di $K[y]^3$, definendo $\psi\colon K[y]^3 \longrightarrow K[y]^4$ tramite l'assegnazione $f_i \mapsto v_i$, con $i = 1, 2, 3$, otteniamo che $M \simeq \operatorname{Coker}\psi$. Inoltre, la forma di Smith associata alla matrice che rappresenta ψ è $\begin{pmatrix} y & 0 & 0 \\ 0 & y & 0 \\ 0 & 0 & y \\ 0 & 0 & 0 \end{pmatrix}$; da ciò segue che $M \simeq K^3 \oplus K[y]$.

Soluzione E. *178* Sia B l'anello $K[x, y]/(x^2 - y^2)$.

1. Gli anelli A e B sono isomorfi e una loro base come $K[x]$-modulo è dunque data da $\{\,\overline{1}\,,\, \overline{y}\,\}$; è chiaro che si tratta di un insieme di generatori. Inoltre, $\overline{1}$ e $\overline{y}$ sono liberi da relazioni; infatti, se esistessero $f(x), g(x) \in K[x]$ tali che $f(x)\overline{1} + g(x)\overline{y} = 0$, avremmo che $f(x) + g(x)y \in (x^2 - y^2)$, cioè $f(x) + g(x)y = (x^2 - y^2)q(x, y)$ per qualche polinomio $q(x, y) \in K[x, y]$. Il grado in y del polinomio a sinistra è al più 1 mentre in quello a destra è almeno 2: questo è possibile solo se $q(x, y) = 0$. Dunque $f(x) + g(x)y = 0$ e infine $f(x) = g(x) = 0$. Pertanto, come $K[x]$-modulo, A è isomorfo a $K[x]^2$.

2. In questo caso $A \simeq K[x, y, y^{-1}]/(y^2 - y^{-1} + x^2)$. In A vale che $\overline{y}^{-1} = \overline{y}^2 + \overline{x}^2$, ovvero che $\overline{1} = \overline{y}^3 + \overline{y}\overline{x}^2$ e pertanto gli elementi $\overline{1}, \overline{y}, \overline{y}^2$ generano A come $K[x]$-modulo.

Questo è un insieme di generatori libero da relazioni e dunque come $K[x]$-modulo A è isomorfo a $K[x]^3$. Infatti, se $f(x), g(x), h(x) \in K[x]$ sono tali che $f(x) + g(x)y + h(x)y^2 = 0$, allora $f(x) + g(x)y + h(x)y^2 = (y^2 - y^{-1} + x^2)q(x, y, y^{-1})$, e pertanto

$$yf(x) + y^2g(x) + y^3h(x) = (y^3 - 1 + x^2y)q(x, y, y^{-1}).$$

Dato che nel membro di sinistra y^{-1} non compare, non può comparire neanche a destra, e pertanto possiamo scrivere $q(x, y, y^{-1}) = q(x, y)$. Inoltre il grado in y nel membro di sinistra è al più 3. Se $\deg_y q(x, y) \geq 1$ allora il grado in y a destra sarebbe almeno 4, quindi y non compare in $q(x, y)$ e possiamo scrivere $q(x, y) = q(x)$. Ne segue che $yf(x) + y^2g(x) + y^3h(x) = (y^3 - 1 + x^2y)q(x)$ e pertanto $h = q$, $f = x^2q$, $g = 0$; infine $0 = q$ e quindi $f = g = h = 0$, come volevamo.

3. L'anello $A \simeq B/(a)$ è il quoziente dell'anello B definito sopra modulo l'ideale generato dall'elemento $a = \overline{x}^4 - \overline{x}^3\overline{y} + \overline{y}$. Dato che, come visto al punto 1, B è un $K[x]$-modulo libero generato da $\overline{1}, \overline{y}$, un generico elemento di (a) si può scrivere come $ap(x, y) = ap_0(x) + ap_1(x)\overline{y}$, e dunque (a), come $K[x]$-modulo, è generato da $a = \overline{x}^4 - \overline{x}^3\overline{y} + \overline{y} = x^4\overline{1} + (1 - x^3)\overline{y}$ e da $a\overline{y} = (-x^5 + x^2)\overline{1} + x^4\overline{y}$. Pertanto A è il conucleo dell'omomorfismo di $K[x]$-moduli $\varphi\colon K[x]^2 \longrightarrow K[x]^2$, definito da $\varphi(e_1) = x^4e_1 + (1 - x^3)e_2$ $\varphi(e_2) = (-x^5 + x^2)e_1 + x^4e_2$, la cui matrice associata è $\begin{pmatrix} x^4 & -x^5 + x^2 \\ 1 - x^3 & x^4 \end{pmatrix}$. Dato che $\Delta_1 = (1)$ e $\Delta_2 = (2x^5 - x^2)$, avremo che $A \simeq K[x]/(2x^5 - x^2)$ è ciclico.

Usando la teoria delle basi di Gröbner possiamo in alcuni casi semplificare lo svolgimento dell'esercizio. Ad esempio, in 3, una base di Gröbner dell'ideale $(x^2 - y^2, x^4 - x^3y + y)$ rispetto all'ordinamento lessicografico con $y > x$ è $\{y + 2x^4, 2x^5 - x^2\}$; pertanto si ha subito che $A \simeq K[x]/(2x^5 - x^2)$.

16.5 Soluzioni del capitolo 12

Soluzione E. *179* È immediato verificare che $\mathrm{Bil}(M, N; P)$ è un gruppo abeliano rispetto a $+$ che ha come elemento neutro la mappa identicamente nulla. Per quanto riguarda il prodotto esterno: $1_A f = f$ è ovvia, mentre per

ogni $a, b \in A$ e $f, g \in \mathrm{Bil}(M, N; P)$, le uguaglianze $(a+b)f = af + bf$, $a(f+g) = af + ag$ e $(ab)f = a(bf)$ seguono dal fatto che P è un A-modulo. Infatti, per ogni $m \in M$ e $n \in N$, si ha

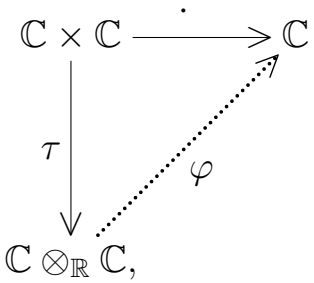
$$((a+b)f)(m,n) = (a+b)f(m,n) = af(m,n) + bf(m,n) = (af+bf)(m,n)\,,$$

$$\begin{aligned}(a(f+g))(m,n) &= a((f+g)(m,n)) = a(f(m,n) + g(m,n)) \\ &= af(m,n) + ag(m,n) = (af+ag)(m,n)\,,\end{aligned}$$

$$((ab)f)(m,n) = (ab)f(m,n) = a(bf(m,n)) = a(bf)(m,n) = (a(bf))(m,n)\,.$$

Soluzione E. *180* Per ipotesi, esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha a + \beta b = 1$. Allora, per ogni tensore elementare $\overline{h} \otimes \overline{k}$ si ha $\overline{h} \otimes \overline{k} = 1(\overline{h} \otimes \overline{k}) = (\alpha a + \beta b)(\overline{h} \otimes \overline{k}) = \alpha a h(\overline{1} \otimes \overline{k}) + \beta b k(\overline{h} \otimes \overline{1})$. Dato che $a(\overline{1} \otimes \overline{k}) = \overline{a} \otimes \overline{k} = 0$ e analogamente, $b(\overline{h} \otimes \overline{1}) = 0$, possiamo concludere che ogni tensore elementare è nullo e la conclusione segue ora da **T.**126.2.

Soluzione E. *181* No, perché come visto in 3 dello stesso esempio in questo caso non tutti gli elementi del prodotto tensore sono tensori elementari. Considerando il diagramma



avremo che, per ogni tensore elementare $x \otimes_{\mathbb{R}} y$, $0 = \varphi(x \otimes y) = xy$ implica che $x = 0$ oppure $y = 0$ e pertanto φ è iniettiva sui tensori elementari. Non è però iniettiva: infatti

$$\varphi(1 \otimes i - i \otimes 1) = i - i = 0.$$

Risulta invece $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C}^2$, cf. **T.**127.6.

Soluzione E. *182* Siano $\{e_i\}_{i \in I}$ e $\{e'_j\}_{j \in J}$ basi di M ed N rispettivamente. Sappiamo già che $\{e_i \otimes e'_j \colon i \in I,\ j \in J\}$ è un insieme di generatori di $M \otimes N$, cf. **T.**126.4. Vogliamo dunque provare che tale insieme è libero. Supponiamo

di avere una combinazione lineare finita $\sum_{i\in I_0, j\in J_0} c_{ij}(e_i \otimes e'_j) = 0$; vogliamo mostrare che i coefficienti c_{ij} sono tutti nulli. Fissiamo una qualunque coppia di indici i_0 e j_0, e proviamo che il coefficiente corrispondente $c_{i_0 j_0}$ è 0. Dati $m = \sum_i a_i e_i$ e $n = \sum_j b_j e'_j$, definiamo la mappa A-bilineare $f(m,n) = a_{i_0} b_{j_0}$ e consideriamo il diagramma

$$\begin{array}{ccc} M \times N & \xrightarrow{f} & A \\ {\scriptstyle\tau}\downarrow & \nearrow_{\tilde f} & \\ M \otimes N. & & \end{array}$$

Il diagramma è commutativo e dunque $\tilde f(m \otimes n) = a_{i_0} b_{j_0}$, per ogni tensore elementare $m \otimes n$. In particolare avremo anche $\tilde f(e_{i_0} \otimes e'_{j_0}) = 1$ e $\tilde f(e_i \otimes e'_j) = 0$ se $(i,j) \neq (i_0, j_0)$. In conclusione avremo $0 = \tilde f(0) = \tilde f(\sum_{i,j} c_{ij}(e_i \otimes e'_j)) = c_{i_0 j_0}$, come volevamo.

Alternativamente, consideriamo i sottomoduli liberi $M_0 \subseteq M$, $N_0 \subseteq N$ finitamente generati da $\{e_i \colon i \in I_0\}$ e $\{e'_j \colon j \in J_0\}$ rispettivamente. Avremo $M_0 \otimes_A N_0 \simeq \bigoplus_{i\in I_0} A \otimes \bigoplus_{j\in J_0} A$, e la conclusione segue da **T.**127.6.

Soluzione E. *183* Da **T.**127.5, discende che $A/I \otimes_A A/J \simeq (A/I)/J(A/I)$, che è $(A/I)/(J + I/I)$ e quindi isomorfo a $A/I + J$ per il secondo teorema di omomorfismo, cf. **T.**87.**II**.

Alternativamente, si può dimostrare la tesi usando la proprietà universale. Costruiamo il diagramma

$$\begin{array}{ccc} A/I \times A/J & \xrightarrow{f} & A\big/_{I+J} \\ {\scriptstyle\tau}\downarrow & \nearrow_{\tilde f} & \\ A/I \otimes A/J, & & \end{array}$$

ove $f(\overline{x}, \overline{y}) = \overline{xy}$: tale f è ben definita e A-bilineare. La bilinearità è immediata, quindi verifichiamo la buona definizione: se $(\overline{x_1}, \overline{y_1}) = (\overline{x_2}, \overline{y_2})$ allora

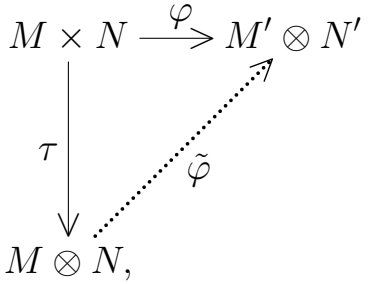
$x_1 - x_2 \in I$, $y_1 - y_2 \in J$ e pertanto $x_1y_1 - x_2y_2 = x_1(y_1 - y_2) + y_2(x_1 - x_2) \in x_1J + y_2I \subseteq I + J$, e dunque $\overline{x_1y_1} = \overline{x_2y_2}$ in $A/I + J$.
Dato che per ogni $\overline{a} \in A/I + J$ si ha $\overline{a} = f(\overline{a}, \overline{1})$, la mappa f è surgettiva e, di conseguenza, lo è anche la mappa indotta $\tilde{f}$ definita da $\tilde{f}(\overline{x} \otimes \overline{y}) = \overline{xy}$.
Per l'iniettività osserviamo che un elemento di $A/I \otimes A/J$ si può scrivere come somma finita

$$\alpha = \sum_{i=1}^{k} \overline{x_i} \otimes \overline{y_i} = \sum_{i=1}^{k} \overline{x_iy_i} \otimes \overline{1} = \overline{\beta} \otimes \overline{1},$$

con $\overline{\beta} = \sum_{i=1}^{k} \overline{x_iy_i} \in A/I$. Allora $\tilde{f}(\overline{\beta} \otimes \overline{1}) = \overline{\beta} = \overline{0}$ implica $\beta \in I + J$. Quindi, se $\beta = x + y$ con $x \in I$ e $y \in J$,

$$\overline{\beta} \otimes \overline{1} = \overline{x + y} \otimes \overline{1} = \overline{y} \otimes \overline{1} = \overline{1} \otimes \overline{y} = \overline{1} \otimes \overline{0} = 0.$$

Soluzione E. *184* Costruiamo il diagramma



ove $\varphi(m, n) = f(m) \otimes g(n)$ è A-bilineare. Allora, per la proprietà universale, $\tilde{\varphi}$ è ben definito e, per la commutatività del diagramma, $\tilde{\varphi} = f \otimes g$.

Soluzione E. *185* Per ogni tensore elementare $m \otimes n$ avremo

$$\begin{aligned}\big((f' \circ f) \otimes (g' \circ g)\big)(m \otimes n) &= (f' \circ f)(m) \otimes (g' \circ g)(n) \\ &= f'(f(m)) \otimes g'(g(n)) \\ &= (f' \otimes g')(f(m) \otimes g(m)) \\ &= (f' \otimes g')((f \otimes g)(m \otimes n)) \\ &= \big((f' \otimes g') \circ (f \otimes g)\big)(m \otimes n),\end{aligned}$$

come volevamo.

Soluzione E. *186* 1. Basta controllare che tutti i tensori elementari $q \otimes_{\mathbb{Z}} \overline{a}$ siano nulli. Abbiamo $q \otimes_{\mathbb{Z}} \overline{a} = \frac{nq}{n} \otimes_{\mathbb{Z}} \overline{a} = \frac{q}{n} \otimes_{\mathbb{Z}} n\overline{a} = \frac{q}{n} \otimes_{\mathbb{Z}} 0 = 0$.

2. Consideriamo la famiglia di $\mathbb{Z}$-moduli $\{\mathbb{Z}/(n) \colon n \in \mathbb{N}_+\}$ e sia $N = \mathbb{Q}$. Allora $\mathbb{Z}/(n) \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ per ogni $n \in \mathbb{N}_+$ per il punto 1, quindi $\prod_{n\in\mathbb{N}_+} (\mathbb{Z}/(n) \otimes_{\mathbb{Z}} \mathbb{Q}) = 0$. Invece $\big(\prod_{n\in\mathbb{N}_+} \mathbb{Z}/(n)\big) \otimes_{\mathbb{Z}} \mathbb{Q} \neq 0$; infatti consideriamo il sottomodulo ciclico generato da $m = (1_{\mathbb{Z}/(n)})_{n\in\mathbb{N}_+} \in \prod_{n\in\mathbb{N}_+} \mathbb{Z}/(n)$. Abbiamo l'inclusione

$$0 \longrightarrow \langle m \rangle_{\mathbb{Z}} \longrightarrow \prod_{n\in\mathbb{N}_+} \mathbb{Z}/(n)$$

e, tensorizzando con $\mathbb{Q}$ che è uno $\mathbb{Z}$-modulo piatto, cf. **T.**142 e **T.**144, si ottiene l'inclusione

$$\begin{array}{ccccc} 0 & \longrightarrow & \langle m \rangle_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q} & \longrightarrow & \big(\prod_{n\in\mathbb{N}_+} \mathbb{Z}/(n)\big) \otimes_{\mathbb{Z}} \mathbb{Q} \\ & & \downarrow \simeq & & \\ & & \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \neq 0. & & \end{array}$$

Soluzione E. *187* 1. Se N_1 e N_2 sono proiettivi allora esistono A-moduli M_1, M_2 e A-moduli liberi F_1, F_2 tali che $F_1 = M_1 \oplus N_1$ e $F_2 = M_2 \oplus N_2$, cf. **T.**106. Quindi $(M_1 \oplus M_2) \oplus (N_1 \oplus N_2) = (M_1 \oplus N_1) \oplus (M_2 \oplus N_2) = F_1 \oplus F_2$, e $N_1 \oplus N_2$ è addendo diretto di un modulo libero.

Viceversa, se $N_1 \oplus N_2$ è proiettivo esistono F libero e M tali che $F = (N_1 \oplus N_2) \oplus M = (M \oplus N_1) \oplus N_2 = (M \oplus N_2) \oplus N_1$ e quindi N_1 e N_2 sono proiettivi.

2. Siano N_1 e N_2 proiettivi; allora con le stesse notazioni del punto precedente, per **T.**127.3, avremo

$$\begin{aligned} F_1 \otimes F_2 &= (N_1 \oplus M_1) \otimes (N_2 \oplus M_2) \\ &= (N_1 \otimes N_2) \oplus (N_1 \otimes M_2) \oplus (M_1 \otimes N_2) \oplus (M_1 \otimes M_2), \end{aligned}$$

ove $F_1 \otimes F_2$ è libero grazie a **T.**127.6.

3. Considerando $\mathbb{Z}/(n)$ come $\mathbb{Z}$-modulo si ha, per esempio, $\mathbb{Z}/(2) \otimes \mathbb{Z}/(3) = 0$, per **E.**183; 0 è proiettivo ma né $\mathbb{Z}/(2)$ né $\mathbb{Z}/(3)$ lo sono, poiché nessuno dei due evidentemente è addendo diretto di qualche $\mathbb{Z}^n$.

4. Dato che il prodotto tensore è esatto a destra, cf. **T.**129, basta controllare che cosa succede tensorizzando le applicazioni iniettive. Siano dunque $f : M \longrightarrow N$ un omomorfismo iniettivo, $\mathrm{i}_1 = \mathrm{id}_{N_1}$ e $\mathrm{i}_2 = \mathrm{id}_{N_2}$; consideriamo il seguente diagramma

$$\begin{array}{ccc} M \otimes (N_1 \oplus N_2) & \xrightarrow{f \otimes (\mathrm{i}_1, \mathrm{i}_2)} & N \otimes (N_1 \oplus N_2) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ (M \otimes N_1) \oplus (M \otimes N_2) & \xrightarrow{(f \otimes \mathrm{i}_1, f \otimes \mathrm{i}_2)} & (N \otimes N_1) \oplus (N \otimes N_2), \end{array}$$

ove α e β sono isomorfismi per **T.**127.4. Quindi $f \otimes (\mathrm{i}_1, \mathrm{i}_2)$ è iniettiva se e solo se $f \otimes \mathrm{i}_1$ e $f \otimes \mathrm{i}_2$ sono iniettive.

