Esercizi di Algebra Commutativa

Andrea Bandini, Patrizia Gianni, Enrico Sbarra

Indice

Prefazione

La scelta degli argomenti raccolti in questo libro rispecchia l'impostazione del corso di Algebra 2 del Dipartimento di Matematica dell'Università di Pisa, di cui siamo stati docenti nell'ultimo decennio. Il corso è rivolto agli studenti del terzo anno della laurea triennale e del primo anno della laurea magistrale, e fornisce una prima introduzione ai concetti fondativi dell'Algebra Commutativa, quali anelli, ideali, moduli, prodotto tensoriale, localizzazione e decomposizione primaria in anelli noetheriani. I prerequisiti richiesti sono pochi, ovvero una conoscenza di base dell'Aritmetica, della Teoria dei Gruppi abeliani e dell'Algebra Lineare.

Abbiamo selezionato circa 400 esercizi di vario grado di difficoltà per esemplificare i principali concetti dell'Algebra Commutativa e per facilitare un apprendimento graduale e motivato di argomenti che spesso risultano astratti e di difficile comprensione. Alcuni degli esercizi sono testi di esame, altri sono pensati per accompagnare le lezioni e le esercitazioni, inclusi quelli più classici che si trovano anche in molti dei libri presenti in bibliografia. Riteniamo che gli esercizi siano essenziali per raggiungere una vera comprensione della teoria, sia quelli teorici che quelli pratici, i quali aiutano a "toccare con mano" le definizioni e le proprietà degli oggetti astratti, a costruire esempi con cui verificarle e a chiarire i tanti concetti introdotti.

Esistono molti libri e manuali di Algebra Commutativa ma, nella maggior parte dei casi, si tratta di testi che prediligono un approccio teorico che può risultare ostico per chi affronta lo studio della materia per la prima volta. Il nostro approccio è costruttivo e pratico; abbiamo voluto esemplificare, quando possibile, i concetti teorici di base applicandoli allo studio dell'anello dei polinomi multivariati e dei moduli su domini a ideali principali (PID). Esistono algoritmi per la manipolazione di questi oggetti che permettono di costruire numerosi esempi; per questo motivo presentiamo anche alcuni metodi computazionali. La struttura dei moduli finitamente generati su un PID viene descritta attraverso la forma canonica di Smith delle matrici. La capacità di calcolare tale forma rende esplicita la struttura di un modulo finitamente generato, evidenziando il significato di forma canonica in un'applicazione concreta. Altrettanto importanti sono gli esempi che si possono costruire con i polinomi multivariati; lo strumento fondamentale che presentiamo in questo contesto è l'Algoritmo di Buchberger per il calcolo delle basi di Gröbner, che hanno naturali applicazioni nello studio

degli ideali, delle varietà e nella risoluzione di sistemi di equazioni polinomiali. Oggi le basi di Gröbner sono impiegate nelle aree più disparate quali Crittografia, Teoria dei codici, Computer Vision, Signal and Image Processing e Robotica, solo per citarne alcune; pensiamo pertanto che la conoscenza di questi metodi debba fare parte del bagaglio culturale di un laureato in Matematica dei nostri tempi.

A nostra conoscenza, gli argomenti proposti non si trovano raccolti in un unico testo; per questo motivo abbiamo deciso di presentare nella prima parte del libro le principali definizioni, le proprietà e i risultati necessari per la comprensione e lo svolgimento degli esercizi. Questa parte è stata pensata come un testo di riferimento e, per renderla di facile e rapida consultazione, abbiamo inserito solo le dimostrazioni che riteniamo più istruttive o che presentano tecniche e metodi fondamentali, e abbiamo raccolto le altre in un capitolo nella parte finale del libro. In questo modo speriamo anche di stimolare la curiosità del lettore e di guidarlo in uno studio più meditato e attivo del materiale, invitandolo a trovare da solo una dimostrazione, senza tuttavia fargli mancare il supporto di una risoluzione dettagliata.

La seconda parte contiene gli esercizi, suddivisi per capitoli corrispondenti alla teoria, e una sezione di esercizi "Vero o Falso?" in cui i vari argomenti non vengono invece separati; riteniamo che questi ultimi siano un valido test per verificare il livello di apprendimento e di comprensione raggiunto. Nella sezione finale includiamo alcuni esercizi di ricapitolazione.

La terza ed ultima parte contiene le dimostrazioni dei risultati teorici che abbiamo scelto di posticipare e le soluzioni di tutti gli esercizi proposti. Abbiamo speso molte energie e impegno nel preparare le soluzioni con la dovuta, e possibilmente ben dosata, quantità di dettagli per guidare gradualmente lo studente nel difficile compito di scrivere in maniera formale, corretta e comprensibile dimostrazioni in Matematica. Vogliamo comunque far notare che le soluzioni proposte non sono necessariamente le uniche possibili e cercarne di alternative può essere un'ulteriore fonte di apprendimento.

Crediamo che questo testo possa accompagnare il lettore nella scoperta dell'Algebra Commutativa e delle sue applicazioni e prepararlo ad approfondire lo studio di questa e di altre materie.

Pisa, 20/10/2022
Andrea Bandini, Patrizia Gianni, Enrico Sbarra

Notazioni

In questo libro gli insiemi dei numeri naturali, interi, razionali e complessi verranno denotati da $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, rispettivamente; useremo la notazione $\mathbb{N}_+$ per indicare $\mathbb{N} \setminus \{0\}$. Denoteremo l'insieme delle classi di equivalenza di $\mathbb{Z}$ modulo n con $\mathbb{Z}/(n)$.

I simboli $\bigcap$, $\bigcup$ e $\bigsqcup$ denoteranno - come è usuale - l'intersezione, l'unione e l'unione disgiunta insiemistica rispettivamente; $\subseteq$ e $\subset$ verrano usati indifferentemente per indicare il contenimento debole, mentre $\subsetneq$ indicherà il contenimento stretto. I simboli $\equiv$ e $\simeq$ denoteranno rispettivamente congruenze e isomorfismi.

Dati un insieme T e interi positivi r ed s denoteremo l'insieme delle matrici $r \times r$, rispettivamente $r \times s$, a coefficienti in T con $M_r(T)$, rispettivamente $M_{rs}(T)$; infine data una matrice B denoteremo con B^{t} la sua trasposta.

Dato un anello A, l'anello dei polinomi e l'anello delle serie formali nella variabile, o indeterminata, x a coefficienti in A verranno denotati con $A[x]$ e $A[[x]]$; similmente $A[x_1, \ldots, x_n]$ denoterà l'anello dei polinomi multivariati in $x_1, \ldots, x_n$ a coefficienti in A. Se A è un dominio, $Q(A)$ denoterà il campo totale dei quozienti di A. La lettera K indicherà sempre un campo e $\overline{K}$ la sua chiusura algebrica; dato un campo K denoteremo con $K(x_1, \ldots, x_n)$ il più piccolo campo che contiene K e $x_1, \ldots, x_n$.

Parte I

Teoria

1

Anelli

In questo capitolo presenteremo le nozioni di base per lo studio della teoria generale degli anelli commutativi con identità. Ricorderemo le definizioni principali e le prime proprietà di tali anelli 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.

1.1 Anelli e ideali

Un *anello* $(A, +, \cdot)$ è un gruppo abeliano $(A, +)$ dotato di un'operazione prodotto $A \times A \xrightarrow{\cdot} A$, $(a, b) \mapsto ab$, 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 è unico.
Osserviamo che si può avere $1 = 0$, ma in questo caso $A = 0$, poiché si ha $a = 1 \cdot a = 0 \cdot a = 0$ per ogni $a \in A$.
Per esempio sia n un intero positivo e K un campo come $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$. 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 $m\mathbb{Z}$ è un anello commutativo senza identità se $m \neq 0, \pm 1$.
Nel seguito considereremo sempre anelli commutativi con identità e 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.

Elementi speciali di un anello A

Sia $a \in A$.
a si dice **invertibile** se esiste $b \in A$ tale che $ab = 1$.
Denotiamo l'insieme degli elementi invertibili di A con A^*.
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 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 si dice **idempotente** se $a^2 = a$.

Osserviamo che, dalle definizioni, si ha subito $\mathcal{N}(A) \subseteq \mathcal{D}(A)$.
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.
Ricordiamo infine che, se $A \neq 0$, vale sempre $\mathcal{D}(A) \cap A^* = \emptyset$.
Per esempio consideriamo $A = \mathbb{Z}/(12)$; allora $A^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$, $\mathcal{D}(A) = \{\overline{0}, \overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}, \overline{10}\}$, $\mathcal{N}(A) = \{\overline{0}, \overline{6}\}$ e gli idempotenti sono $\{\overline{0}, \overline{1}, \overline{4}, \overline{9}\}$. Notiamo che $\mathcal{D}(A) \cap A^* = \emptyset$, $A = A^* \sqcup \mathcal{D}(A)$ e $\mathcal{N}(A) \subsetneq \mathcal{D}(A)$.

T. 1.1. (→ p. 195) Sia A un anello finito; allora $A = A^* \sqcup \mathcal{D}(A)$.

In particolare, un dominio finito è un campo.

Un sottoinsieme $I \subseteq A$ 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 $i \in I$ si ha $ai \in I$.

Un ideale si dice *proprio* se è un sottoinsieme proprio di A. Dalla definizione segue che un ideale è proprio se e solo se $1 \notin I$, cioè se e solo se $A^* \cap I = \emptyset$.
Un ideale proprio di A si dice *massimale* se nessun altro ideale proprio di A lo contiene.
Siano A un anello e $S \subset A$ un sottoinsieme non vuoto; allora l'insieme

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

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 $s_1, \dots, s_n$ 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 $(1) = A$; in generale A contiene anche altri ideali 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. 1.2. Sia $A \neq 0$ un anello.

1. A possiede almeno un ideale $\mathfrak{m}$ massimale.
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. 1.2. 1. Usiamo il Lemma di Zorn. Consideriamo l'insieme degli ideali propri di A

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

parzialmente ordinato tramite $\subseteq$. Dato che $(0) \in \Sigma$, si ha $\Sigma \neq \emptyset$. Consideriamo una catena $\mathcal{C} = \{I_h \colon h \in H\}$ 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 $b \in I_j$ e, dato che $\mathcal{C}$ è totalmente ordinato, possiamo assumere senza perdita di generalità che $I_i \subseteq I_j$. 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 di 1 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 2. □

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. 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 $I_1, \dots, I_k$ 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 $I_1, \dots, I_k$. Viene denotato con $\prod_{i=1}^{k} I_i$.

In particolare si possono considerare le potenze I^n, $n \in \mathbb{N}$, ponendo $I^0 = A$.

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 $0 \colon J$ si chiama l'*annullatore* di J e si indica con $\operatorname{Ann}_A J$ o semplicemente $\operatorname{Ann} J$. Se $I = (a)$ allora scriveremo semplicemente $\operatorname{Ann} a = \operatorname{Ann}(a)$ per indicare l'*annullatore di a*.

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, dato un ideale I, si ha $I \supseteq I^2 \supseteq I^3 \supseteq \dots \supseteq I^h \supseteq \dots$.
È possibile che $I = I^2$, per esempio $(\overline{2}) = (\overline{4})$ in $\mathbb{Z}/(6)$.

T. 1.3. (→ p. 195) Siano I, J ideali di un anello A; allora il quoziente $I \colon J$ e il radicale $\sqrt{I}$ sono ideali.

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 consideriamo $\overline{2}, \overline{3} \in \mathbb{Z}/(6)$, si ha $\overline{2}, \overline{3} \in \mathcal{D}(\mathbb{Z}/(6))$ ma $\overline{2} + \overline{3} = \overline{5} \in (\mathbb{Z}/(6))^*$.

Dalle definizioni segue immediatamente 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*.

T. 1.4. (→ p. 195) Siano $I_1, \dots, I_n$ ideali di A tali che $I_i + I_j = (1)$ per ogni $i \neq j$; allora $\bigcap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_i$.

Valgono anche le seguenti relazioni.

T. 1.5. (→ p. 196) 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
$$I \cap (J+H) = (I\cap J) + (I\cap H).$$
5. $I + JH \subseteq (I+J)\cap(I+H)$.

L'uguaglianza al punto 5 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 al punto 3, infatti $I\cap(J+H) = I\cap(x,y) = I$ e $(I\cap J)+(I\cap H) = (x^2+xy)+(xy+y^2) \neq I$.
È possibile trovare un controesempio all'uguaglianza al punto 3 con $A=\mathbb{Z}$?

Proprietà del radicale

T. 1.6. (→ p. 196) 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. $\sqrt{I+JH} = \sqrt{I+J}\cap\sqrt{I+H}$.

Abbiamo visto in **T.1.2** che in un anello $A\neq 0$ ci sono sempre ideali massimali. Definiamo ora altri tipi di ideali propri che saranno particolarmente rilevanti nel seguito.

Ideali speciali - I

Siano A un anello e $I, I_1, I_2 \subset A$ ideali propri; allora I si dice
primo, se $ab\in I$ implica $a\in I$ oppure $b\in I$;
radicale, se $I=\sqrt{I}$;
primario, se $ab\in I$ implica $a\in I$ oppure $b\in\sqrt{I}$;
irriducibile, se $I = I_1\cap I_2$ implica $I=I_1$ 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. 1.7. (→ p. 196) 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.

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. **T.1.22**.5, **T.1.23** e **E.8.57**.2. Inoltre, se $A = K[x_1, \ldots, x_n]$ possiamo considerare la catena $(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \ldots \subsetneq (x_1, \ldots, x_n)$; dato che gli ideali $(x_1, \ldots, x_i)$ sono tutti primi, cf. **T.1.11**.3, deduciamo subito che $\dim A \geq n$. È più complesso dimostrare che $\dim A = n$, ma non tratteremo qui lo studio della teoria della dimensione.

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 $a - b \in I$, i.e. se e solo se $a \equiv b \mod I$. 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. 1.8. (→ p. 197) La moltiplicazione in A/I sopra descritta è ben definita e gode delle proprietà richieste.

Siano A e B anelli. Un'applicazione $f : A \longrightarrow B$ è un *omomorfismo* di anelli se per ogni $a, b \in A$

i) $f(a+b) = f(a) + f(b)$;

ii) $f(ab) = f(a)f(b)$;

iii) $f(1_A) = 1_B$.

Dalla definizione segue che $f = 0$ 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 $\operatorname{Ker} f = \{a \in A \colon f(a) = 0\} = f^{-1}((0))$ e 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

i) $\operatorname{Ker} f$ è un ideale di A;

ii) f è iniettiva se e solo se $\operatorname{Ker} f = (0)$,

iii) $\operatorname{Im} f$ è un sottoanello di B.

cf. **E.8.42**. Più in generale, è utile tenere a mente che, dato $f \colon A \longrightarrow B$ un omomorfismo di anelli e I, J ideali di A e B rispettivamente,

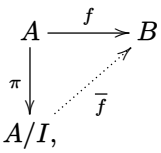
i) $f^{-1}(J) = \{a \in A \colon f(a) \in J\}$ è un ideale di A;

ii) se f è surgettivo allora $f(I)$ 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 $\overline{f} \colon A/I \longrightarrow B$ che rende commutativo il seguente diagramma



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 che è chiaramente surgettiva.
Affinché il diagramma commuti $\overline{f}$ deve essere definita come $\overline{f}(\overline{a}) = f(a)$ e 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, dato che f è un omomorfismo, anche $\overline{f}$ lo è.

Valgono i seguenti teoremi di omomorfismo.

Teoremi di omomorfismo di anelli

T. 1.9. (→ p. 197) 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) $B + I = \{b + i : b \in B, i \in I\} \subset A$ è un sottoanello;

(b) I è un ideale di $B + I$;

(c) $B \cap I$ è un ideale di B.

Infine

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

T. 1.10. (→ p. 197) 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.

In particolare, se tutti i primi che contengono un ideale I sono massimali allora $\dim A/I = 0$. In questo caso diciamo che I è 0-*dimensionale*.

Come corollario dei teoremi di omomorfismo otteniamo le seguenti caratterizzazioni in termini dell'anello quoziente di alcuni degli ideali introdotti in precedenza.

Ideali speciali - II

T. 1.11. (→ p. 197) 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 ridotto;
5. I è primario se e solo se $\mathcal{N}(A/I) = \mathcal{D}(A/I)$.

Inoltre,

6. I massimale $\implies$ I primo;
7. I primo $\implies$ I radicale;
8. I primo $\implies$ I primario.

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. 1.12. 1. [**Lemma di scansamento**] Siano $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ ideali primi e 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 $I_1, \dots, I_n$ ideali e $\mathfrak{p}$ 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 $I_{j_0} = \mathfrak{p}$.

Dimostrazione T. 1.12. 1. Per induzione su n proviamo che se $I \not\subseteq \mathfrak{p}_j$ per ogni $1 \leq j \leq n$ allora $I \not\subseteq \bigcup_{j=1}^n \mathfrak{p}_j$, 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 $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ 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 $I \not\subseteq \bigcup_{j=1}^n \mathfrak{p}_j$. 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 $I \not\subseteq \bigcup_{j=1}^n \mathfrak{p}_j$.

2. Dimostriamo per assurdo supponendo che $\mathfrak{p} \not\supseteq I_j$ per ogni j. In questo caso per ogni j esiste almeno un elemento $a_j \in I_j \setminus \mathfrak{p}$; quindi si ha $\prod_{j=1}^n a_j \in \bigcap_{j=1}^n I_j$ e $\prod_{j=1}^n a_j \notin \mathfrak{p}$, dal momento che $\mathfrak{p}$ è un ideale primo. Dunque $\mathfrak{p} \not\supseteq \bigcap_{j=1}^n I_j$.
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. 1.13. (→ p. 198) Ogni ideale primo è irriducibile.

1.3 Il nilradicale e il radicale di Jacobson. Anelli locali

Per costruzione l'anello $A/\mathcal{N}(A) = A/\sqrt{(0)}$ è ridotto: infatti $\overline{a}^k = \overline{0}$ vuol dire che a^k è nilpotente, quindi lo è anche a e dunque $\overline{a} = \overline{0}$.

T. 1.14. [**Caratterizzazione del radicale**]

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

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. 1.14. 1. Verifichiamo che un elemento nilpotente a appartiene ad ogni ideale primo di A; se $a^n = 0$ per qualche $n \in \mathbb{N}$ allora $a^n \in \mathfrak{p}$ per ogni primo $\mathfrak{p}$, da cui discende che $a \in \mathfrak{p}$ per ogni $\mathfrak{p}$.

Per l'inclusione opposta, utilizziamo di nuovo il 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 tale ideale non contiene a, avremo concluso.
Supponiamo allora che esistano elementi $b, c \notin I$ tali che $bc \in I$; allora l'ideale $I \colon (b)$ 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 $a^n \in I \colon (b)$ e pertanto $I \subsetneq (I, b) \subseteq I \colon (a^n) \notin \Sigma$. Quindi esiste un intero m tale che $a^m \in I \colon (a^n)$ e $a^{n+m} \in I$ che è la contraddizione cercata.

2. Basta considerare l'anello A/I e osservare che $\mathcal{N}(A/I) = \sqrt{I}/I$ 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.1.10**. □

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 l'intersezione di tutti gli ideali massimali di A. Dalla definizione segue dunque subito che

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

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

T. 1.15. (→ p. 198) [**Caratterizzazione del radicale di Jacobson**] Sia A un anello; allora

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

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. 1.16. (→ p. 198) [**Caratterizzazione degli anelli locali**] Sia A un anello.

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 $\mathfrak{m}$.

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 $f\colon A \longrightarrow B$ è 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* di I rispetto a f 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.

Ideali estesi e contratti

T. 1.17. (→ p. 198) Sia $f\colon A \longrightarrow B$ un omomorfismo di anelli e siano $I, I_1, I_2 \subseteq A$ e $J, J_1, J_2 \subseteq B$ ideali.

1. $I_1 \subseteq I_2 \Longrightarrow I_1^e \subseteq I_2^e$;
2. $J_1 \subseteq J_2 \Longrightarrow J_1^c \subseteq J_2^c$;
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.

In generale 7, 8 e 9 non valgono per gli ideali estesi.

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

T. 1.18. (→ p. 199) Siano A e B anelli e sia $f\colon A \longrightarrow B$ un omomorfismo surgettivo. Se $\operatorname{Ker} f \subseteq I \subset A$ e $J \subset B$ sono ideali, allora

1. l'immagine $f(I)$ è un ideale di B e quindi $I^e = f(I)$;
2. $I = I^{ec}$ e $J = J^{ce}$, le operazioni di estensione e contrazione stabiliscono dunque una corrispondenza biunivoca fra gli ideali di A che contengono $\operatorname{Ker} f$ e gli ideali di B;
3. rispetto a tale corrispondenza, gli ideali massimali corrispondono ai massimali, i primi ai primi, i primari ai primari e i radicali ai radicali.

1.5 Teorema cinese del resto

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

$$a + b = (a_1 + b_1, \ldots, a_n + b_n) \quad \text{e} \quad ab = (a_1 b_1, \ldots, a_n b_n),$$

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. 1.19. 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 $e_i e_j = 0$ per ogni $i \neq j$ e $\sum_i e_i = 1_A$.

Dimostrazione T. 1.19. Sia $f\colon A \longrightarrow \prod_{i=1}^{n} A_i$ un isomorfismo di anelli; gli elementi $e_i = f^{-1}(0, \ldots, 0, 1_{A_i}, 0, \ldots, 0)$ sono allora idempotenti ortogonali tali che $\sum_i e_i = 1_A$. Infatti, dato che f è un omomorfismo di anelli $f(e_i e_j) = f(e_i) f(e_j) = 0$ per ogni $i \neq j$ e $f(e_i^2 - e_i) = f(e_i)^2 - f(e_i) = 0$ per ogni i; dunque $e_i e_j = 0$ per ogni $i \neq j$ e $e_i^2 = e_i$ per ogni i poiché f è iniettivo. Infine $f(\sum_i e_i) = \sum_i f(e_i) = (1_{A_1}, \ldots, 1_{A_n})$ implica $\sum_i e_i = 1_A$.

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 facilmente che f è un omomorfismo di anelli. Proviamo che f 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 $f(a) = (e_1 a_1, \ldots, e_n a_n)$ poiché gli e_i sono tra loro ortogonali. □

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

Teorema cinese del resto

T. 1.20. 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. 1.20. Per ipotesi, per ogni $i \neq j$ esistono elementi $\gamma_i^{(j)} \in I_i$ tali che $\gamma_i^{(j)} + \gamma_j^{(i)} = 1$. Per ogni i definiamo $L_i = \prod_{j \neq i} \gamma_j^{(i)}$; allora

$$L_i \equiv 0 \mod I_j \text{ se } j \neq i \quad \text{e} \quad L_i = \prod_{i \neq j} (1 - \gamma_i^{(j)}) \equiv 1 \mod I_i.$$

L'elemento $a = \sum_i a_i L_i \in A$ soddisfa le condizioni richieste. □

T. 1.21. (→ p. 199) 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 $\bigcap_{i=1}^{n} I_i = 0$.

In conclusione, se in A esistono ideali I_i, con $i = 1, \ldots, n$, che sono a due a due comassimali e tali che $\prod_{i=1}^{n} I_i = 0$ avremo che $f \colon A \longrightarrow \prod_{i=1}^{n} A/I_i$ è un isomorfismo per **T.1.4** e **T.1.21**.

1.6 Fattorizzazione in domini d'integrità: PID e UFD

In questa sezione assumeremo che A sia un dominio e analizzeremo il problema della divisione e della fattorizzazione in A, dove vale la legge di cancellazione, cf. **E.8.2**.

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.
Osserviamo che se $b \neq 0$ e $b = ac$ allora c è univocamente determinato da a e b; se $a, c \notin A^*$, diciamo che a è un *divisore proprio* di b. 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 $a = bc$ implica $b \in A^*$ oppure $c \in A^*$; equivalentemente se ogni divisore di a è associato ad a, o ancora se a non ha divisori propri.
Queste definizioni possono essere facilmente espresse in termini di proprietà degli ideali principali generati dagli elementi di A.

T. 1.22. (→ p. 200) Siano $a, b \in A$; allora

1. a è invertibile se e solo se $(a) = (1)$;
2. a divide b se e solo se $(b) \subseteq (a)$;
3. a e b sono associati se e solo se $(a) = (b)$;
4. a è un divisore proprio di $b \neq 0$ se e solo se $(b) \subsetneq (a) \subsetneq (1)$;
5. a è primo se e solo se (a) è un ideale primo.

T. 1.23. (→ p. 200) 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.

Per esempio $\mathbb{Z}$ è PID, i suoi ideali primi non nulli, che sono anche massimali, sono tutti e soli gli ideali (p), con p 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 $\mathbb{Z}[\sqrt{-5}]$ l'elemento 2 è irriducibile, ma non primo.

T. 1.24. (→ p. 200) Sia A un PID; allora ogni catena ascendente $\mathcal{C} = \{I_h\}_{h \in H}$ di ideali di A è stazionaria, i.e. esiste $h_0 \in H$ tale che $\bigcup_{h \in H} I_h = I_{h_0}$.

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

(UFD1) *esistenza di una fattorizzazione in elementi irriducibili*: per ogni elemento $a \in A \setminus \{A^* \cup \{0\}\}$ esistono $b_1, \ldots, b_k \in A$ irriducibili e $u \in A^*$ tali che $a = ub_1 \cdots b_k$;

(UFD2) *unicità della fattorizzazione*: se $a = ub_1 \cdots b_k = vc_1 \cdots c_h$ sono due fattorizzazioni di a in elementi irriducibili con $u, v \in A^*$ allora $k = h$ e, a meno dell'ordine, ogni elemento b_i è associato a c_i per ogni i.

T. 1.25. 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. 1.25. Dimostriamo che se A è un dominio a fattorizzazione unica allora vale (UFD3). Supponiamo che a sia un elemento irriducibile e $b, c \in A$ tali che $a \mid bc$; 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 ed elementi $u, v \in A^*$ tali che $b = u\prod_i b_i$ e $c = v\prod_j c_j$; per l'unicità della fattorizzazione (UFD2), esiste allora $e = b_{i_0}$ oppure $e = c_{j_0}$ tale che a ed e sono associati, visto che a per ipotesi è irriducibile. Avremo allora che $a \mid b$ nel primo caso oppure $a \mid c$ nel secondo, come volevamo.

Viceversa, supponiamo ora che valga (UFD3) e dimostriamo (UFD2); siano $a \in A \setminus \{A^* \cup \{0\}\}$ e $a = u\prod_{i=1}^m a_i = v\prod_{j=1}^n b_j$ due fattorizzazioni in elementi irriducibili con $u, v \in A^*$. 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 $j_1 \in \{1, \dots, n\}$ 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 $u\prod_{i=2}^m a_i = vc_1\prod_{j=2}^n b_j$. 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 $v\prod_{i=1}^m c_i \prod_{j=m+1}^n b_j = u \in A^*$. Abbiamo dimostrato allora che, a meno dell'ordine e di elementi invertibili, le due fattorizzazioni di a coincidono. □

T. 1.26. (→ p. 200) Ogni anello PID è anche UFD.

Un esempio di anello a fattorizzazione unica che non è PID è $\mathbb{Z}[x]$ dove $(3, x)$ non è principale. Un altro esempio è un anello di polinomi A a coefficienti in un campo con almeno due indeterminate x_1 e x_2. Esso è UFD per il Lemma di Gauss, cf. **E.8.9**, e non è PID. Consideriamo l'ideale $I = (x_1, x_2)$; allora I è un ideale non nullo e proprio di A tale che $I \neq (x_1)$ e $I \neq (x_2)$. Se esistesse $d \in A$ tale che $(d) = (x_1, x_2)$ allora $d \neq 0$ e $d \notin A^*$. Dato che A è un dominio $x_i = c_i d$ implica $\deg d = 1$ e $c_i \in K^*$ per motivi di grado. Avremmo infine che x_i è associato a d e dunque $(x_1) = (d) = (x_2)$, che è assurdo.

Sia A un UFD. Dati due elementi $a, b \in A$ non entrambi 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 $c \mid d$ (*massimo*);

si chiama *massimo comun divisore* di a e b, e si denota con $\gcd(a, b)$.

Segue immediatamente dalla definizione che se d_1 e d_2 sono entrambi massimo comune divisore di a e b allora sono associati. 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*, cioè un elemento $m \in A$ tale che

i) $a \mid m$ e $b \mid m$ (*multiplo comune*);

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

lo denotiamo con $\operatorname{lcm}(a, b)$.
Osserviamo che per ogni a non nullo $\gcd(a, 0) = a$ e $\operatorname{lcm}(a, 0) = 0$.

Sia $\mathcal{R}$ la relazione di equivalenza data dall'essere elementi associati. Consideriamo $\{p \neq 0 \colon p \text{ primo }\}/\mathcal{R}$ l'insieme degli elementi primi di A non nulli - o, per quanto dimostrato in **T.1.23** e **T.1.25**, irriducibili - modulo la relazione di equivalenza $\mathcal{R}$ e fissiamo un suo insieme di rappresentanti $\operatorname{Irr}(A)$.
Per ogni coppia di elementi $a, b \in A \setminus \{A^* \cup \{0\}\}$ possiamo scrivere in maniera unica $a = u \prod_{p \in \operatorname{Irr}(A)} p^{a_p}$ e $b = v \prod_{p \in \operatorname{Irr}(A)} p^{b_p}$, con $u, v \in A^*$ e a_p, b_p quasi tutti nulli. Risulta allora che

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

Un dominio d'integrità A si dice *dominio euclideo* se esiste un'applicazione $\delta \colon A \setminus \{0\} \longrightarrow \mathbb{N}$ detta *grado* tale che

i) per ogni $a, b \in A \setminus \{0\}$ si ha $\delta(a) \leq \delta(ab)$;

ii) per ogni $a \in A$ e $b \in A \setminus \{0\}$, esistono unici $q, r \in A$ tali che $a = qb + r$ con $r = 0$ oppure $\delta(r) < \delta(b)$.

Tali elementi q ed r si dicono rispettivamente *quoziente* e *resto* della divisione di a per b.

T. 1.27. (→ p. 201) Un dominio euclideo è PID e quindi è UFD.

Per esempio gli anelli $\mathbb{Z}$, $K[x]$, con K campo, e $\mathbb{Z}[i]$ sono anelli euclidei, con funzioni grado rispettivamente $\delta(n) = |n|$, $\delta(f) = \deg(f)$ e $\delta(a + ib) = a^2 + b^2$, e quindi anche PID e UFD.

T. 1.28. (→ p. 201) 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.

Osserviamo che se A non è UFD l'affermazione precedente non vale, cf. **E.8.66**. 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 $(9) = (a) \cap (b) = (\operatorname{lcm}(a, b))$ 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 in **T.1.13**.

2

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

In questo capitolo studieremo le proprietà dell'anello $A = K[x_1, \ldots, x_n]$ dei polinomi in n indeterminate a coefficienti in un campo K. Useremo la notazione compatta $X = x_1, \ldots, x_n$, per cui ad esempio scriveremo $A = K[X]$. Studieremo le proprietà degli ideali monomiali e introdurremo le basi di Gröbner, uno strumento essenziale per la risoluzione di vari problemi legati allo studio degli ideali e delle operazioni tra ideali come per esempio il Test di appartenenza.

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 $\operatorname{Mon} A$ dei monomi di A e gli elementi di $\mathbb{N}^n$; in questa bigezione il monomio 1 corrisponde all'esponente $\mathbf{0} \in \mathbb{N}^n$. Se $\mathbf{a}, \mathbf{b} \in \mathbb{N}^n$ dire che $X^{\mathbf{a}}$ divide $X^{\mathbf{b}}$ è equivalente a dire che $\mathbf{b} - \mathbf{a} \in \mathbb{N}^n$.
Osserviamo che $\operatorname{Mon} A$ è una K-base di A. Un elemento $f \in A$ è un *polinomio*, che scriviamo come

$$f = \sum_{\mathbf{a}} c_{\mathbf{a}} X^{\mathbf{a}} \quad \text{con} \quad \mathbf{a} \in \mathbb{N}^n \quad \text{e} \quad c_{\mathbf{a}} \neq 0 \quad \text{per un numero finito di } \mathbf{a} \in \mathbb{N}^n.$$

Chiamiamo *termine* di f ogni addendo non nullo $c_{\mathbf{a}} X^{\mathbf{a}}$.
Gli ideali di A sono generati da polinomi, ovvero da elementi che sono somma finita di termini, cioè combinazione K-lineare 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 insieme di generatori composto da monomi.

Il seguente fatto fornisce un criterio per decidere se $f \in A$ appartiene ad I monomiale.

T. 2.1. (→ p. 201) Siano I un ideale monomiale e $f = \sum_{\mathbf{a}} c_{\mathbf{a}} X^{\mathbf{a}}$, per certi $\mathbf{a} \in \mathbb{N}^n$ e $c_{\mathbf{a}} \in K^*$, un polinomio di A; allora

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

Osserviamo che la precedente proprietà caratterizza gli ideali monomiali. Infatti, se I è un ideale che verifica la condizione in **T.2.1** allora I è generato dai monomi dei polinomi che gli appartengono.

Dati un sottoinsieme $E \subseteq \mathbb{N}^n$ e l'ideale monomiale $I = (X^{\mathbf{a}} \colon \mathbf{a} \in E)$, 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, 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 $I = (X^{\mathbf{a}} \colon \mathbf{a} \in E) = (X^{\mathbf{b}} \colon \mathbf{b} \in E')$.
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 rispettivamente a quelle di ideale monomiale e di insieme di generatori.

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

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

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 $\mathbf{a} = \mathbf{b} + \mathbf{c}$.

T. 2.2. (→ p. 201) Sia $I \neq 0$ un ideale monomiale; allora esiste un $\mathcal{E}$-sottoinsieme E tale che $I = (X^{\mathbf{a}} \colon \mathbf{a} \in E)$. Inoltre, se F è una frontiera di E allora

$$I = (X^{\mathbf{a}} \colon \mathbf{a} \in F).$$

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

Lemma di Dickson

T. 2.3. Ogni $\mathcal{E}$-sottoinsieme ammette una frontiera finita, quindi ogni ideale monomiale di A è finitamente generato.

Dimostrazione T. 2.3. Dimostriamo la tesi per induzione su n. Se $n = 1$ allora $E \subset \mathbb{N}$ 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 $F_0 = \{\mathbf{a}_1, \dots, \mathbf{a}_k\} \subset \mathbb{N}^{n+1}$ tale che $\pi(F_0)$ sia una frontiera finita di $\pi(E)$.
Per completare la costruzione di una frontiera di E scriviamo $\mathbf{a}_i = (a_0^{(i)}, \dots, a_n^{(i)})$ per ogni i e poniamo $\overline{a} = \max_i\{a_0^{(i)}\}$. Per ogni $0 \leq a < \overline{a}$ consideriamo i sottoinsiemi $E_a = E \cap (\{a\} \times \mathbb{N}^n)$ costituiti da tutte le $(n+1)$-uple in E con prima coordinata uguale ad a. Se E_a è non vuoto allora $\pi(E_a) \subset \mathbb{N}^n$ è un $\mathcal{E}$-sottoinsieme di $\mathbb{N}^n$; quindi per l'ipotesi induttiva per ogni tale a esiste un insieme finito $F_a \subset E_a$ tale che $\pi(F_a)$ sia una frontiera finita di $\pi(E_a)$. Se invece $E_a = \emptyset$ possiamo trascurarlo e definire $F_a = \emptyset$.
Proviamo ora che

$$F = \left(\bigcup_{0 \leq a < \overline{a}} F_a \right) \cup F_0$$

è una frontiera di E.
Sia $\mathbf{a} = (a_0, \dots, a_{n+1}) \in E$; dobbiamo dimostrare che esiste $\mathbf{b} \in F$ tale che $\mathbf{a} - \mathbf{b} \in \mathbb{N}^{n+1}$. Se $a_0 < \overline{a}$ allora $\mathbf{a} \in E_{a_0}$; dunque esiste $\mathbf{b} \in F_{a_0}$ tale che $\mathbf{a} - \mathbf{b} \in \mathbb{N}^{n+1}$ e abbiamo concluso. Altrimenti, visto che $\pi(\mathbf{a}) \in \pi(E)$, esiste $\mathbf{a}_i \in F_0$ tale che $\pi(\mathbf{a} - \mathbf{a}_i) \in \mathbb{N}^n$. Dato che $a_0 \geq \overline{a} \geq a_0^{(i)}$ si ottiene che $\mathbf{a} - \mathbf{a}_i \in \mathbb{N}^{n+1}$. □

È chiaro che, data una frontiera F di un $\mathcal{E}$-sottoinsieme, se ne può estrarre una 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. 2.4. (→ p. 201) Sia E un $\mathcal{E}$-sottoinsieme di $\mathbb{N}^n$; allora ogni frontiera minimale di E è finita.

T. 2.5. (→ p. 201) Ogni $\mathcal{E}$-sottoinsieme ha un'unica frontiera minimale. Pertanto ogni ideale monomiale I ha un unico insieme minimale di generatori monomiali.

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

Riassumendo, dato un qualsiasi ideale monomiale $I = (X^{\mathbf{a}} \colon X^{\mathbf{a}} \in M)$ e un suo insieme di generatori monomiali M, all'ideale I corrisponde l'$\mathcal{E}$-sottoinsieme $E = \{\mathbf{a} + \mathbb{N}^n \colon X^{\mathbf{a}} \in M\}$. 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 $F = \{\mathbf{a}_1, \dots, \mathbf{a}_k\}$ è la frontiera minimale di E allora l'insieme $M' = \{X^{\mathbf{a}_1}, \dots, X^{\mathbf{a}_k}\} \subseteq M$ 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. 2.6. Siano $I = (m_1, \dots, m_s)$ e $J = (n_1, \dots, n_t)$ ideali monomiali di A con $m_i, n_j \in \operatorname{Mon} A$ per ogni $i = 1, \dots, s$ e $j = 1, \dots, t$.

1. **Decomposizione.** Siano $m, u \in A$ monomi relativamente primi; allora $(I, mu) = (I, m) \cap (I, u)$.
2. **Intersezione.** L'ideale $I \cap J$ è generato dai monomi $\operatorname{lcm}(m_i, n_j)$ per ogni $i = 1, \dots, s$ e $j = 1, \dots, t$.
3. **Quoziente.** Sia m un monomio di A; allora l'ideale $I \colon (m)$ è generato dai monomi $\dfrac{m_i}{\gcd(m_i, m)}$ per ogni $i = 1, \dots, s$.
4. **Radicale.** Dato un monomio m sia $\sqrt{m} = \prod_{x_h \mid m} x_h$ la sua *parte libera da quadrati*; allora $\sqrt{I}$ è generato dai monomi $\sqrt{m_i}$ per ogni $i = 1, \dots, s$.

Dimostrazione T. 2.6. L'intersezione di ideali monomiali è ancora un ideale monomiale; infatti, se $f \in I \cap J$ allora tutti i suoi monomi devono stare sia in I che in J, quindi anche $I \cap J$ è monomiale per la caratterizzazione degli ideali monomiali, cf. l'osservazione dopo **T.2.1**.

1. È chiaro che $(I, m) \cap (I, u) \supseteq (I, mu)$.

Per l'altra inclusione, innanzitutto osserviamo che se $f = \sum_{\mathbf{a}} c_{\mathbf{a}} X^{\mathbf{a}} \in (I, m) \cap (I, u)$ allora, dato che (I, m) e (I, u) sono ancora ideali monomiali, ogni monomio $X^{\mathbf{a}} \in (I, m) \cap (I, u)$ e quindi è sufficiente considerare il caso in cui f sia un monomio v. Possiamo inoltre supporre che $v \notin I$ altrimenti avremmo finito; avremo allora che $v = am = bu$ e, dato che m e u sono relativamente primi, $m \mid b$ e quindi $v = cmu$ per qualche $c \in \operatorname{Mon} A$.

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

Per l'altra inclusione, sia $f \in I \cap J$ che è monomiale; allora ogni monomio di f è del tipo $X^{\mathbf{a}} n_j$ per qualche j e deve essere divisibile per un qualche m_i. Dunque $m_i \mid X^{\mathbf{a}} n_j$ e quindi $d_{ij} \mid X^{\mathbf{a}} n_j$ 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 $a_i, b_i \in \operatorname{Mon} A$ per ogni i. Dato che $I \colon (m) = \{f \in A \colon fm \in I\}$, avremo $a_i m = a_i b_i d_i = b_i m_i \in I$, da cui discende che $(a_1, \dots, a_s) \subset I \colon (m)$.

Per l'altra inclusione, se $f = \sum_i c_i n_i$ con $c_i \in K^*$ e $n_i \in \operatorname{Mon} A$ è la scrittura di f come somma di termini e $fm = \sum_i c_i n_i m \in I$ allora si ha che per ogni i esistono indici k_i e monomi e_i tali che $n_i m = e_i m_{k_i} = e_i a_{k_i} d_{k_i}$. Si

ha anche che $n_i m = n_i b_{k_i} d_{k_i}$ e dunque $e_i a_{k_i} d_{k_i} = n_i b_{k_i} d_{k_i}$. Questo implica che $a_{k_i} \mid n_i$ per ogni i e quindi $f \in (a_1, \dots, a_s)$.

4. Sia $J = (\sqrt{m_1}, \dots, \sqrt{m_s})$; allora certamente

$$I \subseteq J \subseteq \sqrt{I}.$$

Per **T.1.6**.1 e 2 abbiamo che $\sqrt{I} = \sqrt{J}$ e quindi è sufficiente dimostrare che J è radicale.
Dato che $\sqrt{m_i}$ è un prodotto di variabili per ogni i, possiamo applicare ripetutatemente la decomposizione del punto 1 ed ottenere che J è un'intersezione di ideali generati da variabili, che sono primi per **T.1.11**.3. Allora J è radicale per **T.1.6**.3 e **T.1.11**.7. □

Osserviamo che da **T.2.6**.3 e **E.8.17**.5 discende che per un qualsiasi ideale $J = (n_1, \dots, n_t)$ abbiamo

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

Ideali monomiali speciali

T. 2.7. 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 $i \in \{1, \dots, s\}$, ovvero se e solo se $m = \sqrt{m}$ per ogni $m \in G(I)$.

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, per ogni $i \in \{1, \dots, s\}$,

   $m_i = x_1^{a_1} \cdots x_n^{a_n} \implies$ per ogni $a_i \neq 0$ esiste $m_{j_i} = x_i^{b_i}$ per qualche $b_i > 0$,

   ovvero se e solo se $G(I)$ contiene una potenza pura di ogni variabile che compare in almeno un $m \in G(I)$.

Come corollario otteniamo che se I è un ideale monomiale irriducibile allora è primario.

Dimostrazione T. 2.7. 1. Sia $I = (x_{i_1}, \dots, x_{i_k})$; allora A/I è un dominio e quindi I è primo.

Viceversa, per ogni m_i esiste $j_i \in \{1,\dots,n\}$ tale che $x_{j_i} \mid m_i$, ossia $m_i = x_{j_i} n_i$ per qualche $n_i \in \operatorname{Mon} A$. Dato che $G(I)$ è minimale, abbiamo $n_i \notin I$ e quindi $x_{j_i} \in I$ perché I è primo; ciò implica $m_i = x_{j_i}$ ancora per la minimalità di $G(I)$.

2. Per ogni $i = 1,\dots,s$ si ha che m_i è libero da quadrati se e solo se $m_i = \sqrt{m_i}$, i.e. se e solo se $I = \sqrt{I}$, cf. **T.2.6**.4.

3. Sia I irriducibile; se esiste $m_i = um$ con $\gcd(u,m) = 1$ allora $I \subsetneq (I,u)$ e $I \subsetneq (I,m)$ dato che $G(I)$ è un insieme di generatori minimale. Inoltre, $(I,u) \cap (I,m) = I$ per **T.2.6**.1 e 2, contro le ipotesi.

Viceversa, supponiamo di aver riordinato le variabili e i monomi m_i, se necessario, in modo tale che $G(I)$ sia $\{x_1^{a_1},\dots,x_k^{a_k}\}$ per un certo $k \leq n$ e denotiamo $X = x_1,\dots,x_k$ e $Y = x_{k+1},\dots,x_n$. Siano J e L ideali di $A = K[X,Y]$, non necessariamente monomiali, tali che $I = J \cap L$ con $I \subsetneq J$ e $I \subsetneq L$; proviamo che esiste $p(Y) \in K[Y]$ tale che $p(Y)x_1^{a_1-1}\cdots x_k^{a_k-1} \in I$, da cui otteniamo 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 $fg \in I$; possiamo supporre che nessun monomio di f o di g sia in I. Consideriamo f e scriviamolo come polinomio in $K[Y][X]$ come $f = \sum_{\mathbf{a}} c_{\mathbf{a}}(Y)X^{\mathbf{a}}$. Sia $X^{\boldsymbol{\delta}}$ un monomio di f di grado totale $|\boldsymbol{\delta}| = \delta_1 + \ldots + \delta_k$ minimale. Allora dato che $X^{\boldsymbol{\delta}} \notin I$, per ogni i si ha $\delta_i < a_i$ 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 $\gamma_i = a_i - \delta_i - 1 \geq 0$. Per costruzione $X^{\boldsymbol{\gamma}+\boldsymbol{\delta}} = x_1^{a_1-1}\cdots x_k^{a_k-1} \notin I$. Inoltre si ha $X^{\boldsymbol{\gamma}} m \in I$ per ogni monomio m di f diverso da $X^{\boldsymbol{\delta}}$. Quindi otteniamo $X^{\boldsymbol{\gamma}}(f - c_{\boldsymbol{\delta}}(Y)X^{\boldsymbol{\delta}}) \in I \subset J$, da cui segue che

$$c_{\boldsymbol{\delta}}(Y)x_1^{a_1-1}\cdots x_k^{a_k-1} = X^{\boldsymbol{\gamma}} f - X^{\boldsymbol{\gamma}}(f - c_{\boldsymbol{\delta}}(Y)X^{\boldsymbol{\delta}}) \in J.$$

Ripetendo il ragionamento per il polinomio $g = \sum_{\mathbf{a}} d_{\mathbf{a}}(Y)X^{\mathbf{a}} \in L \setminus I$, troviamo opportuni $\boldsymbol{\varepsilon}$, $\boldsymbol{\eta}$ 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 $m = x_k u \in G(I)$ per qualche $u \in \operatorname{Mon} A$; avremo allora che $u \notin I$ e $x_k^a \in I$.