5. Siano $f\colon M \longrightarrow N$ un omomorfismo iniettivo e i_1, i_2 come sopra; allora $M \otimes N_1 \xrightarrow{f \otimes \mathrm{i}_1} N \otimes N_1$ è iniettivo e quindi è iniettivo anche

$$(M \otimes N_1) \otimes N_2 \xrightarrow{(f \otimes \mathrm{i}_1) \otimes \mathrm{i}_2} (N \otimes N_1) \otimes N_2,$$

dove, chiaramente, $(f \otimes \mathrm{i}_1) \otimes \mathrm{i}_2 = f \otimes (\mathrm{i}_1 \otimes \mathrm{i}_2)$.

6. Si consideri nuovamente $\mathbb{Z}/(2) \otimes \mathbb{Z}/(3) = 0$; 0 è piatto, e né $\mathbb{Z}/(2)$ né $\mathbb{Z}/(3)$ lo sono.

Soluzione E. *188* Osserviamo che il campo residuo $K = A/\mathfrak{m}$ è un (A, K)-bimodulo. Per definizione $\mu(M) = \dim_K(M/\mathfrak{m}M) = \dim_K(M \otimes_A K)$, cf. **T.**97; calcoliamo dunque $\mu(M \otimes_A N) = \dim_K((M \otimes_A N) \otimes_A K)$. Utilizzando le proprietà di calcolo del prodotto tensoriale e **T.**131 avremo che

$$\begin{aligned} (M \otimes_A N) \otimes_A K &\simeq M \otimes_A (N \otimes_A K) \simeq M \otimes_A (K \otimes_A N) \\ &\simeq M \otimes_A ((K \otimes_K K) \otimes_A N) \simeq M \otimes_A (K \otimes_K (K \otimes_A N)) \\ &\simeq (M \otimes_A K) \otimes_K (N \otimes_A K) \simeq K^{\mu(M)} \otimes_K K^{\mu(N)} \\ &\simeq K^{\mu(M)\mu(N)}, \end{aligned}$$

da cui discende quello che volevamo provare.

Soluzione E. *189* Dall'esercizio precedente segue che $\mu(M) = 0$ oppure $\mu(N) = 0$. Da ciò segue che $M = \mathfrak{m}M$ oppure $N = \mathfrak{m}N$, e la conclusione discende dal lemma di Nakayama.

Soluzione E. *190* La verifica del fatto che M è un $\mathbb{Z}$ modulo è lasciata al lettore.
Osserviamo che l'omomorfismo da $\mathbb{Z}$ in M, definito da $n \longrightarrow \frac{n}{1}$ è iniettivo. È sufficiente provare che ogni tensore elementare è nullo. Siano $\alpha = \frac{a}{p^m}$ e $\beta = \overline{\frac{b}{p^n}}$, con $a, b \in \mathbb{Z}$ e $m, n \in \mathbb{N}$; avremo che

$$\begin{aligned}\alpha \otimes \beta &= \frac{ap^n}{p^{n+m}} \otimes \beta = p^n \frac{a}{p^{n+m}} \otimes \beta \\ &= \frac{a}{p^{n+m}} \otimes p^n\beta = \frac{a}{p^{n+m}} \otimes \overline{\frac{bp^n}{p^n}} \\ &= \frac{a}{p^{n+m}} \otimes \overline{b} = \frac{a}{p^{n+m}} \otimes 0 = 0.\end{aligned}$$

Soluzione E. *191* 1. Da **E.**183 discende che $\mathbb{Q}[x]/(x) \otimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/(x^2+1) \simeq \mathbb{Q}[x]/(x, x^2+1) = 0$; quindi la dimensione è zero.
2. Abbiamo che $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[x]/(x^5-3)$, e quindi $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}[\alpha] \simeq \mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}[x]/(x^5-3)$. Inoltre, da **T.**128.5, $\mathbb{C} \simeq \mathbb{C}[x]/(x) \simeq \mathbb{C}[x] \otimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/(x)$. Pertanto, dato che $\mathbb{Q}[x]/(x)$ è un $(\mathbb{Q}[x], \mathbb{Q})$-bimodulo, si ha

$$\begin{aligned}\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}[x]/(x^5-3) &\simeq \big(\mathbb{C}[x] \otimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/(x)\big) \otimes_{\mathbb{Q}} \mathbb{Q}[x]/(x^5-3) \\ &\simeq \mathbb{C}[x] \otimes_{\mathbb{Q}[x]} \big(\mathbb{Q}[x]/(x) \otimes_{\mathbb{Q}} \mathbb{Q}[x]/(x^5-3)\big) \\ &\simeq \mathbb{C}[x] \otimes_{\mathbb{Q}[x]} \big(\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}[x]/(x^5-3)\big) \\ &\simeq \mathbb{C}[x] \otimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/(x^5-3) \\ &\simeq \mathbb{C}[x]/(x^5-3) \simeq \mathbb{C}^5.\end{aligned}$$

Alternativamente si può osservare che, come $\mathbb{Q}$-spazio vettoriale, $\mathbb{Q}[\alpha] \simeq \mathbb{Q}^5$; pertanto $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}[\alpha] \simeq \mathbb{C}^5$.

Soluzione E. *192* Siano M un A-modulo proiettivo e $\{m_1, \ldots, m_n\}$ un suo insieme minimale di generatori, che esiste poiché A è locale, cf. **T.**97. Consideriamo l'omomorfismo $\phi\colon A^n \longrightarrow M$, definito da $e_i \mapsto m_i$, ove

$\{e_1, \dots, e_n\}$ è la base canonica di A^n. Avremo allora una sequenza esatta corta $0 \longrightarrow N = \operatorname{Ker} \phi \longrightarrow A^n \longrightarrow M \longrightarrow 0$; visto che per ipotesi M è proiettivo, la sequenza spezza e $A^n \simeq M \oplus N$. Tensorizzando per $A/\mathfrak{m}$ otteniamo che $K^n \simeq M/\mathfrak{m}M \oplus N/\mathfrak{m}N$ come K-spazi vettoriali; dato che per ipotesi $\dim_K M/\mathfrak{m}M = \dim_K K^n = n$, avremo che $N/\mathfrak{m}N = 0$, cioè che $N = \mathfrak{m}N$. Applicando ora il lemma di Nakayama, deduciamo che $N = 0$ e che $M \simeq A^n$ è libero.

Soluzione E. *193* Sia H un qualsiasi ideale di A; tensorizzando la sequenza esatta $0 \longrightarrow H \longrightarrow A \longrightarrow A/H \longrightarrow 0$ con B che è A-piatto, si ottiene il diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H \otimes_A B & \longrightarrow & A \otimes_A B & \longrightarrow & B \otimes_A A/H & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \simeq & & \downarrow \simeq & & \\ 0 & \longrightarrow & HB & \longrightarrow & B & \longrightarrow & B/HB & \longrightarrow & 0. \end{array}$$

Dal lemma del serpente segue che $H \otimes_A B \simeq HB$ per ogni ideale H di A. Tensorizzando con B la sequenza esatta corta di A-moduli

$$0 \longrightarrow I \cap J \longrightarrow I \oplus J \longrightarrow I + J \longrightarrow 0,$$

cf. **E.**144, essa rimane esatta. Otteniamo dunque

$$0 \longrightarrow (I \cap J)B \longrightarrow IB \oplus JB \longrightarrow IB + JB \longrightarrow 0$$

e da questa discende subito la tesi.

Soluzione E. *194* Per $a = 0$ o a invertibile tutte le affermazioni sono ovvie, quindi possiamo supporre $a \neq 0$ e $a \notin A^*$.

$1 \Rightarrow 2$. Proviamo che la successione

$$0 \longrightarrow (a) \xrightarrow{j} A \xrightarrow{\pi} A/(a) \longrightarrow 0$$

spezza, mostrando che esiste $r\colon A \longrightarrow (a)$ tale che $r \circ j = \mathrm{id}_{(a)}$, cf. **T.**102. Dato che $a \in (a^2)$, esiste $c \in A$ tale che $a = ca^2$. Definiamo $r(b) = ca \cdot b$, per ogni $b \in A$. Avremo allora che $r \circ j(a) = ca^2 = a$ da cui segue che $r \circ j = \mathrm{id}_{(a)}$.

$2 \Rightarrow 1$. Se $A \simeq (a) \oplus M$, per qualche A-modulo M, la successione esatta $0 \longrightarrow (a) \longrightarrow A \longrightarrow M \longrightarrow 0$, spezza ed esiste una retrazione $r\colon A \longrightarrow (a)$ determinata da $r(1) = ka$, per qualche $k \in A$. Dato che $r \circ j = \mathrm{id}_{(a)}$, si ha $a = r(j(a)) = ka^2 \in (a^2)$.

$2 \Rightarrow 3$. Dato che A è libero, e dunque piatto, anche i suoi addendi diretti lo sono, per **E.**187.4.

$3 \Rightarrow 1$. Dato che l'omomorfismo di inclusione j di (a) in A è iniettivo e $A/(a)$ è piatto, l'omomorfismo $j \otimes \mathrm{id}_{A/(a)}\colon (a) \otimes A/(a) \longrightarrow A \otimes A/(a)$ è ancora iniettivo; pertanto $(a)/(a^2) \simeq (a) \otimes A/(a) \longrightarrow A/(a)$ è iniettivo, ed è l'omomorfismo nullo. L'unica possibilità è che $(a)/(a^2) = 0$, cioè la tesi.

Soluzione E. *195* 1. Sia $I \neq A$ un ideale; allora esiste $\mathfrak{m}$ massimale tale che $I \subseteq \mathfrak{m}$, quindi $IM \subset \mathfrak{m}M \subsetneq M$ da cui la tesi.

2. Siano $0 \neq n \in N$ e $N_1 = \langle n \rangle \simeq A/\operatorname{Ann} n$. Consideriamo l'omomorfismo di immersione $f\colon N_1 \longrightarrow N$ e tensorizziamo con M; si ottiene che $f \otimes \mathrm{id}_M\colon N_1 \otimes M \longrightarrow N \otimes M$ è un omomorfismo iniettivo, visto che M è piatto. Dato che $N_1 \otimes M \simeq A/\operatorname{Ann} n \otimes M \simeq M/\operatorname{Ann} nM$, basta allora provare che $M/\operatorname{Ann} nM \neq 0$. Ricordando che $\operatorname{Ann} n$ è un ideale proprio poiché $n \neq 0$, la tesi segue ora dal punto 1.

Soluzione E. *196* Dato che a non è un divisore di zero l'omomorfismo di moltiplicazione $\varphi\colon A \xrightarrow{\cdot a} A$ è iniettivo. Tensorizzando con N si ottiene quindi che anche $\bar{\varphi}\colon N \longrightarrow N$, ove $n \mapsto an$ è iniettivo, da cui la tesi.

Soluzione E. *197* 1. Dire che $I,\ J,\ I \cap J = (xy) = IJ$ sono liberi equivale a dire che non esistono elementi $a \neq 0$ tali che ax, ay, axy siano nulli, e ciò è banalmente vero visto che siamo in un dominio.

2. $I + J = (x, y)$ non ha torsione, sempre perché siamo in un dominio.
Consideriamo l'omomorfismo $\phi : I/IJ \oplus J/IJ \longrightarrow K[x, y]/IJ$ definito da $\phi(\overline{f}, \overline{g}) = \overline{f - g}$; è facile vedere che è ben definito e iniettivo. Tensorizzando con $I + J$ e ricordando **T.**127.4, si ottiene un omomorfismo

$$\tilde{\phi} : (I/IJ \otimes (I + J)) \oplus (J/IJ \otimes (I + J)) \longrightarrow (I + J)/IJ,$$

in cui $\tilde{\phi}(\overline{x} \otimes y, \overline{y} \otimes x) = \overline{xy} - \overline{yx} = 0$. Notiamo che se fosse $\overline{x} \otimes y = 0$ allora si avrebbe $I/IJ \otimes J = \langle \overline{x} \otimes y \rangle = 0$, cf. **T.**126.3, ma $I/IJ \otimes J \simeq I/IJ \otimes A \neq 0$. Quindi $\tilde{\phi}$ non è iniettivo e $I + J$ non è piatto.

Soluzione E. *198* Ricordiamo che $\mathrm{Hom}_A(A, M) \simeq M$ per **T.**86. Usando **T.**127 e **E.**126 si ottiene

$$\begin{aligned} \mathrm{Hom}(M, M) \otimes \mathrm{Hom}(N, N) &\simeq \mathrm{Hom}(A^r, A^r) \otimes \mathrm{Hom}(A^s, A^s) \\ &\simeq \mathrm{Hom}(A, A^r)^r \otimes \mathrm{Hom}(A, A^s)^s \\ &\simeq A^{r^2} \otimes A^{s^2} \simeq A^{r^2 s^2}, \end{aligned}$$

che è isomorfo a

$$\begin{aligned} \mathrm{Hom}(A^r \otimes A^s, A^r \otimes A^s) &\simeq \mathrm{Hom}(A^{rs}, A^{rs}) \\ &\simeq \mathrm{Hom}(A, A^{rs})^{rs} \simeq A^{(rs)^2}. \end{aligned}$$

Soluzione E. *199* La matrice associata a φ è $\begin{pmatrix} 4 & 8 \\ 4 & -4 \\ 16 & 20 \end{pmatrix}$ che ha forma di Smith $\begin{pmatrix} 4 & 0 \\ 0 & 12 \\ 0 & 0 \end{pmatrix}$. Dunque $\mathrm{Coker}\,\varphi \simeq \mathbb{Z} \oplus \mathbb{Z}/(4) \oplus \mathbb{Z}/(12)$. Da **T.**127.4 e **E.**183 si ottiene dunque

$$\mathbb{Z}/(15) \otimes_{\mathbb{Z}} (\mathbb{Z}/(4) \oplus \mathbb{Z}/(12)) \simeq \mathbb{Z}/(15, 4) \oplus \mathbb{Z}/(15, 12) \simeq \mathbb{Z}/(3).$$

Soluzione E. *200* La matrice delle relazioni tra gli elementi di M_a è $\begin{pmatrix} 2 & 1 & 1 \\ -1 & 1 & a \\ 0 & 1 & 0 \end{pmatrix}$, che ha forma di Smith $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2a+1 \end{pmatrix}$. Dunque $M_a \simeq \mathbb{Z}/(2a+1)$ e quindi $M_a \otimes \mathbb{Z}/(n) \neq 0$ se e solo se $\gcd(2a+1, n) \neq 1$.

16.6 Soluzioni del capitolo 13

Soluzione E. *201* Sia $a \notin \mathcal{N}(A)$ e consideriamo la localizzazione A_a; questo anello non è banale poiché se fosse $\frac{1}{1} = \frac{0}{1}$, allora avremmo che esiste $n \geq 1$ tale che $a^n = 1a^n = 0$, che è contro l'ipotesi. Esiste quindi un ideale massimale,

e dunque primo, in A_a e per la corrispondenza biunivoca tra gli ideali primi di A e quelli di A_a, deduciamo allora che la sua controimmagine è un ideale primo di A che non contiene a^n per ogni $n \in \mathbb{N}$.

Questa è una dimostrazione alternativa del fatto che $\bigcap_{\mathfrak{p}\in\operatorname{Spec} A} \mathfrak{p} \subseteq \mathcal{N}(A)$, cf. **T.**14.1.

Soluzione E. *202* Se σ_S è un isomorfismo, allora, per ogni $s \in S$, si ha $\sigma_S(s) = \frac{s}{1} \in (S^{-1}A)^* = \sigma_S(A^*)$. Dunque $s \in \sigma_S^{-1}((S^{-1}A)^*) = A^*$ e $S \subseteq A^*$. Viceversa, se $S \subseteq A^*$, allora per la proprietà universale l'omomorfismo identità id_A si fattorizza tramite un omomorfismo ovviamente surgettivo $\varphi\colon S^{-1}A \longrightarrow A$. L'iniettività segue dal fatto che $\varphi\left(\frac{a}{s}\right) = as^{-1} = 0$ implica $a = 0$. Infine osserviamo che $\varphi^{-1} = \sigma_S$.

Soluzione E. *203* Osserviamo innanzitutto che dato che A è finito si ha $A = A^* \sqcup \mathcal{D}(A)$, cf. **T.**1. Dato che f è iniettivo $S \cap \mathcal{D}(A) = \emptyset$ e quindi $S \subseteq A^*$. La conclusione segue dunque da **E.**202.

Soluzione E. *204* 1. Sia $B = \left\{\frac{a}{b} \in \mathbb{Q} : b \not\equiv 0 \mod p\right\}$: è facile verificare che è un sottoanello di $\mathbb{Q}$. Definiamo $f : \mathbb{Z} \longrightarrow B$ tramite $f(a) = \frac{a}{1}$, allora $f(S) \subseteq B^*$ e, per la proprietà universale, otteniamo un omomorfismo $\tilde{f} : S^{-1}\mathbb{Z} \longrightarrow B$ che è ovviamente surgettivo. Per l'iniettività basta osservare che $\tilde{f}\left(\frac{a}{s}\right) = \frac{a}{s} = 0$ se e solo se $a = 0$.

2. Sia $B = \left\{\frac{a}{b} \in \mathbb{Q} : b \not\equiv 0 \mod p_i \text{ per ogni } i\right\}$. Partendo dall'omomorfismo $f : \mathbb{Z} \longrightarrow B$ definito da $f(a) = \frac{a}{1}$ si ottiene un isomorfismo $S^{-1}\mathbb{Z} \simeq B$ esattamente come nel caso precedente.

3. Indichiamo per semplicità notazionale con $n = 0, \ldots, 11$ gli elementi di A. Avremo che $S = \{1, 2, 4, 8\}$ e $\frac{2}{s}, \frac{4}{s}, \frac{8}{s}$ sono elementi invertibili di $S^{-1}A$ per ogni $s \in S$. Inoltre $\frac{0}{s} = \frac{3}{s} = \frac{6}{s} = \frac{9}{s}$, $\frac{1}{s} = \frac{4}{s} = \frac{7}{s} = \frac{10}{s}$ e $\frac{2}{s} = \frac{5}{s} = \frac{8}{s} = \frac{11}{s}$, per ogni $s \in S$. Infine, abbiamo anche che $\frac{1}{2^k} = \frac{2^k}{1}$ per ogni $k = 1, 2, 3$, quindi ogni elemento di $S^{-1}A$ si scrive come $\frac{n}{1}$, per $n = 0, 1, 2$. Pertanto $S^{-1}A$ è un campo di tre elementi ed è dunque isomorfo a $\mathbb{Z}/(3)$.

4. In questo caso $S = \{1, 3, 5, 7, 9, 11\}$ e si verifica facilmente che $\frac{a}{s} = \frac{b}{s}$ se $4|a - b$ e $\frac{a}{s} = \frac{a}{t}$ se $4|s - t$. Dunque è sufficiente considerare numeratori 0,1,2 e 3 e denominatori 1 e 3. Inoltre $\frac{1}{3} = \frac{3}{1}$ e $\frac{2}{3} = \frac{2}{1}$. Quindi $|S^{-1}A| = 4$,

$(S^{-1}A)^* = \left\{\frac{1}{1}, \frac{3}{1}\right\}$ e $\left(\frac{2}{1}\right)$ è l'unico ideale primo e massimale: in conclusione $S^{-1}A \simeq \mathbb{Z}/(4)$.

5. In questo caso $S = \{1, 2, 4, 5, 7, 8, 10, 11\}$ e, analogamente al caso precedente, si osserva che è sufficiente considerare numeratori 0,1 e 2 e denominatori 1 e 2 per descrivere tutti gli elementi di $S^{-1}A$. Inoltre $\frac{1}{2} = \frac{2}{1}$ quindi $S^{-1}A$ è un campo con 3 elementi e dunque $S^{-1}A \simeq \mathbb{Z}/(3)$.