Viceversa, eventualmente riordinando le variabili supponiamo che tutti i monomi di $G(I)$ appartengano a $K[x_1,\dots,x_r]$ con $r \leq n$; allora dall'ipotesi discende che $\sqrt{I} = (x_1,\dots,x_r)$ per **T.2.6**.4. Consideriamo l'omomorfismo di inclusione

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

L'ideale $\sqrt{(\phi(I))} = (x_1,\dots,x_r)$ è massimale in $K(x_{r+1},\dots,x_n)[x_1,\dots,x_r]$ quindi $(\phi(I))$ è primario per **T.1.7**.2. Dato che $(\phi(I))^c = I$, perché gli ideali hanno gli stessi generatori, si ha la tesi per **T.1.17**.8. □

Osserviamo che utilizzando **T.2.6**.1 possiamo sempre scrivere un ideale monomiale come intersezione di ideali monomiali irriducibili. Per esempio sia

$$I = (x_1^3x_2,\ x_1^4x_2x_3^3,\ x_1^7,\ x_1^2x_3^3).$$

Dato che $x_1^2x_3^3 \mid x_1^4x_2x_3^4$, possiamo ridurre l'insieme dei generatori e ottenere $I = (x_1^3x_2,\ x_1^7,\ x_1^2x_3^3)$. Per **T.2.6**.1 usando il monomio $x_1^2x_3^3$ possiamo spezzare l'ideale e ottenere

$$I = (I, x_1^2) \cap (I, x_3^3) = (x_1^2) \cap (x_1^3x_2,\ x_1^7,\ x_3^3).$$

Ripetendo il procedimento usando il monomio $x_1^3x_2$ 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 monomiali irriducibili e quindi anche primari.

2.2 Ordinamenti monomiali

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 $\operatorname{Mon} A$; questo equivale ad ordinare gli elementi di $\mathbb{N}^n$. Fra gli ordinamenti possibili siamo interessati a quelli 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 $\operatorname{Mon} A$ 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 discendente in $\mathbb{N}^n$ è stazionaria, cf. **E.9.1** o **T.7.1**);

iii) per ogni $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n$ si ha che $\mathbf{a} > \mathbf{b} \Longrightarrow \mathbf{a}+\mathbf{c} > \mathbf{b}+\mathbf{c}$.

Tra gli ordinamenti più usati ci sono i seguenti, cf. **E.9.2**.

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

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 o *grado-lessicografico*:
$\mathbf{a} >_{\text{deglex}} \mathbf{b}$ 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.

Osserviamo che nella corrispondenza $X^{\mathbf{a}} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \longleftrightarrow (a_1, a_2, \ldots, a_n)$ l'ordinamento lex ordina le variabili $x_1 > x_2 > \ldots > x_n$; diciamo che questo è l'ordinamento lex con $x_1 > x_2 > \ldots > x_n$. Per esempio prendiamo $m_1 = x^2 y$ e $m_2 = xy^3$ in $K[x, y]$; nell'ordinamento lex con $x > y$ si ha $m_1 = x^2 y > xy^3 = m_2$, mentre nell'ordinamento lex con $y > x$ abbiamo $m_2 = y^3 x > yx^2 = m_1$.

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 è $\operatorname{Deg}(f) = \max_>\{\mathbf{a} \in \mathbb{N}^n \colon c_{\mathbf{a}} \neq 0\}$;

il *coefficiente direttivo* di f è $\operatorname{lc}(f) = c_{\operatorname{Deg}(f)}$;

il *monomio di testa* di f è $\operatorname{lm}(f) = X^{\operatorname{Deg}(f)}$;

il *termine di testa* di f è $\operatorname{lt}(f) = \operatorname{lc}(f) \operatorname{lm}(f) = c_{\operatorname{Deg}(f)} X^{\operatorname{Deg}(f)}$.

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

i) $\operatorname{Deg}(fg) = \operatorname{Deg}(f) + \operatorname{Deg}(g)$;

ii) se $f + g \neq 0$ allora $\operatorname{Deg}(f + g) \leq \max_>\{\operatorname{Deg}(f), \operatorname{Deg}(g)\}$.

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

$$\operatorname{Deg}(I) = \{\operatorname{Deg}(f) \colon f \in I,\ f \neq 0\}.$$

È facile verificare che $\operatorname{Deg}(I)$ è un $\mathcal{E}$-sottoinsieme che dunque ha un escalier per **T.2.5**. Chiamiamo il suo escalier l'*escalier* di I. Possiamo inoltre associare ad I l'ideale monomiale

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

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 $\operatorname{Lt}(F) = (\operatorname{lt}(f) \colon f \in F)$. Chiaramente dato un sottoinsieme G di un ideale I, avremo sempre che $\operatorname{Lt}(G) \subseteq \operatorname{Lt}(I)$.

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

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

Per convenzione, l'insieme vuoto genera l'ideale nullo e diciamo che $\emptyset$ è la base di Gröbner di $I = (0)$.

2.3 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 $h = f - \dfrac{t_{\mathbf{b}}}{\mathrm{lt}(g)} g$. 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 $\mathbf{b}$. Inoltre 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.
Per esempio consideriamo l'anello $K[x, y, z]$ e l'ordinamento lessicografico con $x > y > z$. Siano $f = 3x^2y^3z^2 + xy^2z + 2xy$, $g = 2xy - z$ e $t_{\mathbf{b}} = 3x^2y^3z^2$; allora $\mathrm{lt}(g) = 2xy$ e

$$f \xrightarrow{g} h = f - \frac{3x^2y^3z^2}{2xy} g = xy^2z + 2xy + \tfrac{3}{2}xy^2z^3.$$

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.
Iterando il procedimento otteniamo

$$\begin{aligned} f &\xrightarrow{g} \tfrac{3}{2}xy^2z^3 + xy^2z + 2xy \xrightarrow{g} \tfrac{3}{2}xy^2z^3 + xy^2z + z \\ &\xrightarrow{g} xy^2z + \tfrac{3}{4}yz^4 + z \xrightarrow{g}_* \tfrac{3}{4}yz^4 + \tfrac{1}{2}yz^2 + z. \end{aligned}$$

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 F con $f \xrightarrow{F} r$.

Un polinomio $r \in A$ si dice *ridotto rispetto ad* $F = \{f_1, \ldots, f_s\}$ se r non può essere ridotto ulteriormente modulo F, ossia se $r = 0$ oppure se $\mathrm{lt}(f_i)$ non divide alcun termine di r per ogni $i = 1, \ldots, s$.

Se $f \xrightarrow{F} r$ e r è ridotto rispetto ad 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 $\{f_1, \dots, f_s\}$ usando il procedimento descritto dal seguente algoritmo, tralasciando i casi banali in cui f oppure $f_i = 0$.

Algoritmo di divisione

Input $f, f_1, \dots, f_s \in A \setminus \{0\}$; $>$ ordinamento monomiale.
Output $u_1, \dots, u_s, r \in A$ tali che:

$f = \sum_{i=1}^{s} u_i f_i + r$;

r è ridotto rispetto a $\{f_1, \dots, f_s\}$;

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

Inizializzazione $p := f$; $u_1 := 0$; $u_2 := 0$; $\dots$; $u_s := 0$; $r := 0$;
while $p \neq 0$ **repeat**
if esiste j tale che $\mathrm{lt}(f_j) \,|\, \mathrm{lt}(p)$ **then**
$i := \min\{j : \mathrm{lt}(f_j) \,|\, \mathrm{lt}(p)\}$
$u_i := u_i + \dfrac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)}$
$p := p - \dfrac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)} f_i$
else
$r := r + \mathrm{lt}(p)$
$p := p - \mathrm{lt}(p)$
endif
endwhile
Return $\{u_1, \dots, u_s, r\}$

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

Teorema di divisione

T. 2.8. (→ p. 202) Fissato un ordinamento monomiale, per ogni insieme di polinomi $F = \{f_1, \dots, f_s\}$ e $f \in A$ esistono polinomi $u_1, \dots, u_s, r \in A$ tali

che
i) $f = \sum_{i=1}^{s} u_i f_i + r$;
ii) r è ridotto rispetto a F;
iii) se $u_i f_i \neq 0$ allora $\mathrm{Deg}(u_i f_i) \leq \mathrm{Deg}(f)$.

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

$$\mathrm{lm}(f) = \begin{cases} \max\{\max_{u_i \neq 0}\{\mathrm{lm}(u_i)\mathrm{lm}(f_i)\}, \mathrm{lm}(r)\} & \text{se } r \neq 0; \\ \max_{u_i \neq 0}\{\mathrm{lm}(u_i)\mathrm{lm}(f_i)\} & \text{altrimenti.} \end{cases} \tag{2.1}$$

Osserviamo inoltre che l'algoritmo di divisione appena descritto implicitamente assume che i polinomi $f_1, \dots, f_s$ siano ordinati quando si sceglie il minimo indice i tale che $\mathrm{lt}(f_i) \mid \mathrm{lt}(p)$; in effetti questa scelta può modificare il risultato della divisione, cf. **E.9.5**. 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 $f_1, \dots, f_s$ costituiscono una base di Gröbner per l'ideale che generano; anzi, questa proprietà caratterizza le basi di Gröbner.

2.4 Basi di Gröbner: prime proprietà

Siano $>$ un ordinamento monomiale fissato, $I \neq 0$ un ideale di A e $G = \{g_1, \dots, g_t\} \subset I \setminus \{0\}$; allora, per definizione, G è una base di Gröbner di I se $\mathrm{Lt}(G) = (\mathrm{lt}(g_1), \dots, \mathrm{lt}(g_t)) = \mathrm{Lt}(I)$.
Equivalentemente, G è una base di Gröbner se $\{\mathrm{Deg}(g_1), \dots, \mathrm{Deg}(g_t)\}$ 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 è una base di Gröbner *minimale* se i polinomi g_i sono monici e $\{\mathrm{Deg}(g_1), \dots, \mathrm{Deg}(g_t)\}$ 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 $\{\mathrm{lt}(g_1), \dots, \mathrm{lt}(g_t)\}$. Partendo da G è dunque sempre possibile costruire una base di Gröbner minimale di I.
Osserviamo che una base di Gröbner rispetto ad un ordinamento monomiale $>$ non è in generale una base di Gröbner rispetto ad un altro ordinamento monomiale $>_1$, cf. **E.9.6**.

T. 2.9. (→ p. 203) Siano $I \subset A$ un ideale, $G = \{g_1, \dots, g_t\} \subset I \setminus \{0\}$ e $>$ un ordinamento monomiale; allora 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 $\mathrm{lm}(f) = \max_{u_i \neq 0}\{\mathrm{lm}(u_i)\mathrm{lm}(g_i)\}$.

T. 2.10. (→ p. 203) 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.

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.

Unicità del resto

T. 2.11. (→ p. 203) Sia $G = \{g_1, \ldots, g_t\} \subset I \setminus \{0\}$. Se G è una base di Gröbner di I rispetto a $>$ allora per ogni $f \in A$ il resto della divisione di f per G è unico.

In realtà vale anche il viceversa della precedente affermazione; per una dimostrazione completa vedi [1, Theorem 1.6.7].
Data una base di Gröbner G e un polinomio $f \in A$ esiste dunque *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 notare 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 $f = x_1 x_2$. Non è difficile verificare che G è una base di Gröbner rispetto all'ordinamento lessicografico con $x_1 > x_2 > x_3$. 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 e g_2 nelle due espressioni di f sono diversi.

T. 2.12. (→ p. 203) 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 e r' i resti della divisione di un polinomio $f \in A$ per G e G' rispettivamente; allora $r = r'$.

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

Teorema della base di Hilbert

T. 2.13. Ogni ideale di A è finitamente generato.

Dimostrazione T. 2.13. Fissiamo su A un ordinamento monomiale $>$ e sia $I \neq 0$ un ideale di A; allora l'ideale iniziale $\mathrm{Lt}(I)$ rispetto a $>$ ha un insieme di generatori monomiale finito, diciamo $\mathrm{Lt}(I) = (m_1, \dots, m_t)$. Per ogni $i = 1, \dots, t$ esiste $f_i \in I$ tale che $\mathrm{lt}(f_i) = m_i$; da ciò segue che $\{f_1, \dots, f_t\}$ è una base di Gröbner di I e da **T.2.10** segue che $I = (f_1, \dots, f_t)$. □

T. 2.14. Sia B un anello; allora ogni ideale di B è finitamente generato se e solo se ogni catena ascendente di ideali di B è stazionaria.

Lasciamo al lettore la dimostrazione di questo fatto per esercizio in attesa della dimostrazione generale nel caso dei moduli, cf. **T.7.2**.1.
Un anello in cui ogni catena ascendente di ideali è stazionaria si dice *noetheriano*, cf. Capitolo 7. Abbiamo dunque appena dimostrato che l'anello dei polinomi a coefficienti in K è noetheriano; per il risultato generale cf. **T.7.4**.

2.5 Costruzione di una base di Gröbner: l'algoritmo di Buchberger

Abbiamo visto che se G è una base di Gröbner di I rispetto a qualche ordinamento monomiale 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.
Per esempio siano $I = (f_1, f_2)$ con $f_1 = x_1 x_2^2 + x_1$ e $f_2 = x_1^2 x_2 + x_2$; se consideriamo l'ordinamento lessicografico con $x_1 > x_2$ si ha che il polinomio $f = x_1 f_1 - x_2 f_2 = x_1^2 - x_2^2 \in I$ ma $x_1^2 \notin (x_1 x_2^2,\, x_1^2 x_2) = (\mathrm{lt}(f_1), \mathrm{lt}(f_2))$.

Veniamo ora al problema di come costruire una base di Gröbner. 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 $c_i = \max\{a_i, b_i\}$; allora $X^{\mathbf{c}}$ è il minimo comune multiplo di $\mathrm{lm}(f)$ e $\mathrm{lm}(g)$.

S-polinomio

Definiamo l'*S-polinomio di 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 a [5, Chapter 2, §7].

Criterio di Buchberger

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

Usando il precedente criterio possiamo ottenere un algoritmo per la costruzione di una base di Gröbner di un ideale $I = (f_1, \dots, f_s)$. Procederemo calcolando gli S-polinomi $S(f_i, f_j)$ dei generatori di I ed i loro resti rispetto a $\{f_1, \dots, f_s\}$. 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 $\{f_1, \dots, f_s\}$ 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 $I = (f_1, \dots, f_s) \subseteq A$, $f_i \neq 0$ per $i = 1, \dots, s$; $>$ ordinamento monomiale.
Output Una base di Gröbner G di I rispetto a $>$ tale che $\{f_1, \dots, f_s\} \subseteq G$.
Inizializzazione
  $F := \{f_1, \dots, f_s\}$
  $G := F$
  $\Sigma := \{(f_i, f_j) \in G \times G \colon f_i \neq f_j\}$
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
        $\Sigma := \Sigma \cup \{(h, p) \colon h \in G\}$
        $G := G \cup \{p\}$
      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. 2.15. L'algoritmo di Buchberger termina ed è corretto.

Dimostrazione T. 2.15. Sicuramente l'algoritmo è corretto perché la condizione di terminazione è che $\overline{S(f,g)}^{G} = 0$ per ogni $f, g \in G$; questo garantisce che l'output sia effettivamente una base di Gröbner per il criterio di Buchberger. D'altronde, se l'algoritmo non terminasse, costruiremmo progressivamente una catena ascendente di insiemi $G_1 \subsetneq G_2 \subsetneq \ldots$, dove le inclusioni sono strette perché per costruire G_{i+1} aggiungiamo a G_i un elemento di I che non 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, cf. **T.2.14**. □

Concludiamo questa sezione con il seguente corollario estremamente utile per determinare in certi casi che un insieme G è una base di Gröbner; una dimostrazione si può trovare in [5, Chapter 2, §9 Proposition 4].

T. 2.16. 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 $>$.

2.6 Basi di Gröbner minimali e ridotte

Abbiamo visto che ogni ideale di A ammette una base di Gröbner G' rispetto ad un ordinamento monomiale $>$ e come da essa si può estrarre una base minimale G. 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.
Per esempio sia $I = (x_1, x_2) \subset K[x_1, x_2]$; allora per ogni $a \in K$ e per ogni $k \in \mathbb{N}$ gli insiemi $\{x_1 + ax_2^k, x_2\}$ sono basi di Gröbner minimali di 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 il polinomio g_i sia ridotto rispetto a $G \setminus \{g_i\}$ per ogni $i = 1, \ldots, t$ e quindi che in g_i non esistano termini diversi da zero divisibili per $\mathrm{lt}(g_j)$ con $j \neq i$.

Base di Gröbner ridotta

Una base di Gröbner $G = \{g_1, \ldots, g_t\}$ 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. 2.17. (→ p. 203) Sia $G = \{g_1, \dots, g_t\}$ una base di Gröbner minimale di un ideale $I \subset A$ rispetto ad un ordinamento monomiale $>$. Definiamo elementi $g'_1, \dots, g'_t$ nella maniera seguente

$$
\begin{aligned}
& g_1 \xrightarrow{G'_1}{}_* g'_1\,, && \text{con } G'_1 = \{g_2, \dots, g_t\};\\
& \vdots \\
& g_i \xrightarrow{G'_i}{}_* g'_i\,, && \text{con } G'_i = \{g'_1, \dots, g'_{i-1}, g_{i+1}, \dots, g_t\};\\
& \vdots \\
& g_t \xrightarrow{G'_t}{}_* g'_t\,, && \text{con } G'_t = \{g'_1, \dots, g'_{t-1}\};
\end{aligned}
$$

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

Unicità della base ridotta

T. 2.18. (→ p. 203) Siano $G = \{g_1, \dots, g_t\}$ e $G' = \{g'_1, \dots, g'_t\}$ due basi di Gröbner ridotte di un ideale I rispetto ad uno stesso ordinamento monomiale $>$; allora $G = G'$.

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 minimale di generatori di I non costituisce in generale una base di Gröbner minimale.
Per esempio siano $f_1 = x_1^3$, $f_2 = x_1^2 x_2 - x_2^2$ 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 G di I è $\{f_1, f_2, f_3, f_4\}$ dove $f_3 = x_1 x_2^2$ e $f_4 = x_2^3$. Quindi G contiene 4 elementi mentre I può essere generato da solo 2 elementi.

2.7 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 risolvere alcuni problemi concreti. Per esempio:

1. dato un polinomio $f \in A$ e un ideale $I = (f_1, \dots, f_s) \subseteq A$, decidere se $f \in I$;

1′. in caso affermativo, trovare $c_1, \dots, c_s \in A$ 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.

Per rispondere alla prima di queste domande bisogna calcolare una base di Gröbner G di I e controllare che il resto della divisione di f per G sia 0. Applicando **T.2.9** e **T.2.11** si ottiene il seguente risultato.

Test di appartenenza

T. 2.19. Siano $f \in A$, I un ideale di A e $>$ un ordinamento monomiale fissato. Sia inoltre $G = \{g_1, \dots, g_t\}$ una base di Gröbner di I rispetto a $>$; allora

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

Si può implementare l'algoritmo di Buchberger in modo che nel calcolo di una base di Gröbner G a partire da $\{f_1, \dots, f_s\}$ vengano memorizzati passo passo i coefficienti delle combinazioni degli f_i che danno origine ai g_j; se $\{h_1, \dots, h_l\}$ 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

$$M(f_1, \dots, f_s)^{\mathrm{t}} = (g_1, \dots, g_t)^{\mathrm{t}}. \tag{2.2}$$

Se dividiamo $f \in I$ per $G = \{g_1, \dots, g_t\}$ otteniamo polinomi $u_1, \dots, u_t$ 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 dei polinomi $f_1, \dots, f_s$. Abbiamo in questo modo risposto anche al quesito 1′, cf. **E.9.12** per un esempio esplicito.

Il seguente risultato è un'immediata conseguenza del Teorema di unicità delle basi di Gröbner ridotte **T.2.18** e risponde al problema 2.

Test di uguaglianza tra ideali

T. 2.20. Siano $>$ un ordinamento monomiale fissato, $I, J \subset A$ ideali, G e G'

le basi di Gröbner ridotte di I e J rispettivamente; allora,

$$I = J \iff G = G'.$$

Anche il seguente criterio risulta spesso utile.

T. 2.21. (→ p. 204) Siano $I, J \subseteq A$ ideali tali che $I \subseteq J$; se, per qualche ordinamento $>$, si ha $\mathrm{Lt}(I) = \mathrm{Lt}(J)$ allora $I = J$.

T. 2.22. Sia I un ideale con base di Gröbner G rispetto a $>$.

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

$$f \equiv g \mod I \iff \overline{f}^G = \overline{g}^G.$$

Dimostrazione T. 2.22. 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 $af + bg = a(f - r) + b(g - s) + ar + bs$, dove $f - r$ e $g - s$ 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 $f - g \in I$ che è equivalente a $\overline{f - g}^G = 0$ per **T.2.9**; per il punto 1 allora $\overline{f}^G - \overline{g}^G = 0$. □

Notiamo dunque che $\left\{\overline{f}^G : f \in A\right\}$ è un insieme di rappresentanti di A/I; infatti se $r = \overline{f}^G$ abbiamo che $f - r \in I$ perciò $\overline{f} = \overline{r}$ in A/I, vedi problema 3. Con il seguente risultato rispondiamo al quarto quesito.

K-base di A/I

T. 2.23. (→ p. 204) Siano $I \subset A$ un ideale e $G = \{g_1, \ldots, g_t\}$ una base di Gröbner di I rispetto ad un ordinamento monomiale $>$ fissato.

1. Sia $\mathcal{B} = \{X^{\mathbf{a}} : \mathrm{lm}(g) \nmid X^{\mathbf{a}} \text{ per ogni } g \in G\} = \{X^{\mathbf{a}} : X^{\mathbf{a}} \notin \mathrm{Lt}(I)\}$; allora

$$\overline{\mathcal{B}} = \{\overline{m} \in A/I : m \in \mathcal{B}\}$$

   è una K-base di A/I.

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

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

T. 2.24. (→ p. 204) Un elemento $f \in A$ è invertibile modulo $I = (f_1, \ldots, f_s)$ se e solo se $(I, f) = 1$.

2.7.1 Eliminazione ed ordinamento lessicografico

Gli ordinamenti lessicografici soddisfano una proprietà importante, detta *di eliminazione*, che analizzeremo nel seguito e che ha alcune applicazioni di rilievo. Per il resto della sezione sia $>$ l'ordinamento lessicografico con $x_1 > x_2 > \ldots > x_n$.
Sia $I \subset A$; 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 inclusione $K[x_{k+1}, \ldots, x_n] \longrightarrow A$.

Teorema di eliminazione delle variabili

T. 2.25. Siano $I \subset A$ un ideale e $>$ l'ordinamento lessicografico con $x_1 > x_2 > \ldots > x_n$. Sia inoltre 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-esimo ideale di eliminazione I_k di I per ogni $k = 1, \ldots, n-1$.

Dimostrazione T. 2.25. 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 $\mathrm{lt}(f)$ 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 $f \in I_k \subseteq K[x_{k+1}, \ldots, x_n]$, in $\mathrm{lt}(g)$ possono apparire solo le 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 $g \in G_k$. □

Ecco infine alcune applicazioni del precedente risultato.

T. 2.26. (→ p. 204) Siano $I, J \subseteq A$ ideali.

1. [**Calcolo dell'intersezione di ideali**] Sia t una nuova indeterminata; allora

$$I \cap J = (tI, (1-t)J) \cap A.$$

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

2. [**Calcolo del quoziente di ideali**] Sia $J = (f_1, \ldots, f_s)$; allora

$$I : J = \bigcap_{i=1}^{s} \left(\frac{1}{f_i} (I \cap (f_i)) \right).$$

T. 2.27. (→ p. 205) [**Test di appartenenza al radicale**] Sia $I \subsetneq A$ un ideale e t un'indeterminata; allora

$$f \in \sqrt{I} \quad \text{se e solo se} \quad (I, 1 - tf) = A[t].$$

3

Varietà algebriche affini

In questo capitolo introdurremo le varietà algebriche affini e gli ideali di annullamento e studieremo le loro proprietà collegandole alla teoria degli ideali sviluppata finora. Dimostreremo il Teorema degli zeri di Hilbert e lo applicheremo insieme alla teoria delle basi di Gröbner allo studio delle soluzioni dei sistemi di equazioni polinomiali.

3.1 Definizione e prime proprietà

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

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

rispettivamente

$$\mathbb{V}(I) = \{(a_1, \dots, a_n) \in K^n \colon f(a_1, \dots, a_n) = 0 \text{ per ogni } f \in I\}.$$

Dal Teorema della base di Hilbert **T.2.13** sappiamo che ogni ideale di A è finitamente generato; inoltre, se $I = (F)$ è immediato verificare che $(a_1, \dots, a_n) \in K^n$ è tale che $f(a_1, \dots, a_n) = 0$ per ogni $f \in I$ se e solo se $f(a_1, \dots, a_n) = 0$ per ogni $f \in F$. Avremo dunque che $\mathbb{V}(I) = \mathbb{V}(F)$ per ogni insieme di generatori F di I.
Data una varietà affine $V \subseteq K^n$, chiamiamo *ideale associato a* V l'ideale

$$\mathbb{I}(V) = \{f \in A \colon f(\alpha) = 0 \text{ per ogni } \alpha \in V\} \subseteq A$$

e *anello delle coordinate di* V l'anello

$$A/\mathbb{I}(V).$$

È possibile fornire una definizione analoga per un qualsiasi sottoinsieme di K^n, ma ci occuperemo principalmente di varietà quindi, almeno inizialmente,

supporremo sempre $V = \mathbb{V}(I)$ per qualche ideale I di A, cf. l'approfondimento alla fine di questo capitolo.

Vorremmo ora capire che proprietà hanno le funzioni

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

Varietà: prime proprietà

T. 3.1. (→ p. 205) Siano $I, J \subseteq A$ ideali e $V, W \subseteq K^n$ varietà affini; allora

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

In particolare dai punti 5 e 6 segue che l'intersezione e l'unione di due varietà affini sono varietà affini. Se $V \subseteq W$ allora diremo che V è una *sottovarietà* di W. Inoltre vedremo che su K^n possiamo introdurre la *topologia di Zariski* in cui i chiusi sono le varietà affini, cf. **T.3.20**. Il prossimo risultato dimostra che tale spazio topologico è noetheriano.

T. 3.2. (→ p. 206) Ogni catena discendente di varietà affini è stazionaria.

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

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

T. 3.3. Una varietà V è irriducibile se e solo $\mathbb{I}(V)$ è un ideale primo.

Dimostrazione T. 3.3. Sia $fg \in \mathbb{I}(V)$; vogliamo provare che se V è irriducibile allora $f \in \mathbb{I}(V)$ oppure $g \in \mathbb{I}(V)$. Consideriamo le varietà $V_1 = V \cap \mathbb{V}(f)$ e $V_2 = V \cap \mathbb{V}(g)$ e proviamo che $V_1 \cup V_2 = V$. Da **T.3.1**.7 discende infatti che

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

dove l'ultima uguaglianza è dovuta al fatto che $\mathbb{V}(fg) \supseteq \mathbb{V}(\mathbb{I}(V)) = V$, cf. **T.3.1**.1 e 3. Dato che V è irriducibile si deve avere necessariamente $V = V_1$ oppure $V = V_2$; da ciò segue che $\mathbb{V}(f) \supseteq V$ oppure $\mathbb{V}(g) \supseteq V$ e quindi che $f \in \mathbb{I}(\mathbb{V}(f)) \subseteq \mathbb{I}(V)$ oppure $g \in \mathbb{I}(\mathbb{V}(g)) \subseteq \mathbb{I}(V)$ per **T.3.1**.4.

Viceversa, supponiamo che $\mathbb{I}(V)$ sia primo e che $V = V_1 \cup V_2$; passando agli ideali otteniamo che $\mathbb{I}(V) = \mathbb{I}(V_1 \cup V_2) = \mathbb{I}(V_1) \cap \mathbb{I}(V_2)$, dove l'ultima uguaglianza è di facile verifica. Poiché $\mathbb{I}(V)$ è primo, è anche irriducibile, cf. **T.1.13**; dunque $\mathbb{I}(V_1) = \mathbb{I}(V)$ oppure $\mathbb{I}(V_2) = \mathbb{I}(V)$. Sfruttando il fatto che $\mathbb{V}(\mathbb{I}(V)) = V$ si ha allora che $V_1 = V$ oppure $V_2 = V$ e dunque V è irriducibile. □

Non è sempre vero che la varietà associata ad un ideale primo è irriducibile. Per esempio siano $K = \mathbb{Z}/(2)$, $A = K[x, y]$ e $I = (x + y)$; allora $A/I \simeq K[x]$ è un dominio, quindi I è primo, mentre $\mathbb{V}(I) = \{(0,0), (1,1)\} \subsetneq K^2$ è riducibile in quanto unione di $V_1 = \{(0,0)\} = \mathbb{V}((x,y))$ e $V_2 = \{(1,1)\} = \mathbb{V}((x+1, y+1))$, due varietà strettamente contenute in $\mathbb{V}(I)$. Notiamo inoltre che $V = \mathbb{V}((x,y)(x+1,y+1)) = \mathbb{V}((x^2+x, xy+x, xy+y, y^2+y))$, dunque $\mathbb{I}(\mathbb{V}(I)) \supseteq (x^2+x, xy+x, xy+y, y^2+y) \supsetneq I$ e $\mathbb{I}(\mathbb{V}(I))$ non è primo per il risultato precedente.

Decomposizione in varietà irriducibili

T. 3.4. (→ p. 206) 1. Ogni varietà affine V si decompone come unione finita di varietà irriducibili, cioè esiste un intero t tale che $V = \bigcup_{i=1}^{t} V_i$ con V_i irriducibile per $i = 1, \dots, t$.

2. Se una tale decomposizione è minimale, ovvero se $V_i \not\subseteq V_j$ per ogni $i \neq j$, allora è unica a meno dell'ordine.
Chiamiamo le varietà V_i *componenti irriducibili* di V.

Concludiamo questa parte con un'osservazione sulle varietà costituite da un solo punto.

T. 3.5. (→ p. 206) Sia $\alpha = (a_1, \dots, a_n) \in K^n$; allora $V_\alpha = \{\alpha\}$ è una varietà. Inoltre

$$\mathbb{I}(V_\alpha) = (x_1 - a_1, \dots, x_n - a_n)$$

è un ideale massimale, che denotiamo con $\mathfrak{m}_\alpha$.

Per quanto appena visto ad ogni punto $\alpha = (a_1, \dots, a_n) \in K^n$ corrisponde un ideale massimale di $K[x_1, \dots, x_n]$. 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 $g = \sum_{i=0}^{\ell} b_i x^i$ con $a_m,\ b_\ell \neq 0$ due polinomi in $A[x] \setminus \{0\}$ non entrambi costanti di grado m ed ℓ rispettivamente. Definiamo *matrice di Sylvester di f e g* la matrice quadrata $(m+\ell) \times (m+\ell)$

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

Per l'origine di questa matrice e la sua connessione con l'esistenza di fattori comuni tra f e g, cf. [5, Chapter 3, §6].

Definiamo il *risultante di f, g* come $\mathrm{Ris}(f,g) = \det \mathrm{Syl}(f,g)$.
Se $f, g \in A \setminus \{0\}$ poniamo per definizione $\mathrm{Ris}(f,g) = 1$.
Osserviamo che se $m > 0$ e $\ell = 0$ allora otteniamo la matrice $m \times m$ diagonale con $g = b_0$ sulla diagonale, per cui $\mathrm{Ris}(f,g) = b_0^m$. Analogamente, se $m = 0$ e $\ell > 0$ allora $\mathrm{Ris}(f,g) = a_0^\ell$. Le affermazioni seguenti discendono immediatamente dalle proprietà del determinante.

Proprietà del risultante - I

T. 3.6. Siano $A,\ f$ e g come sopra; allora

1. $\mathrm{Ris}(f,g) \in A$;
2. $\mathrm{Ris}(f,g) = (-1)^{m\ell}\,\mathrm{Ris}(g,f)$;
3. $\mathrm{Ris}(af,g) = a^\ell\,\mathrm{Ris}(f,g)$ e $\mathrm{Ris}(f,bg) = b^m\,\mathrm{Ris}(f,g)$ per ogni $a, b \in A$.

Dimostriamo un altro fatto fondamentale sul risultante.

T. 3.7. Siano $A,\ f$ e g come sopra; allora esistono polinomi $h_1,\ h_2 \in A[x]$ con $\deg h_1 < \deg g$ e $\deg h_2 < \deg f$ tali che

$$\mathrm{Ris}(f,g) = h_1 f + h_2 g.$$

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

Dimostrazione T. 3.7. Sommando all'ultima colonna della matrice di Sylvester la colonna i-esima moltiplicata per $x^{m+\ell-i}$ per ogni $i = 1, \dots, m+\ell-1$, otteniamo

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

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

Vediamo un semplice caso particolare. Sia $f = ax^2 + bx + c \in \mathbb{Q}[x]$ con $a \neq 0$; allora

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

quindi $\operatorname{Ris}(f,f') = 0$ se e solo se f ha una radice doppia, i.e. se e solo se f e f' hanno una radice in comune.
Tale proprietà è di cruciale importanza e vale in generale. Per dimostrarla abbiamo bisogno di alcuni fatti, che includiamo nel seguente enunciato.

T. 3.8. Siano m un intero positivo, $Y = y_1, \dots, y_m$ indeterminate e $f_m(x)$ il polinomio

$$f_m(x) = \prod_{i=1}^{m} (x - y_i) = \sum_{i=0}^{m} a_i^{(m)} x^i \in A[Y][x] \simeq A[Y,x];$$

allora

1. i coefficienti $a_i^{(m)}$ sono funzioni lineari in y_j per ogni $j = 1, \dots, m$;
2. $a_i^{(m)}(y_1, \dots, y_{m-1}, 0) = a_{i-1}^{(m-1)}(y_1, \dots, y_{m-1})$ per ogni $0 < i \leq m$ e inoltre $a_0^{(m)}(y_1, \dots, y_{m-1}, 0) = 0$;
3. dato un polinomio $g = \sum_{i=0}^{\ell} b_i x^i \in A[x]$, 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. 3.8. 1. I coefficienti di f_m sono le funzioni simmetriche elementari nelle variabili $y_1, \dots, y_m$ e quindi si ha

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

da cui segue che gli $a_i^{(m)}$ sono lineari 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 in $y_m = 0$ 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 $i = 0$ segue subito da quanto visto al punto 1.

3. Consideriamo la matrice di Sylvester

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

Moltiplicando la colonna i-esima della matrice per $y_m^{m+\ell-i}$ e sommando il risultato all'ultima colonna per ogni $i = 1, \dots, m + \ell - 1$ otteniamo

$$\begin{pmatrix} a_m^{(m)} & \cdots & a_0^{(m)} & & & y_m^{\ell-1} f_m(y_m) \\ & \ddots & & & & \vdots \\ & & a_m^{(m)} & & \cdots & f_m(y_m) \\ b_\ell & \cdots & b_1 & b_0 & & y_m^{m-1} g(y_m) \\ & \ddots & & & & \vdots \\ & & b_\ell & & \cdots & g(y_m) \end{pmatrix}.$$

Dato che $f_m(y_m) = 0$, dalle proprietà del determinante discende che

$$\operatorname{Ris}(f_m(x), g(x)) = g(y_m) \det \begin{pmatrix} a_m^{(m)} & \cdots & a_0^{(m)} & & & 0 \\ & \ddots & & & & \vdots \\ & & a_m^{(m)} & & \cdots & 0 \\ b_\ell & \cdots & b_1 & b_0 & & y_m^{m-1} \\ & \ddots & & & & \vdots \\ & & b_\ell & & \cdots & 1 \end{pmatrix}$$

Chiamiamo M quest'ultima matrice; abbiamo provato che $\operatorname{Ris}(f_m(x), g(x)) = g(y_m) \det M$.
Dato che A è un dominio, abbiamo che

$$\deg_{y_m}(\operatorname{Ris}(f_m(x), g(x))) = \deg_{y_m}(g(y_m)) + \deg_{y_m}(\det M).$$

Per il punto 1

$$\deg_{y_m}(\operatorname{Ris}(f_m(x), g(x))) = \deg_{y_m}(\det(\operatorname{Syl}(f_m, g))) \leq \ell;$$

inoltre $\deg_{y_m}(g(y_m)) = \ell$ e dunque si deve avere $\deg_{y_m}(\det M) = 0$. Quindi possiamo valutare y_m in 0 senza modificare $\det M$. Usando il punto 2 otteniamo

$$\operatorname{Ris}(f_m(x), g(x)) = g(y_m) \det \begin{pmatrix} a_{m-1}^{(m-1)} & \cdots & a_0^{(m-1)} & \cdots & \cdots & 0 \\ & \ddots & & \ddots & & \vdots \\ & & a_{m-1}^{(m-1)} & \cdots & a_0^{(m-1)} & 0 \\ b_\ell & \cdots & b_1 & b_0 & & \vdots \\ & \ddots & & \ddots & & 0 \\ & & b_\ell & \cdots & b_1 & 1 \end{pmatrix}$$

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

$$= g(y_m) \operatorname{Ris}(f_{m-1}(x), g(x)).$$

□

Proprietà del risultante - II

T. 3.9. (→ p. 207) Siano $A = K$ un campo, $f = \sum_{i=0}^{m} a_i x^i$ e $g = \sum_{i=0}^{\ell} b_i x^i$ polinomi in $K[x]$ con $a_m, b_\ell \neq 0$.

1. Siano $\alpha_1, \ldots, \alpha_m$ e $\beta_1, \ldots, \beta_\ell$ le radici di f e g in $\overline{K}$ rispettivamente; allora
$$\operatorname{Ris}(f,g) = a_m^\ell \prod_{i=1}^{m} g(\alpha_i) = (-1)^{m\ell} b_\ell^m \prod_{j=1}^{\ell} f(\beta_j) \in \overline{K}.$$
2. $\operatorname{Ris}(f,g) = a_m^\ell b_\ell^m \prod_{j=1}^{\ell} \prod_{i=1}^{m} (\alpha_i - \beta_j) \in \overline{K}$.
3. Se $K = \overline{K}$ allora $\operatorname{Ris}(f,g) = 0$ se e solo se f e g hanno una radice in comune.
4. $\operatorname{Ris}(f,g) = 0$ se e solo se f e g hanno un fattore comune di grado positivo.

Concludiamo questa parte con un'osservazione che ci sarà utile nella dimostrazione del Teorema di estensione **T.3.11**.

T. 3.10. (→ p. 207) Siano f e g polinomi in $K[x_1, \ldots, x_n]$ con
$$f = \sum_{i=0}^{m} c_i(x_2, \ldots, x_n) x_1^i \quad \text{e} \quad g = \sum_{i=0}^{\ell} d_i(x_2, \ldots, x_n) x_1^i$$
di grado in x_1 rispettivamente m e ℓ; sia inoltre $\beta \in K^{n-1}$.
Se $f(x_1, \beta)$ ha ancora grado m in x_1 e $g(x_1, \beta)$ è diverso da zero e di grado $\ell - r$ in x_1 per qualche intero $0 \leq r \leq \ell$ allora
$$\operatorname{Ris}_{x_1}(f,g)(\beta) = c_m(\beta)^r \operatorname{Ris}_{x_1}(f(x_1,\beta), g(x_1,\beta)).$$

3.3 Teorema di estensione

Prima di dimostrare il Teorema di estensione ricordiamo i seguenti fatti. Un campo K algebricamente chiuso è infinito; infatti, se fosse $K = \{a_1, \ldots, a_s\}$ finito allora il polinomio $\prod_{i=1}^{s}(x - a_i) + 1$ non avrebbe soluzioni in K, che è assurdo. Di conseguenza è facile verificare per induzione sul numero di variabili 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 $\Sigma = \{f_i = 0 \colon i = 1, \ldots, s\}$. 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* di Σ quando $(a_{k+1}, \ldots, a_n) \in \mathbb{V}(I_k)$.

Teorema di estensione delle soluzioni

T. 3.11. Siano $K = \overline{K}$ un campo algebricamente chiuso, $I = (f_1, \dots, f_s)$ un ideale proprio di A e $I_1 = I \cap K[x_2, \dots, x_n]$ il primo ideale di eliminazione di I. Per ogni $i = 1, \dots, s$ scriviamo

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

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

Dimostrazione T. 3.11. Per ipotesi esiste $i \in \{1, \dots, s\}$ tale che $c_i(\beta) \neq 0$ e dunque $\deg_{x_1} f_i(x_1, \beta) = \deg_{x_1} f_i(x_1, \dots, x_n) = N_i$.
Se $N_i = 0$ allora $f_i(x_1, \dots, x_n) = c_i(x_2, \dots, x_n) \in I_1$ e $c_i(\beta) \neq 0$ contraddice l'ipotesi $\beta \in \mathbb{V}(I_1)$; quindi $N_i \geq 1$.
Consideriamo l'omomorfismo $\varphi\colon A \longrightarrow K[x_1]$ di valutazione in β definito da $f(x_1, x_2, \dots, x_n) \mapsto f(x_1, \beta)$, che è surgettivo. L'immagine $I^e = \varphi(I)$ dell'ideale di partenza è un ideale principale ed esiste $g \in I$ tale che $I^e = (\varphi(g)) = (g(x_1, \beta))$.
In particolare, per ogni $f \in I$ si ha che $g(x_1, \beta)$ divide $f(x_1, \beta)$ e, dato che $f_i(x_1, \beta) \neq 0$, deve essere $g(x_1, \beta) \neq 0$. Quindi, se proviamo che esiste $a_1 \in K$ tale che $g(a_1, \beta) = 0$ otteniamo $f(a_1, \beta) = 0$ per ogni $f \in I$, ossia $(a_1, \beta) \in \mathbb{V}(I)$ estende β ed è la soluzione cercata.
Per trovare tale a_1 definiamo $h(x_2, \dots, x_n) = \operatorname{Ris}_{x_1}(f_i, g)$. Sappiamo che $h \in I_1$ per **T.3.7**; allora $h(\beta) = 0$ per ipotesi, e per **T.3.10** vale che

$$h(\beta) = c_i(\beta)^r \operatorname{Ris}_{x_1}(f_i(x_1, \beta), g(x_1, \beta)),$$

dove $\deg_{x_1} g(x_1, \beta) = \deg_{x_1} g - r$. Se $r = \deg_{x_1} g$, cioè se $g(x_1, \beta)$ è una costante non nulla, otteniamo la contraddizione $h(\beta) = c_i(\beta)^{\deg_{x_1} g} g(x_1, \beta)^{N_i} \neq 0$. Dunque $\deg_{x_1} g(x_1, \beta) \geq 1$ e, dato che K è algebricamente chiuso, ammette almeno una radice a_1. □

3.4 Nullstellensatz e le sue conseguenze

Come nella sezione precedente assumiamo che $K = \overline{K}$ sia algebricamente chiuso e $A = K[x, \dots, x_n]$. Nel seguito è utile ricordare che dato un termine $cX^{\mathbf{a}}$ con $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{N}^n$ 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 $f = f(x_1, \dots, x_n)$ si dice *omogeneo di grado d* se $f(tx_1, tx_2, \dots, tx_n) = t^d f(x_1, \dots, x_n)$. 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.

Per la validità del seguente fatto serve solo che K sia infinito.

T. 3.12. (→ p. 208) Sia $f \in A$ un polinomio di grado $N \geq 1$; allora esistono $\alpha_2, \ldots, \alpha_n \in K$ e un cambiamento lineare di coordinate $\varphi\colon A \longrightarrow K[y_1, \ldots, y_n]$ definito da $x_1 \mapsto y_1$ e $x_i \mapsto y_i + \alpha_i y_1$ per ogni $i = 2, \ldots, n$ tali che

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

Teorema degli zeri di Hilbert

T. 3.13. [**Nullstellensatz, forma debole**] Siano K un campo algebricamente chiuso e $I \subseteq A$ un ideale; allora

$$\mathbb{V}(I) = \emptyset \iff I = (1).$$

T. 3.14. [**Nullstellensatz, forma forte**] Siano K un campo algebricamente chiuso e $I \subseteq A$ un ideale; allora

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

Dimostrazione T. 3.13. È chiaro che se $I = (1)$ allora $\mathbb{V}(I) = \emptyset$.

Viceversa, procediamo per induzione sul numero di variabili n. Se $n = 1$ allora $K[x]$ è PID, dunque $I = (f)$. Poiché K è algebricamente chiuso, gli unici polinomi senza radici sono costanti non nulle 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 $\mathbb{V}(I) = \emptyset$. Se $f_1 \in K^*$ allora la tesi vale; altrimenti supponiamo che f_1 abbia grado totale $N \geq 1$.
Per **T.3.12** esiste un cambiamento lineare di coordinate φ tale che $\varphi(f_1) = cy_1^N + f'$ 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 $\mathbb{V}(\varphi(I)) = \emptyset$. Dal Teorema di estensione segue allora che $\mathbb{V}(\varphi(I)_1) = \emptyset$; infatti, se così non fosse un elemento $\beta \in \mathbb{V}(\varphi(I)_1)$ verrebbe sicuramente esteso ad un elemento $\alpha \in \mathbb{V}(\varphi(I))$, poiché $c \in K^*$ e $\mathbb{V}((c)) = \emptyset$. Per l'ipotesi induttiva allora abbiamo $1 \in \varphi(I)_1 \subseteq \varphi(I)$ e da questo segue che $1 \in I$, come volevamo. □

Dimostrazione T. 3.14. L'inclusione $\sqrt{I} \subseteq \mathbb{I}(\mathbb{V}(I))$ è sempre vera; infatti, da **T.3.1**.2 e 8 segue che $\sqrt{I} \subseteq \mathbb{I}(\mathbb{V}(\sqrt{I})) = \mathbb{I}(\mathbb{V}(I))$.

Per l'altra inclusione, sia $f \in \mathbb{I}(\mathbb{V}(I))$; consideriamo l'ideale $J = (I, 1 - tf) \subseteq K[t, x_1, \ldots, x_n]$ e proviamo che $\mathbb{V}(J) = \emptyset$. Da questo e dal Teorema degli zeri, forma debole, segue che $1 \in J$ e dunque la conclusione discende dal Test di appartenenza al radicale **T.2.27**.
Sia dunque $\alpha = (b, \beta) \in K^{n+1}$ con $\beta = (a_1, \ldots, a_n) \in K^n$. Se $\beta \in \mathbb{V}(I)$ allora $f(\beta) = 0$ e $(1 - tf)(b, \beta) = 1 - bf(\beta) = 1$; da ciò si conclude che $\alpha \notin \mathbb{V}(J)$. Se

invece $\beta \notin \mathbb{V}(I)$ allora esiste i per cui $f_i(\beta) \neq 0$; pensando f_i come un polinomio in $K[t, x_1, \dots, x_n]$ che non dipende da t, abbiamo $f_i(b, \beta) \neq 0$, ovvero anche in questo caso $\alpha \notin \mathbb{V}(J)$. □

Il Teorema degli zeri ha alcune immediate conseguenze. La prima che riportiamo è la caratterizzazione degli ideali massimali in $K[x_1, \dots, x_n]$ quando $K = \overline{K}$, cf. **T.3.5**.

T. 3.15. (→ p. 208) Sia $K = \overline{K}$; allora $\mathfrak{m} \subset A$ è un ideale massimale se e solo se esiste $\alpha = (a_1, \dots, a_n) \in K^n$ tale che $\mathfrak{m} = \mathfrak{m}_\alpha = (x_1 - a_1, \dots, x_n - a_n)$.

T. 3.16. (→ p. 208) Sia $K = \overline{K}$; allora, per ogni ideale $I \subseteq A$, l'insieme $\operatorname{Min} I$ *dei primi minimali contenenti* I è finito. In particolare, $\sqrt{I}$ si scrive come intersezione finita di primi di A.

Vedremo però più avanti che questa proprietà è vera in generale per ogni ideale in un anello noetheriano, cf. **T.7.6** e **T.7.11**; a posteriori quindi l'ipotesi che $K = \overline{K}$ potrà venire rimossa nel caso dell'anello dei polinomi.

3.5 Sistemi di equazioni polinomiali

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

Test di risolubilità di un sistema polinomiale
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 $\mathbb{V}(I) \neq \emptyset$, che equivale a $I \neq (1)$ per il Teorema degli zeri; possiamo controllare se questo sia vero grazie alle basi di Gröbner. Una volta accertata l'esistenza o meno delle soluzioni di Σ vogliamo determinare di quante soluzioni si tratta, ovvero trovare la cardinalità di $\mathbb{V}(I)$.

T. 3.17. Siano $K = \overline{K}$ e $I = (G) \subset A$, con G base di Gröbner di I rispetto ad un ordinamento monomiale fissato; allora i seguenti fatti sono equivalenti:

1. $\mathbb{V}(I)$ è finita;
2. esistono $c_i \in \mathbb{N}$ e $g_{l_i} \in G$ tali che $\operatorname{lm}(g_{l_i}) = x_i^{c_i}$ per ogni $i = 1, \dots, n$;
3. il K-spazio vettoriale A/I ha dimensione finita, i.e. $\dim_K(A/I) < \infty$.

Dimostrazione T. 3.17. Dimostriamo che $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$.
$1 \Rightarrow 2$. Se $\mathbb{V}(I) = \emptyset$ allora dalla forma debole del Nullstellensatz avremo che $I = (1)$, $1 \in G$ e $x_i^0 = 1$ per ogni $i = 1, \dots, n$.
Altrimenti, sia $\mathbb{V}(I) = \{\alpha_1, \dots, \alpha_s\}$ con $\alpha_j = (a_{j1}, \dots, a_{jn}) \in K^n$ per ogni $j = 1, \dots, s$. Per ogni $i = 1, \dots, n$ consideriamo allora il polinomio

$$f_i(X) = \prod_{j=1}^{s} (x_i - a_{ji});$$

avremo che $f_i(\alpha_j) = 0$ per ogni $j = 1, \dots, s$, e pertanto $f_i \in \mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$ per la forma forte del Nullstellensatz. Quindi per ogni $i = 1, \dots, n$ esiste $d_i \in \mathbb{N}$ tale che $f_i^{d_i} \in I$; il suo leading monomial è $x_i^{sd_i}$ e sta in $\mathrm{Lt}(I) = \mathrm{Lt}(G)$. Da ciò segue che per ogni $i = 1, \dots, n$ 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 $c_i \leq sd_i$.
$2 \Rightarrow 3$. Per **T.2.23**.1 è sufficiente dimostrare che l'insieme

$$\mathcal{B} = \{X^{\mathbf{a}} \colon \mathrm{lm}(g) \nmid X^{\mathbf{a}} \text{ per ogni } g \in G\}$$

è finito. Se $X^{\mathbf{a}} \in \mathcal{B}$ allora dall'ipotesi discende che $a_1 < c_1, \dots, a_n < c_n$ e pertanto il numero di tali $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{N}^n$ è finito.
$3 \Rightarrow 1$. Sia $d = \dim_K A/I$; per ogni $i = 1, \dots, n$ l'insieme $\{\overline{1}, \overline{x_i}, \dots, \overline{x_i}^d\}$ è un insieme di vettori linearmente dipendenti e dunque esiste una combinazione K-lineare non banale nulla $\sum_{j=0}^{d} b_{ij} \overline{x_i}^j = 0$. Quindi $\sum_{j=0}^{d} b_{ij} x_i^j \in I \cap K[x_i]$ per ogni $i = 1, \dots, n$. Sia ora $\alpha = (a_1, \dots, a_n) \in \mathbb{V}(I)$; per quanto appena visto ogni a_i deve essere radice di un polinomio in una variabile non nullo, quindi per ogni i ci sono solo un numero finito di possibilità e $\mathbb{V}(I)$ è 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. 3.18. (→ p. 209) Siano $K = \overline{K}$ e $\mathbb{V}(I)$ finita. Se I è radicale allora $|\mathbb{V}(I)| = \dim_K A/I$; inoltre I è un ideale 0-dimensionale, i.e. $\dim(A/I) = 0$, e l'anello A/I è somma diretta di un numero finito di campi.

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.7.17** e **T.7.18**.

T. 3.19. (→ p. 209) Se $K = \overline{K}$ e $\mathbb{V}(I)$ è finita allora

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

In particolare I è un ideale 0-dimensionale.

Se $K \subset \overline{K}$ e $I = (f_1, \dots, f_s)$ allora abbiamo

$$\begin{aligned}\mathbb{V}(I) &= \{\alpha \in K^n \colon f_i(\alpha) = 0 \text{ per ogni } i = 1, \dots, s\} \\ &\subseteq \{\alpha \in \overline{K}^n \colon f_i(\alpha) = 0 \text{ per ogni } i = 1, \dots, s\} \\ &= \mathbb{V}_{\overline{K}}(\{f_i \colon i = 1, \dots, s\}) = \mathbb{V}_{\overline{K}}\left(I\,\overline{K}[X]\right).\end{aligned}$$

Pertanto, se la varietà dei punti nella chiusura algebrica di K è finita allora lo è sicuramente anche la varietà di partenza $\mathbb{V}(I)$. In questo caso abbiamo

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

Come si giustifica l'ultima uguaglianza? Possiamo concludere anche in questo caso che A/I è 0-dimensionale?

3.6 Approfondimento: la topologia di Zariski

In questa sezione introduciamo brevemente la definizione e le prime proprietà della topologia di Zariski su due insiemi che abbiamo già incontrato nei capitoli precedenti cioè K^n e $\operatorname{Spec} A$.

T. 3.20. (→ p. 209) Sia K^n lo spazio affine; diciamo che $\mathcal{Y}$ è un chiuso di K^n se $\mathcal{Y}$ è una varietà affine di K^n e $\mathcal{A}$ è un aperto di K^n se il suo complementare è un chiuso. Sia τ la famiglia degli aperti di K^n; allora τ è una topologia su K^n detta *topologia di Zariski*.

Siano ora S un sottoinsieme di K^n e

$$\mathbb{I}(S) = \{f \in K[x_1, \dots, x_n] \colon f(\alpha) = 0 \text{ per ogni } \alpha \in S\};$$

osserviamo che $\mathbb{I}(S)$ è un ideale e consideriamo la varietà $\overline{S} = \mathbb{V}(\mathbb{I}(S))$. Alla luce del seguente risultato chiamiamo $\overline{S}$ *chiusura di Zariski di* S.

T. 3.21. (→ p. 209) La varietà $\overline{S} = \mathbb{V}(\mathbb{I}(S))$ è la più piccola varietà affine che contiene S.

Teorema di chiusura

T. 3.22. Siano $K = \overline{K}$, $I \subset K[x_1, \dots, x_n]$ un ideale, I_k il k-esimo ideale di eliminazione di I, $V = \mathbb{V}(I)$ e $\pi_k \colon K^n \longrightarrow K^{n-k}$ la proiezione sulle ultime $n-k$ coordinate, $\pi_k(a_1, \dots, a_n) = (a_{k+1}, \dots, a_n)$; allora

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

Dimostrazione T. 3.22. Siano $f \in I_k$ e $\alpha = (a_1, \dots, a_n) \in V$; allora f si annulla in α e $f = f(x_{k+1}, \dots, x_n)$. Dunque $f(\alpha) = f(a_{k+1}, \dots, a_n) = f(\pi_k(\alpha)) = 0$, ovvero f si annulla su tutti i punti di $\pi_k(V)$. Abbiamo allora provato che $\pi_k(V) \subseteq \mathbb{V}(I_k)$, e da **T.3.21** segue la prima inclusione.

Per l'altra inclusione, sia $f \in \mathbb{I}(\pi_k(V)) \subseteq K[x_{k+1}, \dots, x_n]$; considerando f come polinomio in $K[x_1, \dots, x_n]$ si ha $f(\alpha) = f(a_{k+1}, \dots, a_n) = 0$ per ogni $\alpha \in V$. Quindi $f \in \mathbb{I}(V) = \sqrt{I}$ per la forma forte del Nullstellensatz; allora esiste un intero m tale che $f^m \in I \cap K[x_{k+1}, \dots, x_n] = I_k$. Da questo segue che $f \in \sqrt{I_k}$ e dunque $\mathbb{I}(\pi_k(V)) \subseteq \sqrt{I_k}$. Passando alle varietà avremo allora

$$\mathbb{V}(I_k) = \mathbb{V}(\sqrt{I_k}) \subseteq \mathbb{V}(\mathbb{I}(\pi_k(V)) = \overline{\pi_k(V)}. \qquad \square$$

T. 3.23. Siano V una varietà affine, $W \subseteq V$ una sottovarietà e I, J due ideali di $K[x_1, \dots, x_n]$; allora

1. $V = W \cup (\overline{V \setminus W})$;
2. $\mathbb{V}(I \colon J) \supseteq \overline{\mathbb{V}(I) \setminus \mathbb{V}(J)}$;
3. se $K = \overline{K}$ e $I = \sqrt{I}$ allora

$$\mathbb{V}(I \colon J) = \overline{\mathbb{V}(I) \setminus \mathbb{V}(J)}.$$

Dimostrazione T. 3.23. 1. Dato che $V \supseteq V \setminus W$, abbiamo che $V \supseteq \overline{V \setminus W}$ e l'inclusione $\supseteq$ è verificata.

Per l'altra inclusione, abbiamo $V = W \cup (V \setminus W) \subseteq W \cup (\overline{V \setminus W})$.

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

3. Per il punto 2 ci basta provare che $I \colon J \supseteq \mathbb{I}(\mathbb{V}(I) \setminus \mathbb{V}(J))$ e passare poi alle varietà per ottenere la tesi. Siano $f \in \mathbb{I}(\mathbb{V}(I) \setminus \mathbb{V}(J))$ e $g \in J$; bisogna verificare che $fg \in I$. Il polinomio fg si annulla su ogni $\alpha \in \mathbb{V}(I)$; infatti, un tale α annulla f se è in $\mathbb{V}(I) \setminus \mathbb{V}(J)$ oppure annulla g se è in $\mathbb{V}(J)$. Per il Nullstellensatz e l'ipotesi allora $fg \in \mathbb{I}(\mathbb{V}(I)) = \sqrt{I} = I$, come desiderato. $\square$

Definiamo ora una topologia su $\operatorname{Spec} A$, lo *spettro* di A. Siano $\mathcal{X} = \operatorname{Spec} A$ ed E un sottoinsieme di A; definiamo

$$\mathcal{V}(E) = \{\mathfrak{p} \in \mathcal{X} \colon E \subseteq \mathfrak{p}\}.$$

Topologia di Zariski

T. 3.24. (→ p. 209) Siano $E, E' \subseteq A$ sottoinsiemi e I, J, $I_\alpha \subseteq A$ ideali con $\alpha \in \Lambda$ insieme di indici; allora

1. $\mathcal{V}(\{0\}) = \mathcal{X}$ e $\mathcal{V}(A) = \emptyset$;
2. $E \subseteq E' \implies \mathcal{V}(E) \supseteq \mathcal{V}(E')$;
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. $\bigcap_{\alpha\in\Lambda} \mathcal{V}(I_\alpha) = \mathcal{V}(\bigcup_{\alpha\in\Lambda} I_\alpha)$ (Intersezione qualunque).

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

T. 3.25. (→ p. 210) Sia $\mathcal{X} = \operatorname{Spec} A$ dotato della topologia di Zariski; allora gli insiemi

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

al variare di $f \in A$ costituiscono una base di aperti di $\mathcal{X}$.

T. 3.26. (→ p. 210) Sia $\mathcal{X} = \operatorname{Spec} A$ dotato della topologia di Zariski; allora $\mathcal{X}$ è compatto.

T. 3.27. (→ p. 210) Siano $\mathcal{X} = \operatorname{Spec} A$ dotato della topologia di Zariski, $\mathcal{Y} \subset \mathcal{X}$ e $\overline{\mathcal{Y}}$ la sua chiusura; allora $\overline{\mathcal{Y}} = \mathcal{V}(\bigcap_{\mathfrak{p}\in\mathcal{Y}} \mathfrak{p})$.

T. 3.28. (→ p. 211) Siano A un anello di dimensione positiva e $\mathcal{X} = \operatorname{Spec} A$ dotato della topologia di Zariski; allora $\mathcal{X}$ è uno spazio topologico T_0 ma non T_1. In particolare, $\mathcal{X}$ non è uno spazio di Hausdorff.

T. 3.29. (→ p. 211) Siano $\phi \colon A \to B$ un omomorfismo di anelli, $\mathcal{X} = \operatorname{Spec} A$ e $\mathcal{Y} = \operatorname{Spec} B$ dotati della topologia di Zariski; allora $\phi^* \colon \mathcal{Y} \longrightarrow \mathcal{X}$ definita da $\phi^*(\mathfrak{q}) = \phi^{-1}(\mathfrak{q})$ è continua.

T. 3.30. (→ p. 211) Siano $\mathcal{X} = \operatorname{Spec} A$ dotato della topologia di Zariski e $\mathcal{N}(A)$ il nilradicale di A; allora $\mathcal{X}$ e $\operatorname{Spec}(A/\mathcal{N}(A))$ sono omeomorfi.

T. 3.31. Siano $\mathcal{X} = \operatorname{Spec} A$ dotato della topologia di Zariski e $\mathcal{N}(A)$ il nilradicale di A; allora $\mathcal{X}$ è irriducibile se e solo se $\mathcal{N}(A)$ è primo, i.e. se e solo se $|\operatorname{Min} A| = 1$.

Dimostrazione T. 3.31. Ricordiamo che uno spazio topologico $\mathcal{X}$ si dice irriducibile se e solo se per ogni coppia di aperti non vuoti $\mathcal{A}, \mathcal{B} \subset \mathcal{X}$ si ha $\mathcal{A} \cap \mathcal{B} \neq \emptyset$ o, equivalentemente, se e solo se per ogni aperto $\mathcal{A} \neq \emptyset$ si ha $\overline{\mathcal{A}} = \mathcal{X}$.
Per il risultato precedente possiamo supporre che l'anello A sia ridotto e provare che $\mathcal{X}$ è irriducibile se e solo se (0) è primo.

Supponiamo $\mathcal{X}$ irriducibile e siano $f, g \in A$ tali che $fg = 0$; osserviamo che

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

Per ipotesi allora $\mathcal{X}_f = \emptyset$ oppure $\mathcal{X}_g = \emptyset$, ossia $\mathcal{V}(f) = \mathcal{X}$ oppure $\mathcal{V}(g) = \mathcal{X}$. Questo equivale a dire che per ogni primo $\mathfrak{p}$ si ha $f \in \mathfrak{p}$ e quindi $f \in \mathcal{N}(A) = (0)$ oppure, analogamente, $g = 0$.

Viceversa, supponiamo che (0) sia primo e siano $\mathcal{X} \setminus \mathcal{V}(I)$ e $\mathcal{X} \setminus \mathcal{V}(J)$ due aperti non vuoti. Dato che $\mathcal{V}(I) \neq \mathcal{X}$ e $\mathcal{V}(J) \neq \mathcal{X}$, si ha che $I \neq (0)$ e $J \neq (0)$; quindi $(0) \in (\mathcal{X} \setminus \mathcal{V}(I)) \cap (\mathcal{X} \setminus \mathcal{V}(J))$, ossia l'intersezione è non vuota. □

4

Moduli

In questo capitolo studiamo i moduli e gli omomorfismi di moduli su un anello A, sottolineando analogie e differenze con quanto accade per i gruppi abeliani e gli spazi vettoriali, che costituiscono due importanti classi di esempi quando $A = \mathbb{Z}$ e quando A è un campo. Introdurremo anche il linguaggio delle successioni esatte e dei diagrammi commutativi e concluderemo con una dimostrazione costruttiva del Teorema di struttura dei moduli finitamente generati su PID.

4.1 Moduli e sottomoduli

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*, o *moltiplicazione per scalare*, $\cdot \colon A \times M \longrightarrow M,\ (a, m) \mapsto a \cdot m = am$ 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) $1_A m = m$.

Ogni anello A ha una struttura naturale di A-modulo con l'operazione di prodotto esterno data dalla moltiplicazione, o prodotto interno, di A. Quando $A = \mathbb{Z}$ un A-modulo è esattamente un gruppo abeliano. Quando $A = K$ è un campo un A-modulo è esattamente un K-spazio vettoriale. Se A è un sottoanello di B allora $A \times B \longrightarrow B$ data dalla moltiplicazione di $a \in A$ per $b \in B$ come elementi di B verifica le proprietà richieste e quindi B è un A-modulo.

Dato un A-modulo M, un sottoinsieme $N \subseteq M$ si dice *A-sottomodulo* di M, o semplicemente *sottomodulo* ove non ci sia ambiguità, quando

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

ii) N è chiuso rispetto al prodotto esterno definito su M, cioè per ogni $a \in A$ e per ogni $n \in N$ si ha $an \in N$.

Un modulo si dice *semplice* se non possiede sottomoduli non banali.

Per esempio $\{0\}$ è sottomodulo di qualsiasi modulo e lo indicheremo semplicemente con 0. I sottomoduli dell'A-modulo A sono tutti e soli gli ideali di A. Dato un A-modulo M, per ogni ideale $I \subset A$ l'insieme

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

costituito da tutte le combinazioni lineari finite di elementi di M a coefficienti in I 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 ponendo $a\overline{m} = \overline{am}$ per ogni $a \in A$ e $\overline{m} \in M/N$.
Inoltre, dato un ideale $I \subset A$, sul quoziente M/IM, oltre alla precedente 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 verificare la buona definizione di tale prodotto, cf. **E.10.1**.

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, definendo il prodotto esterno

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

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

Questa definizione generalizza il caso visto prima in cui A è un sottoanello di B e B è un A-modulo rispetto alla moltiplicazione interna di B ristretta agli elementi di A, cioè rispetto all'omomorfismo di immersione di A in B.

È utile ricordare che in generale l'unione di sottomoduli non è un sottomodulo, a meno che non siano contenuti uno nell'altro in catena.

Operazioni fra sottomoduli

Sia $\{M_h\}_{h\in H}$ una famiglia qualsiasi di sottomoduli di un A-modulo M.

Somma. L'insieme

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

delle combinazioni lineari finite di elementi di $\bigcup_{h\in H} M_h$ a coefficienti in A è un sottomodulo di M; è il più piccolo sottomodulo che contiene $\bigcup_{h\in H} M_h$.

Intersezione. L'insieme

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

è un sottomodulo di M.

È facile verificare che i sottoinsiemi di M sopra definiti sono effettivamente sottomoduli di M. Inoltre, se N e P sono sottomoduli di M tali che $N \cap P = 0$ allora denotiamo la loro somma con $N \oplus P$ e la chiamiamo *somma diretta dei sottomoduli N e P*.
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 $0\colon P$ viene denotato anche con $\operatorname{Ann} P$ e chiamato *l'annullatore di P*.

È facile vedere che $N\colon P$ e, in particolare, $\operatorname{Ann} P$ sono ideali di A, cf. **E.10.4**.
Per ogni $m \in M$ chiamiamo *annullatore di m* l'ideale $\operatorname{Ann}\langle m\rangle$ che verrà denotato semplicemente con $\operatorname{Ann} m$.

T. 4.1. (→ p. 211) 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 $m \in M$.

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

Un omomorfismo $f\colon M \longrightarrow M$ viene detto *endomorfismo* di M.

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

T. 4.2. (→ p. 211) L'insieme $\mathrm{Hom}_A(M,N)$ degli omomorfismi di A-moduli $f\colon M \longrightarrow N$ 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 $\mathrm{Hom}_A(A,M) \simeq M$.

L'A-modulo $\mathrm{Hom}_A(M,M)$ degli endomorfismi di M si denota con $\mathrm{End}_A M$. Osserviamo che $\mathrm{End}_A M$ con la somma definita sopra e il prodotto interno dato dalla composizione è un anello non commutativo.
Dato un omomorfismo di moduli $f\colon M \longrightarrow N$, risultano definiti i seguenti sottomoduli:

i) $\mathrm{Ker}\, f = \{m \in M\colon \ f(m) = 0\}$;

ii) $\mathrm{Im}\, f = f(M) \subseteq N$;

iii) $\mathrm{Coker}\, f = N/\mathrm{Im}\, f$ il *conucleo di* f.

È immediato verificare che f è iniettiva se e solo se $\mathrm{Ker}\, f = 0$ e f è surgettiva se e solo se $\mathrm{Coker}\, f = 0$.
Per esempio siano $a \in A$ e M un A-modulo. L'applicazione di moltiplicazione per a, $a\cdot\colon M \longrightarrow M$ 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. 4.3. (→ p. 212) Siano M, N e P degli A-moduli.

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

$$M/\mathrm{Ker}\, f \simeq \mathrm{Im}\, f.$$

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

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

III Siano N e P sottomoduli di M; allora

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

4.3 Moduli liberi

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

Generatori, insiemi liberi e basi

Siano M un A-modulo e $S \subseteq M$ un sottoinsieme. L'insieme

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

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 $a_1, \dots, a_k \in A$ e $s_1, \dots, s_k \in S$ tali che $m = \sum_{i=1}^{k} a_i s_i$.

Si dice che S è *libero* se per ogni $a_1, \dots, a_k \in A$ e $s_1, \dots, s_k \in S$ tali che $\sum_{i=1}^{k} a_i s_i = 0$ si ha $a_i = 0$ per ogni $i = 1, \dots, k$; in tal caso gli elementi di S si dicono *linearmente indipendenti*.

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. Chiaramente ogni anello A è un A-modulo libero con base $\{1\}$. L'anello $\mathbb{Z}/(n)$ è libero come modulo su se stesso, ma non è uno $\mathbb{Z}$-modulo libero. L'anello A^n è un A-modulo libero e gli elementi $e_1 = (1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1)$ ne costituiscono una base, detta *base canonica*.

T. 4.4. (→ p. 212) 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.

Non tutte le proprietà degli insiemi di generatori e degli insiemi liberi che valgono nel caso degli spazi vettoriali si generalizzano, cf. **E.10.5**.
Se M è un A-modulo libero tutte le sue basi hanno la stessa cardinalità.

Rango di un modulo libero

T. 4.5. Sia M un A-modulo libero; allora tutte le basi di M sono equipotenti. 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. 4.5. Dimostriamo che se $\mathcal{B} = \{m_h\}_{h\in H}$ è una base di M come A-modulo allora, dato un qualunque ideale massimale $\mathfrak{m}$ di A, l'insieme $\overline{\mathcal{B}} = \{\overline{m_h}\}_{h\in H}$ è una base dell'$A/\mathfrak{m}$-spazio vettoriale $M/\mathfrak{m}M$. La tesi seguirà allora dal corrispondente risultato per gli spazi vettoriali: 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 somma finita $\sum_h a_h m_h$ per certi $a_h \in A$, ogni elemento $\overline{m} \in M/\mathfrak{m}M$ si scrive come

$$\overline{m} = \overline{\sum_h a_h m_h} = \sum_h \overline{a_h m_h} = \sum_h \overline{a_h}\ \overline{m_h}.$$

$\overline{\mathcal{B}}$ è un insieme libero; se $0 = \sum_h \overline{a_h}\ \overline{m_h} = \overline{\sum_h a_h m_h}$ allora $\sum_h a_h m_h \in \mathfrak{m}M$ e quindi esistono elementi $c_j \in \mathfrak{m}$ tali che $\sum_h a_h m_h = \sum_j c_j m_j$, dove, per definizione, tutte le somme considerate sono finite. Riordinando gli indici possiamo scrivere che $\sum_h (a_h - c_h) m_h = 0$. Dato che $\mathcal{B}$ è una base di M, questo implica che $a_h = c_h \in \mathfrak{m}$ per ogni h, ossia $\overline{a_h} = 0$ per ogni h, come volevamo. □

4.4 Somma e prodotto diretto di moduli

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

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

Togliendo il vincolo che gli elementi non nulli 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 una struttura di A-modulo. Osserviamo che il primo modulo risulta essere un sottomodulo del secondo. Inoltre, nel caso di un numero finito di componenti, i.e. se $|H| < +\infty$, i due moduli coincidono.
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 $A_1, \dots, A_k$ useremo dunque indistintamente le notazioni $A_1 \times \cdots \times A_k$ oppure $A_1 \oplus \cdots \oplus A_k$, e le corrispondenti notazioni compatte $\prod_{i=1}^{k} A_i$ oppure $\bigoplus_{i=1}^{k} A_i$.
Dato un insieme S, finito o infinito, l'A-modulo libero

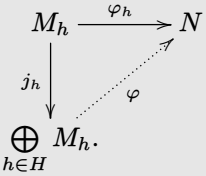
$$A^S = \bigoplus_{s\in S} A$$

è la somma diretta di tante copie di A quanti sono gli elementi di S e ha base canonica $\{e_s \colon s \in S\}$. In particolare, se S è un sottoinsieme di un A-modulo M allora l'assegnazione $e_s \mapsto s$ definisce un omomorfismo surgettivo $A^S \longrightarrow \bigoplus_{s \in S} \langle s \rangle$, dove $\langle s \rangle$ è l'A-modulo ciclico $\langle s \rangle_A = As$ generato da un elemento $s \in S$.

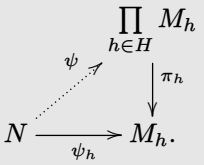
Proprietà universali della somma e del prodotto diretto

T. 4.6. Siano $\{M_h\}_{h \in H}$ una famiglia di A-moduli e N un A-modulo.

1. Per ogni $h \in H$ sia $j_h \colon M_h \longrightarrow \bigoplus_{h \in H} M_h$ l'omomorfismo 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 il seguente diagramma commuta per ogni $h \in H$



2. Per ogni $h \in H$ sia $\pi_h \colon \prod_{h \in H} M_h \longrightarrow M_h$ l'omomorfismo 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 il seguente diagramma commuta per ogni $h \in H$



Dimostrazione T. 4.6. 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 tale m esistono solo un numero finito di $m_h \neq 0$, quindi la somma dei $\varphi_h(m_h)$ è una somma finita di elementi di N. È immediato 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 $h \in H$ allora

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

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

2. 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 $\pi_h \circ \psi = \psi_h$ 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 $\psi = \psi'$. □

Per esempio siano A un anello e x una indeterminata. Consideriamo i moduli ciclici $M_i = \langle x^i\rangle = Ax^i$ per ogni $i \in \mathbb{N}$; allora, per le relative proprietà universali **T.4.6**.1 e 2, risultano definiti 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 dei moduli liberi.

T. 4.7. 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. 4.7. Abbiamo verificato in **T.4.4** 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

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

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

Viceversa, 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 $s \in S$.
Dato che ogni elemento di A^S è del tipo $\sum_i a_i e_{s_i}$, che è immagine di $\sum_i a_i s_i$, abbiamo che $\tilde{f}$ è surgettivo. È anche iniettivo; infatti, dato $m = \sum_i a_i s_i$, abbiamo $0 = \tilde{f}(m) = \sum_i a_i \tilde{f}(s_i) = \sum_i a_i e_{s_i}$ 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. 4.8. (→ p. 212) 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.

T. 4.9. (→ p. 212) Un A-modulo M è libero se e solo se esistono A-moduli $\{M_h\}_{h\in H}$ tali che $M \simeq \bigoplus_{h\in H} M_h$, dove $M_h \simeq A$ per ogni h.

4.5 Lemma di Nakayama e sue conseguenze

Il Lemma di Nakayama 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.

Teorema di Cayley-Hamilton

T. 4.10. Siano M un A-modulo finitamente generato da n elementi, I un ideale di A e $\varphi \in \mathrm{End}_A M$ un endomorfismo di M tale che $\varphi(M) \subseteq IM$. Allora esistono $a_0, \dots, a_{n-1} \in I$ tali che

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

Dimostrazione T. 4.10. 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 $c_{ij} \in I$, per ogni i. In questo modo otteniamo n equazioni lineari

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

dove δ_{ij} denota il delta di Kronecker, 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

$$\det T_\varphi = \varphi^n + \sum_{i=0}^{n-1} a_i \varphi^i \in A[\varphi], \qquad \text{con } a_i \in I \text{ per ogni } i,$$

perché $c_{ij} \in I$ per ogni i, j. Abbiamo allora

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

Di conseguenza, $\det T_\varphi(m_i) = 0$ per ogni $i = 1, \dots, n$. Quindi $\det T_\varphi$ è un endomorfismo che si annulla su ognuno dei generatori di M e coincide con l'endomorfismo nullo. □

Lemma di Nakayama

T. 4.11. 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 tali che $M = IM + N$; allora $M = N$.

Dimostrazione T. 4.11. I forma. Per il Teorema di Cayley-Hamilton applicato all'endomorfismo identità id_M, esistono degli elementi $a_i \in I$ tali che $\mathrm{id}_M + \sum_{i=0}^{n-1} a_i \mathrm{id}_M = 0$. Di conseguenza si ha $(1 + \sum_{i=0}^{n-1} a_i)m = 0$ per ogni $m \in M$. Ponendo $a = 1 + \sum_{i=0}^{n-1} a_i$ 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 $a \equiv 1 \mod I$ e $aM = 0$. Di conseguenza $1 - a \in I \subseteq \mathcal{J}(A)$ e $a \in A^*$, cf. **T.1.15**. 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

$$I\,(M/N) = (IM + N)/N = M/N$$

anche questo enunciato risulta provato. □

Il Lemma di Nakayama non si applica nel caso di moduli che non sono finitamente generati. Per esempio consideriamo $\mathbb{Q}$ come $\mathbb{Z}$-modulo; ovviamente $\mathbb{Q}$ non è finitamente generato (verificarlo) e, per ogni primo p, si ha $p\,\mathbb{Q} = \mathbb{Q}$ ma non esiste $n \equiv 1 \mod (p)$ tale che $n\mathbb{Q} = 0$.

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 K-spazio vettoriale.

T. 4.12. (→ p. 212) 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 $n_1, \ldots, n_k \in M$ sono tali che $\pi(n_i) = \overline{m_i}$ allora $M = \langle n_1, \ldots, n_k \rangle_A$.

T. 4.13. 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 $\mu(M) = \dim_K M/\mathfrak{m}M$.

Dimostrazione T. 4.13. Siano $d = \dim_K M/\mathfrak{m}M$ e $\{m_1, \ldots, m_k\}$ un insieme di generatori minimale di M. Abbiamo che $\overline{m_1}, \ldots, \overline{m_k}$ generano $M/\mathfrak{m}M$ e

quindi $k \geq d$. Se fosse $k > d$ allora $\overline{m_1}, \ldots, \overline{m_k}$ non sarebbero linearmente indipendenti e potremmo estrarre un sottoinsieme di d elementi che sia una base di $M/\mathfrak{m}M$. Dal risultato precedente seguirebbe allora che un sottoinsieme proprio di $\{m_1, \ldots, m_k\}$ 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. 4.14. Siano M un A-modulo finitamente generato e $f \in \mathrm{End}_A M$ un endomorfismo surgettivo; allora f è iniettivo.

Dimostrazione T. 4.14. Sia x una indeterminata. 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 per la prima forma del Lemma di Nakayama 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 $m \in \mathrm{Ker}\, f$; otteniamo

$$m = (p(x) - xq(x))m = p(x)m - xq(x)m = 0,$$

da cui segue $\mathrm{Ker}\, f = 0$ e quindi f è iniettivo. □

Concludiamo questa parte con un'ulteriore proprietà dei moduli liberi.

T. 4.15. (→ p. 213) Sia M un A-modulo libero di rango r; allora ogni insieme di generatori costituito da r elementi è una base di M.

4.6 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 [4], 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.
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 $\mathcal{S}et$, $\mathcal{R}ing$, $\mathcal{T}op$, dove 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:

i) *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 $h \circ (g \circ f) = (h \circ g) \circ f$;

ii) *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 $g \circ \mathrm{id}_A = g$ e $\mathrm{id}_A \circ h = h$.

Per mettere in relazione due categorie $\mathcal{C}$ 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

i) per ogni $A \in \mathrm{Obj}(\mathcal{C}),\ F(A) \in \mathrm{Obj}(\mathcal{D})$;

ii) per ogni $f \in \mathrm{Mor}(\mathcal{C}),\ F(f) \in \mathrm{Mor}(\mathcal{D})$;

iii) per ogni $A \in \mathrm{Obj}(\mathcal{C}),\ F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$;

iv) F deve essere compatibile con la composizione. Dobbiamo distinguere due casi; sia $f \in \mathrm{Mor}(\mathcal{C})$ con $f\colon A \longrightarrow B$,

a) se $F(f)\colon F(A) \longrightarrow F(B)$ allora F si dice *covariante*;

b) se $F(f)\colon F(B) \longrightarrow F(A)$ allora F si dice *controvariante*.

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

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; definiamo il funtore $F\colon \mathcal{C} \longrightarrow \mathcal{D}$ che lascia oggetti e omomorfismi invariati dimenticandosi della moltiplicazione e della struttura che ne deriva.

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

4.7 Successioni esatte

Siano $\{M_i\}_{i \in \mathbb{N}}$ una famiglia di A-moduli e $\{\varphi_i\colon M_{i-1} \longrightarrow M_i\}_{i \in \mathbb{N}}$ 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 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 della forma

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

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 oppure 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 **E.10.28** per un esempio quando $\mathcal{P}$ è "essere finitamente generato".

4.7.1 I funtori $\operatorname{Hom}_A(\bullet, N)$ e $\operatorname{Hom}_A(M, \bullet)$

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

$$\begin{aligned} f^*\colon \operatorname{Hom}_A(M,N) &\longrightarrow \operatorname{Hom}_A(M_1,N), \qquad f^*(\varphi) = \varphi \circ f \\ g_*\colon \operatorname{Hom}_A(M,N) &\longrightarrow \operatorname{Hom}_A(M,N_1), \qquad g_*(\varphi) = g \circ \varphi \end{aligned}$$

in modo che i seguenti diagrammi commutino

$$\begin{array}{ccc} M_1 & \xrightarrow{f} & M \\ & {\scriptstyle f^*(\varphi)}\searrow & \downarrow{\scriptstyle \varphi} \\ & & N, \end{array} \qquad\qquad \begin{array}{ccc} M & & \\ {\scriptstyle \varphi}\downarrow & \searrow{\scriptstyle g_*(\varphi)} & \\ N & \xrightarrow[g]{} & N_1. \end{array}$$

Valgono inoltre le seguenti proprietà:
i) se $f = \mathrm{id}_M$ allora $f^* = \mathrm{id}_{\operatorname{Hom}(M,N)}$ per ogni N;
ii) per ogni A-modulo M_2 e omomorfismo $f'\colon M_2 \longrightarrow M_1$, si ha

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

i′) se $g = \mathrm{id}_N$ allora $g_* = \mathrm{id}_{\mathrm{Hom}(M,N)}$ per ogni M;
ii′) 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 $\mathrm{Hom}_A(M, N)$ e un qualsiasi omomorfismo A-lineare $f \colon M_1 \longrightarrow M$ in un altro omomorfismo A-lineare $\mathrm{Hom}_A(f, N) = f^*$. Trasforma inoltre gli omomorfismi identità in omomorfismi identità e si comporta bene rispetto alla composizione di mappe per i) e ii). Quindi $\mathrm{Hom}_A(\bullet, N)$ è un funtore dalla categoria degli A-moduli in se stessa. Visto poi che

$$\mathrm{Hom}_A(f \circ f', N) = \mathrm{Hom}_A(f', N) \circ \mathrm{Hom}_A(f, N),$$

l'ordine nella composizione viene scambiato e $\mathrm{Hom}_A(\bullet, N)$ è controvariante. Analogamente, fissato M si ha che $\mathrm{Hom}_A(M, \bullet)$ è un funtore covariante.

Esattezza a sinistra di $\mathrm{Hom}(\bullet, N)$ e $\mathrm{Hom}(M, \bullet)$

T. 4.16. 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.

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

Dimostrazione T. 4.16. 1. Dobbiamo provare che la successione è esatta per ogni A-modulo N.

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 $\mathrm{Ker}\, g^* = 0$.

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 $\mathrm{Im}\, g^* \subseteq \mathrm{Ker}\, f^*$.

Per l'altra inclusione, sia $\psi \in \operatorname{Ker} f^*$; dobbiamo costruire $\varphi \in \operatorname{Hom}(M_2, N)$ 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 definire φ ponendo $\varphi(m_2) = \psi(m)$. Bisogna però verificare che φ è ben definita. Sicuramente φ è a valori in N. Sia n un altro elemento di $g^{-1}(m_2)$; allora $m - n \in \operatorname{Ker} g = \operatorname{Im} f$ e quindi esiste $m_1 \in M_1$ tale che $m - n = f(m_1)$. Dunque $\psi(m-n) = \psi(f(m_1)) = f^*(\psi)(m_1) = 0$, poiché $\psi \in \operatorname{Ker} f^*$. Pertanto φ è ben definita, poiché la definizione non dipende dalla scelta dell'elemento nella controimmagine di m_2.

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

$\boxed{\text{In } \operatorname{Hom}_A(M, N_1)}$ ovvero f_* è iniettiva.

Sia $\varphi \in \operatorname{Hom}_A(M, N_1)$ tale che $f_*(\varphi) = f \circ \varphi = 0$; allora $\operatorname{Im} \varphi \subseteq \operatorname{Ker} f$ e $\varphi = 0$ per l'iniettività di f.

$\boxed{\text{In } \operatorname{Hom}_A(M, N)}$ ovvero $\operatorname{Im} f_* = \operatorname{Ker} g_*$.

Dato che vale $g_* \circ f_* = (g \circ f)_* = 0$ si ha immediatamente che $\operatorname{Im} f_* \subseteq \operatorname{Ker} g_*$.

Per l'altra inclusione, sia $\psi \in \operatorname{Ker} g_*$, i.e. $g \circ \psi = 0$. Dobbiamo definire $\varphi \in \operatorname{Hom}_A(M, N_1)$ tale che $f_*(\varphi) = \psi$ e 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 $\operatorname{Im} \psi \subseteq \operatorname{Ker} g = \operatorname{Im} f$. □

Notiamo che i viceversa di entrambe le affermazioni di **T.4.16** sono ancora veri.

T. 4.17. (→ p. 213) 1. Sia $M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ una successione di A-moduli tale che la successione

$$0 \longrightarrow \operatorname{Hom}_A(M_2, N) \xrightarrow{g^*} \operatorname{Hom}_A(M, N) \xrightarrow{f^*} \operatorname{Hom}_A(M_1, N)$$

è esatta per ogni A-modulo N; 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 la successione

$$0 \longrightarrow \operatorname{Hom}_A(M, N_1) \xrightarrow{f_*} \operatorname{Hom}_A(M, N) \xrightarrow{g_*} \operatorname{Hom}_A(M, N_2)$$

è esatta per ogni A-modulo M; allora $0 \longrightarrow N_1 \xrightarrow{f} N \xrightarrow{g} N_2$ è esatta.

4.7.2 Successioni che spezzano

Dalla definizione di somma diretta di moduli segue che 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 per ogni M, N. Non è sempre vero che una successione esatta corta

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

fornisce una decomposizione di N in termini di M e P. Le successioni che hanno questa proprietà sono caratterizzate dalla seguente proposizione.

T. 4.18. Sia $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ 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

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

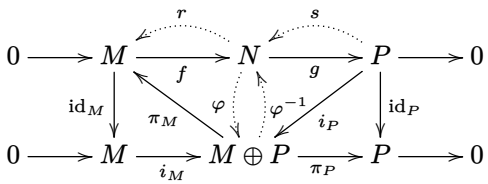
2. esiste un omomorfismo $r\colon N \longrightarrow M$ tale che $r \circ f = \mathrm{id}_M$, ossia r è un inverso sinistro di f;
3. esiste un omomorfismo $s\colon P \longrightarrow N$ tale che $g \circ s = \mathrm{id}_P$, ossia s è un inverso destro di g.

Se vale una delle suddette condizioni equivalenti si dice che la successione *spezza*; in questo caso r si dice una *retrazione di* f e s una *sezione di* g.
Osserviamo che in una successione esatta corta della forma

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

le immersioni e le proiezioni canoniche giocano il ruolo di sezioni e retrazioni, i.e. $\pi_M \circ i_M = \mathrm{id}_M$ e $\pi_P \circ i_P = \mathrm{id}_P$.

Dimostrazione T. 4.18. Consideriamo 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. $r(n) = (\pi_M \circ \varphi)(n)$. Infatti

$$r(f(m)) = \pi_M(\varphi(f(m))) = \pi_M(i_M(\mathrm{id}_M(m))) = (\pi_M \circ i_M)(m) = m.$$

$1 \Rightarrow 3$. Poiché g è surgettivo, per ogni $p \in P$ esiste $n \in N$ tale che $g(n) = p$. Definiamo allora $s(p) = (\varphi^{-1} \circ i_P)(p)$; si ha $\varphi(s(p)) = i_P(p)$ e quindi

$$p = \pi_P(i_P(p)) = \pi_P(\varphi(s(p))) = g(s(p)).$$

$2 \Rightarrow 1$. Per ogni $n \in N$ scriviamo $n = (n - f(r(n))) + f(r(n))$ e notiamo che $r(n - f(r(n))) = r(n) - (r \circ f)(r(n)) = 0$.
Si ha allora $N = \operatorname{Ker} r + \operatorname{Im} f$ e la somma è diretta. Infatti, se $u \in \operatorname{Ker} r \cap \operatorname{Im} f$ allora $u = f(m)$ per qualche $m \in M$; inoltre, $r \circ f = \mathrm{id}_M$ e $u \in \operatorname{Ker} r$ da cui si ottiene $0 = r(u) = r(f(m)) = m$ e quindi $u = 0$. Dato che $\operatorname{Im} f = \operatorname{Ker} g$, si ha che $g_{|\operatorname{Ker} r}$ è un isomorfismo. Dunque $\operatorname{Im} f \simeq M$ poiché f è iniettiva e $\operatorname{Ker} r \simeq \operatorname{Im} g = P$. L'isomorfismo φ è definito da

$$\varphi(n) = \varphi(f(r(n)) + (n - f(r(n)))) = (r(f(r(n))), g(n - f(r(n)))) = (r(n), g(n)).$$

Le verifiche sulla commutatività del diagramma sono immediate

$$\varphi(f(m)) = (r(f(m)), g(f(m)) = (m, 0) = i_M(m)$$

$$\pi_P(\varphi(n)) = \pi_P(r(n), g(n)) = g(n).$$

$3 \Rightarrow 1$. È analoga alla precedente; per ogni $n \in N$ consideriamo $n = (n - s(g(n))) + s(g(n))$. Poiché $n - s(g(n)) \in \operatorname{Ker} g = \operatorname{Im} f$ e $\operatorname{Im} f \cap \operatorname{Im} s = 0$, otteniamo $N = \operatorname{Im} f \oplus \operatorname{Im} s \simeq M \oplus P$. Per concludere prendiamo $\varphi(n) = (f^{-1}(n - s(g(n)), g(n))$ che è ben definita perché $n - s(g(n)) \in \operatorname{Im} f$ e f è iniettiva. □

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 e spezza.

4.7.3 Lemma del serpente

Concludiamo questa sezione con un risultato di grande utilità.

Lemma del serpente

T. 4.19. Dato un diagramma commutativo di A-moduli con righe esatte

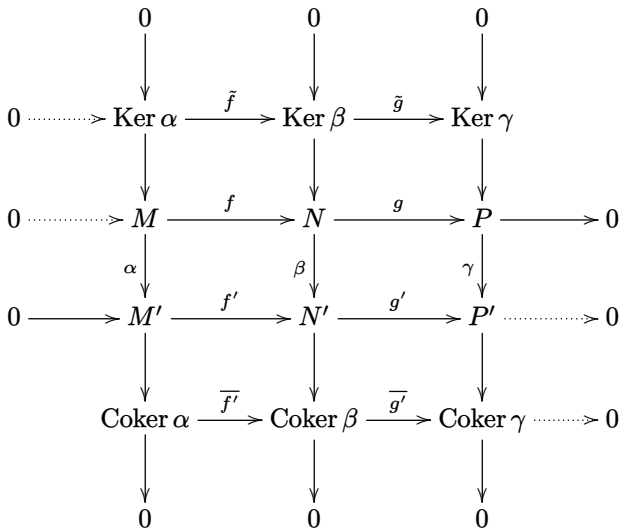
$$\begin{array}{ccccccc} M & \xrightarrow{f} & N & \xrightarrow{g} & P & \longrightarrow & 0 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & M' & \xrightarrow{f'} & N' & \xrightarrow{g'} & P' \end{array}$$

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. 4.19. Consideriamo il seguente diagramma



in cui i quadrati centrali commutano per ipotesi e le colonne, con le ovvie mappe di inclusione e proiezione, sono successioni esatte per costruzione.
In primo luogo studiamo la buona definizione degli altri omomorfismi. Gli omomorfismi $\tilde{f}$ e $\tilde{g}$ sono definiti come le restrizioni $f_{|\operatorname{Ker} f}$ e $g_{|\operatorname{Ker} g}$; quindi $\tilde{f}$ 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 $\tilde{g}$ è 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 $\overline{m} = \overline{m'} \in \operatorname{Coker}\alpha$ abbiamo $m - m' = \alpha(u)$ per qualche $u \in M$ e dunque $f'(m - m') = f'(\alpha(u)) = \beta(f(u)) \in \operatorname{Im}\beta$, da cui discende che $\overline{f'(m)} = \overline{f'(m')} \in \operatorname{Coker}\beta$. La verifica del fatto che $\overline{g'}$ è ben definito è simile.
La costruzione di δ è centrale nella dimostrazione. Vogliamo trovare 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 al diagramma nel modo seguente.
Sia $p \in \operatorname{Ker}\gamma \subseteq P$ 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 $\beta(n) \in \operatorname{Ker} g' = \operatorname{Im} f'$ 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 è 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 $n - n' \in \operatorname{Ker} g = \operatorname{Im} f$, quindi esiste $u \in M$ tale che $f(u) = n - n'$, pertanto $f'(m - m') = \beta(n - n') = \beta(f(u)) = f'(\alpha(u))$. Dato che f' è iniettivo, $m - m' = \alpha(u)$, come volevamo.
È immediato vedere che δ è un omomorfismo.
Possiamo ora verificare l'esattezza della successione della tesi.