Per provare i punti 3, 4 e 5 si può osservare che l'omomorfismo $\sigma_S \colon A \longrightarrow S^{-1}A$ è surgettivo, cf. **E.**205.1, e semplificare le dimostrazioni usando l'isomorfismo $S^{-1}A \simeq A/\operatorname{Ker}\sigma_S$.

Soluzione E. *205* 1. Sia $\frac{a}{s} \in S^{-1}A$ proviamo che esiste $b \in A$ tale che $\frac{a}{s} = \frac{b}{1}$. Dato che S è un insieme finito, se $s \in S$ esistono $r < k \in \mathbb{N}$ tali che $s^k = s^r$. Allora $s^r(a - as^{k-r}) = 0$; quindi $\frac{a}{s} = \frac{as^{k-r-1}}{1} = \sigma_S(as^{k-r-1})$.

2. Si ha $\operatorname{Ker}\sigma_S = \{a \in A : as = 0 \text{ per qualche } s \in S\} = (3)/(24)$, quindi per il punto precedente $S^{-1}A \simeq A/\operatorname{Ker}\sigma_S \simeq \mathbb{Z}/(3)$.

Soluzione E. *206* 1. Dato che I è un ideale, $0 \in I$, e dunque $1 \in S$. Dati poi due elementi $1 + i$, $1 + j \in S$ avremo che il loro prodotto $(1 + i)(1 + j) \in 1 + I + I + I^2 \subseteq 1 + I = S$; pertanto S è un insieme moltiplicativo.

Dimostriamo che ogni elemento $\frac{x}{s} \in S^{-1}I$ è tale che $1 + \frac{x}{s}\frac{y}{t}$ è invertibile in $S^{-1}A$, per ogni $\frac{y}{t} \in S^{-1}A$: a tal scopo basta osservare che $1 + \frac{x}{s}\frac{y}{t} = \frac{st+xy}{st}$ è invertibile in quanto $st + xy \in 1 + I$.

2. Gli ideali non banali distinti di A sono $(2), (3), (4), (5), (6), (10), (12), (15), (20), (30)$. Abbiamo che $-3 = 1 - 4 \in S$, $5 = 1 + 4 \in S$. Pertanto $-\frac{3}{1}$, $\frac{5}{1}$ e, di conseguenza, $\frac{3}{1}$, $\frac{5}{1}$ e $\frac{15}{1}$ sono invertibili in $S^{-1}A$. Da questo segue che $S^{-1}(2) = S^{-1}(6) = S^{-1}(10) = S^{-1}(30)$ e $S^{-1}(3) = S^{-1}(5) = S^{-1}(15) = (1)$. Inoltre, $\frac{4}{1} = 0$ e quindi si ha anche $(0) = S^{-1}(4) = S^{-1}(12) = S^{-1}(20)$. Quindi in $S^{-1}A$ ci sono solo due ideali propri (0) e $S^{-1}(2)$. Segue dunque che $S^{-1}A$ è locale con ideale massimale generato da $\frac{2}{1}$.

3. Osserviamo che i primi di $T^{-1}A$ sono in corrispondenza biunivoca con i primi di A che non intersecano T; ma $(p) \cap T \neq \emptyset$ se e solo se esiste $a \in (p)$ con $a \equiv 1 \mod m$, cioè se e solo se $(m, p) = 1$. Basta allora prendere m prodotto di almeno due primi divisori di 60 (per esempio $m = 6$ o 15) per ottenere un anello non locale $T^{-1}A$.

Soluzione E. *207* 1. Se $a, b \in I^S$ allora esistono $s, t \in S$ tali che $as, bt \in I$: quindi $(a+b)st \in I$ e, se $c \in A$, allora $cas \in I$, cioè $a+b, ac \in I^S$.

Alternativamente, possiamo osservare che da **T.**138.1 parte c) segue $I^S = I^{ec}$ rispetto a σ_S, per ogni ideale I di A.

2.a) Si ha $\sigma(a) = \frac{a}{1} = 0$ se e solo se esiste $u \in S$ tale che $au = 0$, cioè se e solo se $a \in (0)^S$.

2.b) Segue immediatamente dal fatto che $1 \in S$.

2.c) Sia $a \in I^S$, allora esiste $s \in S$ tale che $as \in I \subset J$ e quindi $a \in J^S$.

2.d) Per la parte b) si ha $I^S \subseteq (I^S)^S$.
Viceversa, se $a \in (I^S)^S$ esiste $s \in S$ tale che $as \in I^S$ e quindi esiste $t \in S$ tale che $ast \in I$, ma $st \in S$ da cui $a \in I^S$.

2.e) Dal punto b) segue che $IJ \subseteq I^S J^S$ e quindi $(IJ)^S \subseteq (I^S J^S)^S$ per il punto d).
Viceversa, sia $a = \sum_i a_i b_i \in I^S J^S$ con $a_i \in I^S$ e $b_i \in J^S$ per ogni i, , allora per ogni i esistono $s_i, t_i \in S$ tali che $s_i a_i \in I$ e $t_i b_i \in J$. Posto $u = \prod_i s_i t_i$, si ha $ua \in IJ$ e quindi $a \in (IJ)^S$, cioè $I^S J^S \subseteq (IJ)^S$. Segue immediatamente che $(I^S J^S)^S \subseteq ((IJ)^S)^S = (IJ)^S$, per il punto precedente.

Soluzione E. *208* La dimostrazione di 1 e 2.a) sono del tutto analoghe a quelle di **E.**207.1 e 2.b-c).

2.b) Dal punto precedente abbiamo che $\sigma_S^{-1}(Q) \subseteq \sigma_S^{-1}(Q)^S$. Supponiamo allora che $q \in \sigma_S^{-1}(Q)^S$; esiste pertanto un $s \in S$ tale che $\frac{sq}{1} = \sigma_S(sq) \in Q$, da cui segue che $\frac{q}{1} \in Q$ e $q \in \sigma_S^{-1}(Q)$.

2.c) Dato che ogni sottomodulo di $S^{-1}M$ è del tipo $S^{-1}N$ per qualche sottomodulo N di M, le affermazioni seguono direttamente dal punto precedente.

2.d) È del tutto analoga alla dimostrazione di **E.**207.2.b).

2.e) Discende immediatamente dal punto c) e da **T.**143.2.

2.f) Segue dal punto c) e dal fatto che $\sigma_S^{-1}(N) + \sigma_S^{-1}(P) \subseteq \sigma_S^{-1}(N+P)$.

Soluzione E. *209* 1. Consideriamo l'omomorfismo $f : A \times B \longrightarrow A$ dato da $f(a,b) = a$. Per ogni $s \in S$, $f(s) = 1$ è invertibile. Inoltre, se $f(a,b) = a = 0$, allora $(1,0)(a,b) = (0,0)$ con $(1,0) \in S$. Infine, per ogni $a \in A$, si

ha $a = f(a,b)f(1,0)^{-1}$; allora, per **T.**136 f si estende ad un isomorfismo $\tilde{f}\colon S^{-1}C \longrightarrow A$.

2. La dimostrazione è del tutto analoga a quella del punto precedente, dove in effetti abbiamo usato solo l'elemento $(1,0) \in S$, che appartiene anche a T.

3. Per ogni $b \in B$ abbiamo che $((1,b),(1,1)) \sim ((1,0),(1,0))$. Tuttavia se $b \neq 0$ si ha $((1,b),(1,1)) \not\sim ((1,0),(1,1))$ e quindi $\sim$ non è transitiva.

Soluzione E. *210* Poniamo $B = A[x]/(1-fx)$. Se f è nilpotente, allora esiste n tale che $f^n = 0$, e quindi $A_f = 0$ e $1 = (1-(fx)^n) = (1-fx)(1+fx+\ldots+(fx)^{n-1}) \in (1-fx)$, che implica che anche $B = 0$.

Sia dunque $f^n \neq 0$ per ogni n; definiamo $\varphi : A \xrightarrow{\mathrm{i}} A[x] \xrightarrow{\pi} B$ ponendo $\varphi(a) = \overline{a}$. Dato che $\overline{f}\overline{x} = \overline{1}$ in B, si ha che $\overline{f^k}$ è invertibile in B per ogni k, quindi φ si fattorizza attraverso A_f ed esiste $\psi : A_f \longrightarrow B$ definito da $\psi\left(\frac{a}{f^k}\right) = \varphi(a)\varphi(f^k)^{-1}$.

Proviamo ora che ψ è un isomorfismo. Basta provare che se $\overline{a} = \varphi(a) = \overline{0}$ allora esiste k tale che $f^k a = 0$ in A, e che per ogni $\overline{b} \in B$ esistono $a \in A$ e k tali che $\overline{b} = \varphi(a)\varphi(f^k)^{-1}$.

Sia $a \in A$ tale che $\overline{a} = \overline{0}$; allora esiste $p(x) = \sum_{i=0}^{h} b_i x^i \in A[x]$ tale che $a = p(x)(1-xf)$, da cui deduciamo che $b_0 = a$, $b_1 = fb_0 = fa, \ldots, b_h = fb_{h-1} = f^h a$, e $fb_h = f^{h+1}a = 0$.

Infine, ogni $\overline{b} \in B$ si scrive come $\overline{b} = \sum_{i=0}^{k} \overline{b_i}\overline{x}^i = \frac{1}{\overline{f^k}}\sum_{i=0}^{k} \overline{b_i\ f^{k-i}}$, e quindi è della forma $\varphi(a)\varphi(f^k)^{-1}$ come volevamo.

Soluzione E. *211* 1. Si ha certamente $\mathbb{Z}\left[\frac{2}{3}\right] \subseteq \mathbb{Z}\left[\frac{1}{3}\right] \simeq \mathbb{Z}_3$. Inoltre, poiché $1 - \frac{2}{3} = \frac{1}{3}$, possiamo scrivere ogni elemento $\frac{1}{3^n}$ come somma finita di potenze di $\frac{2}{3}$ a coefficienti interi e vale anche l'inclusione opposta.

2. Sia $A \subset \mathbb{Q}$, denotiamo con P l'insieme di tutti i primi che appaiono come divisori dei denominatori degli elementi di A ridotti ai minimi termini e sia S il più piccolo sistema moltiplicativo che contiene P. Notiamo che se $p \in P$ allora esiste un elemento ridotto ai minimi termini $a = \frac{m}{ps} \in A$; dunque $\frac{m}{p} = sa \in A$ e inoltre esistono $b, c \in \mathbb{Z}$ tali che $bm + cp = 1$, da cui segue che $\frac{1}{p} = bsa + c \in A$. Questo implica che $S^{-1}\mathbb{Z} \subseteq A$, l'altra inclusione segue direttamente dalla definizione di S.

Soluzione E. *212* Sia S l'insieme moltiplicativo delle potenze di 2. Allora si ha che $A = S^{-1}\mathbb{Z} = \{\frac{a}{2^n} \in \mathbb{Q} : a \in \mathbb{Z}, n \in \mathbb{N}\}$.

Se $p \neq 2$, allora $(p) \cap S = \emptyset$ e quindi $S^{-1}(p) = (p)A$ è un ideale primo di A. Dato che $2 \in A \setminus (p)A$ possiamo definire

$$f : A \times \mathbb{Z}_{(p)} \longrightarrow A_{(p)A} \quad \text{tramite l'assegnazione} \quad f\left(\frac{a}{2^n}, \frac{c}{d}\right) = \frac{ac}{2^n d},$$

per ogni $a, c \in \mathbb{Z}$, $n \in \mathbb{N}$ e $d \notin (p)$. Si verifica facilmente che f è un omomorfismo $\mathbb{Z}$-bilineare, perciò otteniamo un diagramma commutativo

$$\begin{array}{ccc} A \times \mathbb{Z}_{(p)} & \xrightarrow{\ f\ } & A_{(p)A} \\ \downarrow & \nearrow_{\tilde{f}} & \\ A \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)} & & \end{array},$$

Dato che $\frac{a}{2^n} \otimes \frac{c}{d} = \frac{1}{2^n} \otimes \frac{ac2^n}{d2^n} = 1 \otimes \frac{ac}{d2^n}$, è facile verificare che $\tilde{f}$, che è ovviamente surgettiva, è un isomorfismo.

Viceversa, se $p = 2$ allora $(2) \cap S \neq \emptyset$ e quindi $A_{(2)A} = A$, mentre $A \otimes_{\mathbb{Z}} \mathbb{Z}_{(2)} \simeq \mathbb{Q}$: per dimostrare l'ultima affermazione basta considerare il diagramma commutativo

$$\begin{array}{ccc} A \times \mathbb{Z}_{(2)} & \xrightarrow{\ g\ } & \mathbb{Q} \\ \downarrow & \nearrow_{\tilde{g}} & \\ A \otimes_{\mathbb{Z}} \mathbb{Z}_{(2)} & & \end{array}$$

indotto da $g\left(\frac{a}{2^n}, \frac{c}{d}\right) = \frac{ac}{2^n d}$ e ragionare come nel caso precedente.

Soluzione E. *213* 1. Sia $a \in A$ tale che $\sigma_S(a) = 0$ allora esiste $s \in S$ tale che $as = 0$; se $s \notin \mathcal{D}(A)$, da questo segue che $a = 0$. D'altra parte, se $T \supset S$, allora T contiene un divisore di zero b tale che $bc = 0$ per qualche $c \neq 0$. Quindi $\sigma_T(c) = \frac{c}{1} = \frac{0}{b}$, che mostra che σ_T non è iniettiva.

2. Sia $\frac{a}{s} \in S^{-1}A$ e supponiamo che non sia un divisore di zero: allora anche $\frac{a}{1}$ non è un divisore di zero e vogliamo dimostrare che $a \notin \mathcal{D}(A)$. Se $ab = 0$, per qualche $b \in A$, allora $\frac{a}{1} \cdot \frac{b}{1} = 0$, da cui segue $\sigma_S(b) = \frac{b}{1} = 0$, e quindi $b = 0$ dato che σ_S è iniettiva per il punto precedente. Otteniamo così che $a \in S$ e $\frac{a}{s}$ è invertibile.

3. Sia ora $A = A^* \sqcup \mathcal{D}(A)$; allora $S = A^*$ e quindi per ogni $\frac{a}{s} \in S^{-1}A$ si ha $\sigma(as^{-1}) = \frac{as^{-1}}{1} = \frac{a}{s}$ e ciò mostra che σ_S è surgettiva.

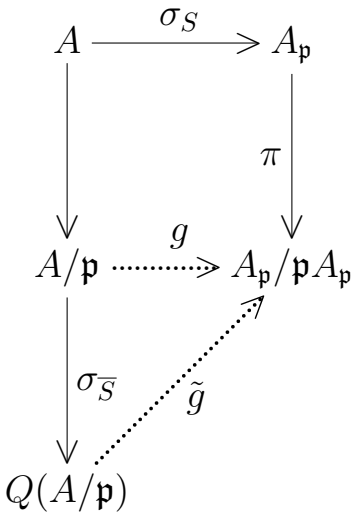
4. Quando $\mathcal{D}(A) = \{0\}$ e $S = A \setminus \{0\}$, per il punto 2. ogni elemento non nullo di $Q(A)$ è invertibile, e dunque $Q(A)$ è un campo che contiene A per il punto 1.

Sia ora K un campo contenente A; allora ogni elemento di S è invertibile in K e l'inclusione di A in K per la proprietà universale induce un'inclusione di $Q(A)$ in K.

Soluzione E. *214* Sia $S = A \setminus \mathfrak{p}$ e consideriamo l'omomorfismo $f\colon A \longrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ definito da

$$A \xrightarrow{\sigma_S} A_\mathfrak{p} \xrightarrow{\pi} A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}.$$

È facile vedere che $\operatorname{Ker} f = \mathfrak{p}$, quindi f induce un omomorfismo iniettivo $g\colon A/\mathfrak{p} \longrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$, $\overline{a} \mapsto \frac{a}{1} + \mathfrak{p}A_\mathfrak{p}$.
Sia ora $\overline{S} = A/\mathfrak{p} \setminus \{\overline{0}\}$; allora per ogni $\overline{s} \in \overline{S}$ si ha $g(\overline{s}) \in (A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})^*$, e quindi g si solleva ad un omomorfismo $\tilde{g}\colon Q(A/\mathfrak{p}) = \overline{S}^{-1}(A/\mathfrak{p}) \longrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Un elemento di $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ si scrive come $\frac{a}{s} + \mathfrak{p}A_\mathfrak{p} = g(\overline{a})g(\overline{s})^{-1}$, e inoltre g è iniettiva, pertanto la conclusione segue da **T.**136.



Soluzione E. *215* 1. Ovviamente $\mathcal{D}(A) \supseteq \overline{\mathfrak{p}}_i$ per ogni i. Per verificare l'altra inclusione, osserviamo che $\overline{a} \in \mathcal{D}(A)$ se e solo se esiste $b \in B$ tale che $\overline{b} \neq 0$ e $ab \in \mathfrak{p}_i$ per ogni i. Dato che $\overline{b} \neq 0$, deve esistere i tale che $b \notin \mathfrak{p}_i$, quindi $a \in \mathfrak{p}_i$.

Considerando $S = A \setminus \bigcup_{i=1}^n \overline{\mathfrak{p}}_i$, si ha dunque che $Q(A) = S^{-1}A$ e gli ideali massimali di $Q(A)$ sono esattamente gli ideali $S^{-1}\overline{\mathfrak{p}}_i$ per $i = 1, \dots, n$. Osserviamo che per ogni $i = 1, \dots, n$ abbiamo che $S^{-1}(A/\overline{\mathfrak{p}}_i) \simeq S^{-1}A/S^{-1}\overline{\mathfrak{p}}_i$ è un campo che contiene $A/\overline{\mathfrak{p}}_i$. Inoltre, dato che $S \subseteq A \setminus \overline{\mathfrak{p}}_i$, avremo $S^{-1}(A/\overline{\mathfrak{p}}_i) \subseteq Q(A/\overline{\mathfrak{p}}_i)$. Pertanto, $S^{-1}(A/\overline{\mathfrak{p}}_i) = Q(A/\overline{\mathfrak{p}}_i)$, per **E.**213.4.
Da **T.**143.2 sappiamo che $\bigcap_{i=1}^n S^{-1}\overline{\mathfrak{p}}_i = S^{-1}\left(\bigcap_{i=1}^n \overline{\mathfrak{p}}_i\right) = 0$ in $S^{-1}A$, e dunque dal teorema cinese del resto segue che

$$Q(A) = S^{-1}A \simeq \bigoplus_{i=1}^n S^{-1}A/S^{-1}\overline{\mathfrak{p}}_i \simeq \bigoplus_{i=1}^n S^{-1}(A/\overline{\mathfrak{p}}_i) \simeq \bigoplus_{i=1}^n S^{-1}(B/\mathfrak{p}_i),$$

e ciò conclude la dimostrazione.

2. In questo caso $A \simeq \mathbb{C}[x,y]/(x) \cap (y)$ e $\mathcal{D}(A) = (x) \cup (y)$, quindi, per il punto 1, $S^{-1}A = \mathbb{C}(x) \oplus \mathbb{C}(y)$.