$\boxed{\text{In } \operatorname{Ker}\beta}$ ovvero $\operatorname{Im}\tilde{f} = \operatorname{Ker}\tilde{g}$.

Dato che $g \circ f = 0$, chiaramente abbiamo $\tilde{g} \circ \tilde{f} = 0$ e dunque $\operatorname{Im}\tilde{f} \subseteq \operatorname{Ker}\tilde{g}$.

Per l'altra inclusione, sia $n \in \operatorname{Ker}\beta$ un elemento tale che $\tilde{g}(n) = 0$; allora $g(n) = 0$, 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'.

$\boxed{\text{In } \operatorname{Ker}\gamma}$ ovvero $\operatorname{Im}\tilde{g} = \operatorname{Ker}\delta$.

Sia $n \in \operatorname{Ker}\beta$. Verifichiamo che $\delta(\tilde{g}(n)) = 0$; dato che $\beta(n) = 0$ abbiamo $\beta(n) = f'(0)$, quindi $\delta(\tilde{g}(n))$ è nullo per definizione di δ.

Per l'altra inclusione, sia $p \in \operatorname{Ker}\delta$. Scrivendo $p = g(n)$ per un certo $n \in N$, si ha $\beta(n) = f'(m)$ con $m \in \operatorname{Im}\alpha$. Sia allora $u \in M$ tale che $\alpha(u) = m$; abbiamo $\beta(f(u)) = f'(\alpha(u)) = \beta(n)$, e quindi $n - f(u) \in \operatorname{Ker}\beta$. 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 $p \in \operatorname{Im}\tilde{g}$.

$\boxed{\text{In } \operatorname{Coker}\alpha}$ ovvero $\operatorname{Im}\delta = \operatorname{Ker}\overline{f'}$.

Sia $p \in \operatorname{Ker}\gamma$. Scrivendo $p = g(n)$ e $\beta(n) = f'(m)$ si ha $\delta(p) = \overline{m} \in \operatorname{Coker}\alpha$; dato che $f'(m) \in \operatorname{Im}\beta$, abbiamo allora $\overline{f'}(\delta(p)) = \overline{f'(m)} = 0$ in $\operatorname{Coker}\beta$, quindi $\operatorname{Im}\delta \subseteq \operatorname{Ker}\overline{f'}$.

Per l'altra inclusione, 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 $\overline{m} = \delta(p)$ per definizione di δ, come volevamo.

$\boxed{\text{In } \operatorname{Coker}\beta}$ ovvero $\operatorname{Im}\overline{f'} = \operatorname{Ker}\overline{g'}$.

Certamente $\overline{g'} \circ \overline{f'} = 0$, i.e. $\operatorname{Im}\overline{f'} \subseteq \operatorname{Ker}\overline{g'}$.

Per l'altra inclusione, 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 $n' - \beta(n)$. Abbiamo $g'(n' - \beta(n)) = g'(n') - g'(\beta(n)) = g'(n') - \gamma(g(n)) = \gamma(p) - \gamma(p) = 0$; 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 $\overline{n'} = \overline{n' - \beta(n)} = \overline{f'(m')} = \overline{f'}(\overline{m'})$, e anche l'altra inclusione è provata.

Inoltre, se f è iniettivo, l'esattezza

$\boxed{\text{in } \operatorname{Ker}\alpha}$ 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. 4.20. (→ p. 214) Dato un 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 e γ sono isomorfismi allora anche il terzo è un isomorfismo.

4.8 Moduli proiettivi

Abbiamo visto in **T.4.16** 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

$$0 \longrightarrow \operatorname{Hom}_A(M_2, N) \xrightarrow{g^*} \operatorname{Hom}_A(M, N) \xrightarrow{f^*} \operatorname{Hom}_A(M_1, N)$$

$$0 \longrightarrow \operatorname{Hom}_A(N, M_1) \xrightarrow{f_*} \operatorname{Hom}_A(N, M) \xrightarrow{g_*} \operatorname{Hom}_A(N, M_2).$$

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 $n \neq 0, \pm 1$ 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

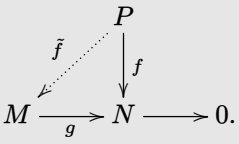
$$\mu_n^*(g)(m) = g \circ \mu_n(m) = g(nm) = ng(m) = 0,$$

per ogni $m \in \mathbb{Z}$; quindi $\mu_n^* = 0$ non è surgettiva, poiché $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/(n)) \simeq \mathbb{Z}/(n) \neq 0$ per **T.4.2**. Inoltre, dato che $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}) = 0$, anche π_* certamente non è surgettiva.

Un funtore si dice *esatto* se trasforma successioni esatte corte in successioni esatte corte. Per caratterizzare i moduli M per cui il funtore $\operatorname{Hom}_A(M, \bullet)$ è esatto anche a destra, e dunque esatto, introduciamo la seguente definizione.

Moduli proiettivi

Un A-modulo P si dice *proiettivo* se, per ogni coppia di A-moduli M, N ed omomorfismi $g\colon M \longrightarrow N$ e $f\colon P \longrightarrow N$ con g surgettivo, esiste un omomorfismo $\tilde{f}\colon P \longrightarrow M$ che fa commutare il diagramma



$$\boxed{g \circ \tilde{f} = f}$$

Osserviamo che il modulo nullo è un modulo proiettivo.

T. 4.21. (→ p. 214) Ogni modulo libero è proiettivo.

Caratterizzazione dei moduli proiettivi

T. 4.22. Sia P un A-modulo. I seguenti fatti sono equivalenti:

1. P è proiettivo;
2. per ogni successione esatta corta di A-moduli

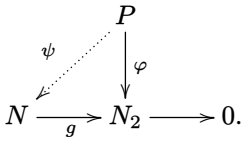
$$0 \longrightarrow N_1 \xrightarrow{f} N \xrightarrow{g} N_2 \longrightarrow 0$$

   la successione

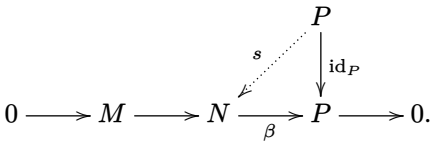
$$0 \longrightarrow \mathrm{Hom}_A(P, N_1) \xrightarrow{f_*} \mathrm{Hom}_A(P, N) \xrightarrow{g_*} \mathrm{Hom}_A(P, N_2) \longrightarrow 0$$

   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. 4.22. $1 \Leftrightarrow 2$. L'equivalenza segue direttamente dalla definizione di modulo proiettivo; dato $g\colon N \to N_2$ surgettivo, l'omomorfismo indotto g^* è surgettivo se e solo se per ogni $\varphi \in \mathrm{Hom}(P, N_2)$ esiste $\psi \in \mathrm{Hom}_A(P, N)$ tale che il seguente diagramma commuta



$1 \Rightarrow 3$. 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

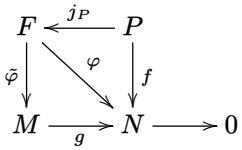


Pertanto $s\colon P \longrightarrow N$ è una sezione di β e la successione spezza, cf. **T.4.18**.

$3 \Rightarrow 4$. Sia M un modulo di cui P è quoziente; abbiamo allora una successione esatta $0 \longrightarrow \operatorname{Ker}\pi \longrightarrow M \xrightarrow{\pi} P \longrightarrow 0$ che per ipotesi spezza, e dunque $M \simeq \operatorname{Ker}\pi \oplus P$.

$4 \Rightarrow 5$. Per **T.4.8**, 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 $\tilde{f}\colon P \longrightarrow M$ tale che $g \circ \tilde{f} = f$. Per ipotesi esiste un A-modulo libero F tale che $F = Q \oplus P$; sia dunque $j_P\colon P \longrightarrow F$ l'omomorfismo di inclusione. Per la proprietà universale della somma diretta **T.4.6**, considerando l'omomorfismo nullo $f'\colon Q \longrightarrow N$, possiamo estendere f ad un unico omomorfismo $\varphi\colon F \longrightarrow N$ tale che $\varphi \circ j_P = f$ e $\varphi \circ j_Q = f' = 0$. Dato che F è libero, e quindi proiettivo per **T.4.21**, esiste $\tilde{\varphi}\colon F \longrightarrow M$ tale che $\varphi = g \circ \tilde{\varphi}$. Dunque abbiamo costruito un diagramma



dove i triangoli commutano. Basta ora definire $\tilde{f}$ come $\tilde{\varphi} \circ j_P$. □

Consideriamo ad esempio 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 $IJ = (\sqrt{-6}) \simeq A$. Inoltre I e J non sono ideali principali e non sono A-moduli liberi, cf. **E.10.39**.
La successione di A-moduli

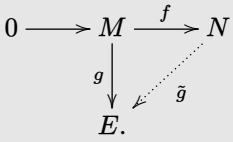
$$\begin{array}{ccccccccc} 0 & \longrightarrow & IJ & \longrightarrow & I \oplus J & \longrightarrow & A & \longrightarrow & 0 \\ & & a & \mapsto & (a, -a) & & & & \\ & & & & (a, b) & \mapsto & a + b & & \end{array}$$

è esatta, cf. **E.10.34**. Dato che A è libero e quindi proiettivo, per **T.4.22** 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 ancora per **T.4.22**.

Concludiamo questa sezione menzionando solamente che, con lo stesso principio, si introduce la definizione di modulo iniettivo per caratterizzare quei moduli M per cui $\operatorname{Hom}_A(\bullet, M)$ è esatto, cf. anche **E.10.41**, **E.10.42** e **E.10.43**.

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 $\tilde{g}\colon N \longrightarrow E$ che fa commutare il diagramma



$$\boxed{\tilde{g} \circ f = g}$$

4.9 Moduli su PID

Studiamo ora in 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. **E.10.5**; diversa è la situazione se A è PID. Ricordiamo che in generale tutte le basi di un modulo libero M sono equipotenti, cf. **T.4.5**, e tale cardinalità è per definizione $\operatorname{rank} M$.

Proprietà dei sottomoduli su un PID

T. 4.23. 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. 4.23. 1. Dimostriamo il caso in cui M è finitamente generato; per il caso generale cf. [6, Capitolo III, Theorem 7.1 e Appendix 2, §2]. Procediamo per induzione sul rango di M. Se M è ciclico 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 $N \simeq (a)$; dato $c \in A$, si ha che $ca = 0$ implica $c = 0$, perché 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 $\{m_1, \ldots, m_{r+1}\}$ una base di M. Definiamo $N_r = N \cap \langle m_1, \ldots, m_r \rangle$. Se $N = N_r$ allora N è libero di rango $\leq \operatorname{rank}\langle m_1, \ldots, m_r\rangle = r < \operatorname{rank} M$, altrimenti si ha $N_r \subsetneq N$ e N_r libero. Ricordando che, per ogni $n \in N$, esistono unici $b_1, \ldots, b_r$ e $a_n \in A$ tali che $n = b_1 m_1 + \ldots + b_r m_r + a_n m_{r+1}$, definiamo

$$I = \{a_n \in A\colon n \in N\}.$$

Dal momento che $a_{n_1} + a_{n_2} = a_{n_1+n_2}$ e $ca_n = a_{cn}$, I è un ideale di A. Inoltre $I \neq 0$ 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 $n_0 = b_1 m_1 + \ldots + b_r m_r + a m_{r+1}$ 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 $m_1, \ldots, m_r, n_0$ sono linearmente indipendenti, abbiamo $N_r \cap \langle n_0 \rangle = 0$. La conclusione discende dall'ipotesi induttiva, una volta osservato che $\langle n_0 \rangle$ è libero. Infine in questo caso abbiamo $\operatorname{rank} N = \operatorname{rank} N_r + 1 \leq r + 1 = \operatorname{rank} M$.

2. Dato un insieme di generatori di M formato da r elementi, possiamo definire un omomorfismo $A^r \xrightarrow{f} M \longrightarrow 0$ surgettivo; dunque $f^{-1}(N)$ è un sottomodulo di A^r ed è libero e finitamente generato. Di conseguenza N è finitamente generato. □

T. 4.24. (→ p. 215) Sia A PID e M un A-modulo; allora M è proiettivo se e solo se è libero.

Nel seguito vogliamo 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 $\mathcal{B}_n = \left\{ e_1^{(n)}, \ldots, e_n^{(n)} \right\}$ la base canonica del modulo A^n e sia $M = \langle m_1, \ldots, m_r \rangle$ un A-modulo finitamente generato; allora M è isomorfo ad un quoziente di A^r, tramite l'omomorfismo $f \colon A^r \longrightarrow M$ 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.4.23**.1; presa 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 le basi canoniche $\mathcal{B}_s$ e $\mathcal{B}_r$ di A^s e A^r possiamo rappresentare l'omomorfismo φ con una matrice $X = (x_{ij}) \in M_{rs}(A)$ *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. $(a_1, \ldots, a_r) \in \operatorname{Ker} f$, se e solo se esiste $u \in A^s$ tale che $Xu^{\mathrm{t}} = (a_1, \ldots, a_r)^{\mathrm{t}}$, i.e. $(a_1, \ldots, a_r) \in \operatorname{Im} \varphi$.
Questo spiega perché, al fine di studiare gli A-moduli finitamente generati, possiamo lavorare sulle matrici a coefficienti in A.

4.9.1 La forma normale di Smith

Sia X una matrice $r \times s$ a coefficienti in un dominio a ideali principali A. Come visto nei corsi di Algebra Lineare, su X possiamo eseguire le seguenti *operazioni elementari di riga*

i) scambiare due righe;
ii) sommare ad una riga un multiplo di un'altra riga;
iii) 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 una relazione d'equivalenza su $M_{rs}(A)$. Diciamo che una matrice, non necessariamente quadrata, $D = (d_{ij}) \in M_{rs}(A)$ 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. 4.25. (→ p. 215) Siano X e Y matrici equivalenti; allora $\Delta_i(X) = \Delta_i(Y)$ per ogni i.

T. 4.26. Sia A un dominio ad ideali principali; allora ogni matrice a coefficienti in A è equivalente ad una matrice diagonale.

Dimostrazione T. 4.26. Consideriamo una matrice $X = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ a coefficienti 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 e dunque è 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. Inoltre, prendendo la trasposta, otteniamo 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, trovando 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. Possono però ricomparire elementi diversi da zero nella prima colonna e quindi si deve ripetere il procedimento. Con applicazioni successive si costruisce una sequenza di 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; quindi tali che $x_{i+1} \mid x_i$. Dal momento che A è PID, esiste n tale che $x_n = x_{n+1}$, cf. **T.1.24**, e questo implica che x_n è il massimo comun divisore sia degli elementi della prima colonna che della prima riga. Quindi, usando x_n che si trova al posto $(1,1)$, 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 riesce cosí a diagonalizzare la matrice di partenza. □

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

i) D è diagonale;

ii) $d_{11} \mid d_{22} \mid \ldots \mid d_{tt}$, dove $t = \min\{r, s\}$.

T. 4.27. Ogni matrice X a coefficienti in A è equivalente ad una matrice in forma di Smith.

In generale esistono interi $0 \leq k_1 \leq k_2 \leq t$ tali che $d_{ii} \in A^*$ per ogni $0 < i \leq k_1$ e $d_{ii} = 0$ per ogni $k_2 < i \leq t$.

Dimostrazione T. 4.27. Grazie a **T.4.26** 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 $sx_{11} + tx_{22} = x$; consideriamo le matrici

$$R = \left(\begin{array}{cc|c} s & t & 0 \\ -x_{22}x^{-1} & x_{11}x^{-1} & \\ \hline 0 & & I_{r-2} \end{array}\right) \quad \text{e} \quad S = \left(\begin{array}{cc|c} 1 & -tx_{22}x^{-1} & 0 \\ 1 & sx_{11}x^{-1} & \\ \hline 0 & & I_{s-2} \end{array}\right).$$

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 $y_{11} \mid y_{22}$. 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 $z_{jj} = y_{22}$. Inoltre, in tale matrice vale 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. 4.28. (→ p. 215) 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 $d_{11} = \delta_1$ e $d_{ii} = \delta_i/\delta_{i-1}$ 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 D è essenzialmente unica e la chiamiamo *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 i fattori invarianti delle rispettive forme di Smith sono associati.

Ricordiamo che le operazioni elementari consentite, descritte all'inizio della sezione, non alterano gli ideali $\Delta_i(X)$; se si procede al calcolo dei $\Delta_i(X)$ tramite tali operazioni 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 ottiene sottraendo alla seconda riga $\frac{3}{2} \notin \mathbb{Z}$ volte la prima, e nemmeno a $\begin{pmatrix} 2 & 4 \\ 0 & 4 \end{pmatrix}$ ottenuta sottraendo al doppio della seconda riga 3 volte la prima.

4.9.2 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 la seguente notazione. Dato $N = \langle w_1, \dots, w_s \rangle$ un sottomodulo di un modulo $L = \langle l_1, \dots, l_r \rangle$, esistono elementi $x_{ij} \in A$ tali che $w_h = \sum_{k=1}^{r} x_{kh} l_k$, per ogni $h = 1, \dots, s$. Se $X = (x_{ij})$ è la matrice $r \times s$ formata con gli elementi x_{ij}, possiamo scrivere queste relazioni usando la notazione matriciale $(w_1, \dots, w_s) = (l_1, \dots, l_r)X$.

T. 4.29. Siano L un A-modulo libero di rango r e $0 \neq N \subseteq L$ un sottomodulo; allora esistono una base $\{v_1, \dots, v_r\}$ di L e scalari $d_1, \dots, d_s \in A$, con $s \leq r$, tali che $\{d_1 v_1, \dots, d_s v_s\}$ è una base di N.

Dimostrazione T. 4.29. Siano $l_1, \dots, l_r$ una base di L e $w_1, \dots, w_s$ una base di N, che è sottomodulo di un modulo libero e quindi libero di rango $s \leq r$, per **T.4.23**.1; allora esiste X matrice $r \times s$ a coefficienti in A tale che $(w_1, \dots, w_s) = (l_1, \dots, l_r)X$. Per quanto provato in **T.4.27**, 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; allora $(w_1, \dots, w_s)S = (l_1, \dots, l_r)XS = (l_1, \dots, l_r)R^{-1}D$. 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, $(w_1, \dots, w_s)S = (v_1, \dots, v_r)D = (d_1 v_1, \dots, d_k v_k, 0, \dots, 0)$, con $k \leq s$. Dal momento che anche S è invertibile, segue che $k = s$ e $\{d_1 v_1, \dots, d_s v_s\}$ 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. Per ogni $i = 1, \dots, s$ notiamo che $dv_i \in N$ se e solo se $d_i \mid d$, dunque $(d_i) = N : \langle v_i \rangle$, cf. anche **T.4.30**. Se $s < i \leq r$ invece $dv_i \in N$ se e solo se $d = 0$, cioè $(0) = N : \langle v_i \rangle$.

T. 4.30. (→ p. 215) Con le stesse notazioni di **T.4.29**,

1. $L/N \simeq \langle \overline{v_1} \rangle \oplus \dots \oplus \langle \overline{v_r} \rangle$.
2. $L/N \simeq A/(d_1) \oplus \dots \oplus A/(d_s) \oplus A^{r-s}$, dove $(d_i) = 0 : \langle \overline{v_i} \rangle$ per ogni $i = 1, \dots, s$.

Teorema di struttura - I

T. 4.31. (→ p. 215) Sia $M = \langle m_1, \dots, m_r \rangle$ un A-modulo finitamente generato; allora esistono ideali $I_1 \supseteq I_2 \supseteq \dots \supseteq I_r$ tali che

$$M \simeq \bigoplus_{i=1}^{r} A/I_i.$$

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 $w'_1, \dots, w'_s$ 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 avessimo scelto un altro insieme di generatori $\{n_1, \dots, n_{r'}\}$ di $M = \langle m_1, \dots, m_r \rangle$. Il seguente risultato, di validità generale, chiarisce la situazione.

T. 4.32. Siano A un anello, $I_1 \supseteq I_2 \supseteq \dots \supseteq I_r$ e $J_1 \supseteq J_2 \supseteq \dots \supseteq J_{r'}$ ideali di A, con $r \leq r'$; supponiamo che

$$M \simeq \bigoplus_{i=1}^{r} A/I_i \simeq \bigoplus_{h=1}^{r'} A/J_h$$

allora

1. $J_1 = J_2 = \dots = J_{r'-r} = A$;
2. $J_{r'-r+i} = I_i$ per ogni $i = 1, \dots, r$.

Dimostrazione T. 4.32. 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 $h > 1$; quindi da **E.10.6** 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, per composizione, un omomorfismo surgettivo da B^r in $B^{r'}$; dato che $r < r'$ questo implica $B = 0$, cf. **E.10.8**. Iterando il ragionamento otteniamo similmente che $J_2 = \dots = J_{r'-r} = A$.

2. Per il punto precedente, possiamo supporre che $r = r'$ e, per simmetria, ci basta dimostrare che $I_h \subseteq J_h$, per ogni $h = 1, \dots, r$. Sia allora $a \in I_h$; da **E.10.7** discende che

$$aM \simeq a\left(\bigoplus_{i=1}^{r} A/I_i\right) \simeq \bigoplus_{i=1}^{r} A/(I_i \colon (a)).$$

Poiché $I_i \subseteq I_{i-1}$, abbiamo anche $a \in I_i$ per ogni $i \leq h$, e quindi $I_i \colon (a) = A$ per tali i. Di conseguenza

$$\bigoplus_{i=h+1}^{r} A/(I_i \colon (a)) \simeq aM \simeq a\left(\bigoplus_{i=1}^{r} A/J_i\right) \simeq \bigoplus_{i=1}^{r} A/(J_i \colon (a)).$$

Dal punto 1 discende allora che $J_i \colon (a) = A$ per ogni $i \leq h$; dunque $a \in J_h$. □

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 l'insieme

$$T(M) = \{m \in M : am = 0 \text{ per qualche } a \in A \setminus \{0\}\},$$

cf. **E.10.45**. 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. 4.33. (→ p. 215) Siano A un PID e M un A-modulo finitamente generato; allora

1. $T(M)$ è finitamente generato;
2. $M \simeq T(M) \oplus A^k$, per qualche $k \geq 0$;
3. $\mathrm{Ann}(T(M)) \neq 0$.

Il risultato precedente mostra che ogni modulo M finitamente generato su un PID si decompone come somma diretta di un modulo di torsione e di un modulo libero, che chiamiamo anche *parte di torsione* e *parte libera* di M. Per decomporre ulteriormente M introduciamo la seguente definizione.
Dati un A-modulo M e $a \in A$ definiamo la *a-componente* di M come

$$M_{[a]} = \{m \in M : \ a^k m = 0 \ \text{ per qualche } k \in \mathbb{N}\} = \bigcup_{k \in \mathbb{N}} 0 :_M (a^k),$$

che risulta essere un sottomodulo di M, cf. **E.10.46**.
Nel caso in cui $p \in A$ 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. 4.34. (→ p. 216) 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. 4.35. (→ p. 216) 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 con 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.

Concludiamo questa parte osservando che se $M \simeq \operatorname{Coker}\varphi$ è un A-modulo generato da r elementi e φ è rappresentato da una matrice $X \in M_{rr'}(A)$, 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.4.30**.

4.10 Approfondimento: la forma canonica razionale e la forma di Jordan

Come caso particolare dei risultati della sezione precedente otteniamo i ben noti teoremi di classificazione dei gruppi abeliani finitamente generati. In questa ultima parte vediamo un'ulteriore applicazione della teoria al caso degli spazi vettoriali.
Sia $V \neq 0$ un K-spazio vettoriale di dimensione finita n e sia $\varphi \in \operatorname{End}_K(V)$ 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.4.14**.
Nel seguito considereremo fissato l'endomorfismo φ e la struttura di $K[x]$-modulo su V appena introdotta; in particolare $\operatorname{Ann} V$ denoterà $\operatorname{Ann}_{K[x]} V$ e, per ogni sottoinsieme $W \subseteq V$, $\langle W \rangle$ indicherà il $K[x]$-sottomodulo di V generato da W.

T. 4.36. Con le notazioni appena introdotte, valgono i seguenti fatti.

1. L'annullatore $\operatorname{Ann} V$ di V è un ideale proprio e non nullo di $K[x]$; il suo generatore monico viene detto *polinomio minimo* di φ.

2. Per ogni $0 \neq v \in V$, l'ideale $\operatorname{Ann}\langle v \rangle$ è proprio e non nullo in $K[x]$.

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. Un qualsiasi $K[x]$-sottomodulo $T \subseteq V$ è un sottospazio vettoriale φ-*invariante* di V, ossia tale che $\varphi(T) \subseteq T$. Visto che φ è fissato, diremo semplicemente invariante.

5. Siano $0 \neq v \in V$, $f_v(x)$ il generatore monico di $\operatorname{Ann}\langle v\rangle$ e d il suo grado; allora la dimensione di $\langle v\rangle$ come K-spazio vettoriale è d e $\{v, \varphi(v), \dots, \varphi^{d-1}(v)\}$ è una sua base. Inoltre $\langle v\rangle$ è il più piccolo sottospazio invariante di V che contiene v.

Dimostrazione T. 4.36. 1. Dato $f(x) \in K[x]$, si ha per definizione che $f(x)v = 0$ se e solo se $f(\varphi)(v) = 0$. Quindi $f(x) \in \operatorname{Ann} V$ 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 $\sum_{i=0}^{n^2} a_i\varphi^i = 0$; allora $f(x) = \sum_{i=0}^{n^2} a_i x^i$ è un elemento non nullo di $\operatorname{Ann} V$.

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 per ogni $a \in K$ e $v \in V$ 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 e ogni suo sottomodulo $\langle W\rangle$ non sono liberi, e dunque non ammettono base.

4. Per ogni $w \in T$ si ha $p(x)w \in T$; in particolare $\varphi(w) = xw \in T$ per ogni $w \in T$, cioè $\varphi(T) \subseteq T$.

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 $\varphi^i(v) = x^i v$. Dato che $f_v(x)v = 0$ e $f_v(x)$ 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 dimostrato che ogni elemento di $\langle v\rangle$ si può scrivere come combinazione K-lineare di $v, \varphi(v), \dots, \varphi^{d-1}(v)$, che quindi 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

$$f(x) = \sum_{i=0}^{d-1} a_i x^i \in \operatorname{Ann}\langle v\rangle = (f_v(x));$$

questo contraddice il fatto che $\deg f_v = d$.
Infine il sottospazio $\langle v\rangle$ è invariante, come visto nel punto precedente. Dato un altro sottospazio T invariante che contiene v, induttivamente avremo che $\varphi^i(v) \subseteq \varphi^i(T) \subseteq \varphi(T) \subseteq T$ per ogni i, cioè $\langle v\rangle \subseteq T$. □

Dal momento che $K[x]$ è PID, il $K[x]$-modulo finitamente generato V che, come visto in **T. 4.36**.1, 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.4.31**.
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.4.36**.5; il grado d_i di f_i è positivo per ogni i e scriviamo

$$f_i = \sum_{j=0}^{d_i} a_j^{(i)} x^j \quad \text{per certi} \quad a_j^{(i)} \in K.$$

La forma canonica razionale

T. 4.37. (→ p. 216) 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.

Ricordiamo che, per il Teorema di struttura, i polinomi f_i che definiscono la forma canonica razionale di φ soddisfano la condizione $f_1 \mid f_2 \mid \dots \mid f_s$.

Consideriamo il seguente esempio; sia $V = \mathbb{Q}^4$ e $\varphi \in \mathrm{End}_{\mathbb{Q}}(V)$ l'endomorfismo dato da $\varphi(v) = Av$ dove

$$A = (a_{ij}) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & -2 & 0 \\ -2 & -1 & 2 & 0 \\ -2 & -1 & -2 & 1 \end{pmatrix}. \tag{4.2}$$

Iniziamo trovando una decomposizione di V come somma diretta di $\mathbb{Q}[x]$-moduli ciclici e determinando 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.4.36**.3, $\mathcal{B}$ costituisce un insieme di generatori di V come $\mathbb{Q}[x]$-modulo. Sia dunque $f\colon \mathbb{Q}[x]^4 \longrightarrow V$ definito da $f(p_1, p_2, p_3, p_4) = p_1\mathbf{e}_1 + p_2\mathbf{e}_2 + p_3\mathbf{e}_3 + p_4\mathbf{e}_4$; allora f è un omomorfismo surgettivo e la successione

$$0 \longrightarrow \operatorname{Ker} f \longrightarrow \mathbb{Q}[x]^4 \xrightarrow{f} V \longrightarrow 0$$

è esatta. Determiniamo ora il sottomodulo $\operatorname{Ker} f$; 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

$$f(x - a_{11}, -a_{21}, -a_{31}, -a_{41}) = 0.$$

Quindi l'elemento $\mathbf{r}_1 = (x - a_{11}, -a_{21}, -a_{31}, -a_{41}) \in \operatorname{Ker} f$. Analogamente possiamo definire $\mathbf{r}_2$, $\mathbf{r}_3$ e $\mathbf{r}_4$ tali che il sottomodulo $\langle \mathbf{r}_i \colon i = 1, \dots, 4\rangle$ sia contenuto in $\operatorname{Ker} f$.
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 $c_i \in \mathbb{Q}$ e $\deg h_i < \deg p_i$ per ogni i. Dunque

$$\begin{aligned}
\begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{pmatrix} &= \begin{pmatrix} h_1(x - a_{11}) + c_1 \\ h_2(x - a_{22}) + c_2 \\ h_3(x - a_{33}) + c_3 \\ h_4(x - a_{44}) + c_4 \end{pmatrix} \\
&= h_1\mathbf{r}_1 + h_2\mathbf{r}_2 + h_3\mathbf{r}_3 + h_4\mathbf{r}_4 + \begin{pmatrix} h_2a_{12} + h_3a_{13} + h_4a_{14} + c_1 \\ h_1a_{21} + h_3a_{23} + h_4a_{24} + c_2 \\ h_1a_{31} + h_2a_{32} + h_4a_{34} + c_3 \\ h_1a_{41} + h_2a_{42} + h_3a_{43} + c_4 \end{pmatrix} \\
&= h_1\mathbf{r}_1 + h_2\mathbf{r}_2 + h_3\mathbf{r}_3 + h_4\mathbf{r}_4 + \begin{pmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \end{pmatrix},
\end{aligned}$$

per certi polinomi $q_1, \dots, q_4$ 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 $g_1, \dots, g_4 \in K[x]$ e $d_1, \dots, d_4 \in \mathbb{Q}$.

Di conseguenza, se $\mathbf{p} = (p_1, p_2, p_3, p_4) \in \operatorname{Ker} f$ allora 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

$$\begin{aligned} A - xI &= \begin{pmatrix} a_{11} - x & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} - x & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} - x & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} - x \end{pmatrix} \\ &= \begin{pmatrix} 1 - x & 0 & 1 & 0 \\ 0 & 1 - x & -2 & 0 \\ -2 & -1 & 2 - x & 0 \\ -2 & -1 & -2 & 1 - x \end{pmatrix}, \end{aligned}$$

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 $f_2 = a_3^{(2)}x^3 + a_2^{(2)}x^2 + a_1^{(2)}x + a_0^{(2)} = x^3 - 4x^2 + 5x - 2$. Abbiamo pertanto

$$M = \left(\begin{array}{c|c} M_{f_1} & 0 \\ \hline 0 & M_{f_2} \end{array}\right) = \left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & \text{-5} \\ 0 & 0 & 1 & 4 \end{array}\right),$$

e ciò conclude la prima parte del nostro esempio.

Ripartiamo dalla decomposizione $V = \bigoplus_{i=1}^{s} \langle v_i \rangle \simeq \bigoplus_{i=1}^{s} K[x]/(f_i)$. Utilizzando la fattorizzazione unica dei polinomi in $K[x]$ e il Teorema cinese del resto possiamo 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. Quest'ultima scrittura è la decomposizione di $\langle v_i\rangle$ in componenti f_{ij}-primarie, cf. **E.10.48**. Date le relazioni di divisibilità tra gli f_i è ovvio che componenti f_{ij}-primarie non banali compaiano anche nei $\langle v_k\rangle$ successivi, cioè per $k \geq i$.
Nel caso particolare 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 osservato sopra, $\lambda_j^{(i)}$ comparirà in generale come radice degli f_k con $k \geq i$.
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 $\mathrm{Ann}\langle w_j^{(i)}\rangle = \left(x - \lambda_j^{(i)}\right)^{e_{ij}}$, 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. 4.38. 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 $\psi_{ij} = (\varphi - \lambda_j^{(i)}\mathrm{id}_V)_{|\langle w_j^{(i)}\rangle}$; allora

1. una base di V è data da

$$\{w_1^{(1)}, \psi_{11}(w_1^{(1)}), \ldots, \psi_{11}^{e_{11}-1}(w_1^{(1)}), \ldots, w_{t_1}^{(1)}, \psi_{1t_1}(w_{t_1}^{(1)}), \ldots, \psi_{1t_1}^{e_{1t_1}-1}(w_{t_1}^{(1)}), \ldots,$$
$$w_1^{(s)}, \psi_{s1}(w_1^{(s)}), \ldots, \psi_{s1}^{e_{s1}-1}(w_1^{(s)}), \ldots, w_{t_s}^{(s)}, \psi_{st_s}(w_{t_s}^{(s)}), \ldots, \psi_{st_s}^{e_{st_s}-1}(w_{t_s}^{(s)})\};$$

2. la matrice associata a φ rispetto a tale base è una matrice diagonale a

blocchi

$$\begin{pmatrix} J_{\lambda_1^{(1)}} & & & & & & & & & \\ & J_{\lambda_2^{(1)}} & & & & & & & & \\ & & \ddots & & & & & 0 & & \\ & & & J_{\lambda_{t_1}^{(1)}} & & & & & & \\ & & & & J_{\lambda_1^{(2)}} & & & & & \\ & & & & & \ddots & & & & \\ & & & & & & J_{\lambda_{t_{s-1}}^{(s-1)}} & & & \\ & & 0 & & & & & J_{\lambda_1^{(s)}} & & \\ & & & & & & & & \ddots & \\ & & & & & & & & & J_{\lambda_{t_s}^{(s)}} \end{pmatrix},$$

dove ogni blocco $J_{\lambda_j^{(i)}}$ è una matrice di Jordan di taglia e_{ij}, della forma

$$J_{\lambda_j^{(i)}} = \begin{pmatrix} \lambda_j^{(i)} & 0 & \dots & & 0 \\ 1 & \lambda_j^{(i)} & 0 & \dots & \vdots \\ 0 & 1 & \lambda_j^{(i)} & \ddots & \\ \vdots & & \ddots & \ddots & 0 \\ 0 & 0 & & 1 & \lambda_j^{(i)} \end{pmatrix}.$$

Dimostrazione T. 4.38. 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 $\psi_{ij} = \varphi - \lambda_j^{(i)} \mathrm{id}_V$. Per semplicità di notazione poniamo $w_j^{(i)} = w$, $\lambda_j^{(i)} = \lambda$ e $\mathrm{Ann}\langle w \rangle = (x-\lambda)^e$, per cui risulta $\psi = \varphi - \lambda \mathrm{id}_V$ 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.4.36**.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 $\varphi^i(w) = (\psi + \lambda \,\mathrm{id}_V)^i(w) \in \langle w, \psi(w), \dots, \psi^{e-1}(w) \rangle$ 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 $\langle w \rangle$

$$\varphi(\psi^i(w)) = (\psi + \lambda \,\mathrm{id}_V)(\psi^i(w)) = \begin{cases} \psi^{i+1}(w) + \lambda \psi^i(w) & \text{se } 0 \le i < e-1 \\ \lambda \psi^{e-1}(w) & \text{se } i = e-1, \end{cases}$$

dove l'ultima uguaglianza segue dal fatto che $\psi^e(w) = (x-\lambda)^e w = 0$. Quindi rispetto alla base $\{w, \psi(w), \dots, \psi^{e-1}(w)\}$ la matrice che rappresenta φ è esattamente

$$J_\lambda = \begin{pmatrix} \lambda & 0 & \dots & \dots & 0 \\ 1 & \lambda & 0 & \dots & 0 \\ 0 & 1 & \lambda & \dots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & \lambda \end{pmatrix}. \qquad \square$$

Riprendiamo l'esempio precedente e troviamo la forma di Jordan su $\mathbb{C}$ della matrice A in (4.2). Dato che $x^3 - 4x^2 + 5x - 2 = (x-1)^2(x-2)$, otteniamo che la forma di Jordan di A è

$$\left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 2 \end{array}\right).$$

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

Introduciamo ora un'operazione di prodotto tra moduli, detta prodotto tensoriale; ne illustriamo la costruzione e le principali proprietà. Fissato un modulo, interpretiamo poi il prodotto tensoriale come funtore e concludiamo con un'applicazione importante, quella dell'estensione degli scalari.

5.1 La proprietà universale del prodotto tensoriale

Siano A un anello e M, N, P degli A-moduli. Diciamo che un'applicazione $b\colon M \times N \longrightarrow P$ è *A-bilineare* se per ogni $m \in M$ la mappa

$$b_{(m,\bullet)}\colon N \longrightarrow P, \quad b_{(m,\bullet)}(n) \mapsto b(m,n),$$

e per ogni $n \in N$ la mappa

$$b_{(\bullet,n)}\colon M \longrightarrow P, \quad b_{(\bullet,n)}(m) \mapsto b(m,n)$$

sono A-lineari.
Denotiamo l'insieme di tutte le mappe A-bilineari definite da $M \times N$ in P con $\mathrm{Bil}(M,N;P)$ e definiamo una struttura di A-modulo ponendo, per ogni $b, b' \in \mathrm{Bil}(M,N;P)$ e $\alpha \in A$

$$(b+b')(m,n) = b(m,n) + b'(m,n) \quad \text{e} \quad (\alpha b)(m,n) = \alpha b(m,n),$$

per ogni $m \in M$ e $n \in N$, cf. **E.11.1**.

T. 5.1. Siano A un anello e M, N, P degli A-moduli. Allora

$$\mathrm{Bil}(M,N;P) \simeq \mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P)).$$

Dimostrazione T. 5.1. 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 $\varphi_b\colon M \longrightarrow \mathrm{Hom}_A(N,P)$ definita da $\varphi_b(m)(n) = b_{(m,\cdot)}(n) = b(m,n)$.
Inoltre, sia

$$\Psi\colon \mathrm{Hom}_A(M,\mathrm{Hom}_A(N,P)) \longrightarrow \mathrm{Bil}(M,N;P)$$

l'applicazione che manda un omomorfismo φ nella mappa bilineare b_φ definita da $b_\varphi(m,n) = \varphi(m)(n)$, per ogni $m \in M$, $n \in N$.
Per concludere la dimostrazione basta eseguire le seguenti facili verifiche

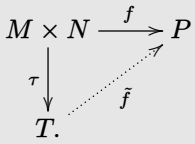
i) Φ e Ψ sono ben definite, i.e. φ_b è un omomorfismo e b_φ è bilineare;

ii) Φ e Ψ sono omomorfismi di A-moduli;

iii) Φ e Ψ sono una inversa dell'altra. □

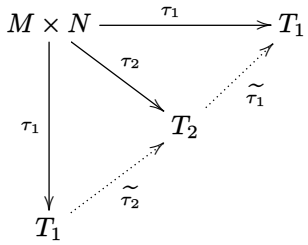
Il prodotto tensoriale viene definito attraverso la seguente proprietà universale; si procede poi a dimostrarne esistenza e unicità.

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 e un'applicazione A-bilineare $\tau\colon M \times N \longrightarrow T$, che verifica 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. 5.2. 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. 5.2. Unicità Supponiamo che (T_1,τ_1) e (T_2,τ_2) siano due prodotti tensoriali di M e N. Usando la proprietà universale prima con $P = T_1$ e poi con $P = T_2$ otteniamo il diagramma



dove gli omomorfismi $\widetilde{\tau_1}$ e $\widetilde{\tau_2}$ sono dati dalla proprietà universale, sono unici e tali che $\tau_2 = \widetilde{\tau_2} \circ \tau_1$ e $\tau_1 = \widetilde{\tau_1} \circ \tau_2$.

Componendo, troviamo che $\widetilde{\tau_1} \circ \widetilde{\tau_2}$ è un omomorfismo di T_1 in sé tale che $(\widetilde{\tau_1} \circ \widetilde{\tau_2}) \circ \tau_1 = \tau_1$; dato che $\mathrm{id}_{T_1} \circ \tau_1 = \tau_1$, l'unicità nella proprietà universale implica $\widetilde{\tau_1} \circ \widetilde{\tau_2} = \mathrm{id}_{T_1}$.
Analogamente vale che $\widetilde{\tau_2} \circ \widetilde{\tau_1} = \mathrm{id}_{T_2}$ e possiamo concludere che $T_1 \simeq T_2$.

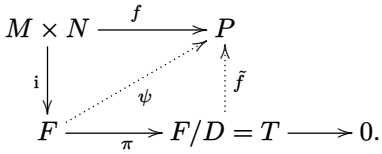
Esistenza Consideriamo l'A-modulo libero $F = A^{M \times N}$, la sua base canonica $\mathcal{B} = \{e_{(m,n)} \colon (m,n) \in M \times N\}$ e la mappa $\mathrm{i} \colon M \times N \longrightarrow F$ che manda (m,n) in $e_{(m,n)}$.
Sia

$$\tau = \pi \circ \mathrm{i} \colon M \times N \longrightarrow F \longrightarrow F/D,$$

dove $\pi \colon F \longrightarrow F/D$ è la proiezione canonica e D è il sottomodulo di F generato da tutti gli elementi di 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. Dimostriamo ora che la coppia $(T = F/D, \tau)$ è un prodotto tensoriale di M e N provando che verifica 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 un unico $\tilde{f}$, 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

$$\tilde{f} \colon F/D \longrightarrow P, \quad \overline{x} \mapsto \psi(x) \ \text{ per ogni } x \in F.$$

Se $\tilde{f}$ è ben definito allora è un omomorfismo perché ψ lo è, e il diagramma commuta per costruzione. Bisogna quindi verificare la buona definizione, cioè che $\psi_{|_D} = 0$, e basta farlo 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 da provare che tale $\tilde{f}$ è unico. Siano $\tilde{f}_1, \tilde{f}_2$ 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 $\overline{x} \in F/D$, esiste $x \in F$ tale che $\tilde{f}_1(\overline{x}) = \tilde{f}_1(\pi(x)) = \tilde{f}_2(\pi(x)) = \tilde{f}_2(\overline{x})$ e la dimostrazione è conclusa. □

Alla luce di quanto appena visto, il prodotto tensoriale di M e 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 $\tau(m, n)$. Tale elemento si dice *tensore elementare* o *monomiale*. Un *tensore* invece è un qualunque elemento di $M \otimes N$.
Dalla costruzione di τ discende immediatamente che per ogni $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ e $a \in A$ si ha

$$\begin{aligned}(m_1 + m_2) \otimes n &= m_1 \otimes n + m_2 \otimes n,\\ m \otimes (n_1 + n_2) &= m \otimes n_1 + m \otimes n_2,\\ a(m \otimes n) &= am \otimes n = m \otimes an.\end{aligned}$$

T. 5.3. (→ p. 216) Siano A un anello e M, N due A-moduli.

1. Per ogni $m \in M$ e $n \in N$ si ha $m \otimes 0 = 0 \otimes n = 0$.
2. L'insieme $\{m \otimes n : m \in M,\ n \in N\}$ dei tensori elementari è un insieme di generatori di $M \otimes N$.
3. Siano $\mathcal{G}_1$ e $\mathcal{G}_2$ insiemi di generatori di M e N rispettivamente; allora l'insieme dei tensori elementari dato da $\mathcal{G}_1 \otimes \mathcal{G}_2 = \{m \otimes n : m \in \mathcal{G}_1,\ n \in \mathcal{G}_2\}$ 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.5.3**.2 segue che un tensore è una combinazione A-lineare finita di tensori elementari. È importante osservare che $M \otimes N$ *può essere uguale a zero anche se* $M \neq 0$ *e* $N \neq 0$; per esempio proviamo 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.5.3**.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.5.3**.2.

Come ulteriore esempio calcoliamo il prodotto tensoriale $A[x] \otimes_A A[y]$ degli A-moduli $M = A[x]$ e $N = A[y]$, che sono generati rispettivamente da $\{x^i : i \in \mathbb{N}\}$ e $\{y^j : j \in \mathbb{N}\}$. Pertanto $M \otimes_A N$ è generato da $\{x^i \otimes y^j : (i, j) \in \mathbb{N}^2\}$. Costruiamo il diagramma

$$\begin{array}{ccc} A[x] \times A[y] & \xrightarrow{\cdot} & A[x, y] \\ \downarrow{\scriptstyle \tau} & \nearrow{\scriptstyle \varphi} & \\ A[x] \otimes_A A[y], & & \end{array}$$

dove $\cdot(x^i, y^j) = x^i y^j$ è l'usuale moltiplicazione in $A[x,y]$, che è A-bilineare, e

$$\varphi(\sum_{i,j} a_{ij}(x^i \otimes y^j)) = \sum_{i,j} a_{ij} x^i y^j.$$

Per ogni polinomio $p = \sum_{i,j} a_{ij} x^i y^j \in A[x,y]$, abbiamo $\varphi(\sum_{i,j} a_{ij}(x^i \otimes y^j)) = p$ e quindi φ è surgettiva. 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.