3. È facile verificare che l'ideale $(x^2 - y^3)$ è primo, di conseguenza $\mathcal{D}(A) = (0)$ e quindi $S^{-1}A = Q(A)$ è il campo dei quozienti di A.

Soluzione E. *216* Dato un qualsiasi $a \neq 0$, in generale avremo che $A_a \subseteq Q(A)$. Siano ora $(0) = \mathfrak{p}_0, \mathfrak{p}_1, \dots, \mathfrak{p}_k$ gli ideali primi distinti di A. Osserviamo che se $k = 0$ allora A è un campo, quindi $A_a \simeq A \simeq Q(A)$ per ogni $a \neq 0$.

Sia allora $k > 0$ e consideriamo $\bigcap_{i=1}^{k} \mathfrak{p}_i$: questa intersezione è diversa da zero poiché altrimenti $\bigcap_{i=1}^{k} \mathfrak{p}_i = \mathfrak{p}_0$, da cui discenderebbe che $\mathfrak{p}_i = \mathfrak{p}_0$ per qualche i. Possiamo dunque considerare $0 \neq a \in \bigcap_{i=1}^{k} \mathfrak{p}_i$ e l'anello A_a, che non ha ideali primi diversi da zero, cioè A_a è un campo che contiene A. Essendo $Q(A)$ il più piccolo campo che contiene A, avremo $Q(A) \subseteq A_a$ e di conseguenza la tesi.

Alternativamente, possiamo provare l'inclusione opposta nel seguente modo: sia $\frac{b}{c} \in Q(A)$ e consideriamo $\sqrt{(c)}$. Si ha che $a \in \bigcap_{i=1}^{k} \mathfrak{p}_i \subseteq \bigcap_{c \in \mathfrak{p}_{i_j}} \mathfrak{p}_{i_j} = \sqrt{(c)}$, ed esiste pertanto un intero $t \in \mathbb{N}$ tale che $a^t = dc$ per qualche $d \in A$. Da ciò segue che $\frac{b}{c} = \frac{bd}{a^t}$, ossia $Q(A) \subseteq A_a$.

Soluzione E. *217* Osserviamo che $\mathbb{Z}_p = \left\{ \frac{a}{p^n} \in \mathbb{Q} \right\}$ ed è sufficiente provare che ogni elemento della forma $\frac{a}{p^n} \otimes \overline{\frac{b}{p^m}}$ è zero in $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}_p/\mathbb{Z}$. Si ha

$$\frac{a}{p^n} \otimes \overline{\frac{b}{p^m}} = \frac{ap^m}{p^{n+m}} \otimes \overline{\frac{b}{p^m}} = \frac{a}{p^{n+m}} \otimes \overline{\frac{p^m b}{p^m}} = \frac{a}{p^{n+m}} \otimes \overline{b} = 0,$$

perché $b \in \mathbb{Z}$.

Soluzione E. *218* Abbiamo visto in **E.**80 che $I = (xz + 2z, y - z, z^2 - z)$. Dato che in $\mathbb{Q}[x, y, z]_{(x,y,z)}$ gli elementi $x + 2$ e $z - 1$ sono invertibili, si ha che J è l'estensione dell'ideale (y, z); dato che $f = x^3 z - y^2$, la sua immagine è un elemento di J.

Soluzione E. *219* Abbiamo visto in **E.**84 che $I = (x^2 + 2y^2 - 3, xy - y^2, y^3 - y)$. Dato che (y), $(y + 1)$ e $(y - 1)$ sono a due a due comassimali, si ricava facilmente che $I = (x^2 - 3, y) \cap (x - 1, y - 1) \cap (x + 1, y + 1)$, dunque $I \subset \mathfrak{p}_1$ e $I_{\mathfrak{p}_1} \cap \mathbb{C}[x, y] \neq (1)$. Si ha che $y^3 - y = (y^2 + y)(y - 1)$ e $y^2 + y$ è invertibile in $\mathbb{C}[x, y]_{\mathfrak{p}_1}$, quindi l'ideale $I_{\mathfrak{p}_1} \cap \mathbb{C}[x, y]$ contiene $y - 1$; anche y è invertibile e pertanto, da $xy - y^2 \in I$, si ricava $x - 1 \in I_{\mathfrak{p}_1}$. Dunque $I_{\mathfrak{p}_1} \cap \mathbb{C}[x, y] = \mathfrak{p}_1$.

Invece $I \not\subset (x, y)$ e così $I_{\mathfrak{p}_2} \cap \mathbb{C}[x, y] = (1)$.

Soluzione E. *220* Abbiamo visto in **E.**86 che $\sqrt{I} = (x, y) \cap (x^4 + 1, x^3 + y)$, quindi, per **T.**140.4, $\sqrt{I_{(x,y)}} = (\sqrt{I})_{(x,y)} = (x, y)_{(x,y)}$. Dato che $f = x^2 + 5x$, avremo che $\frac{f}{1} \in \sqrt{I_{(x,y)}}$.

Soluzione E. *221* Da **E.**89.2 segue che i primi minimali di I sono (x,z), (x,y) e (y,z). Dato che y è invertibile in $\mathbb{R}[x,y,z]_{(x,z)}$, da **E.**89.3 segue che $I_{(x,z)} = (x^2,z)_{(x,z)}$ e quindi

$$\begin{aligned} A_{\mathfrak{p}} &= (\mathbb{R}[x,y,z]/I)_{\mathfrak{p}} \simeq \mathbb{R}[x,y,z]_{(x,z)}/I_{(x,z)} \simeq \mathbb{R}[x,y,z]_{(x,z)}/(x^2,z)_{(x,z)} \\ &\simeq (\mathbb{R}[x,y]/(x^2))_{(x)}. \end{aligned}$$

Soluzione E. *222* Da **E.**95 segue che $I = (x-yz, yz^2-y)$; inoltre z e z^2-1 sono invertibili e pertanto $S^{-1}(A/I) \simeq S^{-1}A/S^{-1}I = K[x,y,z]_{(x,y)}/I_{(x,y)} \simeq K[x,y,z]_{(x,y)}/(x,y)_{(x,y)} \simeq K(z)$.

Soluzione E. *223* Da **E.**105 segue che $I = (x^2-yz, xz-yz, y^2-yz)$; inoltre $z, y-z \notin (x,y)A$ quindi sono invertibili e da $z(x-y) = (y-z)y = 0$ in A otteniamo $\frac{x}{1} = \frac{y}{1} = 0$. Quindi $S^{-1}A \simeq \mathbb{Q}(z)$.

Soluzione E. *224* Abbiamo già visto in **E.**131 che la tesi è vera se B è un anello locale. Localizzando B in un suo ideale massimale $\mathfrak{m}$, otteniamo che, se K fosse finitamente generato come B-modulo, allora $K_{\mathfrak{m}} = K$ sarebbe finitamente generato come $B_{\mathfrak{m}}$-modulo, che non è possibile.

Soluzione E. *225* Osserviamo che A è un dominio e che la struttura di A-modulo di M è definita per restrizione di scalari tramite l'omomorfismo canonico.

1. Abbiamo che $M = K(x)$. Inoltre $M = (x)M$: infatti $m = x\frac{m}{x}$, quindi $M/(x)M = 0$ che è ovviamente finitamente generato.
2. Dato che A è locale con ideale massimale (x) e $M = (x)M$, se M fosse finitamente generato, applicando il lemma di Nakayama si avrebbe che $M = 0$.

Soluzione E. *226* 1. Sia $s \in \operatorname{Ann} M \cap S$; allora per ogni $\frac{m}{t} \in S^{-1}M$ si ha che $\frac{m}{t} = \frac{0}{s}$, e dunque $S^{-1}M = 0$.

2. Sia $M = \langle m_1, \dots, m_r \rangle$ tale che $S^{-1}M = 0$: per ogni $i = 1, \dots, r$ esiste $s_i \in S$ tale che $s_i m_i = 0$. Preso $s = \prod_{i=1}^{r} s_i$, abbiamo che $s \in \operatorname{Ann} M \cap S$.

3. Siano $A = \mathbb{Z}$, $S = \{2^n : n \in \mathbb{N}\}$ e si consideri l'A-modulo $M = \bigoplus_{n\in\mathbb{N}} \mathbb{Z}/(2^{n+1})$. È facile verificare che $\operatorname{Ann} M = 0$, dunque $S \cap \operatorname{Ann} M = \emptyset$. Inoltre, ogni elemento di $\alpha \in S^{-1}M$ si può scrivere come

$$\alpha = \left(\frac{a_0}{s_0}, \dots, \frac{a_m}{s_m}, 0, \dots, 0, \dots \right), \text{ con } a_i \in \mathbb{Z}/(2^{i+1}) \text{ e } s_i \in S \text{ per ogni } i$$

e per qualche intero m. Ovviamente $2^{m+1}\alpha = 0$, dunque $S^{-1}M = 0$.

Soluzione E. *227* Osserviamo preliminarmente che $(1) = (f_h \colon h \in H) \subseteq \sqrt{(f_h^{n_h} \colon h \in H)}$, per ogni scelta degli interi n_h, ovvero anche $\{f_h^{n_h} \colon h \in H\}$ è un insieme di generatori di A.

Ora, dato che $m = 0$ in M_{f_h} per ogni h, esistono interi n_h tali che $f_h^{n_h} m = 0$ in M e, per quanto osservato sopra possiamo scrivere 1 come somma finita di certi $a_i f_i^{n_i}$, con $a_i \in A$. Avremo allora che $m = 1m = \sum a_i f_i^{n_i} m = 0$, come volevamo.

Soluzione E. *228* 1. Sia $M = \langle m_1, \dots, m_k \rangle$. Supponiamo che $\mathfrak{p} \notin \operatorname{Supp} M$; allora $M_\mathfrak{p} = 0$ e quindi per ogni m_i esiste $s_i \notin \mathfrak{p}$ tale che $s_i m_i = 0$. In conclusione, $s = s_1 \cdots s_k \notin \mathfrak{p}$ e $s \in \operatorname{Ann} M$, dunque $\mathfrak{p} \not\supseteq \operatorname{Ann} M$.
Viceversa, se $\mathfrak{p} \not\supseteq \operatorname{Ann} M$, allora esiste $s \in (A \setminus \mathfrak{p}) \cap \operatorname{Ann} M$ e quindi per ogni $\frac{m}{1} \in M_\mathfrak{p}$ si ha $\frac{m}{1} = \frac{sm}{s} = 0$.
2. Dato che per ogni $\mathfrak{p} \in \operatorname{Spec} A$ la successione

$$0 \longrightarrow M'_\mathfrak{p} \longrightarrow M_\mathfrak{p} \longrightarrow M''_\mathfrak{p} \longrightarrow 0$$

è esatta, segue immediatamente che $M_\mathfrak{p} \neq 0$ se e solo se $M'_\mathfrak{p} \neq 0$ o $M''_\mathfrak{p} \neq 0$, da cui la tesi.

3. Sia $\mathfrak{p} \in \operatorname{Spec} A$. Per **T.**144, abbiamo che $(M \otimes_A N)_\mathfrak{p} = M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p}$. Dato che $A_\mathfrak{p}$ è un anello locale $M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p} \neq 0$ se e solo se $M_\mathfrak{p} \neq 0$ e $N_\mathfrak{p} \neq 0$, cf. **E.**189, e la tesi segue immediatamente.

Soluzione E. *229* 1. Dato che M è finitamente generato, si ha $M_{(p)} = 0$ se e solo se esiste $s \in (\mathbb{Z} \setminus (p)) \cap \operatorname{Ann}_\mathbb{Z} M$, i.e. se e solo se $(60) = \operatorname{Ann}_\mathbb{Z} M \not\subset (p)$. Dunque $M_{(p)} \neq 0$ solo per $p = 2, 3$ e 5.
2. Dato che $10 \notin (3)$ si ha

$$M_{(3)} \simeq (\mathbb{Z}/(10))_{(3)} \oplus (\mathbb{Z}/(12))_{(3)} \simeq (\mathbb{Z}/(12))_{(3)},$$

e $(\mathbb{Z}/(12))_{(3)} \simeq \mathbb{Z}/(3)$ per **E.**204.5.

Soluzione E. *230* 1. Per le proprietà del prodotto tensoriale $M \simeq A/(xyz - z^2, xy^2 - 4, yz, x - y^2)$, che è isomorfo a

$$\begin{aligned} A/(xy^2 - 4, x - y^2, yz, z^2) &\simeq A/(x - y^2, y^4 - 4, yz, z^2) \\ &\simeq A/(x - y^2, y^4 - 4, z), \end{aligned}$$

dato che $S(y^4 - 4, yz) = -4z$; quindi M ha dimensione 4.

2. M è un A-modulo finitamente generato per **T.**126.4, quindi $S^{-1}M = 0$ se e solo se $S \cap \operatorname{Ann} M \neq \emptyset$, cf. **E.**226. Dunque $M_{\mathfrak{p}} \neq 0$, se e solo se $A \setminus \mathfrak{p} \subset A \setminus \operatorname{Ann} M$ ossia $\mathfrak{p} \supset \operatorname{Ann} M$. Dato che $\operatorname{Ann} M = (x - y^2, y^4 - 4, z)$ e $\sqrt{\operatorname{Ann} M} = \sqrt{(x - 2, y^2 - 2, z)} \cap \sqrt{(x + 2, y^2 + 2, z)} = \mathfrak{p}_1 \cap \mathfrak{p}_2$ è intersezione di massimali, gli unici primi che contengono $\operatorname{Ann} M$ sono $\mathfrak{p}_1$ e $\mathfrak{p}_2$. Dunque $\operatorname{Supp} M = \{\mathfrak{p}_1, \mathfrak{p}_2\}$.

Soluzione E. *231* Sia $\mathfrak{m} \subset A$ massimale. Se $I_{\mathfrak{m}} = 0$ allora, per **E.**228.1, si ha $\operatorname{Ann} I \not\subset \mathfrak{m}$; se invece $I_{\mathfrak{m}} = A_{\mathfrak{m}}$, allora $I \not\subset \mathfrak{m}$, quindi, in ogni caso $I + \operatorname{Ann} I \not\subset \mathfrak{m}$ per ogni ideale massimale di A. Da questo segue che $I + \operatorname{Ann} I = A$ e che esistono $i \in I$ e $j \in \operatorname{Ann} I$ tali che $i + j = 1$; allora $i \neq 0$ altrimenti $j = 1$ e I sarebbe 0, contro l'ipotesi, e $i = i(i + j) = i^2$ è idempotente. Infine, per ogni $a \in I$, si ha $a = a(i + j) = ai$, e quindi $I = (i)$.

Soluzione E. *232* 1. Ovviamente $1 \in S$, inoltre, dato che se $(q_1, p) = (q_2, p) = 1$ anche $(q_1 q_2, p) = 1$, S è moltiplicativamente chiuso. Notiamo anche che $0 \notin S$.

Alternativamente si può osservare che $S = \mathbb{Q}[x] \setminus ((x - 1) \cup (x^2 + 2))$, dove $(x - 1)$ e $(x^2 + 2)$ sono ideali primi.

2. Con una dimostrazione analoga a **E.**204.1 e **E.**204.2 otteniamo

$$A = \left\{ \frac{f}{g} \in \mathbb{Q}(x) \ : \ (g, p) = 1 \right\}.$$

Gli ideali primi di A sono in corrispondenza con gli ideali primi $\mathfrak{p}$ di $\mathbb{Q}[x]$ tali che $\mathfrak{p} \cap S = \emptyset$. Dato che i primi di $\mathbb{Q}[x]$ sono principali e generati da elementi irriducibili gli unici ideali possibili sono $\mathfrak{p}_1 = (0), \mathfrak{p}_2 = (x - 1)$ e $\mathfrak{p}_3 = (x^2 + 2)$, e quelli non nulli sono massimali.

3. Chiaramente $A/(0) \simeq A$; ricordiamo che $A/IA \simeq S^{-1}(\mathbb{Q}[x]/I)$ per ogni ideale I di $\mathbb{Q}[x]$. Dunque $A/(x-1)A \simeq S^{-1}\mathbb{Q} \simeq \mathbb{Q}$ e $A/(x^2+2)A \simeq S^{-1}\left(\mathbb{Q}[x]/(x^2+2)\right) \simeq \mathbb{Q}(\sqrt{-2})$.

4. Ovviamente $A/\mathfrak{p}_1 \otimes_A A/\mathfrak{p}_i \simeq A/\mathfrak{p}_i$, che abbiamo descritto al punto precedente. Altrimenti, dato che $(x-1)$ e (x^2+2) sono comassimali, si ha $A/\mathfrak{p}_2 \otimes_A A/\mathfrak{p}_3 \simeq A/\mathfrak{p}_2 + \mathfrak{p}_3 = 0$.

Soluzione E. *233* Denotiamo $\overline{A} = A/I$, $\overline{M} = M/IM$ e $\overline{\mathfrak{m}} = \mathfrak{m}/I$, con $\mathfrak{m} \in \operatorname{Max} A$. Basta allora provare che $\overline{M}$, che è naturalmente un $\overline{A}$-modulo, è il modulo nullo. Dato che gli ideali massimali di $\overline{A}$ sono esattamente i massimali di A che contengono I, basta provare che $\overline{M}_{\overline{\mathfrak{m}}} = 0$ per tutti i massimali $\mathfrak{m} \supseteq I$, dato che essere 0 è una proprietà locale, e questo è vero poiché $\overline{M}_{\overline{\mathfrak{m}}} \simeq M_{\mathfrak{m}}/IM_{\mathfrak{m}} = 0$.

Alternativamente, possiamo supporre per assurdo che $IM \subsetneq M$ e quindi che esista $m \in M \setminus IM$. Allora $I \subseteq IM : m \neq A$. Sia allora $\mathfrak{m}$ un ideale massimale tale che $I \subseteq IM : m \subseteq \mathfrak{m}$. Dato che per ipotesi $M_{\mathfrak{m}} = 0$, avremo in particolare che $\frac{m}{1} = 0$ e quindi esiste $a \in A \setminus \mathfrak{m}$ tale che $am = 0$, che contraddice la scelta di $\mathfrak{m}$.

Soluzione E. *234* 1. Dato che gli ideali primi di $A_{\mathfrak{p}}$ sono in corrispondenza biunivoca con gli ideali primi di A contenuti in $\mathfrak{p}$, dall'ipotesi di minimalità discende che $\mathfrak{p}A_{\mathfrak{p}}$ è l'unico primo di $A_{\mathfrak{p}}$ e quindi coincide con il nilradicale di $A_{\mathfrak{p}}$.

2. Sia $a \in \mathfrak{p}$; per il punto precedente, $\frac{a}{1} \in A_{\mathfrak{p}}$ è nilpotente, ed esiste quindi $s \in A \setminus \mathfrak{p}$ tale che $sa^n = 0$ in A per qualche intero n. Scegliendo il minimo n con questa proprietà, otteniamo che $sa^{n-1} \neq 0$ e quindi a è un divisore di zero, come volevamo.

3. Per **T.**146.1, essere ridotto è una proprietà locale, quindi $A_{\mathfrak{p}}$ è ridotto. Dato che, come osservato al punto 1, $\mathfrak{p}A_{\mathfrak{p}} = \mathcal{N}(A_{\mathfrak{p}}) = 0$, l'ideale nullo è l'unico ideale massimale di $A_{\mathfrak{p}}$, che quindi è un campo.