Proprietà del prodotto tensoriale

T. 5.4. (→ p. 217) Siano A un anello, I un ideale di A e M, N, P degli A-moduli; allora

1. $A \otimes M \simeq M$;
2. $M \otimes N \simeq N \otimes M$;
3. $(M \otimes N) \otimes P \simeq M \otimes (N \otimes P)$;
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.

Il punto 6 vale in generale per moduli liberi, cf. **E.11.4**.
Osserviamo che il prodotto tensoriale e la somma diretta commutano per il punto 4; per quanto riguarda prodotto tensoriale e prodotto diretto si veda **VoF.14.92**.

T. 5.5. (→ p. 219) Siano A un anello e M, N, P degli 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 chiamato *formula di aggiunzione* Hom-$\otimes$.

5.2 Il prodotto tensoriale come funtore

Dati $f\colon M \longrightarrow M'$ e $g\colon N \longrightarrow N'$ omomorfismi di A-moduli, risulta ben definito l'omomorfismo

$$f \otimes g\colon M \otimes N \longrightarrow M' \otimes N', \quad (f \otimes g)(m \otimes n) = f(m) \otimes g(n),$$

cf. **E.11.6**.
In virtù di **E.11.7**, dato un A-modulo N, possiamo considerare $\bullet \otimes N$ come un funtore covariante dalla categoria degli A-moduli in sé, che 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, grazie a **T.5.4**.2, possiamo identificare i due funtori.

Esattezza a destra di $\bullet \otimes N$

T. 5.6. Sia $M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ una successione esatta; allora 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 per ogni A-modulo N.

Dimostrazione T. 5.6. Per **T.4.16**.1, l'esattezza di $M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \to 0$ implica quella di

$$\begin{aligned} 0 \longrightarrow \mathrm{Hom}(M_2, \mathrm{Hom}(N, Q)) &\xrightarrow{g^*} \mathrm{Hom}(M, \mathrm{Hom}(N, Q)) \\ &\xrightarrow{f^*} \mathrm{Hom}(M_1, \mathrm{Hom}(N, Q)) \end{aligned}$$

per ogni A-modulo Q. Utilizzando gli isomorfismi definiti in **T.5.1** e **T.5.5**, otteniamo il diagramma commutativo

$$\begin{array}{ccc} \mathrm{Hom}(M, \mathrm{Hom}(N, Q)) & \xrightarrow[\varphi \mapsto \varphi \circ f]{f^*} & \mathrm{Hom}(M_1, \mathrm{Hom}(N, Q)) \\ \downarrow \simeq & & \downarrow \simeq \\ \mathrm{Bil}(M, N; Q) & \xrightarrow[b_\varphi \mapsto b_{\varphi \circ f}]{} & \mathrm{Bil}(M_1, N; Q) \\ \downarrow \simeq & & \downarrow \simeq \\ \mathrm{Hom}(M \otimes N, Q) & \xrightarrow[\widetilde{b_\varphi} \mapsto \widetilde{b_{\varphi \circ f}}]{} & \mathrm{Hom}(M_1 \otimes N, Q). \end{array}$$

Dato che, per ogni $\widetilde{b_\varphi} \in \mathrm{Hom}(M \otimes N, Q)$, si ha

$$\begin{aligned} \left(f \otimes \mathrm{id}_N\right)^* \left(\widetilde{b_\varphi}\right)(m_1 \otimes n) &= \left(\widetilde{b_\varphi} \circ (f \otimes \mathrm{id}_N)\right)(m_1 \otimes n) \\ &= \widetilde{b_\varphi}(f(m_1) \otimes n) = b_\varphi(f(m_1), n) = \varphi(f(m_1))(n) \\ &= b_{\varphi \circ f}(m_1, n) = \widetilde{b_{\varphi \circ f}}(m_1 \otimes n) \end{aligned}$$

per ogni tensore elementare $m_1 \otimes n$, l'ultimo omomorfismo orizzontale è esattamente $(f \otimes \mathrm{id}_N)^*$. Analogamente si verifica che l'omomorfismo indotto su $\mathrm{Hom}(M_2 \otimes N, Q)$ è $(g \otimes \mathrm{id}_N)^*$. Dunque la successione

$$0 \longrightarrow \mathrm{Hom}(M_2 \otimes N, Q) \xrightarrow{(g \otimes \mathrm{id}_N)^*} \mathrm{Hom}(M \otimes N, Q) \xrightarrow{(f \otimes \mathrm{id}_N)^*} \mathrm{Hom}(M_1 \otimes N, Q)$$

è esatta per ogni Q, per cui **T.4.17**.1, implica l'esattezza di

$$M_1 \otimes N \xrightarrow{f\otimes \mathrm{id}_N} M \otimes N \xrightarrow{g\otimes \mathrm{id}_N} M_2 \otimes N \longrightarrow 0,$$

come volevamo. □

Analogamente a quanto visto per i funtori $\mathrm{Hom}_A(M,\bullet)$ e $\mathrm{Hom}_A(\bullet,N)$, cf. **T.4.16** e **T.4.17**, della precedente proposizione vale anche il viceversa.

T. 5.7. (→ p. 219) 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.

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 iniettivo poiché $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(2) \simeq \mathbb{Z}/(2) \neq 0$.

5.3 Estensione di scalari

Abbiamo visto 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 tramite f per restrizione di scalari

$$A \times M \longrightarrow M, \quad (a,m) \longmapsto f(a)m.$$

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 M e N perché, per ogni $m \in M$ e $a \in A$, abbiamo $\tilde{u}(am) = u(f(a)m) = f(a)u(m) = a\tilde{u}(m)$. L'anello B è in maniera naturale un modulo su sé stesso ed ha anche la 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 ogni $b, b' \in B$ e per ogni $a \in A$. Si dice che B è un (A,B)-*bimodulo*.

Sia ora M un A-modulo. Il prodotto tensoriale $M_B = B \otimes_A M$ ha una struttura naturale 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 $K \subset L$, dove l'estensione di scalari trasforma uno spazio vettoriale su L in uno spazio vettoriale su L.
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 risulta essere di grande utilità; per una dimostrazione completa cf. [2, Theorem 8.8].

T. 5.8. Siano A e B anelli, M un A-modulo, N un (A, B)-bimodulo e P un B-modulo; allora esiste un isomorfismo di (A, B)-bimoduli

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

6

Localizzazione

In questo capitolo vogliamo descrivere una costruzione, detta *localizzazione*, che generalizza la costruzione del campo dei numeri razionali a partire dall'anello degli interi e quella del campo dei quozienti di un dominio di integrità. Partendo da anelli arbitrari definiremo delle frazioni usando come denominatori gli elementi di particolari sottoinsiemi.

6.1 Anello delle frazioni

Sia A un anello; diciamo che un insieme $S \subseteq A$ è *moltiplicativo* o *moltiplicativamente chiuso* se $1 \in S$ e $st \in S$ per ogni $s, t \in S$.

T. 6.1. (→ p. 219) La relazione

$$(a, s) \sim (b, t) \iff \text{esiste } u \in S \text{ tale che } u(at - bs) = 0$$

definisce una relazione di equivalenza su $A \times S$.

Denotiamo $(A \times S)/\sim$ con $S^{-1}A$ e indichiamo 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 insieme moltiplicativo di A.

T. 6.2. (→ p. 219) L'insieme $S^{-1}A$ dotato delle operazioni di somma e prodotto definite da

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st},$$

con $a, b \in A$ e $s, t \in S$ è un anello commutativo con $0 = \frac{0}{1}$ e $1 = \frac{1}{1}$.
L'applicazione $\sigma = \sigma_S \colon A \longrightarrow S^{-1}A$ definita da $\sigma(a) = \frac{a}{1}$ è un omomorfismo di anelli, detto *omomorfismo canonico*.

Tale anello viene detto l'*anello delle frazioni di A rispetto a S* o la *localizzazione di A in S*.

T. 6.3. (→ p. 219) Siano S un insieme moltiplicativo di A e σ l'omomorfismo canonico; allora

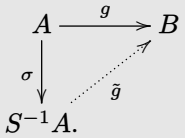
1. σ è iniettivo se e solo se $S \cap \mathcal{D}(A) = \emptyset$;

2. $S^{-1}A = 0$ se e solo se $S \cap \mathcal{N}(A) \neq \emptyset$.

La proprietà fondamentale della localizzazione $S^{-1}A$ è che ogni omomorfismo g da 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. 6.4. 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 commuta



Dimostrazione T. 6.4. Se un tale omomorfismo $\tilde{g}$ esiste, allora si deve avere $\tilde{g}(\frac{a}{1}) = \tilde{g}\sigma(a) = g(a)$ per ogni $a \in A$. Inoltre, $\tilde{g}(\frac{1}{s}) = \tilde{g}((\frac{s}{1})^{-1}) = \tilde{g}(\frac{s}{1})^{-1} = g(s)^{-1}$ per ogni $s \in S$. Dunque

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

Un tale $\tilde{g}$ è dunque univocamente determinato da g.
È sufficiente provare che $\tilde{g}\colon S^{-1}A \longrightarrow B$ è ben definito, il fatto che sia un omomorfismo segue direttamente dal fatto che g lo è. Siano $\frac{a}{s} = \frac{b}{t}$ e $u \in S$ tali che $u(at - bs) = 0$; abbiamo $g(u)(g(a)g(t) - g(b)g(s)) = 0$ e, dato che $g(u) \in B^*$, ciò implica $\tilde{g}\left(\frac{a}{s}\right) = g(a)g(s)^{-1} = g(b)g(t)^{-1} = \tilde{g}\left(\frac{b}{t}\right)$, come volevamo. □

T. 6.5. (→ p. 220) Con le notazioni di **T.6.4**, supponiamo che
i) $g(a) = 0$ implica che esiste $s \in S$ tale che $as = 0$;
ii) per ogni $b \in B$ esistono $a \in A$ e $s \in S$ tali che $b = g(a)g(s)^{-1}$;
allora $\tilde{g}\colon S^{-1}A \longrightarrow B$ è un isomorfismo.

In particolare osserviamo che se g è iniettiva allora $\tilde{g}$ è iniettiva.

Esistono due casi di particolare importanza nella costruzione di anelli di frazioni:

i) $S = S_f = \{f^n\}_{n\in\mathbb{N}}$ è costituito dalle potenze di un elemento $f \in A$; in questo caso $S^{-1}A$ si indica con A_f ed è chiaro che $A_f \neq 0$ se e solo se $f \notin \mathcal{N}(A)$;

ii) $S = A \setminus \mathfrak{p}$ è il complementare di un ideale primo $\mathfrak{p}$ in A; in questo caso indichiamo $S^{-1}A$ con $A_{\mathfrak{p}}$.

Il nome localizzazione proviene dal secondo caso ed è giustificato dal seguente fatto.

T. 6.6. (→ p. 220) L'anello $A_{\mathfrak{p}}$ è un anello locale locale con ideale massimale $\mathfrak{p}A_{\mathfrak{p}} = \{\frac{a}{s}\colon\ a \in \mathfrak{p},\ s \in S\}$.

Ideali estesi e ideali contratti rispetto a σ_S

T. 6.7. (→ p. 220) 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. $I^{ec} = \{a \in A\colon\ as \in I \text{ per qualche } s \in S\} = \bigcup_{s\in S} I\colon(s)$.
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.

T. 6.8. (→ p. 220) 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

$$\operatorname{Spec} S^{-1}A \xleftrightarrow{1:1} \{\mathfrak{p} \in \operatorname{Spec} A\colon\ \mathfrak{p} \cap S = \emptyset\}.$$

È facile verificare che $S = A \setminus \bigcup_{h\in H} \mathfrak{p}_h$ è moltiplicativo per ogni insieme di primi $\{\mathfrak{p}_h \in \operatorname{Spec} A\colon\ h \in H\}$; inoltre, per il Lemma di scansamento, se H è finito allora $S^{-1}A$ è semilocale.

Localizzazione ed operazioni fra ideali

T. 6.9. (→ p. 221) Siano $I, J \subset A$ ideali; allora

1. $S^{-1}(I + J) = S^{-1}I + S^{-1}J$;
2. $S^{-1}(IJ) = S^{-1}I \cdot S^{-1}J$;

3. $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$;
4. $S^{-1}\sqrt{I} = \sqrt{S^{-1}I}$. In particolare $S^{-1}\mathcal{N}(A) = \mathcal{N}(S^{-1}A)$.

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 perché $\frac{2}{1}\frac{3}{6} = \frac{1}{1}$. 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 6.5.

6.2 Modulo delle frazioni

La costruzione descritta per gli anelli può essere generalizzata al caso dei moduli; localizziamo un A-modulo M in un insieme moltiplicativamente chiuso $S \subset A$, ottenendo un $S^{-1}A$-modulo $S^{-1}M$.
Più precisamente

$$(m,s) \sim (n,t) \iff \text{esiste } u \in S \text{ tale che } u(tm - sn) = 0,$$

con $m,n \in M$ e $s,t \in S$, 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 insieme moltiplicativo.
L'insieme $S^{-1}M$ dotato delle operazioni definite da

$$\frac{m}{s} + \frac{n}{t} = \frac{tm + sn}{st}, \qquad \frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st},$$

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 $\operatorname{Ann} M \cap S \neq \emptyset$ allora $S^{-1}M = 0$; infatti, se esiste $s \in \operatorname{Ann}(M) \cap S$ allora, preso un qualunque elemento $\frac{m}{t} \in S^{-1}M$, abbiamo $sm = 0$ e quindi $\frac{m}{t} = \frac{0}{1}$.
Analogamente a quanto fatto per gli anelli denotiamo $S^{-1}M$ con M_f quando $S = \{f^n\}_{n\in\mathbb{N}}$ e con $M_\mathfrak{p}$ quando $S = A \setminus \mathfrak{p}$, rispettivamente. In particolare quando $M = I$ è un ideale di A scriviamo $I_\mathfrak{p} = IA_\mathfrak{p}$.
Considerando l'omomorfismo canonico $\sigma\colon A \longrightarrow S^{-1}A$ di anelli, per restrizione di scalari tramite σ qualsiasi $S^{-1}A$-modulo è dotato di una struttura di A-modulo data da $am = \frac{a}{1}m$ 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. È facile verificare che

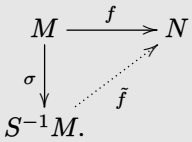
la mappa $\sigma\colon M \longrightarrow S^{-1}M$, definita da $\sigma(m) = \frac{m}{1}$, è un omomorfismo di A-moduli.

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 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 le due strutture devono essere compatibili, cioè tali che $am = \frac{a}{1}m$ per ogni $a \in A$ e $m \in M$.

T. 6.10. (→ p. 221) 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 se e solo se per ogni $s \in S$ la moltiplicazione $\mu_s\colon N \xrightarrow{s} N$ è un isomorfismo. In tale caso la struttura di $S^{-1}A$-modulo su N è unica.

Proprietà universale del modulo delle frazioni

T. 6.11. (→ p. 221) Siano $S \subset A$ un insieme moltiplicativo, M e 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 commuta

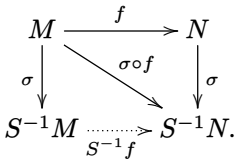


Osserviamo che, per quanto visto in **T.6.10**, si richiede che N sia un $(A, S^{-1}A)$-bimodulo. Inoltre, l'omomorfismo $\tilde{f}$ è anche un omomorfismo di A-moduli per restrizione di scalari.

6.3 Il funtore S^{-1}

Per poter considerare l'operazione di localizzazione come funtore, dobbiamo capire come trasforma gli omomorfismi. Sia $f\colon M \longrightarrow N$ un omomorfismo di

A-moduli; 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 $(A, S^{-1}A)$-bimodulo; 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.

Esattezza di S^{-1}

T. 6.12. (→ p. 222) Il funtore 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 e se g è un omomorfismo surgettivo allora $S^{-1}g$ è surgettivo.

Dati un A-modulo M e una sua localizzazione $S^{-1}M$ è facile vedere che tutti i sottomoduli di $S^{-1}M$ sono del tipo $S^{-1}N$ per qualche sottomodulo N di M, cf. **T.6.7**.2.

Localizzazione ed operazioni fra moduli

T. 6.13. Siano $S \subset A$ un insieme moltiplicativo e M, N, P degli A-moduli.

1. Se M e N sono sottomoduli di 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 è sottomodulo di 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 e N sono sottomoduli di P e N è finitamente generato allora

$$S^{-1}(M : N) = S^{-1}M : S^{-1}N.$$

Dimostrazione T. 6.13. 1. Si ha $\frac{m+n}{s} = \frac{m}{s} + \frac{n}{s}$ per ogni $m \in M$, $n \in N$ e $s \in S$, quindi $S^{-1}(M+N) \subseteq S^{-1}M + S^{-1}N$.

Per l'altra inclusione basta ricordare che $\frac{m}{s} + \frac{n}{t} = \frac{tm+sn}{st}$.

2. L'inclusione $S^{-1}(M \cap N) \subseteq S^{-1}M \cap S^{-1}N$ segue immediatamente dal fatto che $M \cap N$ è contenuto sia in M che in N.

Per l'altra inclusione, sia $\alpha \in S^{-1}M \cap S^{-1}N$; allora esistono $m \in M$, $n \in N$ e $s, t, u \in S$ tali che $\alpha = \frac{m}{s} = \frac{n}{t}$ con $u(tm - sn) = 0$. Da ciò otteniamo $utm = usn \in M \cap N$ e pertanto $\frac{m}{s} = \frac{utm}{uts} = \frac{usn}{uts} \in S^{-1}(M \cap N)$.

3. Applicando S^{-1} alla successione esatta $0 \longrightarrow N \xrightarrow{j} P \xrightarrow{\pi} P/N \longrightarrow 0$, dove 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.6.12**.

Consideriamo il seguente diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S^{-1}N & \xrightarrow{S^{-1}j} & S^{-1}P & \xrightarrow{S^{-1}\pi} & S^{-1}(P/N) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{S^{-1}N}} & & \downarrow{\scriptstyle \mathrm{id}_{S^{-1}P}} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & S^{-1}N & \xrightarrow[S^{-1}j]{} & S^{-1}P & \xrightarrow[\eta]{} & S^{-1}P/S^{-1}N & \longrightarrow & 0, \end{array}$$

dove η è la proiezione canonica sul quoziente $\eta\left(\frac{p}{s}\right) = \frac{p}{s} + S^{-1}N$ 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 funzione γ è ben definita; infatti, se $\frac{\overline{p}}{s} = \frac{\overline{q}}{t}$ allora esiste $u \in S$ tale che $ut\overline{p} = us\overline{q}$, i.e. $utp - usq = n$ per un certo $n \in N$. Quindi

$$\gamma\left(\frac{\overline{p}}{s}\right) = \frac{p}{s} + S^{-1}N = \frac{utp}{uts} + S^{-1}N = \frac{usq}{uts} + \frac{n}{uts} + S^{-1}N = \frac{q}{t} + S^{-1}N = \gamma\left(\frac{\overline{q}}{t}\right).$$

Chiaramente il quadrato a sinistra commuta, mentre per quello a destra abbiamo $\gamma \circ (S^{-1}\pi)\left(\frac{p}{s}\right) = \gamma\left(\frac{\overline{p}}{s}\right) = \eta\left(\frac{p}{s}\right)$. La conclusione segue allora da **T.4.20**.

4. Procediamo per induzione sul numero di generatori di M; se $M = 0$ non c'è nulla da dimostrare.

Supponiamo che $M = \langle m \rangle_A \neq 0$; allora $S^{-1}M = \langle \frac{m}{1} \rangle_{S^{-1}A}$. Se $\frac{a}{s} \in S^{-1} \operatorname{Ann}_A M$ allora $\frac{a}{s}\frac{m}{t} = \frac{am}{st} = 0$ per ogni $\frac{m}{t} \in S^{-1}M$, ossia $\frac{a}{s} \in \operatorname{Ann}_{S^{-1}A} S^{-1}M$.

Per l'altra inclusione, sia $\frac{a}{s} \in \operatorname{Ann}_{S^{-1}A} S^{-1}M$; allora $\frac{am}{s} = \frac{a}{s}\frac{m}{1} = 0$ per ogni $m \in M$, ed esiste $u \in S$ tale che $uam = 0$. Quindi $ua \in \operatorname{Ann}_A M$ e $\frac{a}{s} = \frac{ua}{us} \in S^{-1} \operatorname{Ann}_A M$.

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 i punti 1 e 2 insieme con le proprietà dell'annullatore, cf. **E.8.17**, implicano

$$\begin{aligned} S^{-1}\operatorname{Ann}_A M &= S^{-1}\operatorname{Ann}_A(N_1+N_2) = S^{-1}(\operatorname{Ann}_A N_1 \cap \operatorname{Ann}_A N_2) \\ &= S^{-1}\operatorname{Ann}_A N_1 \cap S^{-1}\operatorname{Ann}_A N_2 \\ &= \operatorname{Ann}_{S^{-1}A} S^{-1}N_1 \cap \operatorname{Ann}_{S^{-1}A} S^{-1}N_2 \\ &= \operatorname{Ann}_{S^{-1}A}(S^{-1}N_1 + S^{-1}N_2) \\ &= \operatorname{Ann}_{S^{-1}A}(S^{-1}(N_1+N_2)) = \operatorname{Ann}_{S^{-1}A} S^{-1}M \end{aligned}$$

dove la quarta uguaglianza è giustificata dall'ipotesi induttiva.

5. Per definizione $a \in M\colon N$ se e solo se $aN \subseteq M$ e questo equivale a dire che $a\,((N+M)/M) = 0$, i.e.

$$M\colon N = \operatorname{Ann}_A\left((N+M)/M\right).$$

Se N è finitamente generato anche $(N+M)/M$ lo è, e basta applicare i punti 4 e 1 per avere

$$\begin{aligned} S^{-1}(M\colon N) &= S^{-1}\operatorname{Ann}_A\left((N+M)/M\right) \\ &= \operatorname{Ann}_{S^{-1}A}\left(S^{-1}\left((N+M)/M\right)\right) \\ &= \operatorname{Ann}_{S^{-1}A}\left(S^{-1}(N+M)/S^{-1}M\right) \\ &= \operatorname{Ann}_{S^{-1}A}\left((S^{-1}N + S^{-1}M)/S^{-1}M\right) = S^{-1}M\colon S^{-1}N. \qquad \square \end{aligned}$$

Osserviamo che il punto 4 è un caso particolare del punto 5 ed entrambe le affermazioni non valgono in generale. Per esempio consideriamo $A = K\left[t, \frac{x}{t^n}\colon n \in \mathbb{N}\right]$ con x e t indeterminate, $M = \langle x\rangle_A$, $N = \langle \frac{x}{t^n}\colon n\in\mathbb{N}\rangle_A$ e $S = \{t^n\colon n\in\mathbb{N}\}$. Allora M e N sono ideali di A e

$$M\colon N = \left\{a\in A\colon \frac{ax}{t^n} \in M \text{ per ogni } n\in\mathbb{N}\right\} = \left(\frac{x}{t^n}\colon n\in\mathbb{N}\right) = N;$$

dunque $S^{-1}(M\colon N) = S^{-1}N = S^{-1}(x) = S^{-1}M$, mentre $S^{-1}M\colon S^{-1}N = S^{-1}A$.

Vediamo infine le seguenti importanti relazioni con il prodotto tensoriale.

Localizzazione e prodotto tensoriale

T. 6.14. (→ p. 222) Siano S un insieme moltiplicativo di un anello A e M un A-modulo; allora abbiamo isomorfismi canonici

1. $S^{-1}M \simeq S^{-1}A \otimes_A M$;
2. $S^{-1}(M\otimes_A N) \simeq S^{-1}M \otimes_{S^{-1}A} S^{-1}N$.

6.4 Proprietà locali

Una proprietà $\mathcal{P}$ di un anello A si dice *locale* se

$$\mathcal{P} \text{ vale per } A \text{ se e solo se } \mathcal{P} \text{ vale per } A_{\mathfrak{p}} \text{ per ogni } \mathfrak{p} \in \operatorname{Spec} A\ .$$

Allo stesso modo, una proprietà $\mathcal{P}$ di un A-modulo M si dice *locale* se

$$\mathcal{P} \text{ vale per } M \text{ se e solo se } \mathcal{P} \text{ vale per l'} A_{\mathfrak{p}}\text{-modulo } M_{\mathfrak{p}} \text{ per ogni } \mathfrak{p} \in \operatorname{Spec} A.$$

Una proprietà locale fondamentale è la seguente.

T. 6.15. (→ p. 222) Sia M un A-modulo; sono fatti equivalenti:

1. $M = 0$;
2. $M_{\mathfrak{p}} = 0$ per ogni ideale $\mathfrak{p} \in \operatorname{Spec} A$;
3. $M_{\mathfrak{m}} = 0$ per ogni ideale $\mathfrak{m} \in \operatorname{Max} A$.

Dati $S = A \setminus \mathfrak{p}$ con $\mathfrak{p}$ primo, e un omomorfismo di A-moduli $f\colon M \longrightarrow N$ indichiamo con $f_{\mathfrak{p}}\colon M_{\mathfrak{p}} \longrightarrow N_{\mathfrak{p}}$ l'omomorfismo $S^{-1}f$.

T. 6.16. Sia $f\colon M \longrightarrow N$ un omomorfismo; allora

1. f è iniettivo se e solo se $f_{\mathfrak{p}}$ è iniettivo per ogni $\mathfrak{p} \in \operatorname{Spec} A$, equivalentemente, se e solo se $f_{\mathfrak{m}}$ è iniettivo per ogni $\mathfrak{m} \in \operatorname{Max} A$;
2. f è surgettivo se e solo se $f_{\mathfrak{p}}$ è surgettivo per ogni $\mathfrak{p} \in \operatorname{Spec} A$, equivalentemente, se e solo se $f_{\mathfrak{m}}$ è surgettivo per ogni $\mathfrak{m} \in \operatorname{Max} A$.

Dimostrazione T. 6.16. 1. Dimostriamo che $(\operatorname{Ker} f)_{\mathfrak{p}} = \operatorname{Ker} f_{\mathfrak{p}}$ per ogni primo $\mathfrak{p}$. Infatti, abbiamo $\frac{m}{s} \in \operatorname{Ker} f_{\mathfrak{p}}$ se e solo se $\frac{f(m)}{s} = f_{\mathfrak{p}}\left(\frac{m}{s}\right) = 0$, cioè quando 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, abbiamo che $\frac{m}{s} \in (\operatorname{Ker} f)_{\mathfrak{p}}$ implica $\frac{m}{s} = \frac{n}{t}$ 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. $\frac{m}{s} \in \operatorname{Ker} f_{\mathfrak{p}}$.
Si conclude allora per **T.6.15**.

2. 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.6.15**. □

T. 6.17. (→ p. 223) Siano A un anello e M un A-modulo; allora le seguenti sono proprietà locali

1. A è ridotto;
2. M è piatto.

Come esempio di proprietà non locale possiamo considerare $\mathcal{P} =$ "essere noetheriano". Definiamo $A = (\mathbb{Z}/(2))[x_i\colon\ i \in \mathbb{N}]/I$ con $I = (x_i^2 - x_i\colon\ i \in \mathbb{N})$. Sicuramente A non è noetheriano. Preso un qualsiasi ideale primo $\mathfrak{p}$ l'anello $A_\mathfrak{p}$ è locale per **T.6.6**. 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.8.13**, si ha allora che $A_\mathfrak{p} \simeq \mathbb{Z}/(2)$ è noetheriano per ogni $\mathfrak{p} \in \operatorname{Spec} A$.

6.5 Approfondimento: la saturazione di un insieme

In questa sezione costruiamo la saturazione di un insieme moltiplicativo $S \subset A$ e descriviamo l'insieme degli invertibili di $S^{-1}A$. Come già osservato in precedenza, è possibile infatti che l'insieme $\left\{\frac{t}{s} \in S^{-1}A\colon\ t \in S\right\}$ non esaurisca $(S^{-1}A)^*$.
Consideriamo un insieme moltiplicativo $S \subset A$; allora $\frac{a}{s} \in (S^{-1}A)^*$ 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 esistono $u \in S$ e $b \in A$ tali 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 l'insieme $S = A \setminus \mathcal{D}(A)$ sono insiemi moltiplicativi saturati.
Osserviamo che se S è saturato allora $S = \{a \in A\colon\ \frac{a}{1} \in (S^{-1}A)^*\}$. 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. 6.18. (→ p. 223) Un insieme moltiplicativo S è saturato se e solo se

$$S = A \setminus \bigcup_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \cap S = \emptyset}} \mathfrak{p}.$$

Definiamo la *saturazione* di un insieme $S \subseteq A$ come l'insieme

$$\overline{S} = \{t \in A\colon\ \text{esiste } a \in A \text{ tale che } at \in S\}.$$

Si verifica facilmente che la saturazione di un insieme moltiplicativo è un insieme moltiplicativo saturato, cf. **E.12.33**.
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. 6.19. Siano $S \subset A$ un insieme moltiplicativo e $\overline{S}$ la sua saturazione; allora

1. $S \subseteq \overline{S}$;
2. se $T \subset A$ è 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. $\overline{S}^{-1}A = S^{-1}A$.

Dimostrazione T. 6.19. 1. Se $s \in S$ allora $s \cdot 1 \in S$ e quindi $s \in \overline{S}$.

2. Sia $s \in \overline{S}$; allora esiste $a \in A$ tale che $as \in S \subseteq T$ e quindi, dato che T è saturato, $s \in T$.

3. Sia $T = A \setminus \bigcup_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \cap S = \emptyset}} \mathfrak{p}$; chiaramente T è un insieme moltiplicativo che contiene S ed è saturato per **T.6.18**. Quindi dal punto 2 segue che $\overline{S} \subseteq T$.

Per l'altra inclusione, osserviamo che $\overline{S}$ è saturato e contiene S; quindi, di nuovo per **T.6.18**,

$$\overline{S} = A \setminus \bigcup_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \cap \overline{S} = \emptyset}} \mathfrak{p} \supseteq A \setminus \bigcup_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \cap S = \emptyset}} \mathfrak{p} = T.$$

4. Consideriamo $\frac{a}{s}$ con $a \in \overline{S}$; allora esiste $t \in A$ tale che $ta \in S$ 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 $uab = ust \in S$ 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 $\frac{u}{1} \in (S^{-1}A)^*$ ed esiste $\frac{b}{t}$ tale che $\frac{u}{1}\frac{b}{t} = \frac{1}{1}$. Pertanto esiste $s \in S$ tale che $sub = st \in S$, quindi $u \in \overline{S}$.

6. Chiaramente $A \times S \subseteq A \times \overline{S}$; se indichiamo con $\sim_S$ e $\sim_{\overline{S}}$ le relazioni di equivalenza associate ad S e $\overline{S}$ rispettivamente, cf. **T.6.1**, abbiamo che

$$(a, s) \sim_S (b, t) \ \text{ se e solo se } \ (a, s) \sim_{\overline{S}} (b, t)$$

per ogni (a, s), (b, t) in $A \times S$. Quindi $S^{-1}A \subseteq \overline{S}^{-1}A$.

Per l'altra inclusione, sia $\frac{b}{t} \in \overline{S}^{-1}A$; allora esiste $a \in A$ tale che $at \in S$ e dunque $\frac{b}{t} = \frac{ab}{at} \in S^{-1}A$. □

In generale, dati $S \subset T$ insiemi moltiplicativi di A, l'esistenza di relazioni di contenimento tra $S^{-1}A$ e $T^{-1}A$ dipende in primo luogo dalla compatibilità tra le relazioni di equivalenza $\sim_S$ e $\sim_T$, cf. **T.6.19**.6. Ad esempio possiamo considerare $A = \mathbb{Z}/(6)$ con $S = \{\overline{1}, \overline{5}\} = A^* \subset T = \{\overline{1}, \overline{5}, \overline{2}, \overline{4}\} = \mathbb{Z}/(6) \setminus (\overline{3})$; abbiamo allora $S^{-1}A \simeq \mathbb{Z}/(6)$ e $T^{-1}A \simeq \mathbb{Z}/(3)$.

T. 6.20. (→ p. 223) Siano S e T insiemi moltiplicativi di A; allora

$$S^{-1}A = T^{-1}A \quad \text{se e solo se} \quad \overline{S} = \overline{T}.$$

7

Anelli noetheriani e artiniani. Decomposizione primaria

In quest'ultimo capitolo introduciamo gli anelli noetheriani e artiniani attraverso le condizioni di stabilizzazione delle catene ascendenti e discendenti. Proviamo che ogni ideale di un anello noetheriano è finitamente generato ed è rappresentabile come intersezione finita di ideali primari. Dimostriamo che un anello A è noetheriano se e solo se l'anello $A[x_1, \ldots, x_n]$ è noetheriano e che A è artiniano se e solo se è una somma diretta finita di anelli artiniani locali, generalizzando le discussioni dei Capitoli 2 e 3 quando A era l'anello dei polinomi $K[x_1, \ldots, x_n]$ o un suo quoziente.

7.1 Moduli noetheriani e artiniani

Sia $(\Sigma, \leq)$ un *poset*, ovvero un insieme Σ parzialmente ordinato da una relazione di ordine $\leq$.

T. 7.1. (→ p. 223) Le seguenti condizioni sono equivalenti:

1. ogni catena $\{s_\alpha\}_{\alpha \in \Lambda}$ di elementi di Σ si *stabilizza*, o è *stazionaria*, cioè esiste $\alpha_0 \in \Lambda$ tale che $s_\alpha = s_{\alpha_0}$ per ogni $\alpha \geq \alpha_0$.

2. ogni sottoinsieme non vuoto di Σ ammette elementi massimali rispetto a $\leq$.

Come esempio fondamentale 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 a.c.c, dall'inglese *ascending chain condition*; nel secondo caso si chiama invece *condizione della catena discendente*, in breve d.c.c., dall'inglese *descending chain condition*. 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..

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.2.13** e **T.2.14**. Siano dunque M un A-modulo e 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.

Moduli noetheriani: prime proprietà

T. 7.2. Siano I un ideale di A, $S \subset A$ un insieme moltiplicativo e M, N, P degli A-moduli.

1. M è noetheriano se e solo se ogni suo sottomodulo è finitamente generato.
2. Sia $0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$ 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. 7.2. 1. Siano 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 mostrare che $N = N_0$ per avere che N è finitamente generato. Supponiamo che $N \neq N_0$ e prendiamo $n \in N \setminus N_0$; allora $N_0 \subsetneq N_0 + \langle n \rangle \subseteq N$, dove $N_0 + \langle n \rangle$ è finitamente generato. Quindi $N_0 + \langle n \rangle \in \Sigma$ e ciò contraddice la massimalità di N_0.

Viceversa, sia $\{M_\alpha\}_{\alpha \in \Lambda}$ una catena ascendente di sottomoduli di M. Allora $\widetilde{M} = \bigcup_\alpha M_\alpha$ è un sottomodulo di M e quindi finitamente generato, diciamo da $m_1, \ldots, m_n$. Pertanto esiste un $\alpha_0 \in \Lambda$ tale che $m_1, \ldots, m_n \in M_{\alpha_0} \subseteq \widetilde{M} = \langle m_1, \ldots, m_n \rangle$. Dunque la catena si stabilizza in M_{α_0}.

2. Siano M noetheriano e $\{N_\alpha\}_\alpha$ una catena ascendente di sottomoduli di N; allora $\{f(N_\alpha)\}_\alpha$ 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 $\{P_\alpha\}_\alpha$ una catena ascendente in P. La catena $\{g^{-1}(P_\alpha)\}_\alpha$ è ascendente in M e quindi stazionaria. Dato che g è surgettiva, la catena $\{P_\alpha = g(g^{-1}(P_\alpha))\}_\alpha$ è stazionaria in P.

Viceversa, supponiamo che N e P siano noetheriani. Data una catena ascendente $\{M_\alpha\}_\alpha$ in M definiamo le catene $\{N_\alpha = f^{-1}(M_\alpha)\}_\alpha$ in N e $\{P_\alpha = g(M_\alpha)\}_\alpha$ in P. Entrambe sono stazionarie per ipotesi ed esiste dunque β tale che $N_\alpha = N_\beta$ e $P_\alpha = P_\beta$ per ogni $\alpha \geq \beta$.
Inoltre la successione

$$0 \longrightarrow N_\alpha \xrightarrow{f_\alpha} M_\alpha \xrightarrow{g_\alpha} P_\alpha \longrightarrow 0,$$

dove $f_\alpha = f_{|N_\alpha}$ e $g_\alpha = g_{|M_\alpha}$ è esatta per ogni α. Sicuramente f_α è iniettiva e g_α è surgettiva; proviamo allora che la successione è esatta in M_α.
Chiaramente $g_\alpha \circ f_\alpha = 0$ e quindi $\operatorname{Im} f_\alpha \subseteq \operatorname{Ker} g_\alpha$.

Per l'altra inclusione, se $m_\alpha \in \operatorname{Ker} g_\alpha \subseteq \operatorname{Ker} g = \operatorname{Im} f$ allora esiste $n \in N$ tale che $f(n) = m_\alpha$ e quindi $n \in N_\alpha$, come volevamo.
Infine consideriamo il diagramma commutativo

$$\begin{array}{ccccccccc}
0 & \longrightarrow & N_\beta & \xrightarrow{f_\beta} & M_\beta & \xrightarrow{g_\beta} & P_\beta & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}_{N_\beta}} & & \downarrow{\scriptstyle j_\beta} & & \downarrow{\scriptstyle \mathrm{id}_{P_\beta}} & & \\
0 & \longrightarrow & N_\alpha & \xrightarrow[f_\alpha]{} & M_\alpha & \xrightarrow[g_\alpha]{} & P_\alpha & \longrightarrow & 0,
\end{array}$$

dove j_β è l'omomorfismo di inclusione per ogni $\alpha \geq \beta$. Basta applicare **T.4.20** per ottenere la tesi.

3. Entrambe le implicazioni seguono dal punto precedente. Se $M = \bigoplus_{i=1}^n M_i$ è noetheriano allora ogni addendo M_i di M è noetheriano.

Viceversa, basta osservare che $0 \longrightarrow M_1 \longrightarrow M \longrightarrow \bigoplus_{i=2}^n M_i \longrightarrow 0$ è una successione esatta e procedere per induzione su n.

4. Consideriamo 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 che gli A/I-sottomoduli di A/I sono in corrispondenza biunivoca con gli ideali di A che contengono I, abbiamo che le catene ascendenti si stabilizzano e quindi che A/I è noetheriano anche come A/I-modulo.

5. Se M è noetheriano la tesi 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 $\varphi(e_i) = m_i$ per ogni i. Dato che A è noetheriano, anche A^n è noetheriano e quindi anche M lo è, per i punti 3 e 2.

6. Basta osservare che $N \subseteq M$ implica $I \subseteq \operatorname{Ann} M \subseteq \operatorname{Ann} N$ e quindi N è un A-sottomodulo di M se e solo se N è un A/I-sottomodulo di M.

7. Sia $N = \langle n_1, \ldots, n_r \rangle_A$ un sottomodulo di M; allora

$$S^{-1}N = \langle \tfrac{n_1}{1}, \ldots, \tfrac{n_r}{1} \rangle_{S^{-1}A}.$$ □

Alcune delle proprietà che valgono per anelli e moduli noetheriani sono analoghe a quelle degli anelli e moduli artiniani, anche se non c'è una vera e propria simmetria, cf. anche **T.7.17**.

T. 7.3. (→ p. 223) Siano I un ideale di un anello A e M, N, P degli 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.

7.2 Anelli noetheriani. Decomposizione primaria

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; l'altra segue da **T.7.2**.2.

Teorema della base di Hilbert

T. 7.4. Sia A un anello noetheriano; allora $A[x_1, \ldots, x_n]$ è noetheriano.

Dimostrazione T. 7.4. Forniamo una dimostrazione non costruttiva, alternativa a quella di **T.2.13** e più generale.
Dato che $A[x_1, \ldots, x_n] \simeq A[x_1, \ldots, x_{n-1}][x_n]$, è sufficiente trattare il caso $n = 1$. 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. Poniamo $\deg f_i = d_i$ e $a_i = \mathrm{lc}(f_i)$ per ogni $i \geq 1$. Abbiamo allora che $d_i \leq d_{i+1}$ per ogni i per costruzione. Inoltre la catena $(a_1) \subseteq \ldots \subseteq (a_1, \ldots, a_i) \subseteq \ldots$ di ideali di A si stabilizza per ipotesi. 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

$$g = f_{k+1} - \sum_{i=1}^{k} b_i x^{d_{k+1} - d_i} f_i;$$

abbiamo che $g \in I \setminus (f_1, \ldots, f_k)$ e, per costruzione, $\deg g < d_{k+1} = \deg f_{k+1}$ oppure $g = 0$, ma entrambi i casi contraddicono la scelta di f_{k+1}. □

Come esempi di anelli noetheriani abbiamo dunque i campi, i domini ad ideali principali, gli anelli di polinomi a coefficienti in anelli noetheriani, i loro quozienti, le loro localizzazioni e le loro somme dirette finite.

Primo teorema di finitezza

T. 7.5. (→ p. 224) Siano A un anello noetheriano e I un ideale di A; allora esiste un intero k tale che $\sqrt{I}^k \subseteq I$.

Studiamo ora la decomposizione primaria e il problema della sua unicità nel caso degli ideali; risultati analoghi sono validi anche nel caso dei sottomoduli, che non trattiamo.

In $\mathbb{Z}$ ogni ideale si scrive come intersezione o, equivalentemente, come prodotto di potenze di ideali primi distinti. Inoltre le potenze di primi sono ideali primari; tale proprietà vale più in generale nei PID, cf. **E.8.63**. In un anello generico le relazioni tra ideali primi e primari sono meno evidenti, cf. **E.8.64**.

I risultati sulla decomposizione primaria vanno considerati dunque come una generalizzazione della fattorizzazione degli ideali in $\mathbb{Z}$.

In generale un ideale I di un anello A si dice *decomponibile* se si può scrivere come intersezione finita di ideali primari di A e chiamiamo tale scrittura una *decomposizione primaria di* I. Un ideale primario che compare in una decomposizione primaria di I si dice *componente primaria di* I.
Dimostriamo ora che la noetherianità dell'anello garantisce l'esistenza di una tale decomposizione per ogni ideale.

T. 7.6. Siano A un anello noetheriano e $I \subsetneq A$ un ideale proprio; allora

1. se I è irriducibile allora I è primario;
2. I è intersezione finita di ideali irriducibili;
3. I è decomponibile.

Dimostrazione T. 7.6. 1. Supponiamo che I sia un ideale irriducibile e non primario; esistono allora $a, b \in A$ tali che $ab \in I$ con $a \notin \sqrt{I}$ e $b \notin I$. Consideriamo la catena ascendente di ideali $I \subseteq I\colon (a) \subseteq I\colon (a)^2 \subseteq \ldots$, che, per ipotesi, è stazionaria. Sia dunque $I\colon (a)^n = I\colon (a)^{n+1}$ per un certo intero n. Proviamo che $I = (I, b) \cap (I, a^n)$; dato che $I \subsetneq (I, b), (I, a^n)$ e I è irriducibile per ipotesi, troviamo una contraddizione.
Chiaramente I è contenuto in tale intersezione.

Per l'altra inclusione, sia $c \in (I, b) \cap (I, a^n)$ e scriviamo $c = da^n + i \in (I, b)$, per qualche $d \in A$ e $i \in I$. Abbiamo $ac = a^{n+1}d + ai \in (aI, ab) \subseteq I$, quindi $d \in I\colon (a)^{n+1} = I\colon (a)^n$, da cui discende che $c \in I$.

2. Consideriamo la famiglia Σ di ideali propri di A che non sono intersezione finita di irriducibili e supponiamo per assurdo che non sia vuota. Dato che A è noetheriano, esistono in Σ elementi massimali che non possono essere irriducibili. Sia J un tale elemento; possiamo scriverlo come $J_1 \cap J_2$, con $J \subsetneq J_1, J_2$. Per

la massimalità di J, abbiamo $J_1, J_2 \notin \Sigma$; dunque J_1 e J_2 si scrivono come intersezione finita di ideali irriducibili. Quindi anche J ammette una tale scrittura che contraddice $J \in \Sigma$.

3. Segue direttamente da 1 e 2. □

Sia $I = \bigcap_{i=1}^{t} \mathfrak{q}_i$ una decomposizione primaria di I; in generale non è unica, ma, usando alcuni accorgimenti, ci si può ridurre ad una decomposizione primaria *minimale*, ossia tale che

i) per ogni $i \neq j$ si ha $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j} = \mathfrak{p}_j$;

ii) per ogni i si ha $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$.

Possiamo subito eliminare quegli ideali primari che contengono l'intersezione degli altri in quanto ridondanti, e ottenere così una decomposizione primaria che verifica ii).

Diciamo che un ideale I di un anello A è $\mathfrak{p}$-*primario* se è primario e $\mathfrak{p}$ è il suo radicale, cf. **T.1.7**.1 Per verificare anche i) possiamo accorpare ideali $\mathfrak{p}$-primari e sostituirli con la loro intersezione. Questo è lecito per il seguente fatto.

T. 7.7. (→ p. 224) 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.

Il seguente risultato è semplice ma importante per il seguito.

T. 7.8. (→ p. 224) 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 $\mathfrak{q} : (a) = \mathfrak{q}$.

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.

Teorema di unicità - I

T. 7.9. Sia $I = \bigcap_{i=1}^{t} \mathfrak{q}_i$ una decomposizione primaria minimale dell'ideale $I \subseteq A$; allora

$$\left\{ \mathfrak{p}_i \in \operatorname{Spec} A : \ \mathfrak{p}_i = \sqrt{\mathfrak{q}_i} \right\} = \left\{ \sqrt{I : (a)} : \ a \in A, \ \sqrt{I : (a)} \in \operatorname{Spec} A \right\}.$$

Dimostrazione T. 7.9. Osserviamo che

$$I : (a) = \left(\bigcap_{i=1}^{t} \mathfrak{q}_i \right) : (a) = \bigcap_{i=1}^{t} (\mathfrak{q}_i : (a))$$

e che, se $a \in \bigcap_{i=1}^{t} \mathfrak{q}_i$ allora $\sqrt{I\colon (a)} = A$ non è primo.
Mostriamo ora le due inclusioni; sia $a \in A$ tale che $\sqrt{I\colon (a)}$ è primo. Possiamo scrivere

$$\sqrt{I\colon (a)} = \sqrt{\bigcap_{i=1}^{t} (\mathfrak{q}_i\colon (a))} = \bigcap_{i=1}^{t} \sqrt{\mathfrak{q}_i\colon (a)} = \bigcap_{i\colon a\notin \mathfrak{q}_i} \mathfrak{p}_i,$$

dove l'ultima uguaglianza è garantita da **T.7.8**. Dato che $\sqrt{I\colon (a)}$ è primo, dovrà necessariamente esistere un indice j tale che $\sqrt{I\colon (a)} = \mathfrak{p}_j$.

Per l'altra inclusione cerchiamo, per ogni $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$, un elemento $a_i \in A$ tale che $\mathfrak{p}_i = \sqrt{I\colon (a_i)}$. Dato che la decomposizione di I è minimale, possiamo trovare $a_i \in \bigcap_{j\neq i} \mathfrak{q}_j \setminus \mathfrak{q}_i$. Vale allora

$$\sqrt{I\colon (a_i)} = \bigcap_{j=1}^{t} \sqrt{\mathfrak{q}_j\colon (a_i)} = \bigcap_{j\neq i} \sqrt{\mathfrak{q}_j\colon (a_i)} \cap \sqrt{\mathfrak{q}_i\colon (a_i)} = \mathfrak{p}_i,$$

dove l'ultima uguaglianza discende nuovamente da **T.7.8**. □

Osserviamo che il risultato precedente vale senza che A sia noetheriano, basta che I sia decomponibile.

T. 7.10. (→ p. 224) Con le stesse notazioni di **T.7.9**, se A è noetheriano allora

$$\{\mathfrak{p}_i \in \operatorname{Spec} A\colon\ \mathfrak{p}_i = \sqrt{\mathfrak{q}_i}\} = \{I\colon (a)\ :\ a \in A,\ I\colon (a) \in \operatorname{Spec} A\}.$$

Chiamiamo i primi $\mathfrak{p}_i$ *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.
La terminologia appena introdotta ha origine geometrica. Dato un ideale $I \subset K[x_1, \dots, x_n]$ con $K = \overline{K}$, una decomposizione primaria di I dà luogo ad una decomposizione di $\mathbb{V}(I)$ in varietà irriducibili, cf. **T.3.4**. I primi minimali corrispondono alle varietà di una decomposizione minimale, mentre i primi immersi corrispondono a varietà *immerse*, cioè contenute in una delle varietà della decomposizione minimale. Infatti, preso $\mathfrak{q}_i$ tale che $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i \in \operatorname{Ass} I \setminus \operatorname{Min} I$, esiste $\mathfrak{p}_j \in \operatorname{Min} I$ tale che $\mathfrak{p}_j \subseteq \mathfrak{p}_i$ e dunque $\mathbb{V}(\mathfrak{q}_i) = \mathbb{V}(\mathfrak{p}_i) \subseteq \mathbb{V}(\mathfrak{p}_j) = \mathbb{V}(\mathfrak{q}_j)$.

T. 7.11. (→ p. 224) 1. Sia I un ideale decomponibile; allora $\operatorname{Min} I$ è costituito esattamente dagli elementi minimali di $\{\mathfrak{p} \in \operatorname{Spec} A\colon\ \mathfrak{p} \supseteq I\}$, cf. **E.8.73**.
2. Sia $0 = \bigcap_{i=1}^{t} \mathfrak{q}_i$ una decomposizione primaria minimale dell'ideale 0 di A

con $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$; allora

$$\mathcal{N}(A) = \bigcap_{\mathfrak{p}_i \in \operatorname{Min}(0)} \mathfrak{p}_i \quad \text{e} \quad \mathcal{D}(A) = \bigcup_{p_i \in \operatorname{Ass}(0)} \mathfrak{p}_i.$$

In virtù del punto 1 del precedente risultato, la notazione $\operatorname{Min} I$ risulta coerente. Inoltre, come corollario abbiamo il *secondo teorema di finitezza*; in un anello noetheriano i primi minimali sono in numero finito e sono proprio i primi minimali della decomposizione di $\sqrt{0}$. In questo senso possiamo scrivere $\operatorname{Min} A = \operatorname{Min}(0)$.

T. 7.12. (→ p. 225) 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 $(S^{-1}\mathfrak{q})^c = \mathfrak{q}$; altrimenti $S^{-1}\mathfrak{q} = S^{-1}A$.

2. Sia $I = \bigcap_{i=1}^{t} \mathfrak{q}_i$ una decomposizione primaria minimale di I, con $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$. Sia inoltre $k \leq t$ 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
$$(S^{-1}I)^c = \bigcap_{\sqrt{\mathfrak{q}} \in \operatorname{Min} I} \mathfrak{q}.$$

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 $I = \bigcap_{i=1}^{t} \mathfrak{q}_i$, eventualmente riordinando gli indici, possiamo scrivere

$$I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_k \cap \mathfrak{q}_{k+1} \cap \ldots \cap \mathfrak{q}_t,$$

con $\operatorname{Ass} I = \{\mathfrak{p}_i = \sqrt{\mathfrak{q}_i} : i = 1, \ldots, t\}$, $\operatorname{Min} I = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ e $k \leq t$.

Teorema di unicità - II

T. 7.13. (→ p. 225) Sia $I = \bigcap_{i=1}^{t} \mathfrak{q}_i$ 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 $i = 1, \ldots, k$

$$\mathfrak{q}_i = (IA_{\mathfrak{p}_i})^c.$$

7.3 Anelli artiniani

Ricordiamo che un anello A si dice artiniano se verifica d.c.c.. Vediamo ora alcune delle principali proprietà di tali anelli.

T. 7.14. 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 $k \in \mathbb{N}$ tale che $\mathcal{N}(A)^k = 0$.

Dimostrazione T. 7.14. 1. Siano $\mathfrak{p} \subset A$ un ideale primo e $B = A/\mathfrak{p}$; allora 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 $(b) \supseteq (b^2) \supseteq \ldots$. Per ipotesi esiste k tale che $(b^k) = (b^{k+1})$. Pertanto $b^k \in (b^{k+1})$ ed esiste $c \in B$ tale che $b^k = cb^{k+1}$. Quindi $b^k(1 - cb) = 0$ e, poiché B è un dominio, $cb = 1$, come volevamo.

2. Consideriamo la famiglia Σ 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 $I_0 = \bigcap_{i=1}^{k} \mathfrak{m}_i \in \Sigma$, cf. **T.7.1**. Per ogni ideale massimale $\mathfrak{m}$ di A abbiamo $I_0 \cap \mathfrak{m} = I_0$ per la minimalità di I_0. Allora $\mathfrak{m} \supseteq \bigcap_{i=1}^{k} \mathfrak{m}_i$ e pertanto $\mathfrak{m} \supseteq \mathfrak{m}_i$ per qualche i, cf. **T.1.12**.2. Per la massimalità di $\mathfrak{m}_i$, deve essere $\mathfrak{m} = \mathfrak{m}_i$ e abbiamo concluso.

3. Per d.c.c. esiste k tale che la catena discendente $\mathcal{N}(A) \supseteq \mathcal{N}(A)^2 \ldots$ si stabilizza, i.e. $\mathcal{N}(A)^k = \mathcal{N}(A)^{k+1}$. Sia $I = \mathcal{N}(A)^k$ e supponiamo per assurdo che $I \neq 0$; allora la famiglia Σ di tutti gli ideali J tali che $JI \neq 0$, è non vuota (perché?) e possiede un elemento minimale J_0. Quindi esiste $b \in J_0 \setminus \{0\}$ tale che $bI \neq 0$ e $(b) \subseteq J_0$; dunque $J_0 = (b)$ per la minimalità di J_0. Dato che $(b)I \in \Sigma$ e $(b)I\, I = (b)I^2 = (b)I \neq 0$, la minimalità di (b) implica $(b)I = (b)$. Abbiamo dunque $b = bc$ con $c \in I$, da cui segue $b = bc = bc^2 = \ldots = bc^h = \ldots$. Dato che $c \in I$ è nilpotente, esiste un intero positivo s tale che $c^s = 0$ e possiamo concludere che $b = bc^s = 0$, trovando la contraddizione cercata. □

T. 7.15. (→ p. 225) Sia $(A, \mathfrak{m})$ un anello artiniano locale; allora ogni elemento di A è invertibile o nilpotente.

T. 7.16. Siano $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ ideali massimali di un anello A, non necessariamente distinti; allora

$$A/\prod_{i=1}^{t} \mathfrak{m}_i \quad \text{è artiniano se e solo se è noetheriano.}$$

In particolare, se $\prod_{i=1}^{t} \mathfrak{m}_i = 0$ allora A è artiniano se e solo se è noetheriano.

Dimostrazione T. 7.16. Dimostriamo l'enunciato per induzione su t. Se $t = 1$ allora $A/\mathfrak{m}_1$ è un campo, che è artiniano e noetheriano.
Sia ora $t > 1$. Consideriamo $N = \left(\prod_{i=1}^{t-1} \mathfrak{m}_i\right) / \left(\prod_{i=1}^{t} \mathfrak{m}_i\right)$ e la successione esatta

$$0 \longrightarrow N \longrightarrow A/\prod_{i=1}^{t} \mathfrak{m}_i \longrightarrow A/\prod_{i=1}^{t-1} \mathfrak{m}_i \longrightarrow 0.$$

Per **T.4.1**, N è un $(A/\mathfrak{m}_t)$-spazio vettoriale, dunque artiniano se e solo se noetheriano per **E.13.2**. Inoltre $A/\prod_{i=1}^{t-1} \mathfrak{m}_i$ è artiniano se e solo se noetheriano per ipotesi induttiva, quindi la tesi segue da **T.7.2**.2 e **T.7.3**. □

Caratterizzazione degli anelli artiniani

T. 7.17. (→ p. 225) Un anello è artiniano se e solo se è noetheriano di dimensione 0.

L'ultimo enunciato generalizza quanto visto nella discussione che seguiva la dimostrazione di **T.3.18**.

Teorema di struttura degli anelli artiniani

T. 7.18. Un anello A è artiniano se e solo se A è isomorfo ad una somma diretta finita di anelli artiniani locali.

Dimostrazione T. 7.18. Nella dimostrazione di **T.7.17** abbiamo visto che $0 = \prod_{i=1}^{s} \mathfrak{m}_i^k$ è un prodotto di potenze di ideali massimali e possiamo ovviamente supporre che tali ideali siano distinti. È facile verificare che gli ideali $\mathfrak{m}_i^k$ sono a coppie comassimali; quindi per il Teorema cinese del resto abbiamo

$$A \simeq A/0 \simeq A/\prod_{i=1}^{s} \mathfrak{m}_i^k \simeq \prod_{i=1}^{s} A/\mathfrak{m}_i^k,$$

dove gli anelli $A/\mathfrak{m}_i^k$ sono anelli artiniani locali.

Il viceversa è una diretta applicazione di **T.7.3**. □

Parte II

Esercizi

8

Esercizi su anelli e ideali

E. 8.1. (→ p. 227) Sia S un sottoinsieme di un anello A. Provare che (S) è l'intersezione di tutti gli ideali che contengono S.

E. 8.2. (→ p. 227) 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. 8.3. (→ p. 227) Sia $A = \mathbb{Z}/(n)$ con $n \neq 0, \pm 1$.

1. Per $n = 24$ determinare $\mathcal{D}(A)$, A^*, gli ideali primi e gli ideali massimali di A.
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. 8.4. (→ p. 228) Sia a un elemento nilpotente di A. Provare che $1 - a$ è un elemento invertibile in A.
Dedurre che la somma di un invertibile e di un nilpotente è invertibile.

E. 8.5. (→ p. 228) 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. 8.6. (→ p. 228) Provare che, per ogni anello A, il radicale di Jacobson e il nilradicale di $A[x]$ sono uguali.

E. 8.7. (→ p. 229) 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. 8.8. (→ p. 229) Siano A un anello e I un ideale di A. Provare che l'insieme

$$I[x] = \left\{ f(x) = \sum_i a_i x^i \in A[x] \colon \ a_i \in I \ \text{ per ogni } i \right\}$$

dei polinomi di $A[x]$ che hanno tutti i coefficienti in I è un ideale di $A[x]$.
Provare inoltre che

$$A[x]/I[x] \simeq (A/I)\,[x].$$

E. 8.9. (→ p. 229) [**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 $f, g \in A[x]$ sono primitivi se e solo se fg è primitivo.

E. 8.10. (→ p. 229) 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. 8.11. (→ p. 229) 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. 8.12. (→ p. 230) Siano I e J ideali di un anello A.
Provare che se $I \subseteq \mathcal{J}(A)$ e $(I, J) = 1$ allora $J = (1)$.

E. 8.13. (→ p. 230) Un anello locale A non contiene idempotenti diversi da 0 e 1.

E. 8.14. (→ p. 230) 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. 8.15. (→ p. 230) Provare che se ogni ideale proprio di A è primo allora A è un campo.

E. 8.16. (→ p. 230) [**Operazioni in $\mathbb{Z}$**] Siano $I = (m)$, $J = (n)$, $H = (h)$ ideali di $\mathbb{Z}$.
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. 8.17. (→ p. 231) [**Proprietà del quoziente di ideali**] Siano I, J, H, I_α, con α che varia in un insieme di indici Λ, ideali di un anello A.
Provare 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. $I : \sum_{\alpha\in\Lambda} I_\alpha = \bigcap_{\alpha\in\Lambda} I : I_\alpha$.

E. 8.18. (→ p. 231) Siano $I \subset A$ un ideale e $f \in A$.
Provare che

$$I : (f) = \frac{1}{f}(I \cap (f)).$$

E. 8.19. (→ p. 231) Siano $I \subset A$ un ideale e $f, g \in A$. Provare che

$$(I, f, g) = (1) \implies (I, f) \cap (I, g) = (I, fg).$$

E. 8.20. (→ p. 231) Siano I, J e 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. 8.21. (→ p. 231) Siano I, J, $H_1, \ldots, H_n \subseteq A$ ideali.
Provare che

1. se $I + H_i = A$ per ogni i allora $I + H_1 H_2 \cdots H_n = A$;

2. se $I + J = A$ allora $I^m + J^n = A$ per ogni n, $m \in \mathbb{N}$.

E. 8.22. (→ p. 232) 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 $I = \mathfrak{p}$ oppure $J = \mathfrak{p}$.

E. 8.23. (→ p. 232) 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. 8.24. (→ p. 232) Mostrare con un esempio che

$$\sqrt{I} + \sqrt{J} \neq \sqrt{I + J}.$$

E. 8.25. (→ p. 232) Siano $A = K[x, y]$ e $I = (x^2, xy)$.
Provare che $\sqrt{I}$ è primo e I non è primario.

E. 8.26. (→ p. 232) 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. 8.27. (→ p. 232) Sia A un anello. 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. 8.28. (→ p. 233) Sia A un anello. Dato un qualsiasi sottoinsieme E di A definiamo il suo *radicale* come l'insieme

$$\sqrt{E} = \{a \in A\colon\ a^n \in E \text{ per qualche } n \in \mathbb{N}\}.$$

Sia $\{E_\alpha\}_{\alpha\in\Lambda}$ una famiglia di sottoinsiemi di A.
Provare che $\sqrt{\bigcup_\alpha E_\alpha} = \bigcup_\alpha \sqrt{E_\alpha}$.

E. 8.29. (→ p. 233) Provare che in un anello A si ha

$$\mathcal{D}(A) = \bigcup_{0\neq a\in A} \sqrt{\operatorname{Ann} a}.$$

E. 8.30. (→ p. 233) Sia A un anello. 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. 8.31. (→ p. 233) Siano A un anello e $a \in \mathcal{J}(A)$.
Provare che se a è idempotente modulo un ideale $I \subset A$ allora $a \in I$.

E. 8.32. (→ p. 233) Sia A un dominio infinito con un numero finito di invertibili.
Dimostrare che A possiede un numero infinito di ideali massimali.

E. 8.33. (→ p. 233) Siano A e B anelli. Descrivere gli ideali, gli ideali primi e gli ideali massimali di $A \times B$.

E. 8.34. (→ p. 234) 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. 8.35. (→ p. 234) 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. 8.36. (→ p. 235) 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. 8.37. (→ p. 235) 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. 8.38. (→ p. 236) Provare che il prodotto diretto di un numero finito di anelli semilocali è semilocale e che non è vero il viceversa.

E. 8.39. (→ p. 236) 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. 8.40. (→ p. 237) [**$\mathcal{D}(A)$ è unione di primi**] 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. 8.41. (→ p. 237) Sia A un anello tale che ogni ideale primo è principale. Provare che A è PIR.

E. 8.42. (→ p. 237) Sia $f\colon A \longrightarrow B$ un omomorfismo di anelli. Verificare che

1. $\operatorname{Ker} f$ è un ideale di A;
2. f è iniettivo se e solo se $\operatorname{Ker} f = (0)$;
3. $\operatorname{Im} f$ è un sottoanello di B.

E. 8.43. (→ p. 238) Dimostrare che esiste un unico omomorfismo di anelli $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$.

E. 8.44. (→ p. 238) Siano A un anello, $I \subseteq A$ un ideale e $a \in A$ e consideriamo l'insieme

$$J = \{f \in A[x]\colon\ f(a) \in I\}.$$

1. Provare che J è un ideale.
2. Provare che J è primo se e solo se I è primo.
3. Dati $A = \mathbb{Q}[y]$, $a = y - 1$ e $I = (y - 2)$, trovare J.

E. 8.45. (→ p. 238) Sia $A \neq 0$ un anello. 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 $A \longrightarrow B$, con B anello non nullo, è iniettivo.

E. 8.46. (→ p. 238) [**Proprietà di estensione e contrazione di ideali**] Siano $f\colon A \longrightarrow B$ un omomorfismo di anelli, $I_1, I_2 \subset A$ e $J_1, J_2 \subset B$ ideali. Provare che

1. $(I_1 + I_2)^e = I_1^e + I_2^e$;
2. $(I_1 I_2)^e = I_1^e I_2^e$;
3. $(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e$;
4. $(J_1 + J_2)^c \supseteq J_1^c + J_2^c$;
5. $(J_1 J_2)^c \supseteq J_1^c J_2^c$;
6. $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$.

Mostrare con esempi che i contenimenti in 3, 4 e 5 possono essere stretti.

E. 8.47. (→ p. 239) Si consideri l'omomorfismo di inclusione $j\colon A \longrightarrow A[x]$ 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.8.8**. Provare che

1. $I[x]$ è l'ideale esteso I^e rispetto ad j;
2. I è primo se e solo se $I[x]$ è primo.
3. È vero che se I è massimale allora $I[x]$ è massimale?

E. 8.48. (→ p. 239) Siano $f\colon A \longrightarrow B$ un omomorfismo di anelli e $I \subset A$ un ideale. Provare che

1. $(f(\sqrt{I})) \subseteq \sqrt{(f(I))}$, i.e. $(\sqrt{I}\,)^e \subseteq \sqrt{I^e}$;
2. se f è surgettivo e $\operatorname{Ker} f \subseteq I$ 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. 8.49. (→ p. 240) Consideriamo l'omomorfismo di inclusione $\mathbb{Z} \longrightarrow \mathbb{Z}[i]$ e sia p un primo di $\mathbb{Z}$. Provare che

$$(p)^e = \begin{cases} (1+i)^2 & \text{se } p = 2; \\ (a+ib)(a-ib) & \text{se } p \equiv 1 \mod 4; \\ (p) & \text{se } p \equiv 3 \mod 4. \end{cases}$$

E. 8.50. (→ p. 240) Per ogni primo dispari p sia ζ_p una radice primitiva p-esima dell'unità e consideriamo l'omomorfismo di inclusione $\mathbb{Z} \longrightarrow \mathbb{Z}[\zeta_p]$.
Provare che

$$\frac{1-\zeta_p^a}{1-\zeta_p} \in \mathbb{Z}[\zeta_p]^* \quad \text{per ogni } \ a = 1, \dots, p-1.$$

Dedurre che in $\mathbb{Z}[\zeta_p]$ vale

$$(p)^e = (1-\zeta_p)^{p-1}.$$

E. 8.51. (→ p. 240) 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. 8.52. (→ p. 241) Siano A un anello 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. 8.53. (→ p. 241) 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. 8.54. (→ p. 241) Sia A un PID. Provare che se $d = \gcd(a, b)$ allora esistono $u, v \in A$ tali che $ua + vb = d$. In particolare vale che $(a, b) = (\gcd(a, b))$.
Trovare un esempio di anello A per cui la proprietà precedente non è vera.

E. 8.55. (→ p. 241) Sia A un PID e siano $I, J \subset A$ ideali di A.
Provare che $(I + J)^2 = I^2 + J^2$.

E. 8.56. (→ p. 241) Sia A un PIR. Provare che se $\mathcal{J}(A) = \mathcal{D}(A) \neq (0)$ allora A è un anello locale.

E. 8.57. (→ p. 242) Sia A un PID.

1. Provare che $a \in A$ è irriducibile se e solo se $A/(a)$ è un campo.
2. Provare che gli ideali massimali di A sono gli ideali generati da elementi irriducibili.
3. Siano $A = K[x]$ e $f \in A$ di grado positivo. Verificare che (f) è primo se e solo se f è irriducibile.

E. 8.58. (→ p. 242) Siano K un campo e $f \in K[x] \setminus \{0\}$ un polinomio monico. Diciamo che f è *libero da quadrati* se gli elementi irriducibili che compaiono nella sua fattorizzazione sono distinti.
Provare che l'anello $A = K[x]/(f)$ è ridotto se e solo se f è libero da quadrati.

E. 8.59. (→ p. 242) Siano K un campo perfetto, $f \in K[x] \setminus \{0\}$ un polinomio monico e f' la sua derivata prima.

1. Provare che f è libero da quadrati se e solo se $\gcd(f, f') = 1$.
2. Sia $K \subseteq L$ un'estensione di campi; provare che f è libero da quadrati in $K[x]$ se e solo se f è libero da quadrati in $L[x]$.

In particolare, le affermazioni precedenti valgono quando K ha caratteristica 0 oppure K è algebricamente chiuso.

E. 8.60. (→ p. 242) Siano $r \leq n$ interi positivi e K un campo perfetto. Siano inoltre $h_{i_j}(x_{i_j}) \in K[x_{i_j}] \setminus K$ con $j = 1, \ldots, r$ polinomi liberi da quadrati.
Provare che $(h_{i_1}, \ldots, h_{i_r}) \subset K[x_1, \ldots, x_n]$ è radicale.

E. 8.61. (→ p. 243) [**Interpolazione di Lagrange**] Siano $\alpha_1, \ldots, \alpha_n$ elementi distinti di un campo K e $\beta_1, \ldots, \beta_n \in K$.
Provare che esiste un polinomio $f(x) \in K[x]$ di grado n tale che $f(\alpha_i) = \beta_i$ per ogni i.

E. 8.62. (→ p. 243) [**Algoritmo di Berlekamp**] Siano p un primo di $\mathbb{Z}$, $A = (\mathbb{Z}/(p))[x]$ e $f \in A$ un polinomio monico libero da quadrati.
Siano inoltre $B = A/(f)$ e $\varphi_p \colon B \longrightarrow B$ l'omomorfismo di Frobenius dato da $\varphi_p(\overline{g}) = \overline{g}^p$. Provare che

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 $\overline{g} \in \mathrm{Ker}(\varphi_p - \mathrm{id}_B)$ 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 $\overline{g}$.

E. 8.63. (→ p. 243) Sia A un PID. Provare che gli ideali primari di A sono generati da potenze di elementi primi.

E. 8.64. (→ p. 244) 1. Sia A un UFD; provare che se $p \in A$ è primo allora (p^i) è primario per ogni $i \in \mathbb{N}_+$.

2. Trovare un ideale primario che non sia potenza di un ideale primo.

3. Siano $A = K[x, y, z]$ e $I = (xy - z^2)$, $B = A/I$ e $\mathfrak{p} = (\bar{x}, \bar{z}) \subset B$. Provare che $\mathfrak{p}$ è primo e $\mathfrak{p}^2$ non è primario.

E. 8.65. (→ p. 244) Sia A un anello. Provare che

$$A[x] \text{ è un PID se e solo se } A \text{ è un campo.}$$

E. 8.66. (→ p. 244) Provare che nell'anello $\mathbb{Z}[\sqrt{-5}]$ l'elemento 3 è irriducibile, ma l'ideale (3) non è irriducibile.

E. 8.67. (→ p. 244) Sia A un dominio di integrità. Provare che se ogni catena ascendente di ideali principali di A è stazionaria allora A verifica (UFD1).

E. 8.68. (→ p. 244) Provare che un dominio che è quoziente di un UFD non è necessariamente UFD.

E. 8.69. (→ p. 245) 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. 8.70. (→ p. 245) 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 $\mathfrak{m} \in \mathrm{Max}\, A$ 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 sono ideali di A e $\mathfrak{m} \in \mathrm{Max}\, A$ allora $J\mathfrak{m} = H\mathfrak{m}$ implica $J = H$.

E. 8.71. (→ p. 245) Siano A un anello e I, J ideali di A. Provare che

1. se I è primario e $J \not\subseteq \sqrt{I}$ allora $\sqrt{I \colon J^m} = \sqrt{I}$ per ogni $m \geqslant 1$;

2. se $I = \sqrt{I}$ e $h \notin I$ allora $I\colon h$ è radicale.

E. 8.72. (→ p. 246) Sia $p = \sum_{i\in\mathbb{N}} a_i x^i \in A[[x]]$. Provare 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 e solo se $a_0 \in \mathcal{J}(A)$;
4. la contrazione di un ideale massimale $\mathfrak{m}$ di $A[[x]]$, rispetto all'inclusione $A \longrightarrow A[[x]]$, è un ideale massimale di A.

   Mostrare inoltre che $\mathfrak{m}$ è generato da $\mathfrak{m}^c$ e x.

E. 8.73. (→ p. 247) Siano A un anello e $I \subset A$ un ideale. Provare che se un elemento $g \in A$ verifica $I\colon (g^m) = I\colon (g^{m+1})$ per qualche $m \in \mathbb{N}$ allora

1. $I\colon (g^{m+s}) = I\colon (g^m)$ per ogni $s \in \mathbb{N}_+$;
2. $I = (I\colon (g^m)) \cap (I, g^m)$.

E. 8.74. (→ p. 247) [**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

$$\mathcal{V}(I) = \{\mathfrak{p} \in \operatorname{Spec} A\colon\ \mathfrak{p} \supseteq I\}$$

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. 8.75. (→ p. 247) Siano A un anello ridotto e $a \in A$ un divisore di zero. Provare che a appartiene ad uno dei primi minimali di A.

E. 8.76. (→ p. 247) Si consideri l'anello $A = \mathbb{Z}[x, y]$ e l'ideale

$$I = (9x^2 - y,\ 7y^2 + 2x + y,\ 63).$$

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. Provare che se B è un dominio ed esiste un omomorfismo di anelli $f\colon B \longrightarrow A/I$ iniettivo allora B è un campo.

E. 8.77. (→ p. 248) 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.

9

Esercizi su anello di polinomi, basi di Gröbner, risultante e varietà

E. 9.1. (→ p. 249) Provare che una relazione d'ordine $>$ è un buon ordinamento su $\mathbb{N}^n$ se e solo se ogni catena discendente in $\mathbb{N}^n$ è stazionaria.

E. 9.2. (→ p. 249) Provare che le relazioni d'ordine lex, deglex, degrevlex sono ordinamenti monomiali.

E. 9.3. (→ p. 250) Sia $>$ un ordinamento totale su $\mathbb{N}^n$ tale che se $\mathbf{a} > \mathbf{b}$ allora $\mathbf{a}+\mathbf{c} > \mathbf{b}+\mathbf{c}$ per ogni $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n$.
Dimostrare che $>$ è un ordinamento monomiale se e solo se $\mathbf{a} \geq 0$ per ogni $\mathbf{a} \in \mathbb{N}^n$.

E. 9.4. (→ p. 250) Siano $K \subset K'$ 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 $K'[x_1, \ldots, x_n]$.
Provare che 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 un qualunque ordinamento monomiale, l'escalier di I è uguale all'escalier di I^e.

E. 9.5. (→ p. 251) 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. 9.6. (→ p. 251) 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 con $z > y > x$ e $>_2$ l'ordinamento lex con $x > y > z$.
Mostrare che G è una base di Gröbner di I rispetto a $>_1$ ma non rispetto a $>_2$.

E. 9.7. (→ p. 251) [**Test di monomialità**] Provare che I è monomiale se e solo se, rispetto ad un qualsiasi ordinamento monomiale, la sua base di Gröbner ridotta è costituita da monomi.

E. 9.8. (→ p. 251) Sia $I = (x^2 - xy,\ xz - y^2,\ yz^2 - z^4) \subseteq \mathbb{R}[x, y, z]$.
Calcolare una base di Gröbner minimale di I rispetto all'ordinamento lessicografico con $x > y > z$ e ridurla.

E. 9.9. (→ p. 252) Siano $I = (yz - y,\ xy + 2z^2,\ y - z) \subset \mathbb{Q}[x, y, z]$ e $f = x^3 z - y^2$.

Determinare se $f \in I$.

E. 9.10. (→ p. 253) Siano $I = (x^2 + xy + y^2, xy^2 + 1) \subset A = (\mathbb{Z}/(2))[x, y]$, $f_1 = x^3 + y^5 + xy^2$ e $f_2 = y(x^2 + x + y)$.
Determinare se $\overline{f_1} = \overline{f_2}$ in A/I.

E. 9.11. (→ p. 253) 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. 9.12. (→ p. 253) 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 $f = xy^2z + y^3 \in I$ ed esprimere f come combinazione lineare degli elementi di G e dei generatori dati.

E. 9.13. (→ p. 254) 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. 9.14. (→ p. 254) Siano $I, J \subset K[x, y]$, con $I = (x(x + y)^2,\ y)$ e $J = (x^2,\ x + y)$.
Calcolare $I : J$.

E. 9.15. (→ p. 255) Sia K un campo di caratteristica diversa da 2; siano inoltre $I = (x^2 + y^2,\ x^3y^3 + y^4) \subset K[x, y]$ e $f = x^2 + 5x$.
Determinare se $f \in \sqrt{I}$.

E. 9.16. (→ p. 255) 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. 9.17. (→ p. 256) 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. 9.18. (→ p. 256) 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 $(x^2y^3, y^3z) \subsetneq I \subsetneq (x^2, z)$.

E. 9.19. (→ p. 257) Siano $f,\ g_1,\ g_2 \in K[x] \setminus \{0\}$ e $a_m = \mathrm{lc}(f)$. Provare che

1. $\mathrm{Ris}(f, g_1g_2) = \mathrm{Ris}(f, g_1)\,\mathrm{Ris}(f, g_2)$;

2. se $g_1f + g_2 \neq 0$ e $N = \deg(g_1f + g_2)$ allora

$$\mathrm{Ris}(f, g_1f + g_2) = a_m^{N-\deg(g_2)}\,\mathrm{Ris}(f, g_2).$$

E. 9.20. (→ p. 257) [**Costruzione di polinomi con radici assegnate**] Siano $f, g \in K[x]$ di gradi $m, n > 0$, $\alpha_1, \ldots, \alpha_m$ e $\beta_1, \ldots, \beta_n$ le radici in $\overline{K}$ di f e g rispettivamente. Provare che

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. 9.21. (→ p. 258) Siano $f, g \in \mathbb{Q}[x]$ di grado positivo. Provare che se $f(0) = 1$ allora $\mathrm{Ris}(f, x^kg) = \mathrm{Ris}(f, g)$ per ogni intero pari k.

E. 9.22. (→ p. 258) 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. 9.23. (→ p. 258) 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. 9.24. (→ p. 258) Siano $A = K[x, y, z]$ e $I = (xz - y,\ yz - x) \subset A$. Decomporre $\mathbb{V}(I)$ come unione di varietà irriducibili.

E. 9.25. (→ p. 259) Sia $I = (x^2 - yzt,\ t - yt,\ zt - y)$ un ideale di $\mathbb{C}[x, y, z, t]$.

1. Trovare le componenti irriducibili di $\mathbb{V}(I)$.

2. Determinare se $f = xt + y \in I$.

E. 9.26. (→ p. 259) 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. $\mathbb{V}(I) \cap \mathbb{V}(z-1)$.

E. 9.27. (→ p. 260) Sia $I = (xy^3,\, xy+y^2,\, y^2-z^2) \subset \mathbb{C}[x,y,z]$.

1. Calcolare $I_1 = I \cap \mathbb{C}[y,z]$ e $I_2 = I \cap \mathbb{C}[z]$.

2. Sia $\pi_1 \colon \mathbb{C}^3 \longrightarrow \mathbb{C}^2$ la proiezione sulle ultime due componenti data da $\pi_1(a_1,a_2,a_3) = (a_2,a_3)$. Determinare se $\pi_1(\mathbb{V}(I)) = \mathbb{V}(I_1)$.

E. 9.28. (→ p. 260) 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 $\mathbb{V}(J) \subset \mathbb{C}^2$ si estende ad un elemento di $\mathbb{V}(I) \subset \mathbb{C}^4$.

E. 9.29. (→ p. 260) Siano

$$I = (x^2-y^2-yz,\, xy-y^2z) \text{ e } J = (x^2-y^2-yz,\, xy-y^2z,\, y^3z^2-y^3-y^2z)$$

ideali in $\mathbb{C}[x,y,z]$.
Determinare se $I = J$ e se $\mathbb{I}(\mathbb{V}(I)) = I$.

E. 9.30. (→ p. 260) Sia $I = (x+y+z,\, xy+yz+zx,\, xyz-1) \subseteq \mathbb{C}[x,y,z]$.
Provare che

1. $\mathbb{V}(I)$ 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. 9.31. (→ p. 261) 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. $\mathbb{V}(I) \subset \overline{\mathbb{Z}/(2)}^{\,3}$ è finita?

2. Decomporre $\mathbb{V}(I)$ come unione di varietà irriducibili.

E. 9.32. (→ p. 261) 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 I^c rispetto all'omomorfismo di immersione $\mathbb{Q}[y,z] \longrightarrow \mathbb{Q}[x,y,z]$.

3. Determinare se $\mathbb{V}(I) \subset \mathbb{Q}^3$ è finita.

4. Determinare $\operatorname{Min} I$.

E. 9.33. (→ p. 261) 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 $\mathbb{V}(I)$ è finita.

E. 9.34. (→ p. 262) Siano $I = (y^2 - xz,\, x^2 - y^2,\, x^2 - yz) \subset \mathbb{Q}[x,y,z]$ e $A = \mathbb{Q}[x,y,z]/I$.

1. Trovare le componenti irriducibili di $\mathbb{V}(I)$ e stabilire se $\mathbb{V}(I)$ è finita.

2. Determinare se $f = y(x^2 + x + y) \in \sqrt{I}$.

E. 9.35. (→ p. 262) Sia $I = (x^2 z,\, y^2 z^2 - yz,\, y^2 - z^2) \subset \mathbb{C}[x,y,z]$.
Stabilire se $\mathbb{V}(I)$ è finita e se $I \subseteq (x^2, y+1, z-1)$.

E. 9.36. (→ p. 262) Sia $I = (xyz - 2,\, y^2 z - x,\, 3x^2 z^2 - y) \subset K[x,y,z]$.

1. Provare che se $K = \mathbb{C}$ allora $\mathbb{V}(I)$ è finita.

2. Trovare, se esistono, primi $p \in \mathbb{Z}$ tali che, se $K = \overline{\mathbb{Z}/(p)}$ allora $\mathbb{V}(I)$ è vuota oppure infinita.

E. 9.37. (→ p. 263) 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 $f = x^2 + y^2 z + 2y + 1$ rispetto alla base trovata sopra.

3. Stabilire se $\dim_{\mathbb{Q}} A = |\,\mathbb{V}_{\mathbb{C}}(I)|$.

4. Decomporre $\sqrt{I}$ come intersezione di ideali massimali in $\mathbb{Q}[x,y,z]$, se possibile.

E. 9.38. (→ p. 263) Sia Σ il sistema

$$\begin{cases} f_1 = x^2 - 3xy + y^2 = 0 \\ f_2 = x^3 - 8x + 3y = 0 \\ f_3 = x^2 y - 3x + y = 0. \end{cases}$$

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 $V = \mathbb{V}_{\mathbb{R}}(f_1, f_2, f_3)$ come unione di varietà irriducibili.

E. 9.39. (→ p. 264) 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 $\Sigma = \{q(y) \in \mathbb{Q}[y] \colon \mathbb{V}_{\mathbb{Q}}((q, I)) \neq \emptyset\}$ e dire se è un ideale.

E. 9.40. (→ p. 264) Siano $V = \{\alpha_1, \ldots, \alpha_m\} \subset \mathbb{C}^n$ con $\alpha_i \neq \alpha_j$ per $i \neq j$ e $A = \mathbb{C}[x_1, \ldots, x_n]/\mathbb{I}(V)$ l'anello delle coordinate di V.

1. Provare che esistono m elementi non nulli $a_1, \ldots, a_m \in A$, tali che

$$a_i^2 = a_i \text{ per ogni } i, \quad a_i a_j = 0 \text{ per } i \neq j \quad \text{e} \quad \sum_{i=1}^{m} a_i = 1.$$

2. Determinare quanti e quali sono gli elementi idempotenti di A.

10

Esercizi sui moduli

10.1 Moduli, sottomoduli e omomorfismi

E. 10.1. (→ p. 264) Dati un ideale $I \subset A$ e un A-modulo M, provare che, ponendo $\overline{a}\,\overline{m} = \overline{am}$ per ogni $\overline{a} \in A/I$ e $\overline{m} \in M/IM$, si definisce su M/IM una struttura di A/I-modulo.

E. 10.2. (→ p. 265) Verificare che l'operazione di restrizione di scalari induce effettivamente una struttura di modulo.

E. 10.3. (→ p. 265) 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. 10.4. (→ p. 265) Siano M un A-modulo e N, P sottomoduli di M. Sia inoltre $N\colon P = \{a \in A\colon aP \subseteq N\}$.
Verificare che $N\colon P$ e, in particolare, $\operatorname{Ann} P = 0\colon P$ sono ideali di A.

E. 10.5. (→ p. 265) Provare che

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 di un modulo non è necessariamente una sua 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.

E. 10.6. (→ p. 265) Siano $I, J_1, J_2 \subset A$ ideali e sia $M = A/J_1 \oplus A/J_2$.
Provare che

$$M/IM \simeq A/(J_1 + I) \oplus A/(J_2 + I).$$

E. 10.7. (→ p. 265) Siano $J \subset A$ un ideale, $M = A/J$ e $a \in A$.
Provare che

$$aM \simeq A/(J\colon a).$$

E. 10.8. (→ p. 265) Sia A un anello e sia $f\colon A^m \longrightarrow A^n$ un omomorfismo surgettivo di A-moduli.
Dimostrare che se $n > m$ allora $A = 0$.

E. 10.9. (→ p. 265) Sia M un A-modulo libero di rango r.
Dimostrare che ogni insieme di generatori ha cardinalità maggiore o uguale a r.

E. 10.10. (→ p. 266) Siano A un anello, $I \subset A$ un ideale nilpotente e $\varphi\colon M \longrightarrow N$ un omomorfismo di A-moduli.
Provare che se l'omomorfismo indotto $\overline{\varphi}\colon M/IM \longrightarrow N/IN$ è surgettivo allora anche φ è surgettivo.

E. 10.11. (→ p. 266) Siano $m, n \in \mathbb{N}$, $A \neq 0$ un anello e $f\colon A^m \longrightarrow A^n$ 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. 10.12. (→ p. 266) 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. 10.13. (→ p. 266) Siano A un anello e M, N due A-moduli. Provare che

1. $M \neq 0$ è semplice se e solo se $M \simeq A/\mathfrak{m}$ con $\mathfrak{m}$ ideale massimale di A;
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. 10.14. (→ p. 267) 1. Provare che un A-modulo $M \neq 0$ è semplice se e solo se per ogni $0 \neq m \in M$ si ha $\langle m \rangle = M$.

2. Determinare tutti gli $\mathbb{Z}$-moduli semplici.

E. 10.15. (→ p. 267) 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 tali che $\operatorname{Ann} N = (p)$, $\operatorname{Ann} P = (q)$ e $\operatorname{Ann} M = (pq)$ allora $M = N \oplus P$.

E. 10.16. (→ p. 267) Siano M, N, P degli A-moduli; dimostrare che

$$\mathrm{Hom}_A(M,P) \oplus \mathrm{Hom}_A(N,P) \simeq \mathrm{Hom}_A(M \oplus N, P),$$

$$\mathrm{Hom}_A(P,M) \oplus \mathrm{Hom}_A(P,N) \simeq \mathrm{Hom}_A(P, M \oplus N).$$

E. 10.17. (→ p. 268) Sia $n \neq 1$ un intero positivo. 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. 10.18. (→ p. 268) Siano A un anello, $I, J \subsetneq A$ ideali e $0 \neq M$ un A-modulo. Provare che

1. $\mathrm{Hom}_A(A/I, M) \simeq 0 :_M I = \{m \in M \colon Im = 0\}$;
2. $\mathrm{Hom}_A(A/I, M)$ ha una struttura di A/I-modulo;
3. se $M = A/J$ allora $\mathrm{Hom}_A(A/I, M) \simeq (J \colon I)/J$.

E. 10.19. (→ p. 269) 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. 10.20. (→ p. 269) Siano $(A, \mathfrak{m})$ un anello locale e $M \neq 0$ un A-modulo finitamente generato.
Provare che $\mathrm{Hom}_A(M, A/\mathfrak{m}) \neq 0$.

E. 10.21. (→ p. 269) 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. 10.22. (→ p. 269) Siano M un A-modulo finitamente generato e $I \subset A$ un ideale.
Dimostrare che

$$\sqrt{\mathrm{Ann}(M/IM)} = \sqrt{\mathrm{Ann}\, M + I}.$$

E. 10.23. (→ p. 270) 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. 10.24. (→ p. 270) Fornire un controesempio all'enunciato della II forma del Lemma di Nakayama nel caso in cui il modulo M non sia finitamente generato.

10.2 Successioni esatte e moduli proiettivi

E. 10.25. (→ p. 270) [**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 e $\alpha_2,\ \alpha_4$ sono isomorfismi allora α_3 è un isomorfismo.

E. 10.26. (→ p. 271) Siano M, N, P tre $\mathbb{Z}$-moduli e p, q primi distinti di $\mathbb{Z}$. Provare che se $pN = qP = 0$ allora ogni successione esatta

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

spezza.

E. 10.27. (→ p. 271) Siano $M = \mathbb{Z}/(2)$, $N = \mathbb{Z}/(4)$ e $P = \mathbb{Z}/(8)$. Trovare, se possibile, successioni esatte corte di $\mathbb{Z}$-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. 10.28. (→ p. 272) Sia $0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$ una successione esatta corta di A-moduli.
Dimostrare che se N e P sono finitamente generati, allora M è finitamente generato.

E. 10.29. (→ p. 272) Siano $f\colon M \longrightarrow N$ e $g\colon N \longrightarrow M$ omomorfismi di A-moduli tali che $g \circ f = \mathrm{id}_M$.
Provare che $N \simeq \operatorname{Ker} g \oplus \operatorname{Im} f$.

E. 10.30. (→ p. 272) Siano

$$0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{f} P \longrightarrow 0$$

e

$$0 \longrightarrow P \xrightarrow{g} T \xrightarrow{\psi} W \longrightarrow 0$$

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. 10.31. (→ p. 272) Sia $n \neq 0, 1$. Provare che $\mathbb{Z}/(n)$ è uno $\mathbb{Z}/(n)$-modulo proiettivo ma non è proiettivo come $\mathbb{Z}$-modulo.

E. 10.32. (→ p. 272) Sia $A = \mathbb{Z}/(12)$. Verificare che $\mathbb{Z}/(4)$ è un A-modulo proiettivo non libero.

E. 10.33. (→ p. 273) 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-moduli e come B-moduli rispettivamente.

E. 10.34. (→ p. 273) Siano I e 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. 10.35. (→ p. 273) 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. 10.36. (→ p. 274) Siano $N \subset M$, $N' \subset M'$ degli A-moduli tali che $M/N \simeq M'/N' \simeq A$. 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. 10.37. (→ p. 274) 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. 10.38. (→ p. 274) Provare che un dominio A è un campo se e solo se ogni A-modulo è proiettivo.

E. 10.39. (→ p. 274) Siano $A = \mathbb{Z}[\sqrt{-5}]$ e $I = (3, 1-\sqrt{-5})$, $J = (3, 1+\sqrt{-5})$ 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. 10.40. (→ p. 275) 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. 10.41. (→ p. 275) [**Caratterizzazione dei moduli iniettivi**] Sia E un A-modulo. Provare 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. 10.42. (→ p. 277) Siano A un anello e F un A-modulo libero.

1. Provare che se A è un campo allora F è iniettivo.
2. L'affermazione precedente è ancora valida per un anello qualsiasi?

E. 10.43. (→ p. 277) [**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 $\tilde{f}\colon A \longrightarrow E$.

10.3 Moduli su PID e forma normale di Smith

E. 10.44. (→ p. 278) Sia A PID; provare che ogni sottomodulo di un modulo proiettivo è proiettivo.

E. 10.45. (→ p. 278) Siano A un dominio e M un A-modulo. Verificare che il sottoinsieme $T(M)$ degli elementi di torsione di M è un sottomodulo.

E. 10.46. (→ p. 278) Siano A un anello, $a \in A$, M un A-modulo e $M_{[a]}$ la a-componente di M.
Provare che $M_{[a]}$ è un sottomodulo di M.

E. 10.47. (→ p. 278) Siano A PID, M un A-modulo finitamente generato e $0 \neq a, b \in A$ tali che $\gcd(a, b) = 1$. Provare che

1. $M_{[ab]} \simeq M_{[a]} \oplus M_{[b]}$;
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
$$\pi_a(m) = cm \quad \text{e} \quad \pi_b(m) = dm;$$
3. $M_{[ab]}$ è ciclico se e solo se $M_{[a]}$ e $M_{[b]}$ sono ciclici.