Soluzione E. *235* Ovviamente $1 \cdot 1 \in S$ quindi $1 \in \overline{S}$. Siano $s, t \in \overline{S}$, allora esistono $a, b \in A$ tali che $as, bt \in S$; dato che S è moltiplicativo, si ha $asbt \in S$ che per definizione implica $st \in \overline{S}$, i.e. $\overline{S}$ è un insieme moltiplicativo. Adesso

supponiamo $st \in \overline{S}$, allora $ast \in S$ per qualche $a \in A$: quindi $s(at) = t(as) \in S$ implica $s, t \in \overline{S}$.

Soluzione E. *236* Siano $S_A = \{18^n : n \in \mathbb{N}\}$ e $S_B = \{6^n : n \in \mathbb{N}\}$ entrambi contenuti in $\mathbb{Z}/(200)$: per **T.**148.3

$$\overline{S}_B = \mathbb{Z}/(200) \setminus \bigcup_{\mathfrak{p} \cap S_B = \emptyset} \mathfrak{p} = \mathbb{Z}/(200) \setminus \bigcup_{2,3 \notin \mathfrak{p}} \mathfrak{p} = \overline{S}_A.$$

Dunque

$$\begin{aligned}(\mathbb{Z}/(200))_{18} &= S_A^{-1}\mathbb{Z}/(200) \simeq \overline{S}_A^{-1}\mathbb{Z}/(200) \\ &= \overline{S}_B^{-1}\mathbb{Z}/(200) \simeq S_B^{-1}\mathbb{Z}/(200) = (\mathbb{Z}/(200))_6,\end{aligned}$$

ove gli isomorfismi sono dovuti a **T.**148.6. Inoltre $\overline{S}_B^{-1}\mathbb{Z}/(200) = \overline{S}_B^{-1}\mathbb{Z}/(8) \times \overline{S}_B^{-1}\mathbb{Z}/(25)$: dato che $2 \in \overline{S}_B$ si ha $\overline{S}_B^{-1}\mathbb{Z}/(8) = (0)$, mentre l'omomorfismo $\sigma_{\overline{S}_B} : \mathbb{Z}/(25) \longrightarrow \overline{S}_B^{-1}\mathbb{Z}/(25)$ è surgettivo, cf. **E.**205, ed iniettivo perché $5 \notin \overline{S}_B$, cf. **E.**207.2.a).
Pertanto, $S_A^{-1}\mathbb{Z}/(200) \simeq S_B^{-1}\mathbb{Z}/(200) \simeq \mathbb{Z}/(25)$. Da **E.**183 segue che $C \simeq \mathbb{Z}/(25, 40) \simeq \mathbb{Z}/(5)$ e dunque $A \simeq B \not\simeq C$.

Adesso consideriamo l'omomorfismo $\varphi : \mathbb{Z}_{(3)}[x] \longrightarrow (\mathbb{Z}_{(3)})_6$ dato da $\varphi(x) = \frac{1}{6}$. Il nucleo di φ contiene $(6x - 1)$; dato che $6x - 1$ è irriducibile in $\mathbb{Z}_{(3)}[x]$, perché ha grado 1 e i coefficienti sono coprimi, si ha $\operatorname{Ker}\varphi = (6x - 1)$. Inoltre φ è surgettivo, perché ogni elemento di $(\mathbb{Z}_{(3)})_6$ si può scrivere $\frac{a}{6^k} = a\varphi(x^k) = \varphi(ax^k)$, dunque $D \simeq (\mathbb{Z}_{(3)})_6$.

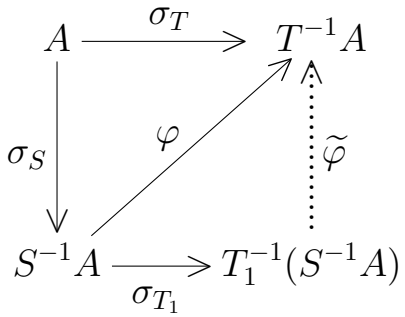
Osserviamo che l'isomorfismo appena dimostrato poteva essere dedotto direttamente da **E.**210.

Infine, $\mathbb{Z}_{(3)}$ è un anello locale con unico ideale massimale generato dall'immagine di 3, ma in $(\mathbb{Z}_{(3)})_6$ si ha $\frac{1}{3} = \frac{2}{6}$, cioè 3 invertibile, $(\mathbb{Z}_{(3)})_6 \subseteq \mathbb{Q}$ è un campo contenente $\mathbb{Z}$ e quindi $D \simeq \mathbb{Q} \not\simeq A, B, C$.

Soluzione E. *237* 1. Ovviamente $1 \in f^{-1}(T)$, inoltre, $a, b \in f^{-1}(T)$ implica $f(ab) = f(a)f(b) \in T$, quindi $ab \in f^{-1}(T)$.
Per il viceversa, osserviamo che per ipotesi $1 \in T$. Presi $s, t \in T$ esistono $a, b \in f^{-1}(T)$ tali che $f(a) = s$ e $f(b) = t$; dato che $f^{-1}(T)$ è moltiplicativo, si ha $ab \in f^{-1}(T)$ e dunque $f(ab) = st \in T$.

2. Sia $a \in \overline{f^{-1}(T)}$, allora esiste $t \in A$ tale che $at \in f^{-1}(T)$, cioè $f(at) = f(a)f(t) \in T$. Dal fatto che T è saturato, segue che $f(a) \in T$ e quindi $a \in f^{-1}(T)$, come volevamo.
Per il viceversa, siano $s \in \overline{T}$ e $t \in B$ tale che $st \in T$; per ipotesi esistono $a, b \in A$ tali che $f(a) = s$ e $f(b) = t$. Dunque $f(ab) = st \in T$ implica che $ab \in f^{-1}(T)$; di conseguenza $a, b \in \overline{f^{-1}(T)} = f^{-1}(T)$, e $s = f(a) \in T$.

Soluzione E. *238* 1. L'omomorfismo $\varphi\colon S^{-1}A \longrightarrow T^{-1}A$ definito da $\varphi\left(\frac{a}{s}\right) = \frac{a}{s}$, verifica $\varphi(T_1) \subseteq (T^{-1}A)^*$ e, per la proprietà universale, definisce un omomorfismo $\widetilde{\varphi}\colon T_1^{-1}(S^{-1}A) \longrightarrow T^{-1}A$. Osserviamo che $\varphi\left(\frac{a}{s}\right) = 0$ se e solo se esiste $t \in T$ tale che $ta = 0$, quindi $\sigma_S(t)\frac{a}{s} = \frac{ta}{s} = 0$, con $\sigma_S(t) \in T_1$. Infine, per ogni $\frac{a}{t} \in T^{-1}A$ possiamo scrivere $\frac{a}{t} = \varphi\left(\frac{a}{1}\right)\varphi(\sigma_S(t))^{-1}$, dunque $\widetilde{\varphi}$ è un isomorfismo per **T.**136.



L'isomorfismo $T^{-1}A \simeq T^{-1}(S^{-1}A)$ si dimostra analogamente applicando la proprietà universale all'omomorfismo $\sigma_T : S^{-1}A \longrightarrow T^{-1}A$ definito da $\sigma_T\left(\frac{a}{s}\right) = \frac{\frac{a}{s}}{1}$.
2. È facile vedere che U è un sistema moltiplicativo che contiene S e T. Dal punto precedente otteniamo allora che $U^{-1}(S^{-1}A) \simeq U^{-1}A \simeq U^{-1}(T^{-1}A)$.

Per ottenere l'isomorfismo $U^{-1}(S^{-1}A) \simeq T^{-1}(S^{-1}A)$ procediamo come segue; in maniera del tutto analoga si potrà dimostrare che $U^{-1}(T^{-1}A) \simeq S^{-1}(T^{-1}A)$. Consideriamo l'omomorfismo $\varphi\colon S^{-1}A \longrightarrow U^{-1}A$ definito da $\varphi\left(\frac{a}{s}\right) = \frac{a}{s}$ e osserviamo che $\varphi(T) \subseteq (U^{-1}A)^*$. Per la proprietà universale esiste un omomorfismo $\widetilde{\varphi}\colon T^{-1}(S^{-1}A) \longrightarrow U^{-1}A$: per ogni $\frac{a}{u} \in U^{-1}A$ esistono $s \in S$ e $t \in T$ tali che $u = st$, quindi $\frac{a}{u} = \frac{a}{st} = \varphi\left(\frac{a}{s}\right)\varphi(t)^{-1}$. Infine se $\varphi\left(\frac{a}{u}\right) = 0$, allora esiste $u_1 = s_1t_1 \in U$ tale che $s_1t_1a = 0$, dunque per $\frac{a}{u} = \frac{as_1}{us_1}$ esiste $t_1 \in T$ tale che $t_1\frac{as_1}{us_1} = 0$. L'isomorfismo cercato segue da **T.**136.

Soluzione E. *239* Se $\mathfrak{p}$ è un primo non minimale, allora $\mathfrak{p}$ contiene propriamente un certo $\mathfrak{q} \in \operatorname{Min} A$ e dunque $S = A \setminus \mathfrak{p} \subsetneq A \setminus \mathfrak{q} = T$ non è massimale.

Sia $\mathfrak{p}$ un primo minimale di A, $S = A \setminus \mathfrak{p}$ e supponiamo che T sia un insieme moltiplicativo con $T \supsetneq S$. Per **T.**148, punti 1 e 3, possiamo supporre senza perdita di generalità che T sia saturato e

$$T = A \setminus \bigcup_{\substack{\mathfrak{q} \in \operatorname{Spec} A \\ \mathfrak{q} \cap T = \emptyset}} \mathfrak{q}.$$

Ora, $\mathfrak{q} \cap T = \emptyset$ implica $\mathfrak{q} \subseteq A \setminus T \subsetneq A \setminus S = \mathfrak{p}$, il che contraddice la minimalità di $\mathfrak{p}$.

Soluzione E. *240* 1. Per **T.**148.3, è sufficiente dimostrare che

$$\bigcup_{\mathfrak{p} \in \mathcal{V}(I)} \mathfrak{p} = \bigcup_{\mathfrak{q} \cap S = \emptyset} \mathfrak{q} = A \setminus \overline{S}.$$

Ovviamente se $\mathfrak{p} \in \mathcal{V}(I)$ si ha $\mathfrak{p} \cap S = \emptyset$, altrimenti $1 \in \mathfrak{p}$: quindi abbiamo l'inclusione $\subseteq$.

Per l'inclusione opposta, sia $\mathfrak{q}$ un primo che non interseca S; allora l'ideale $(I, \mathfrak{q}) \neq 1$, altrimenti esisterebbero $a \in I$ e $b \in \mathfrak{q}$ tali che $a + b = 1$ e quindi $b = 1 - a \in \mathfrak{q} \cap S$, contraddizione. Dunque esiste un primo $\mathfrak{q}' \supseteq (I, \mathfrak{q})$ e quindi $\mathfrak{q} \subseteq \mathfrak{q}' \in \mathcal{V}(I)$, che implica la conclusione.

2. Dato che per un primo $\mathfrak{p}$ di A si ha $S_f \cap \mathfrak{p} = \emptyset$ se e solo se $f \notin \mathfrak{p}$ possiamo scrivere $\overline{S}_f = A \setminus \bigcup_{f \notin \mathfrak{p}} \mathfrak{p}$. Dunque

$$\overline{S}_f = A \setminus \bigcup_{f \notin \mathfrak{p}} \mathfrak{p} \subseteq \overline{S}_g = A \setminus \bigcup_{g \notin \mathfrak{q}} \mathfrak{q}$$

se e solo se $\bigcup_{f \notin \mathfrak{p}} \mathfrak{p} \supseteq \bigcup_{g \notin \mathfrak{q}} \mathfrak{q}$, cioè se e solo se per ogni primo $\mathfrak{q}$ che non contiene g si ha $\mathfrak{q} \subseteq \bigcup_{f \notin \mathfrak{p}} \mathfrak{p}$. Per il lemma di scansamento **T.**12, questo è equivalente a dire che $\mathfrak{q} \subseteq \mathfrak{p}$ per qualche $\mathfrak{p}$ non contenente f. In conclusione, $\overline{S}_f \subseteq \overline{S}_g$ se e solo se per ogni primo $\mathfrak{q}$, $g \notin \mathfrak{q}$ implica $f \notin \mathfrak{q}$. L'ultima affermazione equivale a: per ogni primo $\mathfrak{p}$, $f \in \mathfrak{p}$ implica $g \in \mathfrak{p}$, cioè

$$\sqrt{(f)} = \bigcap_{f \in \mathfrak{p}} \mathfrak{p} \supseteq \bigcap_{g \in \mathfrak{q}} \mathfrak{q} = \sqrt{(g)}.$$

Soluzione E. *241* 1. I primi di $A_\mathfrak{q}$ sono in corrispondenza 1:1 con gli ideali primi di A che sono contenuti in $\mathfrak{q}$, che a loro volta corrispondono ai primi I in $K[x,y]$ tali che $(x,y) \supseteq I \supseteq (x^2-y^2)$ e quindi tali che $I \supseteq (x+y)$ oppure $I \supseteq (x-y)$.

Se $(x,y) \supset I \supsetneq (x \pm y)$, allora $I = (x,y)$; infatti $K[x,y]/(x \pm y) \simeq K[x]$ e $(x,y)/(x \pm y) \simeq (x)$ e non ci sono primi fra (0) e (x). Quindi gli unici primi di $A_\mathfrak{q}$ sono $(x-y)A_\mathfrak{q}$, $(x+y)A_\mathfrak{q}$ e $(x,y)A_\mathfrak{q}$, che è l'unico massimale.

2. Sia $S = A_\mathfrak{q} \setminus \mathfrak{p}A_\mathfrak{q}$, allora in $S^{-1}A_\mathfrak{q}$ rimane solo un primo, quindi massimale, che è $S^{-1}\mathfrak{p}A_\mathfrak{q}$. Inoltre, dato che $\operatorname{char} K \neq 2$, $x-y \notin (x+y)$ e $\frac{x-y}{1} \in S$. Infine, l'ideale massimale $\mathfrak{p}A_\mathfrak{q} = \left(\frac{x+y}{1}\right) = \left(\frac{0}{x-y}\right)$ di $S^{-1}A_\mathfrak{q}$ è nullo, e $S^{-1}A_\mathfrak{q}$ è un campo.

Per descriverlo, osserviamo dapprima che $(A_\mathfrak{q})_{\mathfrak{p}A_\mathfrak{q}} \simeq A_\mathfrak{p}$, per **E.**238. Inoltre, $S^{-1}(x^2-y^2) = S^{-1}(x+y)$. Quindi

$$\begin{aligned}(A_\mathfrak{q})_{\mathfrak{p}A_\mathfrak{q}} &\simeq A_\mathfrak{p} \simeq S^{-1}(K[x,y]/(x^2-y^2)) \\ &\simeq S^{-1}K[x,y]/S^{-1}(x^2-y^2) \simeq S^{-1}K[x,y]/S^{-1}(x+y) \\ &\simeq S^{-1}(K[x,y]/(x+y)) \simeq K(x),\end{aligned}$$

dove l'ultimo isomorfismo segue dal fatto che $x-y \in S$ si riduce a $2x$ modulo $x+y$.

16.7 Soluzioni del capitolo 14

Soluzione E. *242* 1. Basta osservare che, dati due ideali $(a), (b) \subseteq \mathbb{Z}$, si ha che $(a) \subseteq (b)$ se e solo se $b|a$, quindi una catena ascendente che inizia con (a) ha al più tanti elementi quanti sono i divisori di a. Per lo stesso motivo, dato un elemento $a \neq 0, 1$ di $\mathbb{Z}$ si può ottenere una catena discendente infinita $(a) \supset (a^2) \supset \cdots \supset (a^k) \supset \cdots$.

2. È sufficiente osservare che l'anello dato è un campo.

Soluzione E. *243* 1. Consideriamo gli ideali $K_i = \operatorname{Ker}(\varphi^i)$; dato che A è noetheriano la catena di ideali $K_1 \subseteq K_2 \subseteq \cdots$ si stabilizza ed esiste un intero n tale che $K_n = K_{n+1}$.

Sia ora $a \in K_1$; vogliamo provare che $a = 0$. Dato che φ, e quindi anche φ^n, è surgettivo, esiste $b \in A$ tale che $\varphi^n(b) = a$. Da ciò segue che $\varphi(a) = \varphi^{n+1}(b) = 0$ ossia $b \in K_{n+1} = K_n$ e pertanto $a = 0$ come volevamo.

2. Ricordiamo che se φ è surgettivo allora, per ogni ideale $I \subset A$, $\varphi(I)$ è un ideale di A. È sempre vero che $\varphi(I \cap J) \subseteq \varphi(I) \cap \varphi(J)$; basta dunque provare l'altra inclusione. Sia $a \in \varphi(I) \cap \varphi(J)$; allora $a = \varphi(i) = \varphi(j)$ per certi $i \in I$ e $j \in J$. Da questo segue che $0 = \varphi(i - j)$ e quindi, dato che φ è iniettiva per il punto 1, $i = j \in I \cap J$ come volevamo.

3. Se A non è noetheriano entrambe le affermazioni sono false. Consideriamo $A = K[x_i \colon i \in \mathbb{N}]$, con K campo, e φ definita da $\varphi(x_1) = 0$ e $\varphi(x_i) = x_{i-1}$ per $i > 1$; allora è immediato vedere che φ è surgettiva ma non iniettiva.
Siano ora $I = (x_1 + x_2)$ e $J = (x_2)$ ideali di A. Dato che I e J sono principali e generati da elementi relativamente primi, $I \cap J = IJ$; quindi $\varphi(I \cap J) = (\varphi(x_1 + x_2)\varphi(x_2)) = (x_1^2)$, mentre $\varphi(I) \cap \varphi(J) = (x_1)$.

Soluzione E. *244* Dato che A è noetheriano, I è un A-modulo finitamente generato; allora applicando il lemma di Nakayama otteniamo che esiste un elemento $b \in A$, $b \equiv 1 \mod I$ tale che $bI = 0$.
Sia $a = 1 - b \in I$ allora $(a) \subseteq I = 1 \cdot I = (a + b)I \subseteq aI \subseteq (a)$ da cui segue che $I = (a)$. Inoltre, dato che $a(1 - a) = 0$, otteniamo che a è idempotente.

Soluzione E. *245* Consideriamo la successione $0 \longrightarrow N_1 \cap N_2 \longrightarrow M \xrightarrow{f} M/N_1 \oplus M/N_2$; è immediato verificare che essa è esatta. Allora $M/(N_1 \cap N_2) \simeq \operatorname{Im} f \subseteq M/N_1 \oplus M/N_2$, e quest'ultimo è noetheriano, in quanto somma diretta di noetheriani, cf. **T.**152.3.

Soluzione E. *246* Sia M noetheriano; allora tutti i suoi quozienti sono noetheriani, cf. **T.**152.2.

Viceversa, siano M/fM e M/g^2M noetheriani. Per l'esercizio **E.**245, basta dimostrare che $0 = (fg^2)M = fM \cap g^2M$, ove la prima uguaglianza è ovvia dalla definizione di A. Per dimostrare la seconda uguaglianza, osserviamo subito che l'inclusione "$\subseteq$" è chiara e che dall'ipotesi discende che esistono $i, j \in A$ tali che $if + jg^2 = 1$.

Sia ora $m \in fM \cap g^2M$; allora $m = afm_1 = bg^2n_1$, con $a, b \in A$ e $m_1, n_1 \in M$. Pertanto, $m = (if + jg^2)m = if(bg^2n_1) + jg^2(afm_1) = (ibfg^2)n_1 + (jafg^2)m_1 \in fg^2M$, come volevamo.

Soluzione E. *247* Osserviamo che per ipotesi tale d è necessariamente non nullo.

1. Dato che $(d) = IJ$, si ha $d = \sum_{i=1}^{k} f_i g_i$ per qualche $f_i \in I$, $g_i \in J$ e qualche intero k. Sia allora $\bar{J} = (g_1, \ldots, g_k)$; avremo che $(d) \subseteq I\bar{J} \subseteq IJ = (d)$.

2. Sia $f \in I$; allora, per ogni i, $fg_i \in IJ = (d)$ da cui segue che esiste h_i tale che $fg_i = h_i d$.

3. Proviamo la tesi dimostrando che ogni ideale I di A è finitamente generato utilizzando i punti precedenti. Sia $\bar{J}$ l'ideale finitamente generato costruito al punto 1. Per ogni $f \in I$ si ha che $fd \in I\bar{J}$ e quindi $fd = f\sum_{i=1}^{k} f_i g_i = \sum_{i=1}^{k} f_i(fg_i) = d\sum_{i=1}^{k} f_i h_i$. Poiché A è un dominio, da questo segue che $f = \sum_{i=1}^{k} f_i h_i$, e quindi che $I = (f_1, \ldots, f_k)$.

Soluzione E. *248* 1. La verifica è facile e discende dalla linearità di f e g.

2. Siano ora $\pi_A : A \times_C B \longrightarrow A$ e $\pi_B : A \times_C B \longrightarrow B$ gli omomorfismi di proiezione sulle componenti, che sono surgettivi, dato che f e g lo sono: ad esempio, dato $a \in A$, avremo $f(a) = c$ per qualche $c \in C$ e dunque per la surgettività di g esiste $b \in B$ tale che $g(b) = c = f(a)$; pertanto $(a, b) \in A \times_C B$ e $\pi_A(a, b) = a$.
Per **E.**114, gli ideali di A e di B sono $A \times_C B$ sottomoduli di A e B rispettivamente e, se A e B sono noetheriani come anelli, allora sono noetheriani come $A \times_C B$-moduli. Da questo segue che $A \times B$ è noetheriano come $(A \times_C B)$-modulo; allora $A \times_C B$, che è sottomodulo di un $(A \times_C B)$-modulo noetheriano è a sua volta un $(A \times_C B)$-modulo noetheriano per **T.**152.2, e quindi è noetheriano come anello.

Soluzione E. *249* 1. Supponiamo che ogni elemento non nullo in $\mathfrak{m}$ possegga tale fattorizzazione e supponiamo per contraddizione che esista $0 \neq a = um^k$, con $u \in A^*$ e $a \in \bigcap_{n\in\mathbb{N}} \mathfrak{m}^n$. Allora $a \in \mathfrak{m}^n$ per ogni n; si ottiene che $\mathfrak{m}^k \subseteq (a) \subseteq \mathfrak{m}^n \subseteq \mathfrak{m}^k$ per ogni $n > k$ e pertanto per un tale n avremo $\mathfrak{m}^n = \mathfrak{m}^k$, da

cui segue $m^k = bm^n$ e $m^k(1 - bm^{n-k}) = 0$. Dato che $1 - bm^{n-k}$ è invertibile per **T.**15, si avrà che $m^k = 0$ e $a = 0$, che è la contraddizione cercata.

Viceversa, se $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = 0$ e $0 \neq a \in \mathfrak{m}$, sia k il massimo esponente tale che $a \in \mathfrak{m}^k$; allora $a = bm^k$ e $b \notin \mathfrak{m}$; poiché A è locale, segue subito che b è invertibile.

2. Sia $I \subset A$ un ideale proprio; allora $I \subset \mathfrak{m}$ e, per il punto precedente, ogni elemento $a \in I$ si scrive come $a = um^k$ con $u \in A^*$: dunque $a \in I$ implica $m^k \in I$ per qualche intero k. Sia h il più piccolo esponente per cui $m^h \in I$; allora $I \supseteq \mathfrak{m}^h$ e ogni $a \in I$ è del tipo $a = um^k = um^h m^{k-h} \in \mathfrak{m}^h$, come volevamo.

3. Per il punto precedente, è sufficiente provare che se A è noetheriano, valgono le condizioni equivalenti del punto 1. Sia dunque $0 \neq a \in \mathfrak{m}$, con $a = b_1 m$. Se b_1 è invertibile abbiamo finito. Altrimenti, esiste $b_2 \in A$ tale che $b_1 = b_2 m \in \mathfrak{m}$; inoltre $a = b_2 m^2$ e $(b_1) \subsetneq (b_2)$. Possiamo procedere in questo modo e costruire una catena ascendente di ideali di A $(b_1) \subsetneq (b_2) \subsetneq \cdots \subsetneq (b_n) \subsetneq \cdots$ generati da elementi tali che $b_i m^i = a$ per ogni i. Se tutti i b_i fossero non invertibili allora la catena sarebbe infinita il che non è possibile visto che A è noetheriano, dunque esiste b_k invertibile tale che $a = b_k m^k$.

Soluzione E. *250* 1. Siano $\mathfrak{m} = (m)$ l'ideale massimale di A e $I \subset A$ un ideale proprio. Allora, $I \subset \mathfrak{m}$ ed è finitamente generato, diciamo da $b_1, \ldots, b_k$, poiché A è noetheriano. Ne segue che, per ogni $i = 1, \ldots, k$, esiste un intero k_i tale che $b_i = u_i m^{k_i}$ e da questo è facile vedere che $I = (m^k)$ con $k = \min_i k_i$, cf. la dimostrazione di **E.**249.

2. Ogni ideale di una catena ascendente $\mathcal{C}$ di ideali primi di A è contenuto in un ideale massimale $\mathfrak{m}_\mathcal{C}$ che, per ipotesi, è principale. Localizzando A in $\mathfrak{m}_\mathcal{C}$ e applicando il punto precedente, otteniamo che la lunghezza della catena $\mathcal{C}_\mathfrak{m}$ dei primi localizzati può essere uguale a 1, se $A_{\mathfrak{m}_\mathcal{C}}$ è un dominio, e altrimenti 0. Abbiamo dunque mostrato che la dimensione di ogni localizzazione di A in un ideale massimale è minore o uguale a 1. Dalla corrispondenza tra gli ideali primi di A e gli ideali primi delle sue localizzazioni, discende immediatamente che $\dim A \leq \max\{\dim A_\mathfrak{m} : \mathfrak{m} \in \operatorname{Max} A\} \leq 1$.

***Soluzione E.** 251* Per ipotesi M è noetheriano e quindi finitamente generato, diciamo da $m_1, \dots, m_n$. Consideriamo l'omomorfismo $\varphi\colon A \longrightarrow M^n$ dato da $\varphi(a) = (am_1, \dots, am_n)$ e proviamo che $\operatorname{Ker}\varphi = I$. Sia $a \in \operatorname{Ker}\varphi$; allora $am_i = 0$ per ogni $i = 1, \dots, n$ e quindi per ogni $m = \sum_i b_i m_i \in M$ si ha che $am = \sum_i b_i(am_i) = 0$ e $a \in I$. L'altra inclusione è ovvia.
Da questo segue che $A/I \simeq \operatorname{Im}\varphi \subseteq M^n$ è isomorfo ad un sottomodulo di M^n, che è un A-modulo noetheriano, ed è noetheriano come A-modulo e quindi anche come A/I-modulo.

***Soluzione E.** 252* 1. Supponiamo che $I + J \subsetneq A$; allora esiste un ideale massimale $\mathfrak{m}$ tale che $I, J \subseteq I + J \subseteq \mathfrak{m}$, che è contro l'ipotesi.

2. Dato che $IJ \subseteq I, J$, allora IJ è contenuto in ogni ideale primo di A, e quindi nel nilradicale $\mathcal{N}(A)$. Dato che A è noetheriano, l'ideale $\mathcal{N}(A)$ è nilpotente per il primo teorema di finitezza; esiste pertanto $n \in N$ tale che $(IJ)^n \subseteq \mathcal{N}(A)^n = 0$, come richiesto.

***Soluzione E.** 253* Ricordiamo innanzitutto che, per ogni A-modulo M, $\mu(M) = \dim_K(M \otimes_A K) = \dim_K M/\mathfrak{m}M$.

1. Siano $g_1, \dots, g_n$ un insieme minimale di generatori di I, ove $n = \mu(I) > 1$ per ipotesi. Allora I^2 è generato da tutti i prodotti $g_i g_j$, che sono $\frac{n(n+1)}{2} < n^2$; ne segue che $\mu(I^2) < n^2$, come richiesto.

2. Dato che ogni ideale J di A è piatto, tensorizzando per J la successione esatta $0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0$ si ottiene la successione esatta $0 \longrightarrow I \otimes J \longrightarrow J \longrightarrow J/IJ \longrightarrow 0$. Considerando allora il diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I \otimes J & \longrightarrow & J & \longrightarrow & J/IJ & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & IJ & \longrightarrow & J & \longrightarrow & J/IJ & \longrightarrow & 0, \end{array}$$

ove β e γ sono isomorfismi, dal lemma del serpente, o direttamente da **T.**104, deduciamo che $I \otimes J \simeq IJ$. Sia ora $J = I$; da **E.**188 discende che $\mu(I)^2 = \mu(I \otimes I) = \mu(I^2)$; di conseguenza, il punto precedente implica che $\mu(I) \leq 1$ per ogni I, cioè A è PIR.

Resta da provare che A è un dominio: siano $a, b \in A$ tali che $ab = 0$; allora $(a)(b) = (a) \otimes (b) = 0$, ed essendo A locale, si deduce da **E.**189 che $(a) = 0$ oppure $(b) = 0$, come volevamo.

Soluzione E. *254* 1. Dato che A è noetheriano, $\sqrt{I} = \bigcap_{i=1}^{m} \mathfrak{p}_i$, $\sqrt{J} = \bigcap_{j=1}^{n} \mathfrak{q}_j$ con $\mathfrak{p}_i \in \operatorname{Min} I$ e $\mathfrak{q}_\mathfrak{j} \in \operatorname{Min} J$, cf. **T.**159.2.
Dunque se I e J hanno gli stessi primi minimali, sicuramente hanno anche lo stesso radicale.

Viceversa, sia $\mathfrak{p}$ un primo minimale di I. Allora, $\bigcap_{j=1}^{n} \mathfrak{q}_j = \sqrt{I} \subseteq \mathfrak{p}$ e quindi esiste un ideale $\mathfrak{q}_\mathfrak{i}$ tale che $\mathfrak{q}_i \subseteq \mathfrak{p}$, cf. **T**12.2. Per lo stesso motivo, esiste $\mathfrak{p}_j$ tale che $\mathfrak{p}_j \subseteq \mathfrak{q}_i \subseteq \mathfrak{p}$; allora, per la minimalità di $\mathfrak{p}$, segue che $\mathfrak{p} = \mathfrak{q}_i$. In questo modo abbiamo mostrato che i primi minimali di I sono primi minimali di J. Scambiando i ruoli di I e J otteniamo la tesi.

2. Segue dal punto precedente e dalle definizioni di altezza e dimensione, osservando che, per ogni ideale I si ha che $\operatorname{ht} I = \min\{\operatorname{ht} \mathfrak{p} : \mathfrak{p} \in \operatorname{Min} I\}$ e che le catene di primi di A/I che contribuiscono al calcolo della dimensione di A/I corrispondono effettivamente alle catene di primi di A che iniziano con i primi minimali di I.

Soluzione E. *255* Sia $\bigcap_{i=1}^{n} \mathfrak{q}_i$ una decomposizione primaria minimale di $\operatorname{Ann} M$. Dato che $\operatorname{Ann} M$ è zero dimensionale, per ogni i abbiamo che $\mathfrak{m}_i = \sqrt{\mathfrak{q}_i}$ è un ideale massimale ed esiste s_i tale che $\mathfrak{m}^{s_i} \subseteq \mathfrak{q}_i$ per il primo teorema di finitezza, cf. **T.**153; per ogni i scegliamo s_i minimo rispetto a questa proprietà.
Sia ora $J = \mathfrak{m}_1^{s_1 - 1} \cap \bigcap_{i=2}^{n} \mathfrak{m}_i{}^{s_i}$; per costruzione $J \not\subset \operatorname{Ann} M$; dunque $0 \neq JM \subseteq M$ e $\operatorname{Ann}(JM) = \mathfrak{m}_1$. Da questo segue che se $0 \neq m \in JM$, allora il sottomodulo $\langle m \rangle \subseteq M$ è semplice: infatti l'omomorfismo da A in M definito da $1 \mapsto m$ è surgettivo su $\langle m \rangle$ e il suo nucleo è l'ideale proprio $\operatorname{Ann} m \supseteq \operatorname{Ann} M = \mathfrak{m}_1$; la conclusione segue allora da **E.**123.1.

Soluzione E. *256* Sia $\mathfrak{p} \in \operatorname{Min} A$ un primo minimale e consideriamo la decomposizione del nilradicale di A come intersezione finita di primi minimali, cf. **E.**68 e **T.**159.1, $\mathcal{N}(A) = \sqrt{(0)} = \mathfrak{p} \cap \bigcap_i \mathfrak{p}_i$.
Per la minimalità degli ideali della decomposizione, possiamo scegliere $b \in \bigcap_i \mathfrak{p}_i$ tale che $b \notin \mathfrak{p}$; allora b non è nilpotente ed è tale che $b\mathfrak{p} \subset \mathcal{N}(A)$. Quindi esiste $n \in \mathbb{N}$ tale che $(b\mathfrak{p})^n = (0)$, e pertanto $a = b^n$ è l'elemento cercato.

Viceversa, se esiste $a \in A \setminus \mathcal{N}(A)$ tale che $a\mathfrak{p}^n = 0$, allora $a^n\mathfrak{p}^n = 0$ e quindi $a\mathfrak{p} \subseteq \mathcal{N}(A)$. Se $\mathcal{N}(A) = \bigcap_i \mathfrak{p}_i$, con $\mathfrak{p}_i$ primi minimali di A, dato che $a \notin \mathcal{N}(A)$ esiste $\mathfrak{p}_j$ tale che $a \notin \mathfrak{p}_j$ e quindi $\mathfrak{p} \subset \mathfrak{p}_j$, poiché $\mathfrak{p}_j$ è primo. Da questo e dalla minimalità di $\mathfrak{p}_j$ segue che $\mathfrak{p} = \mathfrak{p}_j$ è un primo minimale, come volevamo.

Soluzione E. *257* Sia Q un ideale radicale contenuto in J e di dimensione zero; allora $Q = \sqrt{Q} = \bigcap_i \mathfrak{m}_i$, è intersezione finita di ideali $\mathfrak{m}_i$ massimali distinti, dunque

$$J = (\bigcap_i \mathfrak{m}_i) + J = (\prod_i \mathfrak{m}_i) + J = \prod_i (\mathfrak{m}_i + J) = \bigcap_i (\mathfrak{m}_i + J)\,.$$

Dal momento che l'ideale $\mathfrak{m}_i + J$ è uguale a $\mathfrak{m}_i$ oppure a (1) a seconda che $J \subseteq \mathfrak{m}_i$ oppure no, dalla precedente uguaglianza otteniamo che $J = (1)$ se $\mathfrak{m}_i + J = (1)$ per ogni i; altrimenti avremo che $J = \bigcap_{\{i\,:\,J\subseteq\mathfrak{m}_i\}} \mathfrak{m}_i$, e dunque J è radicale.

Dato che A/J è isomorfo ad un quoziente di A/Q, se J è radicale allora è 0 dimensionale.

Soluzione E. *258* È sufficiente trovare una decomposizione del radicale di I, che è l'ideale $(xzt, yt,\ xyzt, xz) = (yt, xz)$. Si ha $\sqrt{I} = (x, y) \cap (y, z) \cap (x, t) \cap (z, t)$; pertanto $\operatorname{Min} I = \{(x, y),\ (y, z),\ (x, t),\ (z, t)\}$.

Soluzione E. *259* 1. Osserviamo subito che $I = (x^2z, x^2y^4t + x^2y^3, xt^2)$ e la base di Gröbner ridotta di I rispetto all'ordinamento lessicografico con $x > y > z > t$ è $\{x^2z, x^2y^3, xt^2\}$, quindi I è monomiale.
2. Usando più volte **T.**33.1, troviamo $I = (x) \cap (x^2, t^2) \cap (x^2, z, t^2) \cap (y^3, z, t^2)$; dunque $(x) \cap (x^2, t^2) \cap (y^3, z, t^2)$ è una decomposizione primaria minimale di I, con $\operatorname{Ass} I = \{(x), (x, t), (y, z, t)\}$ e $\operatorname{Min} I = \{(x), (y, z, t)\}$.

3. Dato che i divisori di zero e i nilpotenti sono dati rispettivamente dall'unione dei primi associati a (0) e dall'intersezione dei primi minimali in A/I, cf. **T.**159.2, per quanto detto sopra avremo

$$\mathcal{D}(A/I) = (\overline{x}, \overline{t}) \cup (\overline{y}, \overline{z}, \overline{t}) \quad \text{e} \quad \mathcal{N}(A/I) = (\overline{y}, \overline{z}, \overline{t}) \cap (\overline{x}) = (\overline{xy}, \overline{xz}, \overline{xt}).$$

Soluzione E. *260* 1. Si ha che $(x^5 - 3x^2) = (x^2) \cap (x^3 - 3)$ e quindi i primi associati a zero in $\mathbb{Q}[x]/(x^5 - 3x^2)$ sono $(\overline{x})$ e $\left(\overline{x^3 - 3}\right)$, che sono minimali. Gli ideali primi di A sono

$$\mathfrak{p}_1 = (\overline{x}) \oplus (\overline{1}), \ \mathfrak{p}_2 = \left(\overline{x^3 - 3}\right) \oplus (\overline{1}), \ \mathfrak{p}_3 = (\overline{1}) \oplus (\overline{2}) \text{ e } \mathfrak{p}_4 = (\overline{1}) \oplus (\overline{3}),$$

e sono tutti primi associati a 0_A (perché?).
Dunque $\mathcal{N}(A) = \bigcap_i \mathfrak{p}_i = \left(\overline{x^4 - 3x}\right) \oplus (\overline{6})$ e $\mathcal{D}(A) = \bigcup_{i=1}^4 \mathfrak{p}_i$, per **T.**159.2.
2. Per $i = 1, \ldots, 4$ siano $\mathfrak{p}_i = \mathfrak{q}_i \oplus \mathfrak{t}_i$ e $S_i = A \setminus \mathfrak{p}_i$.
In $S_1^{-1}A$ ogni elemento del tipo $(\overline{1}, \overline{\beta})$ è invertibile. Dunque

$$\begin{aligned} S_1^{-1}A &\simeq (\mathbb{Q}[x]/(x^5 - 3x^2))_{\mathfrak{q}_1} \oplus 0 \\ &\simeq (\mathbb{Q}[x]/(x^2))_{\mathfrak{q}_1} \oplus (\mathbb{Q}[x]/(x^3 - 3))_{\mathfrak{q}_1} \simeq (\mathbb{Q}[x]/(x^2))_{(x)}. \end{aligned}$$

In particolare $S_1^{-1}A$ contiene l'elemento nilpotente non banale x e quindi non è un dominio.
Analogamente si osserva che

$$S_2^{-1}A \simeq (\mathbb{Q}[x]/(x^5 - 3x^2))_{\mathfrak{q}_2} \oplus 0 \simeq \big(\mathbb{Q}[x]/(x^3 - 3)\big)_{(x^3-3)}$$

è il campo dei quozienti di $\mathbb{Q}[x]/(x^3 - 3)$.
Infine per $i = 3, 4$ si ottiene che

$$S_i^{-1}A \simeq 0 \oplus (\mathbb{Z}/(12))_{\mathfrak{t}_i} \simeq (\mathbb{Z}/(4))_{\mathfrak{t}_i} \oplus (\mathbb{Z}/(3))_{\mathfrak{t}_i}$$

per cui $S_3^{-1}A \simeq (\mathbb{Z}/(4))_{(2)}$ e $S_4^{-1}A \simeq (\mathbb{Z}/(3))_{(3)}$ e solo il secondo è un dominio.