E. 10.48. (→ p. 279) Sia $M \neq 0$ un A-modulo ciclico, con A PID e $M \not\simeq A$. Provare che esistono primi $p_1, \dots, p_h \in A$ e sottomoduli ciclici p_i-primari $M_i \subseteq M$ tali che $M \simeq \bigoplus_{i=1}^{h} M_i$.

E. 10.49. (→ p. 279) Sia A un dominio e M un A-modulo. Provare che

1. ogni A-modulo libero è libero da torsione;
2. se A è PID e 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. 10.50. (→ p. 280) 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. 10.51. (→ p. 280) Sia $\varphi\colon \mathbb{Q}[x]^4 \longrightarrow \mathbb{Q}[x]^4$ 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. 10.52. (→ p. 280) Siano $a \in \mathbb{Z}$ e $\varphi\colon \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ 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. 10.53. (→ p. 281) Sia $\varphi\colon \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ l'omomorfismo definito dalla matrice

$$\begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \quad \text{con } a, b, c \in \mathbb{Z}.$$

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. 10.54. (→ p. 281) Sia $\varphi\colon \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ l'omomorfismo definito dalla matrice

$$\begin{pmatrix} a & 6 & 6 \\ -3 & 6 & 0 \\ a & 3 & 3 \end{pmatrix} \quad \text{con } a \in \mathbb{Z}.$$

Trovare, se esistono, i valori di a per cui

1. $\operatorname{Coker} \varphi$ è finito;
2. $\operatorname{Coker} \varphi$ non è ciclico.

E. 10.55. (→ p. 281) Sia $M = \mathbb{Z}^3/N$, dove 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. 10.56. (→ p. 282) Sia $M = \mathbb{Z}^3/N$, dove 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. 10.57. (→ p. 282) Siano A, B, $C \in M_3(\mathbb{Z})$ e sia

$$D = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix}.$$

Sapendo che $\det A = 28$ e $\det B = 7$, trovare le forme di Smith di D esibendo un esempio di A, B e C per ciascuno dei casi possibili.

E. 10.58. (→ p. 282) 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. 10.59. (→ p. 282) Siano $R \in M_n(\mathbb{Z})$ e M lo $\mathbb{Z}$-modulo $\mathbb{Z}^n/R\mathbb{Z}^n$.
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 R è n e che esiste $p \in \mathbb{Z}$ primo tale che $\det R = \pm p^k$ con $k \leq n$.

E. 10.60. (→ p. 282) 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. 10.61. (→ p. 283) Siano $G_1 = \langle a, b, c, d \rangle_{\mathbb{Z}}$, dove 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 $G_2(\alpha) = \operatorname{Coker} \varphi_\alpha$, dove $\varphi_\alpha \colon \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ 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. 10.62. (→ p. 284) Siano $\alpha, \beta \in \mathbb{N}$ e $R = R_{\alpha,\beta} \in M_6(\mathbb{R})$ con polinomio caratteristico

$$p_R(x) = (x-1)^\alpha (x-2)^\beta (x^2+1).$$

Determinare, se esistono, valori di α e β per cui le possibili forme di Smith della matrice caratteristica $R - xI$ siano esattamente 4.

E. 10.63. (→ p. 284) Sia M lo $\mathbb{Z}$-modulo generato da elementi m_1, m_2, m_3, m_4 che soddisfano le relazioni $3m_1 = 0$, $am_1 + 3m_2 = 0$, $bm_2 + 3m_3 = 0$ 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 e b.

E. 10.64. (→ p. 285) Siano a un intero, N il sottomodulo di $\mathbb{Z}^3$ generato da $m_1 = (2, 2, a)$, $m_2 = (2, a, 0)$, $m_3 = (0, 4, 2)$ e $M = \mathbb{Z}^3/N$.

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. 10.65. (→ p. 285) Sia $M = \langle m_1, m_2, m_3 \rangle_{\mathbb{Z}}$, dove $2m_1 = m_2$, $m_1 = 3m_2$, $m_1 + m_2 = am_3$ al variare di $a \in \mathbb{Z}$.

1. Costruire, se possibile, un omomorfismo non banale $\varphi \colon \mathbb{Z}/(20) \longrightarrow M$ quando $a = 3$.

2. Descrivere $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(20), M)$ al variare di a.

E. 10.66. (→ p. 286) 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 $m_1 = (2,4,6)$, $m_2 = (0,a,2a)$ e $m_3 = (b,4,6)$ al variare di a, $b \in \mathbb{Z}$.
Trovare, se esistono, i valori di a, b per cui M è semplice.

E. 10.67. (→ p. 286) 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 conucleo di un omomorfismo di $K[x]$-moduli e decomporlo come somma diretta di moduli ciclici.

E. 10.68. (→ p. 287) 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. 10.69. (→ p. 287) 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. 10.70. (→ p. 288) 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. $A = K[x,y]/(x^2 - y^2, x^4 - x^3y + y)$.

11

Esercizi sul prodotto tensoriale

E. 11.1. (→ p. 289) Siano A un anello e M, N, P degli A-moduli. Per ogni $b, b' \in \mathrm{Bil}(M, N; P)$ e $\alpha \in A$ definiamo

$$(b + b')(m, n) = b(m, n) + b'(m, n) \quad \text{e} \quad (\alpha b)(m, n) = \alpha b(m, n),$$

per ogni $m \in M$, $n \in N$.
Mostrare che $\mathrm{Bil}(M, N; P)$ dotato di tali operazioni è un A-modulo.

E. 11.2. (→ p. 289) Calcolare $\mathbb{Z}/(a) \otimes \mathbb{Z}/(b)$ quando $\gcd(a, b) = 1$.

E. 11.3. (→ p. 289) Siano I, J ideali di un anello A. Dimostrare che

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

E. 11.4. (→ p. 290) Siano A un anello e M, N due A-moduli liberi. Dimostrare che $M \otimes N$ è libero.

E. 11.5. (→ p. 291) 1. Provare che $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}$.

2. Consideriamo $\mathbb{C}$ con la struttura di $\mathbb{R}$-modulo data dalla restrizione di scalari tramite l'omomorfismo di inclusione di anelli $\mathbb{R} \longrightarrow \mathbb{C}$.
Provare che in $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ non tutti i tensori sono tensori elementari.

3. È possibile utilizzare la stessa dimostrazione di 1 per provare che $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C}$?

E. 11.6. (→ p. 292) Siano A un anello e $f\colon M \longrightarrow M'$, $g\colon N \longrightarrow N'$ omomorfismi di A-moduli. Mostrare che

$$f \otimes g\colon M \otimes N \longrightarrow M' \otimes N' \quad \text{definito da} \quad (f \otimes g)(m \otimes n) = f(m) \otimes g(n)$$

è un omomorfismo di A-moduli.

E. 11.7. (→ p. 292) Siano A un anello 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.
Provare che $(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$.

E. 11.8. (→ p. 292) Provare che $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/(n) = 0$ per ogni $n \in \mathbb{N}_+$.

E. 11.9. (→ p. 292) 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 non è vero in generale;
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 non è vero in generale.

E. 11.10. (→ p. 293) Siano $(A, \mathfrak{m}, K)$ un anello locale e M, N due A-moduli finitamente generati. Provare che

$$\mu(M \otimes_A N) = \mu(M)\mu(N).$$

E. 11.11. (→ p. 294) Siano $(A, \mathfrak{m}, K)$ un anello locale e M, N due A-moduli finitamente generati. Provare che

$$M \otimes_A N = 0 \quad \text{implica} \quad M = 0 \ \text{ oppure } \ N = 0.$$

E. 11.12. (→ p. 294) Siano $p \in \mathbb{Z}$ primo e

$$M = \left\{ \tfrac{a}{p^n} : \ a \in \mathbb{Z}, \ n \in \mathbb{N} \right\}.$$

Verificare che M è uno $\mathbb{Z}$-modulo e provare che $M \otimes_{\mathbb{Z}} (M/\mathbb{Z}) = 0$.

E. 11.13. (→ p. 294) 1. Calcolare la dimensione del $\mathbb{Q}$-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. 11.14. (→ p. 294) Sia $(A, \mathfrak{m}, K)$ un anello locale.
Provare che ogni A-modulo proiettivo finitamente generato è libero.

E. 11.15. (→ p. 295) 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. 11.16. (→ p. 295) 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. 11.17. (→ p. 296) 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 per ogni A-modulo $N \neq 0$, si ha $M \otimes N \neq 0$.

E. 11.18. (→ p. 296) Siano A un anello e $a \in A \setminus \mathcal{D}(A)$.
Provare che se N è un A-modulo piatto allora $an \neq 0$ per ogni $n \in N \setminus \{0\}$.

E. 11.19. (→ p. 296) 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 libero da torsione, ma non è piatto.

E. 11.20. (→ p. 296) Siano M e N due A-moduli liberi di rango finito. Provare che

$$\operatorname{End}_A(M) \otimes \operatorname{End}_A(N) \simeq \operatorname{End}_A(M \otimes N).$$

E. 11.21. (→ p. 297) Siano $M = \mathbb{Z}/(15)$ e $\varphi\colon \mathbb{Z}^2 \longrightarrow \mathbb{Z}^3$ l'omomorfismo dato da $\varphi(x, y) = (4x + 8y,\, 4x - 4y,\, 16x + 20y)$.
Determinare $M \otimes_{\mathbb{Z}} T(\operatorname{Coker} \varphi)$.

E. 11.22. (→ p. 297) 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

$$2m_1 - m_2 = 0\,, \quad m_1 + m_2 + m_3 = 0 \quad \text{e} \quad m_1 + am_2 = 0.$$

Determinare, se esistono, i valori $n \in \mathbb{N}$ per cui $M_a \otimes_{\mathbb{Z}} \mathbb{Z}/(n) \neq 0$ al variare di a.

12

Esercizi sulla localizzazione

E. 12.1. (→ p. 297) Sia $a \notin \mathcal{N}(A)$; dimostrare che esiste un ideale primo $\mathfrak{p}$ di A che non contiene a.

E. 12.2. (→ p. 297) 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. 12.3. (→ p. 297) Siano A un anello finito e $S \subset A$ un insieme moltiplicativo tale che l'omomorfismo canonico è iniettivo.
Provare che $S^{-1}A \simeq A$.

E. 12.4. (→ p. 298) Descrivere l'anello $S^{-1}A$ quando

1. $A = \mathbb{Z}$ e $S = A \setminus (p)$ con p primo;
2. $A = \mathbb{Z}$ e $S = A \setminus \bigcup_{i=1}^{n} (p_i)$ 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. 12.5. (→ p. 298) Sia A un anello finito e $S \subset A$ un insieme moltiplicativo.

1. Provare che σ_S è surgettivo.
2. Siano $A = \mathbb{Z}/(24)$ e $S = \{\overline{2}^n : n \in \mathbb{N}\}$. Trovare $\operatorname{Ker} \sigma_S$ e $S^{-1}A$.

E. 12.6. (→ p. 298) Siano A un anello e $I \subset A$ un ideale.

1. Sia
$$S = 1 + I = \{1 + i : i \in I\}.$$
Mostrare che S è moltiplicativo e che $S^{-1}I \subseteq \mathcal{J}(S^{-1}A)$.
2. Siano $A = \mathbb{Z}/(60)$ e $S = 1 + \overline{4}A$. Trovare tutti gli ideali di $S^{-1}A$.
$S^{-1}A$ è un anello locale?
3. Sia ancora $A = \mathbb{Z}/(60)$; esiste $\overline{m} \neq \overline{4}$ tale che $T^{-1}A = (1 + \overline{m}A)^{-1}A$ non è locale?

E. 12.7. (→ p. 299) Siano A e B anelli commutativi con identità con $B \neq 0$ 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. Definiamo su $C \times T$ la relazione $(x,s) \sim (y,t)$ se e solo se $xt = ys$.

   Provare che $\sim$ non è una relazione di equivalenza.

E. 12.8. (→ p. 299) Siano A un anello e $f \in A$. Provare che

$$A_f \simeq A[x]/(1 - fx).$$

E. 12.9. (→ p. 300) 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 $\mathbb{Z} \subsetneq A \subsetneq \mathbb{Q}$ e descriverli come localizzazione di $\mathbb{Z}$.

E. 12.10. (→ p. 300) Nelle ipotesi di **E.9.9**, 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. 12.11. (→ p. 300) Nelle ipotesi di **E.9.13**, 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. 12.12. (→ p. 300) Nelle ipotesi di **E.9.15**, verificare se l'immagine di f in $K[x,y]_{(x,y)}$ è un elemento di $\sqrt{I_{(x,y)}}$.

E. 12.13. (→ p. 300) Nelle ipotesi di **E.9.18**, sia $\mathfrak{p} = (\overline{x}, \overline{z})A$. Determinare $A_{\mathfrak{p}}$.

E. 12.14. (→ p. 301) Nelle ipotesi di **E.9.24**, sia $S = A \setminus (x,y)$.
Descrivere $S^{-1}(A/I)$.

E. 12.15. (→ p. 301) Nelle ipotesi di **E.9.34**, sia $S = A \setminus (\overline{x}, \overline{y})A$.
Calcolare $S^{-1}A$.

E. 12.16. (→ p. 301) Sia p un primo di $\mathbb{Z}$; provare che $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}_p/\mathbb{Z} = 0$.

E. 12.17. (→ p. 301) Sia p un primo di $\mathbb{Z}$. Provare che

$$\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)} \simeq \begin{cases} (\mathbb{Z}_2)_{(p)\mathbb{Z}_2} & \text{se } p \neq 2 \\ \mathbb{Q} & \text{se } p = 2. \end{cases}$$

E. 12.18. (→ p. 302) [**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 insieme moltiplicativo tale che $\sigma_S \colon A \longrightarrow S^{-1}A$ 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. In questo caso $Q(A)$ si chiama *campo dei quozienti* o *delle frazioni di* A.

E. 12.19. (→ p. 302) 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. 12.20. (→ p. 302) 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 $Q(A) = A_a$.

E. 12.21. (→ p. 303) Sia $A = B/\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n$, con $\mathfrak{p}_i \subset B$ ideali primi tali che $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ se $i \neq j$. Sia inoltre $Q(A)$ 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. 12.22. (→ p. 303) 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. 12.23. (→ p. 303) Sia K un campo, $A = K[x]_{(x)}$ e $Q(A)$ il campo delle frazioni di A. Provare che

1. $Q(A)/(x)Q(A)$ è un A-modulo finitamente generato;

2. $Q(A)$ non è un A-modulo finitamente generato.

E. 12.24. (→ p. 304) Siano A un anello, $S \subset A$ un insieme moltiplicativo 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 allora 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. 12.25. (→ p. 304) 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. 12.26. (→ p. 304) Sia M un A-modulo e definiamo *supporto* di M l'insieme

$$\operatorname{Supp} M = \{\mathfrak{p} \in \operatorname{Spec} A \colon M_{\mathfrak{p}} \neq 0\}.$$

Provare che

1. se M è finitamente generato allora $\mathfrak{p} \in \operatorname{Supp} M$ se e solo se $\mathfrak{p} \supseteq \operatorname{Ann} M$;
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. 12.27. (→ p. 304) 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. 12.28. (→ p. 305) Siano $A = \mathbb{Q}[x, y, z]$ e 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. 12.29. (→ p. 305) Siano A un anello e $0 \neq I \subset A$ un ideale finitamente generato tale che, per ogni ideale massimale $\mathfrak{m} \subset A$, si ha $I_{\mathfrak{m}} = 0$ oppure $I_{\mathfrak{m}} = A_{\mathfrak{m}}$.
Provare che I è principale ed è generato da un elemento idempotente.

E. 12.30. (→ p. 305) Siano

$$p(x) = (x-1)^2(x^2+2) \in \mathbb{Q}[x]\,, \quad S = \{q(x) \in \mathbb{Q}[x] \colon (q(x), p(x)) = 1\}$$

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. 12.31. (→ p. 306) 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. 12.32. (→ p. 306) Siano A un anello 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. 12.33. (→ p. 306) Sia S un insieme moltiplicativo di un anello A. Dimostrare che $\overline{S}$ è un insieme moltiplicativo saturato.

E. 12.34. (→ p. 306) Siano A e B anelli, $T \subset B$ un sottoinsieme e $f\colon A \longrightarrow B$ un omomorfismo. Provare che

1. se T è moltiplicativo allora $f^{-1}(T)$ è moltiplicativo e se f è surgettivo vale anche il viceversa;
2. se T è saturato allora $f^{-1}(T)$ è saturato e se f è surgettivo vale anche il viceversa.

E. 12.35. (→ p. 306) Dati sottoinsiemi $I, S \subset A$, definiamo la *saturazione* di I rispetto a S come l'insieme

$$I^S = \bigcup_{s \in S} I\colon (s) = \{a \in A\colon \text{ esiste } s \in S \text{ tale che } as \in I\}.$$

Diciamo che I è *saturato rispetto ad* S se $I = I^S$.
Siano S un insieme moltiplicativo e I un ideale.

1. Provare che I^S è un ideale.
2. Siano $J \subset A$ un ideale 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. 12.36. (→ p. 307) 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

$$N^S = \bigcup_{s \in S} N :_M s = \{m \in M\colon \text{ esiste } s \in S \text{ tale che } sm \in N\}.$$

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 $S^{-1}M$. Provare che

   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. $\sigma_S^{-1}(S^{-1}N) = N^S$ e, 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. $N^S + P^S \subseteq (N + P)^S$.

E. 12.37. (→ p. 307) Siano

$$A = (\mathbb{Z}/(200))_{\overline{18}}, \quad B = (\mathbb{Z}/(200))_{\overline{6}},$$

$$C = (\mathbb{Z}/25) \otimes_{\mathbb{Z}} (\mathbb{Z}/40) \quad \text{e} \quad D = \mathbb{Z}_{(3)}[x]/(6x - 1).$$

Stabilire quali di questi anelli sono isomorfi tra loro.

E. 12.38. (→ p. 308) 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

$$T^{-1}A \simeq T_1^{-1}(S^{-1}A);$$

2. si ha

$$\sigma_S(T)^{-1}(S^{-1}A) \simeq \sigma_T(S)^{-1}(T^{-1}A).$$

E. 12.39. (→ p. 309) Siano A un anello e $S \subset A$ un insieme moltiplicativo. Provare che S è massimale rispetto all'inclusione tra gli insiemi moltiplicativi di A se e solo se $A \setminus S$ è un primo minimale.

E. 12.40. (→ p. 309) Siano $S = \{24^n\}_{n \in \mathbb{N}}$ e $T = \{4^n 6^m\}_{n,m \in \mathbb{N}}$. Provare che $S^{-1}\mathbb{Z} = T^{-1}\mathbb{Z}$.

E. 12.41. (→ p. 309) 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 $\mathcal{V}(I) = \{\mathfrak{p} \in \operatorname{Spec} A \colon \mathfrak{p} \supseteq I\}$.

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. 12.42. (→ p. 310) Sia K un campo di caratteristica diversa da 2 e siano $A = K[x,y]/(x^2 - y^2)$, $\mathfrak{p} = (x+y)A$ e $\mathfrak{q} = (x,y)A$.

1. Quali sono gli ideali primi di $A_\mathfrak{q}$?

2. Descrivere $(A_\mathfrak{q})_{\mathfrak{p}A_\mathfrak{q}}$.

13

Esercizi su moduli noetheriani e artiniani

E. 13.1. (→ p. 310) Sia Σ la famiglia degli ideali di un anello A. Provare che

1. se $A = \mathbb{Z}$ allora A soddisfa a.c.c. ma non d.c.c.;

2. se $A = \mathbb{R}[x]/(x^2 + 2)$ allora A soddisfa sia a.c.c. sia d.c.c..

E. 13.2. (→ p. 310) Siano K un campo e V un K-spazio vettoriale; allora sono fatti sono equivalenti:

1. $\dim_K V < \infty$;

2. V è un K-modulo noetheriano;

3. V è un K-modulo artiniano.

E. 13.3. (→ p. 311) Fornire una dimostrazione alternativa di **T.7.2**.2 utilizzando la caratterizzazione dei moduli noetheriani data in **T.7.2**.1.

E. 13.4. (→ p. 311) 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. 13.5. (→ p. 311) 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. 13.6. (→ p. 311) Siano N_1, N_2 sottomoduli di un A-modulo M tali che M/N_1 e M/N_2 sono noetheriani.
Provare che $M/(N_1 \cap N_2)$ è noetheriano.

E. 13.7. (→ p. 312) Sia $A = K[x]/(fg^2)$ con $(f, g) = 1$.
Provare che un A-modulo M è noetheriano se e solo se $M/\overline{f}M$ e $M/\overline{g}^2 M$ sono noetheriani.

E. 13.8. (→ p. 312) 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 $\tilde{J} = (g_1, \ldots, g_k)$ tale che $I\tilde{J} = (d)$;
2. A è noetheriano.

E. 13.9. (→ p. 312) Siano $f\colon A \longrightarrow C$ e $g\colon B \longrightarrow C$ omomorfismi surgettivi di anelli. Definiamo $A \times_C B = \{(a, b) \in A \times B\colon f(a) = g(b)\}$.

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. 13.10. (→ p. 312) 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 e k intero, 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. 13.11. (→ p. 313) Sia A un anello noetheriano. Provare che se ogni ideale massimale di A è principale allora $\dim A \leq 1$.

E. 13.12. (→ p. 313) Siano M un A-modulo noetheriano e $I = \operatorname{Ann}_A M$. Provare che A/I è noetheriano.

E. 13.13. (→ p. 313) Siano A un anello noetheriano e I, J ideali di A tali che ogni ideale primo di A contiene I oppure J ma non entrambi. Provare che

1. $A = I + J$;
2. esiste $n \in \mathbb{N}$ tale che $(IJ)^n = 0$.

E. 13.14. (→ p. 314) 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. 13.15. (→ p. 314) Sia A un anello. 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. 13.16. (→ p. 314) Siano A un anello noetheriano e M un A-modulo tale che $0 \neq \operatorname{Ann} M$ è un ideale 0-dimensionale.
Provare che M contiene un sottomodulo semplice non banale.

E. 13.17. (→ p. 315) 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. 13.18. (→ p. 315) Sia A un anello noetheriano. Provare che ogni ideale $J \subseteq A$ che contiene un ideale radicale 0-dimensionale I è radicale 0-dimensionale oppure $J = (1)$.

E. 13.19. (→ p. 315) Nell'anello $K[x, y, z, t]$ trovare i primi minimali dell'ideale

$$I = (x^2zt,\ yt^3,\ xyzt,\ x^5z^6).$$

E. 13.20. (→ p. 315) Siano $A = \mathbb{Q}[x, y, z, t]$ e

$$I = (x^2z - x^2t^3,\ x^2y^4t + x^2y^3 - x^3z,\ xt^2) \subset A.$$

1. Dire se I è un ideale monomiale.
2. Trovare una decomposizione di I come intersezione di ideali primari, individuando i primi associati e quelli minimali.
3. Determinare i nilpotenti e i divisori di zero di A/I.

E. 13.21. (→ p. 316) Sia $A = \mathbb{Q}[x]/(x^5 - 3x^2) \oplus \mathbb{Z}/(12)$. Trovare

1. gli elementi nilpotenti e i divisori di zero di A;
2. gli ideali primi $\mathfrak{p}$ di A per cui $A_\mathfrak{p}$ è un campo, se esistono.

E. 13.22. (→ p. 316) 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. 13.23. (→ p. 317) Siano $K = \overline{K}$ e $I \subsetneq A = K[x_1, \dots, x_n]$ un ideale. Provare che i seguenti fatti sono equivalenti:

1. $\dim A/I = 0$;
2. $I \cap K[x_i] \neq 0$ per ogni $i = 1, \dots, n$.

E. 13.24. (→ p. 317) [**Calcolo del radicale di un ideale 0-dimensionale**] Siano $K = \overline{K}$ e $I \subsetneq K[x_1, \dots, x_n]$ un ideale 0-dimensionale. Per ogni $i = 1, \dots, n$ sia $0 \neq h_i \in I \cap K[x_i]$ e $\sqrt{h_i}$ la sua parte libera da quadrati.
Provare che

$$\sqrt{I} = (I, \sqrt{h_1}, \dots, \sqrt{h_n}).$$

E. 13.25. (→ p. 317) Sia M un A-modulo. Definiamo *l'insieme dei primi associati ad* M come

$$\operatorname{Ass} M = \{\mathfrak{p} \in \operatorname{Spec} A \colon \text{ esiste } m \in M \setminus \{0\} \text{ tale che } \mathfrak{p} = \operatorname{Ann} m\}.$$

Provare che

1. gli elementi massimali dell'insieme $\Sigma = \{\operatorname{Ann} m \colon 0 \neq m \in M\}$ sono ideali primi, e quindi appartengono ad $\operatorname{Ass} M$;
2. se A noetheriano e $M \neq 0$ allora $\operatorname{Ass} M \neq \emptyset$.

E. 13.26. (→ p. 318) Siano M un A-modulo e $\mathfrak{p} \in \operatorname{Spec} A$; provare che $\mathfrak{p} \in \operatorname{Ass} M$ se e solo se esiste un omomorfismo iniettivo $A/\mathfrak{p} \longrightarrow M$, i.e. se e solo se M contiene un sottomodulo isomorfo a $A/\mathfrak{p}$.

E. 13.27. (→ p. 318) 1. Sia $0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$ una successione esatta di A-moduli; provare che

$$\operatorname{Ass} N \subseteq \operatorname{Ass} M \subseteq \operatorname{Ass} N \cup \operatorname{Ass} P.$$

2. Siano A e M un anello e un A-modulo non nulli, entrambi noetheriani; provare che esistono una catena di sottomoduli $M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_t = M$ e ideali primi $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ tali che $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$ per ogni i.

3. [**Terzo teorema di finitezza**] Siano A un anello noetheriano e M un A-modulo finitamente generato; provare che $\operatorname{Ass} M$ è finito.

E. 13.28. (→ p. 318) Siano M un A-modulo e $I \subseteq \operatorname{Ann} M$.
Provare che M è artiniano come A-modulo se e solo se è artiniano come A/I-modulo.

E. 13.29. (→ p. 318) Siano M un A-modulo artiniano e $\varphi \colon M \longrightarrow M$ un omomorfismo iniettivo. Dimostrare che φ è un isomorfismo.

E. 13.30. (→ p. 319) Sia A un anello artiniano. Provare che

1. $A = A^* \sqcup \mathcal{D}(A)$;
2. se A è locale e $S \subseteq A$ è un insieme moltiplicativo allora l'omomorfismo canonico $\sigma_S \colon A \longrightarrow S^{-1}A$ è surgettivo.

E. 13.31. (→ p. 319) 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 M è noetheriano se e solo se M è artiniano.

14

Vero o Falso?

Dire quali delle seguenti affermazioni sono vere e quali false. Giustificare le risposte con una dimostrazione o un controesempio.

VoF. 14.1. (→ p. 319) Siano 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 $I : a = I$.

VoF. 14.2. (→ p. 319) Siano A un dominio e Q il suo campo dei quozienti; allora

$$Q[x] \otimes_{A[x]} Q[x] \simeq Q[x].$$

VoF. 14.3. (→ p. 319) 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.

VoF. 14.4. (→ p. 320) Siano $I, J, H \subset A$ ideali; allora

1. $\sqrt{I + JH} = \sqrt{I + J} \cap \sqrt{I + H}$;
2. $\sqrt{I + \sqrt{J}} = \sqrt{I + J}$;
3. $\sqrt{I} + \sqrt{J} = \sqrt{I + J}$.

VoF. 14.5. (→ p. 320) Dato un anello A, la somma di ideali gode della proprietà distributiva rispetto all'intersezione.

VoF. 14.6. (→ p. 320) Siano A un anello e $I \subset A$ un ideale tale che $\mathcal{N}(A/I) = (\overline{0})$; allora I è primo.

VoF. 14.7. (→ p. 320) Il $\mathbb{Q}[x]$-modulo $\mathbb{Q}[x]/(x^2 - 1) \otimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/(x^2 + 1)$ è nullo.

VoF. 14.8. (→ p. 320) Sia $A[x]$ noetheriano; allora A è noetheriano.

VoF. 14.9. (→ p. 320) Siano $>$ un ordinamento monomiale su $K[X]$ e $I \neq 0$ un ideale; se $\mathrm{Lt}_>(I)$ è primo allora I è primo.

VoF. 14.10. (→ p. 320) Siano $I, J \subset A$ ideali; allora $\sqrt{I : J} \subseteq \sqrt{I} : \sqrt{J}$.

VoF. 14.11. (→ p. 320) Siano $I, J \subset A$ ideali massimali tali che $I \cap J = (0)$; allora A è artiniano.

VoF. 14.12. (→ p. 320) Siano A un dominio e M, N due A-moduli; allora $T(M \otimes N) \simeq T(M) \otimes T(N)$.

VoF. 14.13. (→ p. 320) Siano $f, g \in \mathbb{C}[x,y] \setminus \mathbb{C}$ e $I = (f,g)$; allora $\mathbb{V}_{\mathbb{C}}(I)$ è infinita se e solo se $\gcd(f,g) \neq 1$.

VoF. 14.14. (→ p. 321) Siano A un anello e $I \subset A$ un ideale; allora A^n/IA^n è isomorfo a $\prod_{i=1}^{n} A/IA$.

VoF. 14.15. (→ p. 321) Sia $p(x) \in K[x]$ un polinomio irriducibile; allora l'ideale $(p(x), p(y))$ è primo in $K[x,y]$.

VoF. 14.16. (→ p. 321) Siano M un A-modulo proiettivo e $N \subseteq M$ un sottomodulo; allora N è proiettivo.

VoF. 14.17. (→ p. 321) Sia $I \subset A$ un ideale proprio; I è massimale se e solo se per ogni ideale J di A si ha $J \subseteq I$ oppure $I + J = A$.

VoF. 14.18. (→ p. 321) Sia $\mathfrak{p} \subset A$ un ideale primo tale che $A/\mathfrak{p}$ è finito; allora $\mathfrak{p}$ è massimale.

VoF. 14.19. (→ p. 321) 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. $\sqrt{I \colon J} \subseteq \sqrt{I} \colon J$;
3. $\sqrt{I \colon J} = \sqrt{I} \colon J$;
4. $I \colon J = I \colon \sqrt{J}$.

VoF. 14.20. (→ p. 321) Siano $I = (x^2+1, y^2-1)$ e $J = (x^2+xy, y^2+xy+1)$ ideali di $\mathbb{Q}[x,y]$; allora $\mathbb{Q}[x,y]/I \simeq \mathbb{Q}[x,y]/J$.

VoF. 14.21. (→ p. 322) Siano $I \subset K[x,y]$ un ideale tale che $I \cap K[x] = 0$ e $\varphi \colon K[x,y] \longrightarrow K(x)[y]$ l'omomorfismo di inclusione; I è primo se e solo se I^e è primo e $I^{ec} = I$.

VoF. 14.22. (→ p. 322) Siano $f, g \in K[x,y]$; allora $\sqrt{(f,g)} = \sqrt{(f^2, g^3)}$.

VoF. 14.23. (→ p. 322) 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 $\pi(a) \in (A/\mathfrak{m})^*$.

VoF. 14.24. (→ p. 322) Sia $(A, \mathfrak{m})$ un anello noetheriano locale; se le immagini in $A/\mathfrak{m}^2$ di certi elementi $a_1, \ldots, a_n \in A$ generano $\mathfrak{m}/\mathfrak{m}^2$ come $A/\mathfrak{m}$-spazio vettoriale allora $\mathfrak{m} = (a_1, \ldots, a_n)$.

VoF. 14.25. (→ p. 322) Un sottoanello di un anello noetheriano è noetheriano.

VoF. 14.26. (→ p. 322) Siano $A = \mathbb{Z}/(18)$ e M_1, M_2 gli A-moduli $(\overline{2})$ e $(\overline{3})$ rispettivamente; allora

1. M_1 è proiettivo;
2. M_2 è proiettivo;
3. M_1 è libero;

4. M_2 è libero.

VoF. 14.27. (→ p. 322) La successione di $K[x]$-moduli

$$0 \longrightarrow (x) \longrightarrow K[x] \longrightarrow K \longrightarrow 0$$

spezza.

VoF. 14.28. (→ p. 322) Sia M lo $\mathbb{Z}$-modulo $\mathbb{Z}/(12) \otimes_{\mathbb{Z}} \mathbb{Z}/(30)$; allora $\operatorname{Supp} M = \{(2), (3)\}$.

VoF. 14.29. (→ p. 322) Sia $A = K[x,y]/(xy)$; un elemento $a \notin \mathcal{D}(A)$ se e solo se $a \in K$.

VoF. 14.30. (→ p. 323) Siano $K = \overline{K}$ e $f, g \in K[X]$ con f irriducibile; se $\mathbb{V}(f) \subseteq \mathbb{V}(g)$ allora f divide g.

VoF. 14.31. (→ p. 323) Siano P, Q due A-moduli proiettivi e $\varphi \in \operatorname{Hom}_A(P,Q)$ un omomorfismo surgettivo di A-moduli; allora $\operatorname{Ker}\varphi$ è proiettivo.

VoF. 14.32. (→ p. 323) Sia $f \in \mathbb{Q}[x]$ un polinomio tale che $\gcd(f, f') = 1$; allora $\mathcal{N}(\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}[x]/(f)) \neq 0$.

VoF. 14.33. (→ p. 323) Siano $S \subset A$ un insieme moltiplicativo e M un A-modulo noetheriano; allora $S^{-1}M$ è un A-modulo noetheriano.

VoF. 14.34. (→ p. 323) Siano $\mathfrak{m}, \mathfrak{n} \subset A$ ideali massimali distinti e M un A-modulo; allora $M/\mathfrak{m}M \otimes_A M/\mathfrak{n}M = 0$.

VoF. 14.35. (→ p. 323) Siano $>$ un ordinamento monomiale su $K[X]$ e I un ideale; se $\operatorname{Lt}_>(I)$ è primario allora I è primario.

VoF. 14.36. (→ p. 323) 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 $\dim_{\mathbb{Q}} \operatorname{Coker}\varphi = 6$.

VoF. 14.37. (→ p. 323) Sia $A \neq 0$ un anello; ogni A-modulo M è libero se e solo se A è un campo.

VoF. 14.38. (→ p. 323) Siano A un dominio e $M \neq 0$ un A-modulo; se per ogni primo $\mathfrak{p} \subset A$ il modulo $M_{\mathfrak{p}}$ è libero da torsione allora M è libero da torsione.

VoF. 14.39. (→ p. 323) Sia $f\colon A \longrightarrow B$ un omomorfismo di anelli; se M è un A-modulo libero di rango k allora $M \otimes_A B$ è un B-modulo libero di rango k.

VoF. 14.40. (→ p. 324) Siano A un anello, $f \in A \setminus \mathcal{N}(A)$ e $I \subset A$ un ideale; allora $\sqrt{I} = \sqrt{IA_f \cap A} \cap \sqrt{(I, f)}$.

VoF. 14.41. (→ p. 324) Ogni dominio artiniano è un campo.

VoF. 14.42. (→ p. 324) Il radicale di Jacobson di un PID è sempre nullo.

VoF. 14.43. (→ p. 324) Gli $\mathbb{Z}$-moduli $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{R}$ e $\mathbb{R}$ sono isomorfi.

VoF. 14.44. (→ p. 324) Siano N e N' sottomoduli di un A-modulo M; se $N'_{\mathfrak{m}} \subseteq N_{\mathfrak{m}}$ per ogni ideale massimale $\mathfrak{m}$ di A allora $N' \subseteq N$.

VoF. 14.45. (→ p. 324) 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.

VoF. 14.46. (→ p. 324) Siano $A = \mathbb{C}[t]$ e $M = A[x]/(x^2 - t)$; allora M è un A-modulo piatto.

VoF. 14.47. (→ p. 325) Siano A un PID e M un A-modulo libero da torsione; allora M è libero.

VoF. 14.48. (→ p. 325) Siano $A = \mathbb{Z}$, $S = \{3^n 5^m : m, n \in \mathbb{N}\}$ e $T = \{15^n : n \in \mathbb{N}\}$; allora $S^{-1}\mathbb{Z} = T^{-1}\mathbb{Z}$.

VoF. 14.49. (→ p. 325) Siano M, N due A-moduli finitamente generati tali che $M \otimes_A N = 0$; allora $\operatorname{Ann} M + \operatorname{Ann} N = A$.

VoF. 14.50. (→ p. 325) Siano $(A, \mathfrak{m}, K)$ un anello locale e $M \neq 0$ un A-modulo finitamente generato; allora $\mathcal{V}(\operatorname{Ann}(M/\mathfrak{m}M)) = \{\mathfrak{m}\}$.

VoF. 14.51. (→ p. 325) Sia M un A-modulo piatto; allora $I \otimes_A M \simeq IM$ per ogni ideale $I \subset A$.

VoF. 14.52. (→ p. 325) Sia A un anello noetheriano; allora ogni endomorfismo surgettivo di A è un isomorfismo.

VoF. 14.53. (→ p. 325) Siano A un anello e $S \subset A$ un insieme moltiplicativo tale che $A \simeq S^{-1}A$; allora $S \subset A^*$.

VoF. 14.54. (→ p. 325) Sia A un anello tale che ogni sottomodulo di un A-modulo libero è libero; allora A è PID.

VoF. 14.55. (→ p. 326) Sia A un anello locale; allora esistono un anello B e un ideale primo $\mathfrak{p}$ di B tali che $A \simeq B_{\mathfrak{p}}$.

VoF. 14.56. (→ p. 326) Il polinomio $p(x) = \overline{30}x^5 + \overline{60}x^3 + \overline{90}x + \overline{7}$ è invertibile in $\mathbb{Z}/(540)[x]$.

VoF. 14.57. (→ p. 326) In $\mathbb{Z}_{(2)}[x]$ ogni ideale massimale ha almeno di due generatori.

VoF. 14.58. (→ p. 326) Sia $M = (\mathbb{Z}/(15) \oplus \mathbb{Z}/(18))_{(3)}$; allora M è ciclico.

VoF. 14.59. (→ p. 326) Siano $a \in \mathbb{Z}$ e M uno $\mathbb{Z}$-modulo generato da elementi m_1, m_2, m_3 che soddisfano le relazioni

$$2m_1 - m_2 = 0, \quad m_1 + m_2 + m_3 = 0, \quad m_1 + am_2 = 0;$$

allora per ogni a positivo esiste un intero n per cui $M \otimes_{\mathbb{Z}} \mathbb{Z}/(n) \neq 0$.

VoF. 14.60. (→ p. 326) 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.

VoF. 14.61. (→ p. 326) Sia $f(x,y) \in K[x,y]$ un polinomio di grado totale n. Siano inoltre $\mathcal{C} = \mathbb{V}(f)$ la curva piana di K^2 definita da f e ℓ una retta non contenuta in $\mathcal{C}$; allora $|\mathcal{C} \cap \ell| \leq n$.

VoF. 14.62. (→ p. 326) Siano A un dominio e M un A-modulo piatto; allora M è libero da torsione.

VoF. 14.63. (→ p. 327) Siano A un PID, $Q(A)$ il suo campo delle frazioni e $M \simeq A^n \oplus \bigoplus_{i=1}^{k} A/(a_i)$ con $a_i \neq 0$ per ogni i; allora $\dim_{Q(A)} Q(A) \otimes_A M = n$.

VoF. 14.64. (→ p. 327) Siano A un anello e M un A-modulo tali che $\mathcal{J}(A)$ è finitamente generato e $\mathcal{J}(A)M = M$; allora $M = 0$.

VoF. 14.65. (→ p. 327) Sia $I \subset \mathbb{Z}[x]$; se $\sqrt{I} = (f)$ con f irriducibile modulo p per ogni p primo in $\mathbb{Z}$ allora I è primario.

VoF. 14.66. (→ p. 327) Un addendo diretto di un modulo finitamente generato è finitamente generato.

VoF. 14.67. (→ p. 327) Sia $I = (y^2 - z^2,\, x^3y^3 - yz) \subseteq \mathbb{Q}[x,y,z]$; allora $f = x^3y^2 + x^3yz + y + z \in \sqrt{I}$.

VoF. 14.68. (→ p. 327) Sia I un ideale di un anello A tale che A/I è un A-modulo piatto; allora $I = I^2$.

VoF. 14.69. (→ p. 327) Siano A un dominio e $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} L \longrightarrow 0$ una successione esatta di A-moduli; allora

1. si ha $\operatorname{Ann} N \subseteq \operatorname{Ann} M$, $\operatorname{Ann} N \subseteq \operatorname{Ann} L$ e $\operatorname{Ann} M \cdot \operatorname{Ann} L \subseteq \operatorname{Ann} N$;
2. la successione $T(M) \xrightarrow{f_{|T(M)}} T(N) \xrightarrow{g_{|T(N)}} T(L)$ è ben definita;
3. la successione $T(M) \xrightarrow{f_{|T(M)}} T(N) \xrightarrow{g_{|T(N)}} T(L) \longrightarrow 0$ è esatta;
4. la successione $0 \longrightarrow T(M) \xrightarrow{f_{|T(M)}} T(N) \xrightarrow{g_{|T(N)}} T(L)$ è esatta.

VoF. 14.70. (→ p. 328) Sia $I = \{p(x) \in \mathbb{Z}[x] \colon p(5) \text{ è pari }\}$; allora $\mathbb{Z}[x]/I$ è un campo.

VoF. 14.71. (→ p. 328) Esiste un unico omomorfismo di anelli $\varphi \colon \mathbb{C} \longrightarrow \mathbb{R}$.

VoF. 14.72. (→ p. 328) Siano A un anello, $\mathfrak{p} \subset A$ un ideale primo e M un A-modulo finitamente generato; se l'$A/\mathfrak{p}$-modulo $M/\mathfrak{p}M$ è nullo allora $M_{\mathfrak{p}} = 0$.

VoF. 14.73. (→ p. 328) Un ideale irriducibile e radicale I in un anello A è primo.

VoF. 14.74. (→ p. 328) Sia $I_1 \supset I_2 \supset I_3 \supset \dots$ una catena di ideali primi in un anello A; allora $I = \bigcap_j I_j$ è un ideale primo.

VoF. 14.75. (→ p. 329) L'anello $K[[x_1, \dots, x_n]]$ è locale.

VoF. 14.76. (→ p. 329) Siano A un anello noetheriano e $\operatorname{Min}(A) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_d\}$ gli ideali primi minimali di A; allora per ogni $i = 1, \dots, d$ si ha

$$\dim A = \dim A_{\mathfrak{p}_i} + \max_i \{\dim A/\mathfrak{p}_i\}.$$

VoF. 14.77. (→ p. 329) Sia A è un dominio tale che $IJ = I \cap J$ per ogni coppia di ideali I, J di A; allora A è un campo.

VoF. 14.78. (→ p. 329) Sia A un PID; allora un A-modulo finitamente generato è piatto se e solo se è libero.

VoF. 14.79. (→ p. 329) Siano $A = K[x,y]/(xy)$, $\mathfrak{p} = (x)$ e $\mathfrak{q} = (x,y)$; allora esiste un omomorfismo iniettivo di $A_{\mathfrak{q}}$ in $A_{\mathfrak{p}}$.

VoF. 14.80. (→ p. 329) Ogni localizzazione di un modulo proiettivo è ancora proiettiva.

VoF. 14.81. (→ p. 330) Siano $f, g \in \mathbb{Q}[x,y]$ polinomi irriducibili di grado totale $n \geq 1$; allora $\dim_{\mathbb{Q}} \left(\mathbb{Q}[x,y]/(f) \otimes_{\mathbb{Q}[x,y]} \mathbb{Q}[x,y]/(g)\right) = n$.

VoF. 14.82. (→ p. 330) Sia $f\colon K[x] \longrightarrow K[x,y]/(xy-1)$ l'omomorfismo dato dalla composizione dell'inclusione $K[x] \longrightarrow K[x,y]$ con la proiezione su $K[x,y]/(xy-1)$; allora esiste un ideale primo $\mathfrak{p} \subset K[x,y]/(xy-1)$ la cui contrazione tramite f è uguale a (x).

VoF. 14.83. (→ p. 330) Siano $I, J \subset A$ ideali; allora $I \subset J$ se e solo se $I_{\mathfrak{m}} \subset J_{\mathfrak{m}}$ per ogni $\mathfrak{m} \in \operatorname{Max} A$.

VoF. 14.84. (→ p. 330) Siano A un anello locale e M un A-modulo finitamente generato; allora M è proiettivo se e solo se è libero.

VoF. 14.85. (→ p. 330) Sia $n \in \mathbb{Z} \setminus \{0\}$; allora $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}/(n)$.

VoF. 14.86. (→ p. 330) Siano $A = \mathbb{Q}[x]$, $\varphi : A^3 \longrightarrow A^3$ l'omomorfismo dato da

$$\varphi(f,g,h) = ((x-1)f, (x^3-1)g, (x^2-1)h)$$

e $M = \operatorname{Coker} \varphi$; allora $M \simeq \mathbb{Q}^6$ come A-modulo.

VoF. 14.87. (→ p. 330) Siano S un sottoinsieme di K^n e $\mathbb{I}(S) \subset K[x_1, \dots, x_n]$ il suo ideale di annullamento; allora $\mathbb{V}(\mathbb{I}(S)) = S$.

VoF. 14.88. (→ p. 330) Sia A un anello con $\dim A = n$; allora per ogni sistema moltiplicativo $S \subseteq A$ si ha $\dim S^{-1}A \leq n$ ed esiste almeno un sistema moltiplicativo $T \subseteq A$ tale che $\dim T^{-1}A = n$.

VoF. 14.89. (→ p. 331) Sia $\varphi\colon \mathbb{Z}[x] \longrightarrow K$ un omomorfismo surgettivo di anelli; allora K è un campo finito.

VoF. 14.90. (→ p. 331) Siano A un anello e P un A-modulo proiettivo finitamente generato; allora $\operatorname{Hom}_A(P, A)$ è proiettivo.

VoF. 14.91. (→ p. 331) Sia $S = \mathbb{Z} \setminus \{0\}$; allora

$$S^{-1}\left(\prod_{n\in\mathbb{N}_+} \mathbb{Z}/(n)\right) \simeq \prod_{n\in\mathbb{N}_+} S^{-1}(\mathbb{Z}/(n)).$$

VoF. 14.92. (→ p. 331) Il prodotto diretto e il prodotto tensoriale commutano.