Soluzione E. *261* Siano $\mathfrak{m}_1 = (x + 2, y - 2, 3)$, $\mathfrak{m}_2 = (x + 2, y - 2, 5)$ e $\mathfrak{m}_3 = (x - 2, y + 2, 5)$ e osserviamo che tali ideali sono massimali e dunque a due a due comassimali.

1. Sia $\mathfrak{p}$ un ideale primo che contiene I. Allora $\mathfrak{p} \supseteq (I,3)$ oppure $\mathfrak{p} \supseteq (I,5)$. È facile vedere che $(I,3) = (y-2,(x+y)^3,3) = (y-2,(x+2)^3,3)$ e $(I,5) = (x^2-4,(x+y)^3,5)$.
Da ciò segue che $\sqrt{(I,3)} = \mathfrak{m}_1$; inoltre si verifica che

$$\begin{aligned}(I,5) &= (x+2,(x+y)^3,5) \cap (x-2,(x+y)^3,5)\\ &= (x+2,(y-2)^3,5) \cap (x-2,(y+2)^3,5),\end{aligned}$$

e gli ideali di questa intersezione sono primari, dato che i loro radicali sono $\mathfrak{m}_2$ e $\mathfrak{m}_3$. Segue allora che

$$\mathcal{D}(A) = \mathfrak{m}_1 \cup \mathfrak{m}_2 \cup \mathfrak{m}_3.$$

2. Dato che (9) e (5) sono comassimali, come sono a due a due comassimali gli ideali $\mathfrak{q}_1 = (I,9)$, $\mathfrak{q}_2 = (x+2,(y-2)^3,5)$ e $\mathfrak{q}_3 = (x-2,(y+2)^3,5)$, avremo che $I = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \mathfrak{q}_3$ e

$$\begin{aligned}A &\simeq A/\mathfrak{q}_1 \oplus A/\mathfrak{q}_2 \oplus A/\mathfrak{q}_3\\ &\simeq \mathbb{Z}[x,y]/\mathfrak{q}_1 \oplus \mathbb{Z}[x,y]/\mathfrak{q}_2 \oplus \mathbb{Z}[x,y]/\mathfrak{q}_3\\ &\simeq \mathbb{Z}[x,y]/(I,9) \oplus \mathbb{Z}/(5)[y]/(y-2)^3 \oplus \mathbb{Z}/(5)[y]/(y+2)^3.\end{aligned}$$

Notiamo che $A_{\mathfrak{m}_i} \simeq \bigoplus_{j=1}^{3} (A/\mathfrak{q}_j)_{\mathfrak{m}_i}$ e che $(A/\mathfrak{q}_j)_{\mathfrak{m}_i} = 0$ per ogni $i \neq j$ perché $\mathfrak{q}_j \not\subseteq \mathfrak{m}_i$. Dunque per ogni $i = 1,2,3$ si ha $(A/\mathfrak{q}_i)_{\mathfrak{m}_i} \simeq A_{\mathfrak{m}_i}$ e nessuno è un dominio perché tutti contengono dei nilpotenti. In conclusione $A_{\mathfrak{p}}$ non è un dominio per ogni $\mathfrak{p} \in \operatorname{Spec} A$.

Soluzione E. *262* Basta osservare che $N \subseteq M$ implica che $I \subseteq \operatorname{Ann} M \subseteq \operatorname{Ann} N$ e che N è un A-sottomodulo se e solo se N è un A/I-sottomodulo.

Soluzione E. *263* Consideriamo la successione di A-moduli $\operatorname{Im} u \supseteq \operatorname{Im} u^2 \supseteq \cdots \supseteq \operatorname{Im} u^n \supseteq \cdots$. Dato che M è artiniano, la catena è stazionaria ed esiste un intero k tale che $\operatorname{Im} u^k = \operatorname{Im} u^{k+1}$. Allora, per ogni $m \in M$, esiste $n \in M$ tale che $u^k(m) = u^{k+1}(n)$ ossia $u^k(m - u(n)) = 0$. Dall'iniettività di u, e quindi da quella di u^k, segue la tesi.

Soluzione E. *264* 1. Sia $a \in A \setminus A^*$ e dimostriamo che a è un divisore di zero. Consideriamo la catena $(a) \supseteq (a^2) \supseteq \cdots$; per d.c.c. esiste un intero k

tale che $(a^k) = (a^{k+1})$, e da ciò segue che esiste $b \in A$ tale che $a^k(ab-1) = 0$. Ora, dato che a non è invertibile, $ab - 1 \neq 0$, dunque a^k, e di conseguenza a, è zero divisore.

2. Sia $(A, \mathfrak{m})$ locale, e consideriamo i due casi $S \cap \mathfrak{m} \neq \emptyset$ e $S \cap \mathfrak{m} = \emptyset$, tenendo a mente che, per la prima parte dell'esercizio, ogni elemento di A è un'unità oppure un divisore di zero.
Se S contiene un elemento di $\mathfrak{m}$, che è il nilradicale di A, poiché A è artiniano, cf. **T.**166.1 e 3, allora $0 \in S$ e $S^{-1}A = 0$.
Se invece $S \cap \mathfrak{m} = \emptyset$, allora ogni elemento di S è un'unità e quindi $S^{-1}A = A$.

In entrambi i casi σ_S è ovviamente surgettiva.

Soluzione E. *265* Dimostriamo l'asserto per induzione su n. Se $n = 1$ e $\mathfrak{m}_1 M = 0$, allora $\mathfrak{m}_1 \subseteq \operatorname{Ann} M$ e M è un $A/\mathfrak{m}_1$-modulo, quindi M è uno spazio vettoriale che, per **T.**169, come $(A/\mathfrak{m}_1)$-modulo è noetheriano se e solo se artiniano; la conclusione discende allora da **T.**152.6 e **E.**262.

Sia ora $n > 1$ e consideriamo la successione esatta $0 \longrightarrow \mathfrak{m}_n M \longrightarrow M \longrightarrow M/\mathfrak{m}_n M \longrightarrow 0$. Dall'ipotesi induttiva segue che $M/\mathfrak{m}_n M$ è noetheriano se e solo se artiniano; inoltre, dato che $\mathfrak{m}_1 \cdots \mathfrak{m}_{n-1} \subseteq \operatorname{Ann}(\mathfrak{m}_n M)$, anche $\mathfrak{m}_n M$ è noetheriano se e solo se artiniano. Dato che la successione è esatta, la tesi segue allora da **T.**152.2 e **T.**165.

16.8 Soluzioni del capitolo 15

Soluzione E. *266* Vero. Un elemento $a \in A$ non è divisore di zero in A/I se e solo se $b \in A$ tale che $ab \equiv 0 \mod I$ implica $b \equiv 0 \mod I$, cioè $b \in A$ tale che $ab \in I$ implica $b \in I$. Dunque $b \in I : a$ implica $b \in I$ e quindi, dato che $I \subseteq (I : a)$, abbiamo dimostrato la tesi.

Soluzione E. *267* Vero. Basta osservare che, se $p \in Q[x]$, esiste $0 \neq d \in A$ tale che $dp = p' \in A[x]$; quindi se $p, q \in Q[x]$, $p \otimes q = \frac{p'}{d} \otimes q\frac{d}{d} = 1 \otimes pq$. L'omomorfismo dato dall'assegnazione $p \otimes q \longrightarrow pq$, indotto dal prodotto $(p(x), q(x)) \mapsto p(x)q(x)$ in $Q[x]$ che è $A[x]$-bilineare, fornisce l'isomorfismo desiderato.

Soluzione E. *268* Vero. Dato che φ è un omomorfismo surgettivo, per il primo teorema di omomorfismo $B \simeq A/\operatorname{Ker}\varphi$; quindi $\operatorname{Ker}\varphi$ è un ideale primo. Se $\operatorname{Ker}\varphi = 0$ abbiamo un isomorfismo, altrimenti $\operatorname{Ker}\varphi$ è un primo non nullo di un anello PID, ed è dunque massimale, cf. **T.**24 ed **E.**56; in questo caso B è un campo.

Soluzione E. *269* Le prime due uguaglianze sono vere, cf. **T.**6.7 e **E.**24.2, mentre la terza è falsa. Per esempio consideriamo in $\mathbb{Q}[x,y]$ gli ideali $I = (x^2+y)$ e $J = (x^2-y)$. Si ha $\sqrt{I} = I$ e $\sqrt{J} = J$ così $\sqrt{I}+\sqrt{J} = (x^2, y)$ mentre $\sqrt{I+J} = (x,y)$.

Soluzione E. *270* Falso. Ad esempio $\mathcal{N}(\mathbb{Z}/(6)) = 0$ ma (6) non è primo in $\mathbb{Z}$.

Soluzione E. *271* Vero. Il modulo dato è isomorfo a $\mathbb{Q}[x]/(x^2-1, x^2+1)$ per **E.**183, e quest'ultimo è chiaramente nullo.

Soluzione E. *272* Vero. A è quoziente di $A[X]$ ed è dunque noetheriano per **T.**152.2.

Soluzione E. *273* Vero. Ricordiamo che se $\operatorname{Lt}(I)$ è primo allora un insieme minimale di generatori è dato da un sottoinsieme delle indeterminate per **T.**34.1. Siano G una base di Gröbner di I e $f, g \in K[X]$ tali che $fg \in I$; se per assurdo $f, g \notin I$ allora per **T.**36 $f \xrightarrow{G}_* r$ e $g \xrightarrow{G}_* s$ con $r, s \neq 0$ e nessuna delle indeterminate di $G(\operatorname{Lt}(I))$ divide i monomi di r e s. Lo stesso vale per ogni monomio di rs e dunque $0 \neq rs \notin I$; pertanto $fg \notin I$, che è contro l'ipotesi.

Soluzione E. *274* Vero. Sia $b \in \sqrt{I : J}$, allora esiste n tale che $b^n J \subseteq I$. Dobbiamo provare che se $c \in \sqrt{J}$ allora $bc \in \sqrt{I}$. Dato che $c^m \in J$ per qualche m, avremo che $b^n c^m \in I$. Se $n \geq m$ moltiplicando per c^{n-m} si ottiene $(bc)^n \in I$, da cui segue $bc \in \sqrt{I}$; se $n < m$ concludiamo in maniera analoga.

Soluzione E. *275* Vero. Dato che I, J sono comassimali e $I \cap J = 0$ dal teorema cinese del resto si ha $A \simeq A/I \oplus A/J$ ossia A è somma diretta di campi; a questo punto è immediato concludere che A è artiniano, ad esempio osservando che certamente in A vale d.c.c.

Soluzione E. *276* Falso. Consideriamo gli $\mathbb{Z}$-moduli $M = \mathbb{Z}/(4)$ e $N = \mathbb{Z}$; allora N non ha torsione e M è di torsione; inoltre $T(M \otimes_{\mathbb{Z}} N) = T(M) = M = \mathbb{Z}/(4)$. Invece $T(M) \otimes T(N) = \mathbb{Z}/(4) \otimes 0 = 0$.

Soluzione E. *277* Vero. "$\Longrightarrow$": se $\gcd(f, g) = 1$ i polinomi $p(x) = \mathrm{Ris}_y(f, g)$ e $q(y) = \mathrm{Ris}_x(f, g)$ sono diversi da zero e $p(x), q(y) \in I$, cf. **T.**61; dunque I verifica **T.**71.2 e $\mathbf{V}_{\mathbb{C}}(I)$ è finita.

"$\Longleftarrow$": sia $h = h(x, y) = \gcd(f, g) \neq 1$ e $f = f_1 h$ e $g = g_1 h$, per certi $f_1, g_1 \in \mathbb{C}[x, y]$; allora $\mathbf{V}_{\mathbb{C}}(I) = \mathbf{V}(h) \cup \mathbf{V}(f_1, g_1)$ per **T.**55.6 e basta provare che $\mathbf{V}_{\mathbb{C}}(h)$ è infinita. Questo segue da **T.**71, dato che (h) ovviamente non verifica la condizione 2.

Soluzione E. *278* Vero. Si consideri l'omomorfismo $\varphi\colon A^n \longrightarrow (A/I)^n$ definito da $\varphi(a_1, \ldots, a_n) = (\overline{a_1}, \ldots, \overline{a_n})$, che è banalmente surgettivo e il cui nucleo è IA^n.

Soluzione E. *279* Falso. Siano $K = \mathbb{Q}$ e $p(x) = x^2 + 1$; allora $p(x)$ è irriducibile in $K[x]$, ma l'ideale $(x^2 + 1, y^2 + 1) = (x^2 - y^2, y^2 + 1) = (x - y, y^2 + 1) \cap (x + y, y^2 + 1)$ è intersezione di primi distinti, che lo contengono propriamente.

Soluzione E. *280* Falso. Sia $A = \mathbb{Z}/(4)$ e siano $M = A$ e $N = (2)A \simeq \mathbb{Z}/(2)$. Allora M è libero, quindi proiettivo, ma N non può essere proiettivo perché in caso contrario le successione $0 \longrightarrow \mathbb{Z}/(2) \xrightarrow{\cdot 2} \mathbb{Z}/(4) \longrightarrow N \longrightarrow 0$ spezzerebbe, mentre $\mathbb{Z}/(4) \not\simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.

Soluzione E. *281* Vero. Sia I massimale. Se $J \not\subseteq I$ esiste $0 \neq a \in J \setminus I$ e quindi $A = I + (a) \subseteq I + J$.

Viceversa, consideriamo A/I e proviamo che ogni elemento diverso da zero è invertibile. Sia $0 \neq \overline{a} \in A/I$; dato che $(a) \not\subseteq I$, per ipotesi $I + (a) = A$ e quindi esistono $i \in I$ e $b \in A$ tali che $i + ba = 1$, da cui segue che $\overline{a}$ è invertibile.

Soluzione E. *282* Vero. $A/\mathfrak{p}$ è un dominio finito, dunque è un campo, cf. **T.** 1.

Soluzione E. *283* 1. Vero. Basta provare che se $I + J = A$ allora per ogni $n \in \mathbb{N}$ $I^n + J^n = A$, dato che l'altra implicazione è immediata. Siano $i \in I$ e $j \in J$ tali che $i + j = 1$, allora per ogni $n \in \mathbb{N}$ si ha che

$$1 = (i+j)^{2n-1} = \sum_{k=0}^{n-1} \binom{2n-1}{k} i^{2n-1-k} j^k + \sum_{k=n}^{2n-1} \binom{2n-1}{k} i^{2n-1-k} j^k$$

appartiene a $I^n + J^n$.

2. Vero. Sia $a \in \sqrt{I : J}$; allora esiste m tale che $a^m j \in I$ per ogni $j \in J$; quindi $(aj)^m \in I$ da cui segue che $aj \in \sqrt{I}$ e infine che $a \in \sqrt{I} : J$.

3. Falso. Basta considerare gli ideali $I = (8)$ e $J = (6)$ in $\mathbb{Z}$; si ha infatti $\sqrt{I} : J = (2) : (6) = \mathbb{Z}$, mentre $\sqrt{I : J} = \sqrt{(4)} = (2)$, cf. **E.**17.4.

4. Falso. Consideriamo gli ideali $I = (12)$ e $J = (8)$ in $\mathbb{Z}$; si ha $I : J = (3)$, mentre $I : \sqrt{J} = (12) : (2) = (6)$.

Soluzione E. *284* Falso. Fissiamo l'ordinamento lex con $x > y$; i generatori dati di I formano già una base di Gröbner, mentre una base di Gröbner di J è data da $\{x, y^2 + 1\}$. Quindi gli anelli $A_1 = \mathbb{Q}[x,y]/I$ e $A_2 = \mathbb{Q}[x,y]/J$ sono $\mathbb{Q}$-spazi vettoriali con basi $\{1, x, y, xy\}$ e $\{1, y\}$ rispettivamente e non possono dunque essere isomorfi come anelli. Ricordiamo che un omomorfismo di anelli φ verifica $\varphi(1) = 1$ e quindi nel nostro caso $\varphi(a) = a$ per ogni $a \in \mathbb{Q}$. Supponiamo allora che esista un isomorfismo di anelli $\varphi\colon A_1 \longrightarrow A_2$ con $v_1 = \varphi(1), v_2 = \varphi(x), v_3 = \varphi(y), v_4 = \varphi(xy) \in A_2$. Questi elementi sono linearmente dipendenti su $\mathbb{Q}$ e quindi esistono $a_1, \ldots, a_4 \in \mathbb{Q}$ non tutti nulli tali che $\varphi(a_1 + a_2 x + a_3 y + a_4 xy) = a_1 v_1 + a_2 v_2 + a_3 v_3 + a_4 v_4 = 0$; da ciò si deduce che $1, x, y, xy$ sono linearmente dipendenti in A_1, che è la contraddizione cercata.

Soluzione E. *285* Vero. Se $I = I^{ec}$ e I^e è primo, allora I è primo per **T.**17. Per il viceversa, osserviamo che $K(x)[y] = S^{-1}(K[x,y])$, con $S = K[x] \setminus 0$ e che esiste un corrispondenza biunivoca fra i primi I di $K[x,y]$ tali che $I \cap S = \emptyset$ e i primi di $K(x)[y]$ data da $I \longrightarrow I^e$, cf. **T.**139.

Soluzione E. *286* Vero. Basta provare che $\sqrt{(f,g)} \subseteq \sqrt{(f^2, g^3)}$, dato che l'altro contenimento è ovvio. Sia $h \in \sqrt{(f,g)}$ allora esiste n tale che $h^n = af + bg$ e quindi per $m = 4n$, $h^m = (af + bg)^4 \in (f^2, g^3)$.

Soluzione E. *287* Vero. Dato che A è locale si ha $A^* = A \setminus \mathfrak{m}$; inoltre $A/\mathfrak{m}$ è un campo. Quindi $\pi(a) \in (A/\mathfrak{m})^*$ se e solo se $a \notin \mathfrak{m}$, i.e. se e solo se $a \in A^*$.

Soluzione E. *288* Vero. L'ideale $\mathfrak{m}$ è un A-modulo finitamente generato; inoltre per ipotesi $(a_1, \ldots, a_n) + \mathfrak{m}^2 = \mathfrak{m}$. Poiché A è locale, dalla III forma del lemma di Nakayama **T.**95 segue che $(a_1, \ldots, a_n) = \mathfrak{m}$.

Soluzione E. *289* Falso. Si consideri $A = K[x_n \colon n \in \mathbb{N}]$; allora A è un dominio e quindi $A \subseteq Q(A)$, che è un campo, e dunque è noetheriano.

Soluzione E. *290* Chiaramente $B \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(9)$, $M_1 \simeq \mathbb{Z}/(9)$ e $M_2 \simeq \mathbb{Z}/(6)$. Pertanto la prima affermazione è vera, in quanto M_1 è addendo diretto di B e quindi è proiettivo, mentre le altre sono false: M_2 non è addendo diretto di B^n per nessun n, pertanto non è proiettivo e tantomeno libero; infine $\overline{9}M_1 = 0$, dunque M_1 certamente non è libero.

Soluzione E. *291* Falso. Dato che è annullato da x, il campo K è un $K[x]$-modulo di torsione, quindi non può essere addendo diretto del modulo libero $K[x]$.

Soluzione E. *292* Vero. Dato che M è finitamente generato, si ha che $\mathfrak{p} \in \operatorname{Supp} M$ se e solo se $\operatorname{Ann} M \subseteq \mathfrak{p}$, per **E.**228.1. Inoltre, $M = \mathbb{Z}/(12) \otimes_{\mathbb{Z}} \mathbb{Z}/(30) \simeq \mathbb{Z}/(6)$ quindi il suo annullatore è (6) e si ha $\operatorname{Supp} M = \{(2), (3)\}$.

Soluzione E. *293* Falso. A è noetheriano quindi $\mathcal{D}(A)$ è uguale all' unione dei primi associati a (0), cf. **T.**159.2, quindi $\mathcal{D}(A) = (\overline{x}) \cup (\overline{y})$ e l'elemento $a = \overline{x} + \overline{y} \in A$ non appartiene a $\mathcal{D}(A)$ e nemmeno a K.

Soluzione E. *294* Vero. K è algebricamente chiuso e (f) è primo per **T.**26, dato che f è irriducibile; quindi per la forma forte del Nullstellensatz e **T.**55.4 si ha che $\sqrt{(g)} = \mathbf{I}(\mathbf{V}(g)) \subseteq \mathbf{I}(\mathbf{V}(f)) = (f)$, da cui discende la tesi dato che $K[X]$ è UFD.

Soluzione E. *295* Vero. Dato che Q è proiettivo, la successione esatta

$$0 \longrightarrow \operatorname{Ker} \varphi \longrightarrow P \longrightarrow Q \longrightarrow 0$$

spezza e quindi $P \simeq \operatorname{Ker} \varphi \oplus Q$; allora $\operatorname{Ker} \varphi$ è addendo diretto di un modulo proiettivo e quindi è proiettivo, cf **T.**107.

***Soluzione E.** 296* Falso. Si ha $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}[x]/(f) \simeq \mathbb{C}[x]/(f)$, cf. la dimostrazione di **E.**191.2. Dato che f è libero da quadrati in $\mathbb{C}[x]$, avremo $f(x) = \prod_{i=1}^{k}(x - \alpha_i)$, con $\alpha_i \neq \alpha_j$ se $i \neq j$, e per il teorema cinese del resto $\mathbb{C}[x]/(f) \simeq \prod_{i=1}^{k} \mathbb{C}[x]/(x - \alpha_i) \simeq \mathbb{C}^k$; pertanto non esistono nilpotenti diversi da zero.

***Soluzione E.** 297* Vero. Se M è proiettivo e finitamente generato allora M è addendo diretto di A^n per qualche intero n, diciamo $A^n \simeq M \oplus N$. Dato che $M \oplus N$ è finitamente generato, anche N lo è, poiché suo addendo diretto. Sia allora $\{r_1, \dots, r_m\}$ un insieme di generatori di N, possiamo costruire una successione della forma cercata nel seguente modo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & N \oplus M \simeq A^n & \longrightarrow & M & \longrightarrow & 0 \\ & & \uparrow & \nearrow & & & & & \\ & & e_i \mapsto r_i & & & & & & \\ & & A^m & & & & & & \end{array},$$

ed essa risulta esatta in M ed in A^n, come volevamo.
È chiaro che il viceversa vale per qualunque A-modulo.

***Soluzione E.** 298* Falso. Siano $A = \mathbb{Z} = M$ e $S = A \setminus \{0\}$; allora $S^{-1}M = \mathbb{Q}$ che non è finitamente generato come $\mathbb{Z}$-modulo.

***Soluzione E.** 299* Vero. Da **T.**127, punti 2, 3 e 5 segue che

$$M/\mathfrak{m}M \otimes M/\mathfrak{n}M \simeq (A/\mathfrak{m} \otimes M) \otimes (A/\mathfrak{n} \otimes M) \simeq (A/\mathfrak{m} + \mathfrak{n}) \otimes M \otimes M$$

che è nullo dato che $\mathfrak{m} + \mathfrak{n} = A$.

***Soluzione E.** 300* Vero. Da **T.**148.3 segue che $V = \{2^n 3^m\}_{n,m \in \mathbb{N}}$ è il saturato sia di S che di T. Allora $S^{-1}\mathbb{Z} \simeq V^{-1}\mathbb{Z} \simeq T^{-1}\mathbb{Z}$ per **T.**148.6.

***Soluzione E.** 301* Falso. Consideriamo l'ideale $(x^2-1) = (x+1) \cap (x-1) \subset K[x]$; esso è intersezione di due primi distinti e quindi non è primario, mentre $\mathrm{Lt}(I) = (x^2)$ è primario.

***Soluzione E.** 302* Vero. La matrice è già in forma diagonale, dunque $\operatorname{Coker} \varphi \simeq \mathbb{Q}[x]/(x(x-1)) \oplus \mathbb{Q}[x]/(x(x-1)^3)$, che ha dimensione 6.

Soluzione E. *303* Vero. Se A è un campo M è uno spazio vettoriale quindi è libero.

Viceversa, per ogni ideale $I \subset A$, l'A-modulo A/I deve essere libero quindi $I = \operatorname{Ann}(A/I) = 0$. Se non esistono ideali non banali in A, A deve essere un campo per **T.**2.1.

Soluzione E. *304* Vero. Sia per assurdo $0 \neq m \in T(M)$; allora $A \supsetneq \operatorname{Ann} m \neq 0$. Quindi esistono $0 \neq a \in A$ tale che $am = 0$ e $\mathfrak{m} \in \operatorname{Max} A$ tale che $\operatorname{Ann} m \subseteq \mathfrak{m}$; allora per ogni $b \in A \setminus \mathfrak{m}$ si ha $bm \neq 0$ e dunque $\frac{m}{1} \neq 0$ in $M_{\mathfrak{m}}$. Infine $a\frac{m}{1} = \frac{am}{1} = 0$, cioè $\frac{m}{1}$ è un elemento di torsione non banale di $M_{\mathfrak{m}}$, che è contro l'ipotesi.

Soluzione E. *305* Vero. Se M è libero di rango k allora $M \simeq A^k$ da cui $M_B = M \otimes_A B \simeq A^k \otimes_A B \simeq B^k$ per **T.**127.1 e 3.

Soluzione E. *306* Vero. Osserviamo che se $f \in I$ la relazione è banalmente vera, infatti in questo caso $IA_f \cap A = A$. Supponiamo quindi che $f \notin I$. Dato che $I \subseteq (I, f)$ e, per **T.**17.3, $I \subseteq IA_f \cap A$ l'inclusione "$\subseteq$" è verificata.

Per dimostrare l'altra inclusione, sia $a \in \sqrt{IA_f \cap A} \cap \sqrt{(I, f)}$; allora esistono $n \in \mathbb{N}$, $i \in I$, $b \in A$ e $j \in IA_f \cap A$ tali che $a^n = j = i + bf$. Dal momento che $j \in IA_f \cap A$ esiste m tale che $f^m j \in I$ e da ciò segue che $bf^{m+1} = (j - i)f^m = f^m j - f^m i \in I$. Allora $a^{n(m+1)} = (i + bf)^{m+1} \in I$ e quindi $a \in \sqrt{I}$.

Soluzione E. *307* Vero. Sia $0 \neq a \in A$. La catena discendente di $(a) \supseteq (a^2) \supseteq \ldots \supseteq (a^n) \supseteq \ldots$ per ipotesi si stabilizza, quindi esiste k tale che $(a^k) = (a^{k+1})$. Allora esiste $b \in A$ tale che $a^k = ba^{k+1}$ e quindi, dato che A è un dominio, $1 = ba$, ossia a è invertibile.

Soluzione E. *308* Falso. Consideriamo $A = \mathbb{Z}_{(p)}$, con p primo: è un dominio perché lo è $\mathbb{Z}$. In A ogni ideale è esteso per **T.**138.2, dunque A è PID; infine A è locale per **T.**137 e $\mathcal{J}(A) = (p)A \neq 0$.

Soluzione E. *309* Vero. Consideriamo $\varphi\colon \mathbb{Q} \times \mathbb{R} \longrightarrow \mathbb{R}$ data da $\varphi(x, y) = xy$; φ è $\mathbb{Z}$-bilineare e quindi induce un unico omomorfismo di $\mathbb{Z}$-moduli $\tilde{\varphi}\colon \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{R} \longrightarrow \mathbb{R}$, $\tilde{\varphi}(x \otimes y) = xy$, che è ovviamente surgettivo.

Dato che $\frac{a}{b} \otimes_{\mathbb{Z}} y = \frac{a}{b} \otimes_{\mathbb{Z}} \frac{by}{b} = a \otimes_{\mathbb{Z}} \frac{y}{b} = 1 \otimes_{\mathbb{Z}} \frac{ay}{b}$, ogni elemento di $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{R}$ è della forma $1 \otimes y$ con $y \in \mathbb{R}$. Pertanto se $0 = \tilde{\varphi}(1 \otimes y) = y$, allora $y = 0$, ossia $\tilde{\varphi}$ è anche iniettivo.

Soluzione E. *310* Vero. Consideriamo l'A-modulo $N'/(N' \cap N)$ e localizziamo in un ideale $\mathfrak{m} \in \operatorname{Max} A$; utilizzando **T.**142 e **T.**143.2 otterremo $(N'/(N' \cap N))_{\mathfrak{m}} \simeq N'_{\mathfrak{m}}/(N' \cap N)_{\mathfrak{m}} \simeq N'_{\mathfrak{m}}/(N'_{\mathfrak{m}} \cap N_{\mathfrak{m}})$. Dato che per ipotesi $N'_{\mathfrak{m}} \subseteq N_{\mathfrak{m}}$ abbiamo mostrato che $(N'/(N' \cap N))_{\mathfrak{m}} = 0$ per ogni ideale massimale di A; la tesi segue immediatamente da **T.**145.

Soluzione E. *311* Falso. Si veda l'Esempio 6.2.1.

Soluzione E. *312* Vero. $A[x]/(x^2 - t)$ è un A-modulo libero con base $\{1, x\}$, quindi è piatto.

Soluzione E. *313* Falso. Consideriamo $\mathbb{Q}$, che è uno $\mathbb{Z}$-modulo non finitamente generato. È sicuramente privo di torsione e non è ciclico, ma, per ogni coppia di elementi $\frac{a}{b} \neq \frac{c}{d}$ di $\mathbb{Q}$, abbiamo una relazione non banale $bc\frac{a}{b} - ad\frac{c}{d} = 0$, quindi non è libero.

Soluzione E. *314* Vero. Da **T.**148.3 segue che S è il saturato di T; si conclude grazie a **T.**148.6.

Soluzione E. *315* Vero. La tesi è ovvia se uno dei due moduli è nullo; supponiamo allora $M \neq 0$ e $N \neq 0$. Ricordiamo inoltre che per **E.**189 la tesi è vera se A è locale.
Supponiamo allora che $J = \operatorname{Ann} M + \operatorname{Ann} N \subsetneq A$; esiste quindi un ideale massimale $\mathfrak{m} \subset A$ tale che $J \subseteq \mathfrak{m}$. Localizzando in $\mathfrak{m}$ otteniamo che $0 = (M \otimes_A N)_{\mathfrak{m}} \simeq M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} N_{\mathfrak{m}}$ e quindi o $M_{\mathfrak{m}} = 0$ oppure $N_{\mathfrak{m}} = 0$. Se $M_{\mathfrak{m}} = 0$, allora, dato che M è finitamente generato, esiste $s \notin \mathfrak{m}$ tale che $sM = 0$, cf. **E.**226, e questo è assurdo dato che $\operatorname{Ann} M \subseteq J \subseteq \mathfrak{m}$. Si conclude analogamente se $N_{\mathfrak{m}} = 0$.

Soluzione E. *316* Vero. Chiaramente $\mathfrak{m} \subseteq \operatorname{Ann}(M/\mathfrak{m}M)$; d'altro lato $\operatorname{Ann}(M/\mathfrak{m}M) \neq A$, perché in tal caso $M = \mathfrak{m}M$ e per il lemma di Nakayama M sarebbe 0, contro le ipotesi. Allora $\operatorname{Ann}(M/\mathfrak{m}M) = \mathfrak{m}$ e dunque $\mathcal{V}(\mathfrak{m}) = \{\mathfrak{m}\}$.

Soluzione E. *317* Vero. Si argomenta in maniera del tutto analoga a quanto fatto nella prima parte della dimostrazione di **E.**193.

Soluzione E. *318* Vero. È un caso particolare di quanto visto in **E.**310.

Soluzione E. *319* Vero. Si veda la dimostrazione di **E.**243.1.

Soluzione E. *320* Vero. Dato che A è libero su stesso allora ogni ideale $I \subset A$ è libero. Dal fatto che ogni ideale principale $I = (a)$ è libero, segue che A è un dominio. Inoltre se esiste un ideale non principale I, allora sia $\{a_h : h \in H\}$ un suo insieme di generatori; avremmo che $a_1 a_2 = a_2 a_1$, ovvero una relazione di dipendenza non banale, contraddicendo il fatto che I deve essere libero.

Soluzione E. *321* Vero. Basta considerare $B = A$ e prendere come $\mathfrak{p}$ l'ideale massimale di A.

Soluzione E. *322* Vero. Sia $A = \mathbb{Z}/(540)$; per **E.**5.1 basta osservare che $7 \in A^*$ e $30, 60, 90 \in \mathcal{N}(A)$.

Soluzione E. *323* Falso. L'ideale $(2x+1)$ è principale e massimale dato che $\mathbb{Z}_{(2)}[x]/(2x+1) \simeq \mathbb{Q}$. Per verificare l'esistenza di questo isomorfismo si può osservare che $\mathbb{Z}_{(2)}[x]/(2x+1) \simeq (\mathbb{Z}_{(2)})_2$, per **E.**210; cf. anche con la seconda parte della dimostrazione di **E.**236.

Soluzione E. *324* Falso. $M = (\mathbb{Z}/(15) \oplus \mathbb{Z}/(18))_{(3)} \simeq \mathbb{Z}/(3) \oplus \mathbb{Z}/(9)$ che non è ciclico.

Soluzione E. *325* Vero. La matrice delle relazioni è data da $\begin{pmatrix} 2 & 1 & 1 \\ -1 & 1 & a \\ 0 & 1 & 0 \end{pmatrix}$ che ha forma di Smith $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2a+1 \end{pmatrix}$ da cui segue che $M \simeq \mathbb{Z}/(2a+1)$. Se $a > 0$, $2a + 1 \neq \pm 1$, quindi per ogni n tale che $\gcd(2a+1, n) \neq 1$, $M \otimes_{\mathbb{Z}} \mathbb{Z}/(n) \neq 0$.

Soluzione E. *326* Falso. Consideriamo $I = (12) \subset \mathfrak{p} = (2) \subset \mathbb{Z}$; allora I non è primario, $\mathfrak{p}$ è primo e $I_{(2)} = (4)\mathbb{Z}_{(2)}$ è primario.

Soluzione E. *327* Vero. Sia $ax + by + c = 0$ l'equazione di ℓ . Allora per **T.**55.5 avremo $\mathcal{C} \cap \ell = \mathbf{V}(f, ax + by + c)$, quindi $\mathcal{C} \cap \ell = \mathbf{V}(f(x, -\frac{ax+c}{b}))$ se $b \neq 0$, oppure $\mathcal{C} \cap \ell = \mathbf{V}(f(-\frac{c}{a}, y))$. Dato che per ipotesi $\ell \not\subseteq \mathcal{C}$, in entrambi i casi la varietà che ci interessa è definita da un polinomio non nullo univariato di grado $\leq n$ e che quindi ha al più n radici; da ciò segue la tesi.

Soluzione E. *328* Vero. Per ogni $a \in A$ si ha $Q(A) \otimes A/(a) = 0$: infatti $\frac{b}{c} \otimes_A \overline{d} = \frac{ab}{ac} \otimes_A \overline{d} = \frac{b}{ac} \otimes_A a\overline{d} = 0$. Quindi da **T.**127, punti 1 e 4, segue che

$$Q(A) \otimes_A M \simeq (Q(A) \otimes_A A^n) \oplus \bigoplus_{i=1}^{k} (Q(A) \otimes_A A/(a_i^{n_i})) \simeq Q(A)^n.$$

Soluzione E. *329* Falso. Siano $A = \mathbb{Q}[x]_{(x)}$, $F = A^{\mathbb{N}}$ con base $\{e_i\}_{i\in\mathbb{N}}$ e $N \subset F$ il sottomodulo $N = \langle xe_0, xe_1 - e_0, xe_2 - e_1, \ldots, xe_{i+1} - e_i, \ldots\rangle$. Avremo allora che $\mathcal{J}(A) = (x)$, che ovviamente è finitamente generato. Consideriamo ora il modulo quoziente $M = F/N$: non è difficile verificare che $M \neq 0$ e che $xM = (\langle xe_i : i \in \mathbb{N}\rangle + N)/N = M$.

Si confronti l'enunciato con quello di **E.**133.

Riferimenti bibliografici

AL. W. W. Adams, P. Loustaunau. An Introduction to Gröbner bases. Memoirs of the American Mathematical Society, vol. 3, American Mathematical Soc., 1994.

AM. M. F. Atiyah, I. G. Macdonald. Introduction to Commutative Algebra. Addison-Wesley series in mathematics Avalon Publishing, 1994.

CLS. D. Cox, J. Little, D. O'Shea. Ideals, Varieties, and Algorithms. Undergraduate Texts in Mathematics. Springer Science & Business Media, 2007.

CE. H. Cartan, S. Eilenberg. Homological Algebra. Princeton mathematical series, vol. 19, 7.a ristampa, 1973.

E. D. Eisenbud. Commutative Algebra - with a view toward Algebraic Geometry. Graduate text in Mathematics **150**. Springer Science & Business Media, 1995.

L. S. Lang. Algebra. Graduate text in Mathematics **211**. Springer Science & Business Media, 2005.

M. Matsumura. Commutative ring theory. Cambridge University Press, 1989.

MRR. R. Mines, F. Richman, W. Ruitenburg. A Course in Constructive Algebra. Springer Science & Business Media, 2012.

R. M. Reid Undergraduate Commutative Algebra. London Mathematical Society, vol. 29, London Mathematical Society Student texts.

Indice analitico