15

Esercizi di riepilogo

E. 15.1. (→ p. 332) Siano $A = \mathbb{C}[x_1, \ldots, x_n]$, con $n \geq 2$, dotato di un ordinamento monomiale $>$ e $m_1, m_2 \in A$ monomi tali che

$$m_1^k < m_2 \quad \text{per ogni } k \in \mathbb{N}.$$

Provare che esistono indici $i \neq j$ tali che $x_i^k < x_j$ per ogni $k \in \mathbb{N}$.

E. 15.2. (→ p. 332) Siano $A = K[x, y, z]$ e $B = K[t]$ anelli di polinomi.

1. Provare che $x \mapsto t$, $y \mapsto t^2$, $z \mapsto t^3$ induce un omomorfismo surgettivo $\varphi\colon A \longrightarrow B$.
2. Determinare $\operatorname{Ker} \varphi$.

E. 15.3. (→ p. 333) Siano M, N e L degli A-moduli. Provare che

1. $\operatorname{Hom}(A^n, M) \otimes N \simeq \operatorname{Hom}(A^n, M \otimes N)$ per ogni $n \in \mathbb{N}$;
2. se N è piatto e L è finitamente generato allora esiste un omomorfismo iniettivo
$$\psi : \operatorname{Hom}(L, M) \otimes N \longrightarrow \operatorname{Hom}(L, M \otimes N).$$

E. 15.4. (→ p. 334) Sia A un anello tale che ogni ideale primo è finitamente generato.
Provare che ogni ideale di A è finitamente generato.

E. 15.5. (→ p. 334) Siano $A = \mathbb{Q}[x, y, z]$ e $I = (x^2 - x^2 z,\, xz + xyz) \subset A$.

1. Dimostrare che $\dim A/I \geq 2$.
2. Dire se l'escalier di I rispetto all'ordinamento lex con $x > y > z$ è uguale all'escalier di I rispetto all'ordinamento degrevlex con $x > y > z$.
3. Calcolare $I \cap \mathbb{Q}[y, z]$ e $I \cap \mathbb{Q}[x, y]$.
4. Trovare le componenti irriducibili di $\mathbb{V}(I)$.

5. È vero che $(A/I)_{\mathfrak{p}} \neq 0$ per ogni $\mathfrak{p} \in \operatorname{Min} I$? È vero che $(A/I)_{\mathfrak{p}} \neq 0$ se e solo se $\mathfrak{p} \in \operatorname{Ass} I$?

6. Determinare le componenti primarie di I associate ai primi minimali.

E. 15.6. (→ p. 335) Siano I_1 e I_2 ideali di un anello noetheriano A.
Provare che esistono un intero t e un ideale J tali che

$$I_1^t \subseteq J \quad \text{e} \quad I_1 I_2 = J \cap I_2.$$

E. 15.7. (→ p. 335) Sia $0 \longrightarrow M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3 \longrightarrow 0$ una successione esatta di A-moduli, con M_3 piatto.
Provare che per ogni A-modulo N la successione

$$0 \longrightarrow N \otimes M_1 \longrightarrow N \otimes M_2 \longrightarrow N \otimes M_3 \longrightarrow 0$$

è ancora esatta.

E. 15.8. (→ p. 336) Siano n un intero positivo e $\mathfrak{p}$ un ideale primo di un anello A. Definiamo $\mathfrak{p}^{(n)} = \mathfrak{p}^n A_{\mathfrak{p}} \cap A$.

1. Dimostrare che se $\mathfrak{p}^n$ è primario allora $\mathfrak{p}^{(n)} = \mathfrak{p}^n$.

2. L'affermazione precedente rimane vera anche se $\mathfrak{p}^n$ non è primario?

E. 15.9. (→ p. 336) Siano $A = \mathbb{C}[x]$ e $M = \langle m_1, \ldots, m_4 \rangle_A$ un A-modulo tale che

$$\begin{aligned}
(x^2-1)m_1 + (3x+3)m_2 + (3x+3)m_3 + (3x+3)m_4 &= 0 \\
(x^2+x)m_2 + (x+1)m_3 + (x+1)m_4 &= 0 \\
(x^2-1)m_1 + (x+1)m_2 + (x+1)m_3 + (x+1)m_4 &= 0 \\
(x^2-1)m_1 + (2x+2)m_2 + (2x+2)m_3 + (2x+2)m_4 &= 0.
\end{aligned}$$

1. Determinare la parte libera di M, $T(M)$ e $\operatorname{Ann}_A(M)$.

2. Calcolare $M \otimes_A A/(x-1)$ e $M \otimes_A A/(x-i)$.

3. Trovare, se possibile, un A-modulo non nullo N tale che $\operatorname{Hom}_A(M, N) \simeq N$.

E. 15.10. (→ p. 337) Siano A un PIR, $\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{Spec} A$ e $\mathfrak{q}$ un ideale primario. Provare che

1. se $\mathfrak{q} \subseteq \mathfrak{p}_1$ e $\mathfrak{p}_2 \subsetneq \mathfrak{p}_1$ allora $\mathfrak{p}_2 \subseteq \mathfrak{q}$;

2. se $\mathfrak{p}_2 = \sqrt{\mathfrak{q}} \subsetneq \mathfrak{p}_1$ allora $\mathfrak{p}_2 = \mathfrak{q}$;

3. se $\mathfrak{p}_2 \subsetneq \mathfrak{p}_1$ allora $\mathfrak{p}_2$ è l'intersezione di tutti gli ideali primari contenuti in $\mathfrak{p}_1$;

4. se $\mathfrak{p}_1$ e $\mathfrak{p}_2$ non sono comassimali allora uno contiene l'altro.

E. 15.11. (→ p. 338) Sia $I = (x^2y - y^2,\, x^3 - xy) \subset \mathbb{R}[x,y]$.

1. Provare che $\{g_1 = x^2y - y^2,\, g_2 = x^3 - xy\}$ è una base di Gröbner di I rispetto a tutti i possibili ordinamenti monomiali lessicografici.

2. Decomporre $\sqrt{I}$ come intersezione di ideali primi e dire se I è radicale.

3. Sia $J = (xz^2 + z^2, yz^2 + z^2, I) \subseteq \mathbb{R}[x,y,z]$. È vero che per ogni $\alpha \in \mathbb{V}_{\mathbb{R}}(I)$ esiste $b \in \mathbb{R}$ tale che $(\alpha, b) \in \mathbb{V}_{\mathbb{R}}(J)$?

E. 15.12. (→ p. 338) Siano $A = \mathbb{Q}[x,y]$ e $I = (x^2 - y^2,\, x^4 - x^3y + y,\, xy + y^2) \subset A$.

1. Decomporre il radicale di I come intersezione di ideali primi.

2. Decomporre I come intersezione di ideali primari.

3. Calcolare $\mathcal{D}(A/I)$ e $\mathcal{N}(A/I)$.

4. Siano $\mathfrak{p} = (x,y)$ e $\mathfrak{q} = (y)$; calcolare $I_{\mathfrak{p}} \cap A$ e $I_{\mathfrak{q}} \cap A$.

5. Descrivere $(A/I)_{\mathfrak{p}}$ e $(A/I)_{\mathfrak{q}}$.

E. 15.13. (→ p. 339) Siano $\varphi_{ab} \colon \mathbb{Q}[x]^3 \to \mathbb{Q}[x]^3$ con $a, b \in \mathbb{Q}$, gli omomorfismi definiti dalle matrici

$$B_{ab} = \begin{pmatrix} x - a & 0 & 0 \\ 0 & 1 - x & x - a \\ b & a - x^2 & 0 \end{pmatrix}.$$

1. Trovare tutti i valori $a, b \in \mathbb{Q}$ per cui $\operatorname{Coker} \varphi_{ab}$ è ciclico.

2. Calcolare $\operatorname{Coker} \varphi_{ab}$ per tutti i valori di a e b per i quali non è ciclico.

E. 15.14. (→ p. 340) Siano $I = (xy, x - yz)$, $\mathfrak{q}_1 = (x,z)$ e $\mathfrak{q}_2 = (y^2, x - yz)$ ideali di $K[x,y,z]$.
Provare che $I = \mathfrak{q}_1 \cap \mathfrak{q}_2$ è una decomposizione primaria minimale di I.

E. 15.15. (→ p. 340) Sia A un anello tale che

i) $A_{\mathfrak{m}}$ è noetheriano per ogni ideale $\mathfrak{m} \in \operatorname{Max} A$;

ii) l'insieme $\mathcal{M}_x = \{\mathfrak{m} \in \operatorname{Max} A \colon x \in \mathfrak{m}\}$ è finito per ogni $x \in A \setminus \{0\}$.

Provare che A è noetheriano.

E. 15.16. (→ p. 341) Sia I un ideale di un anello A; per ogni $n \in \mathbb{N}$ sia $I^{[n]}$ l'ideale generato da $\{a^n \colon a \in I\}$.

1. Provare che se $A = \mathbb{Q}[x, y]$ allora $I^2 = I^{[2]}$.

2. Dare un esempio di un anello B e di un ideale I per cui $I^2 \neq I^{[2]}$.

3. Provare che se $A = \mathbb{Q}[x, y]$ e $I = (x, y)$ allora $I^n = I^{[n]}$ per ogni $n \in \mathbb{N}$.

E. 15.17. (→ p. 341) Siano I e J ideali di un anello A; definiamo $I\colon J^\infty = \bigcup_{n\in\mathbb{N}}(I\colon J^n)$.
Provare che

1. $I\colon J^\infty$ è un ideale di A;

2. se A è noetheriano e $a, b \in A$ allora $I\colon (b)^\infty = I\colon (a, b)^\infty$ se e solo se ogni primo associato di I che contiene b contiene anche a.

E. 15.18. (→ p. 342) Siano $I = (x^2 + xy + y^2, y^3 - 1) \subset K[x, y]$ e $\mathbb{V}_K(I) \subset K^2$ la varietà affine associata a I.

1. Trovare $\mathbb{V}_\mathbb{Q}(I)$ e $\mathbb{V}_\mathbb{C}(I)$.

2. Trovare $\mathcal{D}(\mathbb{Q}[x, y]/I)$ e $\mathcal{N}(\mathbb{Q}[x, y]/I)$.

3. Descrivere gli ideali primi di $\mathbb{Q}[x, y]/I$.

4. Trovare, se esiste, un ideale primo $\mathfrak{p} \subset \mathbb{Q}[x, y]/I$ tale che $(\mathbb{Q}[x, y]/I)_\mathfrak{p}$ è un campo.

E. 15.19. (→ p. 342) Siano A un dominio d'integrità e K il suo campo dei quozienti. Per ogni ideale I di A definiamo

$$I^{-1} = \{x \in K\colon xI \subseteq A\}$$

e diciamo che I è *invertibile* se $I\, I^{-1} = A$.
Provare che se I è invertibile allora

1. I è finitamente generato;

2. I è un A-modulo proiettivo.

E. 15.20. (→ p. 343) Sia $I \subset \mathbb{C}[x_1, \ldots, x_n]$ un ideale radicale 0-dimensionale tale che

i) $I \cap \mathbb{C}[x_n] = (x_n^m + a_{m-1}x_n^{m-1} + \ldots + a_0 = p_n)$;

ii) $|\mathbb{V}(I)| = m$.

Provare che esistono $p_1, \ldots, p_{n-1} \in \mathbb{C}[x_n]$, con $\deg p_i < m$ per ogni i, tali che la base di Gröbner ridotta di I rispetto all'ordinamento lessicografico con $x_1 > \ldots > x_n$ è

$$\{x_1 - p_1,\, x_2 - p_2, \ldots,\, x_{n-1} - p_{n-1},\, p_n\}.$$

E. 15.21. (→ p. 343) [**Lemma di Schanuel**] Siano

$$0 \longrightarrow N \xrightarrow{\varphi} P \xrightarrow{\psi} M \longrightarrow 0,$$

$$0 \longrightarrow N' \xrightarrow{\varphi'} P' \xrightarrow{\psi'} M \longrightarrow 0$$

due successioni esatte di A-moduli, con P proiettivo.

1. Provare che esistono omomorfismi $f\colon P \longrightarrow P'$ e $g\colon N \longrightarrow N'$ tali che $\operatorname{Ker} f \simeq \operatorname{Ker} g$ e $\operatorname{Coker} f \simeq \operatorname{Coker} g$.
2. Provare che se anche P' è proiettivo allora $N \oplus P' \simeq N' \oplus P$.

Parte III

Soluzioni

16

Dimostrazioni dei risultati teorici

16.1 Dimostrazioni del capitolo 1

Dimostrazione T. 1.1. 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 $m_a(b) = ab$; allora 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 $a \in A^*$. □

Dimostrazione T. 1.3. È ovvio che $0 \in I : J$. Siano $a, b \in I : J$; allora per ogni $j \in J$ abbiamo $aj, bj \in I$ e, dato che I è un ideale, si ha $(a-b)j = aj - bj \in I$, ossia $a - b \in I : J$. Infine, se $aj \in I$ per ogni $j \in J$ allora, per ogni $c \in A$, abbiamo $c(aj) = (ca)j \in I$ e quindi $ca \in I : J$.

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

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

$$= b^m \sum_{k=0}^{n-1} \binom{n+m-1}{k} a^k b^{n-1-k} + a^n \sum_{k=n}^{n+m-1} \binom{n+m-1}{k} a^{k-n} b^{n+m-1-k}$$

e osserviamo che sia il primo che il secondo addendo appartengono ad I, da cui $(a+b)^{n+m-1} \in I$ e $a + b \in \sqrt{I}$. □

Dimostrazione T. 1.4. Per induzione sul numero n degli ideali. 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 $1 = \prod_{j=1}^{n-1}(a_j + b_j) = a + b_1 \cdots b_{n-1} \in I_n + I$. Dato che I e I_n sono comassimali

$$\prod_{i=1}^{n} I_i = \prod_{i=1}^{n-1} I_i \cdot I_n = I\, I_n = I \cap I_n = \bigcap_{i=1}^{n} I_i. \qquad \square$$

Dimostrazione T. 1.5. Ricordiamo che la somma di due ideali $I + J$ è per definizione il più piccolo ideale che contiene I e J.
1. Siano $i \in I,\ j \in J$ e $h \in H$. Allora $(i+j)h = ih + jh \in IH + JH$; dato che l'ideale $(I+J)H$ è generato dagli elementi del tipo $(i+j)h$, abbiamo provato che $(I+J)H \subseteq IH + JH$.

Per l'altra inclusione, dato che $IH \subseteq (I+J)H$ e $JH \subseteq (I+J)H$, si ha $IH + JH \subseteq (I+J)H$.

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 $i = j + h \in J + I \cap H$.

5. La verifica è immediata, dato che JH è contenuto sia in J che in H. □

Dimostrazione T. 1.6. 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 $m, n \in \mathbb{N}$, $a^m \in I$ e $a^n \in J$, dunque $a^{m+n} = a^m a^n \in IJ$ e abbiamo concluso.

5. Chiaramente $1 = 1^n \in I$ se e solo se $1 \in \sqrt{I}$.

6. Dal punto 1 segue che $I + J \subseteq \sqrt{I} + \sqrt{J}$ e l'inclusione $\subseteq$ si ottiene applicando nuovamente 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 intero t. Se inoltre $n, m \in \mathbb{N}$ sono tali che $i^n \in I$ e $j^m \in J$ allora

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

appartiene a $I + J$; dunque $a \in \sqrt{I+J}$.

7. L'inclusione $\subseteq$ segue da **T.1.5**.5 e dal punto 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 $a \in \sqrt{I + JH}$. □

Dimostrazione T. 1.7. 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 che $a^m \in I$ 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 $1 = 1^n = (cb+m)^n \in (b) + I$. Moltiplicando per a, otteniamo che $a \in (ab) + I \subseteq I$, come volevamo. □

Dimostrazione T. 1.8. Bisogna provare che se $\overline{a} = \overline{c}$ e $\overline{b} = \overline{d}$ 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. Le proprietà di tale prodotto sono di facile verifica. □

Dimostrazione T. 1.9. **I**. Per dimostrare il primo teorema, in virtù della precedente discussione, basta 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. Siano $\overline{j_1}, \overline{j_2} \in J/I = \{\overline{j}\colon j \in J\}$ e $\overline{a} \in A/I$; abbiamo allora $\overline{j_1} + \overline{j_2} = \overline{j_1 + j_2}$, con $j_1 + j_2 \in J$, e $\overline{a}\overline{j_1} = \overline{aj_1}$, con $aj_1 \in J$. Quindi J/I è un ideale di A/I e possiamo definire l'anello quoziente $(A/I)/(J/I)$.
Consideriamo ora la mappa $\pi\colon A/I \longrightarrow A/J$, dove $\overline{a} \mapsto \overline{\overline{a}}$ e verifichiamo che 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 $\overline{a} \in \operatorname{Ker}\pi$, 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 I Teorema di omomorfismo.

III. (a), (b) e (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 dell'omomorfismo di inclusione di B in $B + I$ e della proiezione sul quoziente. In quanto tale f è un omomorfismo, che risulta essere surgettivo perché ogni elemento $\overline{b+i}$ è immagine di $b \in B$. Inoltre, se $b \in B$ è tale che $\overline{b} = 0$ allora $b \in I$ e dunque $b \in B \cap I$. Il nucleo di f è $B \cap I$, da cui la tesi segue nuovamente per il I Teorema di omomorfismo. □

Dimostrazione T. 1.10. Sia J un ideale di A che contiene I; dato che la proiezione è surgettiva, $\pi(J)$ è un ideale di A/I, cf. **T.1.18**.1.

Viceversa, dato un ideale H in A/I, la sua controimmagine è un ideale di A che contiene I, poiché $\pi(I) = \overline{0} \in H$.
La corrispondenza biunivoca sugli ideali massimali discende subito dalla definizione di ideale massimale.
La controimmagine di un ideale primo è sempre un ideale primo, cf. **T.1.17**.7.

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 $\mathfrak{p}$. □

Dimostrazione T. 1.11. 1. L'anello quoziente A/I è non banale se e solo se $\overline{1} \neq \overline{0}$ in A/I, ossia 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 $(\overline{0})$ e $(\overline{1})$. Per **T.1.10**, 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 $\mathcal{N}(A/I) = (\overline{0})$, i.e. se $\overline{a}^k = \overline{0}$ implica $\overline{a} = \overline{0}$. Quindi A/I è ridotto se e solo se $a^k \in I$ 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 provare che se $a, b \in A$ sono tali che $a \notin I$ e $ab \in I$ allora $b^n \in I$ per qualche intero n. Infatti, $\overline{a} \neq \overline{0}$ 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; quindi $b \in \sqrt{I}$.

Viceversa, rovesciando le implicazioni si dimostra che se I è primario allora $\mathcal{D}(A/I) \subseteq \mathcal{N}(A/I)$. Dato che $\mathcal{N}(A/I) \subseteq \mathcal{D}(A/I))$ è sempre vera, abbiamo concluso.

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

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

8. Se I è primo allora $\mathcal{N}(A/I) = \mathcal{D}(A/I) = \{\overline{0}\}$; la tesi segue applicando il punto 5. □

Dimostrazione T. 1.13. Siano $I \subset A$ un ideale primo e $I = J \cap H$ una decomposizione di I; allora $I = J$ oppure $I = H$ per **T.1.12**.2, ovvero la decomposizione data è banale. □

Dimostrazione T. 1.15. Sia $a \in A$ tale che $a \notin \mathcal{J}(A)$; 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, nuovamente per contraddizione, che esista $b \in A$ per cui $1 - ab$ non è invertibile. Allora, per **T.1.2**.3, $1 - ab \in \mathfrak{m}$, per qualche $\mathfrak{m} \in \operatorname{Max} A$. Dato che $ab \in \mathfrak{m}$, da ciò segue $1 \in \mathfrak{m}$, che è assurdo. □

Dimostrazione T. 1.16. 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 $b \in A$ e $m \in \mathfrak{m}$ tali che $ba + m = 1$ e quindi $ba = 1 - m \in A^*$ per ipotesi; da ciò segue che $a \in A^*$. □

Dimostrazione T. 1.17. 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 considerano l'immersione $\mathbb{Z} \longrightarrow \mathbb{Q}$ e $I = (n)$ con $n \neq 0, \pm 1$, allora $I^e = \mathbb{Q}$ e dunque $I^{ec} = \mathbb{Z} \supsetneq I$.

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

5. Per i punti 3 e 1, $I \subseteq I^{ec}$ implica $I^e \subseteq I^{ece}$.

Per l'altra inclusione, si ha $I^{ec} = f^{-1}(I^e)$ 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 $f(J^c) \subseteq J^{ce}$; 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 $a \in J^c$. Dato che l'altra inclusione è sempre vera, ciò mostra che J^c è radicale.

Infine, l'immersione $\mathbb{Z} \longrightarrow \mathbb{Q}$ e un ideale primo non nullo (p) di $\mathbb{Z}$ mostrano che le affermazioni 7 e 8 non valgono per ideali estesi. L'immersione $\mathbb{Z} \longrightarrow \mathbb{Z}[i]$ e l'ideale (2) mostrano che l'estensione di un ideale radicale non è necessariamente radicale, visto che $(2)^e = (1+i)^2$. □

Dimostrazione T. 1.18. 1. Ovviamente $f(I) \subseteq I^e$.

Per l'altra inclusione, sia $b \in I^e = (f(I))$; allora b si scrive come somma finita $b = \sum_j b_j f(i_j)$ con $b_j \in B$ e $i_j \in I$ per ogni j. Dal momento che f è surgettiva, per ogni j esiste $a_j \in A$ tale che $b_j = f(a_j)$ e quindi

$$b = \sum_j b_j f(i_j) = \sum_j f(a_j)f(i_j) = \sum_j f(a_j i_j) = f(\sum_j a_j i_j) \in f(I),$$

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

2. Abbiamo che $I^{ec} = f^{-1}(I^e)$; inoltre, per il punto precedente, $I^e = f(I)$. 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 $a \in I$.
Sempre dalla surgettività di f segue che $J^{ce} = f(J^c) = f(f^{-1}(J)) = J$.

3. Osserviamo che l'omomorfismo $A \xrightarrow{f} B \xrightarrow{\pi} B/I^e$ è surgettivo e, dato che $\operatorname{Ker} f \subseteq I$, ha nucleo I. Per il I Teorema di omomorfismo si ha $A/I \simeq B/I^e$. Analogamente si dimostra che $A/J^c \simeq B/J$.
Tutte le affermazioni seguono allora facilmente da **T.1.11**.3, 4 e 5. □

Dimostrazione T. 1.21. 1. Se gli ideali in questione sono a due a due comassimali, da **T.1.20** segue che f è surgettivo.

Viceversa, se f è surgettivo allora per ogni i possiamo scegliere elementi $a_i \in A$ tali che $f(a_i) = (0, \ldots, 0, 1, 0, \ldots, 0)$, dove 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 $\bigcap_{i=1}^{n} I_i$. □

Dimostrazione T. 1.22. 1. Per ogni $a \in A$ si ha $(a) \subseteq (1)$; l'elemento a è invertibile se e solo se esiste $b \in A$ tale che $ab = 1$, dunque se e solo se $(1) \subseteq (a)$.

2. L'elemento a è un divisore di b se e solo se esiste $c \in A$ tale che $ac = b$, che equivale a $(b) \subseteq (a)$.

3. Due elementi 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 $(a) \subseteq (b)$.

4. Se a è un divisore proprio di $b \neq 0$, non può essere $(a) = (b)$. Infatti in tal caso avremmo $b = ac = bdc$ per qualche $c, d \in A$. Allora, visto che A è un dominio, $b(1 - dc) = 0$ implica c invertibile, che è contro l'ipotesi.
Visto che anche a non è invertibile, avremo $(b) \subsetneq (a) \subsetneq (1)$.

5. Sia $a \notin A^*$; la condizione di primalità di a, cioè $a \,|\, bc$ se e solo se $a \,|\, b$ oppure $a \,|\, c$, per quanto visto al punto 2 è equivalente a $(bc) \subseteq (a)$ se e solo se $(b) \subseteq (a)$ oppure $(c) \subseteq (a)$. Quest'ultima è equivalente alla condizione di primalità dell'ideale (a), i.e. $bc \in (a)$ se e solo se $b \in (a)$ oppure $c \in (a)$. □

Dimostrazione T. 1.23. 1. Supponiamo che a non sia irriducibile; quindi esistono $b, c \notin A^*$ tali che $a = bc$. Allora né b né c sono elementi di (a); consideriamo ad esempio il caso $b = ab_1$ per qualche $b_1 \in A$. Si ha $a = bc = ab_1c$, da cui segue che c è invertibile, che non è possibile. Abbiamo pertanto trovato $b, c \notin (a)$ tali che $bc \in (a)$ quindi (a) non è primo e, per **T.1.22**.5, ciò 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; dunque abbiamo che $a = da_1$, con $a_1 \notin A^*$, altrimenti $b \in (d) = (a)$. Se dimostriamo 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. □

Dimostrazione T. 1.24. L'unione I degli ideali di $\mathcal{C}$ 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 $I = (a)$. Allora esiste h_0 tale che $I_{h_0} \subseteq I = (a) \subseteq I_{h_0}$. □

Dimostrazione T. 1.26. Sia A un anello. Sappiamo da **T.1.23**.2 che in un PID ogni elemento irriducibile è anche primo. Dunque grazie a **T.1.25** 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 esisterebbero elementi non invertibili $a_1, b_1 \in A$ tali che $a = a_1b_1$. 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.1.24**. □

Dimostrazione T. 1.27. 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 $\mathbb{N}$ e dunque ha un minimo. Sia $a \in I \setminus \{0\}$ un elemento per cui $\delta(a)$ è minimo e mostriamo che $I = (a)$, provando che A è PID e dunque anche UFD, per **T.1.26**. 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. □

Dimostrazione T. 1.28. Supponiamo che l'elemento a sia irriducibile e siano $I, J \subset A$ ideali tali che $(a) = I \cap J$; quindi $(a) \subseteq I$ e $(a) \subseteq J$. Se per assurdo $(a) \neq I$ 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 $a \nmid b$ e $a \nmid c$ ma $a \mid bc$, il che è impossibile se a è irriducibile e quindi primo per **T.1.25**. □

16.2 Dimostrazioni del capitolo 2

Dimostrazione T. 2.1. Dato che I è un ideale, se $X^{\mathbf{a}} \in I$ per ogni $\mathbf{a}$ allora $f \in I$.

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

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

per certi $\mathbf{a}, \mathbf{b} \in \mathbb{N}^n$, $c_{\mathbf{b},\mathbf{a}} \in K$ e $p_{\mathbf{b}}(X) = \sum_{\mathbf{a}} c_{\mathbf{b},\mathbf{a}} X^{\mathbf{a}} \in A$.
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 $\mathbf{a} \in \mathbb{N}^n$. □

Dimostrazione T. 2.2. Sia S un insieme di generatori monomiali di I e poniamo $E = \{\mathbf{a} + \mathbb{N}^n \colon X^{\mathbf{a}} \in S\}$. Chiaramente $E \neq \emptyset$ ed è un $\mathcal{E}$-sottoinsieme per costruzione. Data una frontiera F di E, abbiamo $(X^{\mathbf{a}} \colon \mathbf{a} \in F) \subseteq I$ per definizione. Sia adesso $\mathbf{b} \in E$; allora esistono $\mathbf{a} \in F$ e $\mathbf{c} \in \mathbb{N}^n$ tali che $\mathbf{b} = \mathbf{a} + \mathbf{c}$. Quindi $X^{\mathbf{b}} = X^{\mathbf{a}} X^{\mathbf{c}} \in (X^{\mathbf{a}} \colon \mathbf{a} \in F)$. □

Dimostrazione T. 2.4. Sia F una frontiera minimale di E e sia F' una frontiera finita di E che esiste per il Lemma di Dickson. Per ogni $\mathbf{a} \in F$ esistono $\mathbf{b} \in F'$ e $\mathbf{c} \in \mathbb{N}^n$ tali che $\mathbf{a} = \mathbf{b} + \mathbf{c}$; esistono inoltre $\mathbf{a}_1 \in F$ e $\mathbf{c}_1 \in \mathbb{N}^n$ tali che $\mathbf{b} = \mathbf{a}_1 + \mathbf{c}_1$. Per la minimalità di F segue allora che $\mathbf{a} = \mathbf{b} = \mathbf{a}_1$ e dunque $F \subseteq F'$. □

Dimostrazione T. 2.5. Siano $F = \{\mathbf{a}_1, \dots, \mathbf{a}_s\}$ e $F' = \{\mathbf{b}_1, \dots, \mathbf{b}_t\}$ due frontiere minimali di un $\mathcal{E}$-sottoinsieme E; allora

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

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 $\eta\colon \{1, \dots, s\} \to \{1, \dots, t\}$ tramite $\eta(i) = \min\{j\colon\ \mathbf{a}_i \in \mathbf{b}_j + \mathbb{N}^n\}$. 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. Abbiamo dunque $s \geq t$; scambiando i ruoli di F e F' si ottiene una mappa surgettiva $\nu\colon \{1, \dots, t\} \to \{1, \dots, s\}$ e quindi $t \geq s$. Allora $s = t$ e di conseguenza η e ν sono permutazioni. Si ha infine $\mathbf{a}_i \in \mathbf{b}_{\eta(i)} + \mathbb{N}^n \subseteq \mathbf{a}_{\nu(\eta(i))} + \mathbb{N}^n$; la minimalità di F implica $\mathbf{a}_i = \mathbf{a}_{\nu(\eta(i))}$ e quindi $\mathbf{a}_i = \mathbf{b}_{\eta(i)}$ per ogni i. □

Dimostrazione T. 2.8. Bisogna provare che l'algoritmo di divisione termina e che i polinomi $u_1, \dots, u_s$ e r ottenuti soddisfano le condizioni richieste. Cominciamo col dimostrare che ad ogni passo vale la formula

$$f = u_1 f_1 + \ldots + u_s f_s + p + r. \tag{16.1}$$

Sicuramente la relazione è vera al primo passo. Supponiamo che sia vera al passo $(n-1)$-esimo. Eseguendo il passo n-esimo, l'algoritmo procede in uno dei due modi seguenti:

a) se $\mathrm{lt}(f_i) \,|\, \mathrm{lt}(p)$ allora 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;

b) 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 (16.1) 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 il leading term di un polinomio, $p - \mathrm{lt}(p)$ oppure $p - \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)} f_i$, che ha multigrado strettamente minore del multigrado di p.

L'algoritmo termina con $p = 0$ e quindi (16.1) restituisce la relazione i).

Per verificare ii) osserviamo che l'algoritmo aggiunge ad r solo monomi non divisibili per $\mathrm{lt}(f_i)$ per ogni i; quindi r è ridotto rispetto ad F per costruzione.

Infine verifichiamo che vale iii). Innanzitutto $\mathrm{Deg}(p) \leq \mathrm{Deg}(f)$; quando ad un passo si modifica u_i, lo si fa aggiungendogli un addendo del tipo $\frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)}$, dove $\frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)} f_i$ cancella il termine 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. □

Dimostrazione T. 2.9. 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 $f \in (G) \subseteq I$.

Viceversa, 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 $f \in I$.

Viceversa, sia $f \in I$; per ipotesi si ha $f \xrightarrow{G}_* 0$ e 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 da (2.1) 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 $\mathrm{lm}(f) \in (\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t))$. 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. □

Dimostrazione T. 2.10. È una diretta applicazione di **T.2.9**. Infatti 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 $I \subseteq (g_1, \ldots, g_t)$. □

Dimostrazione T. 2.11. Siano $f \in A \setminus \{0\}$ e G una base di Gröbner di I. 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 può appartenere a $\mathrm{Lt}(I)$ dunque si deve avere necessariamente $r - r' = 0$. □

Dimostrazione T. 2.12. 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 esisterebbero $g_i \in G$ e $g'_j \in G'$ tali che $\mathrm{lt}(g_i)$ e $\mathrm{lt}(g'_j)$ dividono $\mathrm{lt}(r - r')$, ma tale monomio 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 $\mathrm{Lt}(G) = \mathrm{Lt}(G')$. □

Dimostrazione T. 2.17. 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 anche G' è una base di Gröbner minimale 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. □

Dimostrazione T. 2.18. Dato che sia G che G' sono minimali, possiamo supporre senza perdita di generalità che $\mathrm{lm}(g_i) = \mathrm{lm}(g'_i)$ per ogni $i = 1, \ldots, t$, cf. **T.2.5**. Fissato i consideriamo il polinomio $g_i - g'_i \in I$; se $g_i - g'_i \neq 0$ allora

esiste g_j tale che $\mathrm{lm}(g_j) \mid \mathrm{lm}(g_i - g_i')$. 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 oppure di g_i', che è assurdo perché sia G che G' sono ridotte. □

Dimostrazione T. 2.21. Sia $G = \{g_1, \ldots, g_t\}$ 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 $j \xrightarrow{G}_* 0$. Chiamiamo r il resto di j e possiamo scrivere $r = j - \sum_{i=1}^{t} u_i g_i \in J + I \subseteq J$. Se $r \neq 0$ allora 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 $\mathrm{lt}(r) \in \mathrm{Lt}(J)$. Pertanto $r = 0$, come volevamo. □

Dimostrazione T. 2.23. 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, l'elemento $\overline{r}$ 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 $\overline{m_1} = \sum_{i=2}^{k} a_i \overline{m_i}$ per certi $a_i \in K$. 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. □

Dimostrazione T. 2.24. Esiste $g \in A$ tale che $fg \equiv 1 \mod I$ 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) 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 (2.2), determiniamo la combinazione $1 = h_1 f_1 + \ldots + h_s f_s + fg$. In questo modo abbiamo anche calcolato g. □

Dimostrazione T. 2.26. 1. Sia $f \in I \cap J$; allora $f = tf + (1-t)f \in (tI, (1-t)J)$ e un'inclusione è provata.

Per l'altra inclusione, osserviamo 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 $f(X) = g(t, X) + h(t, X) \in (tI, (1-t)J) \cap A$ con $g(t, X) \in tI$ e $h(t, X) \in (1-t)J$ allora

$$f(X) = g(1, X) = h(0, X) \in I \cap J$$

per l'osservazione precedente.
Per concludere la dimostrazione ora basta considerare su $A[t]$ un ordinamento lessicografico tale che $t > x_i$ per ogni $i = 1, \ldots, n$. Applicando **T.2.25** all'ideale $(tI, (1-t)J)$ abbiamo la tesi.

2. Per **E.8.17**.5 si ha che $I\colon J = \bigcap_{i=1}^{s} I\colon (f_i)$; inoltre, per ogni $f \in A$ si ha $I\colon (f) = \frac{1}{f}(I \cap (f))$, cf. **E.8.18**. Il calcolo del quoziente si riduce dunque al calcolo di intersezioni di ideali di A che possono essere ottenute applicando il punto 1. □

Dimostrazione T. 2.27. L'enunciato è ovvio per $f = 0$, quindi supponiamo $f \neq 0$. Sia $f \in \sqrt{I}$; allora esiste un intero m tale che $f^m \in I$.
Scriviamo

$$1 = t^m f^m + (1 - t^m f^m) = t^m f^m + (1 - tf) \sum_{i=0}^{m-1} t^i f^i$$

e otteniamo che $1 \in (I, 1 - tf)$.

Viceversa, se $I = (f_1, \ldots, f_k)$ e $(I, 1 - tf) = (1)$ allora 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 positivo m tali che $f^m = \sum_{i=1}^{k} g_i f_i \in I$. □

16.3 Dimostrazioni del capitolo 3

Dimostrazione T. 3.1. 1. Sia $\alpha \in \mathbb{V}(J)$; allora si ha $f(\alpha) = 0$ per ogni $f \in J$. Quindi per ipotesi $f(\alpha) = 0$ per ogni $f \in I$, da cui segue che $\alpha \in \mathbb{V}(I)$.

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

3. Certamente $\mathbb{V}(I) \subseteq \mathbb{V}(\mathbb{I}(\mathbb{V}(I)))$.

Per l'altra inclusione, basta notare che $I \subseteq \mathbb{I}(\mathbb{V}(I))$ per il punto 2, e dunque $\mathbb{V}(\mathbb{I}(\mathbb{V}(I))) \subseteq \mathbb{V}(I)$ per il punto 1.

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

Per l'altra implicazione, supponiamo $\mathbb{I}(W) \subseteq \mathbb{I}(V)$; se $\alpha \in V$ allora per ogni $f \in \mathbb{I}(V)$ si ha $f(\alpha) = 0$ e quindi anche $f(\alpha) = 0$ per ogni $f \in \mathbb{I}(W)$, ossia $\alpha \in \mathbb{V}(\mathbb{I}(W)) = W$, dove l'ultima uguaglianza è data dal punto 3.

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

Per l'altra inclusione, se $\alpha \in \mathbb{V}(I) \cap \mathbb{V}(J)$ allora per ogni $f = i + j \in I + J$ avremo $f(\alpha) = i(\alpha) + j(\alpha) = 0$ e quindi $\alpha \in \mathbb{V}(I + J)$.

6. Dato che $IJ \subseteq I, J$, abbiamo $\mathbb{V}(I) \cup \mathbb{V}(J) \subseteq \mathbb{V}(IJ)$.

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

7. Dato che $I \cap J \subseteq I, J$, abbiamo $\mathbb{V}(I) \cup \mathbb{V}(J) \subseteq \mathbb{V}(I \cap J)$.

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

8. Dato che $I \subseteq \sqrt{I}$, abbiamo $\mathbb{V}(I) \supseteq \mathbb{V}(\sqrt{I})$.

Per l'altra inclusione, se $f \in \sqrt{I}$ allora esiste $m \in \mathbb{N}$ tale che $f^m \in I$. Di conseguenza, dato $\alpha \in \mathbb{V}(I)$, si ha $f^m(\alpha) = 0$ da cui segue che $f(\alpha) = 0$ e quindi $\alpha \in \mathbb{V}(\sqrt{I})$. □

Dimostrazione T. 3.2. Sia $\{V_h\}_{h \in H}$ una catena discendente di varietà affini di K^n; per **T.3.1**.4 otteniamo una catena ascendente di ideali $\{\mathbb{I}(V_h)\}_{h \in H}$ di A. Per il Teorema della base di Hilbert A è noetheriano e tale catena è stazionaria; necessariamente anche la catena $\{\mathbb{V}(\mathbb{I}(V_h))\}_{h \in H}$ è stazionaria e la conclusione segue allora da **T.3.1**.3. □

Dimostrazione T. 3.4. 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.3.2** sappiamo che ogni catena discendente ammette un elemento massimale rispetto a $\supseteq$ e dunque esiste un elemento minimale in Σ che non è irriducibile; indichiamolo con W. 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 irriducibili $W_{1,j}$ con $j = 1, \dots, r$ e $W_{2,h}$ con $h = 1, \dots, s$ 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 che $V = \bigcup_{i=1}^{r} V_i = \bigcup_{j=1}^{s} W_j$ siano due decomposizioni minimali di V; allora, $V_1 = V_1 \cap V = \bigcup_{j=1}^{s} (V_1 \cap W_j)$. Dato che V_1 è irriducibile, si deve avere $V_1 = V_1 \cap W_{j_0}$ per qualche $j_0 \in \{1, \dots, s\}$. Allo stesso modo deduciamo che esiste un $i_0 \in \{1, \dots, r\}$ per cui $W_{j_0} = W_{j_0} \cap V_{i_0}$. Pertanto avremo $V_1 \subseteq W_{j_0} \subseteq V_{i_0}$. Dato che la prima decomposizione è minimale, dobbiamo allora avere $V_1 = W_{j_0}$. Iterando su ogni V_i e usando la minimalità della seconda decomposizione arriviamo a concludere che $r = s$ e che le due decomposizioni sono uguali a meno di una permutazione degli indici. □

Dimostrazione T. 3.5. Sia $f \in A$; dividendo f per i polinomi $x_i - a_i$ otteniamo che $f(x_1, \dots, x_n) = \sum_i h_i(x_i - a_i) + r$ 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.2.16**, $f \in \mathbb{I}(V_\alpha)$ se e solo se $f(\alpha) = r = 0$, ovvero se e solo se $f \in (x_1 - a_1, \dots, x_n - a_n)$. □

Dimostrazione T. 3.9. 1. Dato che $\alpha_1, \dots, \alpha_m \in \overline{K}$ sono le radici di f, allora $f = a_m \prod_{i=1}^m (x - \alpha_i)$ e $\operatorname{Ris}(f, g) = a_m^\ell \operatorname{Ris}(\hat{f}, g)$ per **T.3.6**.3 con , dove $\hat{f} = \frac{f}{a_m}$. Quindi, applicando m volte **T.3.8**.3 a $\hat{f}$ e g e valutando il risultato in $y_1 = \alpha_1, \dots, y_m = \alpha_m$, otteniamo

$$\operatorname{Ris}(f, g) = a_m^\ell \prod_{i=1}^m g(\alpha_i) \operatorname{Ris}(1, g(x)) = a_m^\ell \prod_{i=1}^m g(\alpha_i).$$

Per l'altra relazione, da **T.3.6**.2 e da quanto appena visto otteniamo che

$$\operatorname{Ris}(f, g) = (-1)^{m\ell} \operatorname{Ris}(g, f) = (-1)^{m\ell} b_\ell^m \prod_{j=1}^\ell f(\beta_j).$$

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

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

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. □

Dimostrazione T. 3.10. Sia $h = h(x_2, \dots, x_n) = \operatorname{Ris}_{x_1}(f, g)$; allora

$$h(\beta) = \det \begin{pmatrix} c_m(\beta) & \cdots & \cdots & c_0(\beta) & 0 & \cdots & 0 \\ 0 & c_m(\beta) & \cdots & \cdots & c_0(\beta) & & \vdots \\ \vdots & & \ddots & & & \ddots & 0 \\ 0 & \cdots & 0 & c_m(\beta) & \cdots & \cdots & c_0(\beta) \\ d_\ell(\beta) & \cdots & \cdots & d_0(\beta) & 0 & \cdots & 0 \\ 0 & d_\ell(\beta) & & & \ddots & & \vdots \\ \vdots & & \ddots & & & \ddots & 0 \\ 0 & \cdots & 0 & d_\ell(\beta) & \cdots & \cdots & d_0(\beta) \end{pmatrix}.$$

Se $d_\ell(\beta) \neq 0$, cioè se $r = 0$, questo determinante è proprio quello della matrice di Sylvester di $f(x_1, \beta)$ e $g(x_1, \beta)$ e abbiamo concluso.

Se invece $d_\ell(\beta) = 0$ allora sviluppando il determinante sulla prima colonna, il cui unico elemento diverso da zero è $c_m(\beta)$, si ottiene

$$h(\beta) = c_m(\beta) \det \begin{pmatrix} c_m(\beta) & \cdots & c_0(\beta) & \cdots & 0 \\ \vdots & \ddots & & \ddots & \vdots \\ 0 & \cdots & c_m(\beta) & \cdots & c_0(\beta) \\ d_{\ell-1}(\beta) & \cdots & d_0(\beta) & \cdots & 0 \\ \vdots & \ddots & & \ddots & \vdots \\ 0 & \cdots & d_{\ell-1}(\beta) & \cdots & d_0(\beta) \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} \ell - 1 \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} m \end{matrix} .$$

Se $d_{\ell-1}(\beta) \neq 0$, cioè se $r = 1$, il determinante è quello della matrice di Sylvester di $f(x_1, \beta)$ e $g(x_1, \beta)$ e abbiamo di nuovo concluso.
Se $d_{\ell-1}(\beta) = 0$ allora iteriamo il procedimento fino a trovare un $d_{\ell-r}(\beta) \neq 0$, che esiste perché $g(x_1, \beta) \neq 0$ per ipotesi. □

Dimostrazione T. 3.12. Scriviamo $f = f_N + f_{N-1} + \ldots + f_0$ con ognuno degli f_i omogeneo di grado totale i. Osservando che un monomio $X^{\mathbf{a}}$ con $\sum_{i=1}^n a_i = N$ ha immagine $y_1^{a_1}(y_2 + \alpha_2 y_1)^{a_2} \cdots (y_n + \alpha_n y_1)^{a_n}$, possiamo scrivere

$$\varphi(f) = f(y_1, y_2 + \alpha_2 y_1, \ldots, y_n + \alpha_n y_1) = f_N(1, \alpha_2, \ldots, \alpha_n) y_1^N + f'$$

con $\deg_{y_1} f' < N$.
Dal momento che $0 \neq f_N(x_1, \ldots, x_n) = x_1^N f_N\left(1, \frac{x_2}{x_1}, \ldots, \frac{x_n}{x_1}\right)$ e il campo K è infinito, esistono $\alpha_2, \ldots, \alpha_n \in K$ tali che $f_N(1, \alpha_2, \ldots, \alpha_n) = c \neq 0$. □

Dimostrazione T. 3.15. Abbiamo già visto in **T.3.5** che un ideale della forma $(x_1 - a_1, \ldots, x_n - a_n)$ è massimale ed è $\mathfrak{m}_\alpha$ con $\alpha = (a_1, \ldots, a_n) \in K^n$.

Per provare il viceversa dobbiamo utilizzare l'ipotesi $K = \overline{K}$. Sia $\mathfrak{m} \subset A$ un ideale massimale; dalla forma debole del Nullstellensatz discende che $\mathbb{V}(\mathfrak{m}) \neq \emptyset$ e quindi esiste $\alpha \in \mathbb{V}(\mathfrak{m})$. Pertanto

$$\mathfrak{m}_\alpha = \mathbb{I}(\{\alpha\}) \supseteq \mathbb{I}(\mathbb{V}(\mathfrak{m})) = \sqrt{\mathfrak{m}} = \mathfrak{m},$$

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

Dimostrazione T. 3.16. Per **T.3.1**.8 si ha $\mathbb{V}(I) = \mathbb{V}(\sqrt{I})$ e consideriamo la sua decomposizione minimale in sottovarietà irriducibili $\mathbb{V}(I) = V_1 \cup \ldots \cup V_r$, cf. **T.3.4**. Passando agli ideali associati, per la forma forte del Nullstellensatz avremo che

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

Grazie a **T.3.3** possiamo concludere che $\sqrt{I}$ è intersezione finita 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.1.12**.2 e **T.1.14** deduciamo che tali primi sono tutti e soli gli elementi di $\operatorname{Min} I$. □

Dimostrazione T. 3.18. Se $K = \overline{K}$, $\mathbb{V}(I) = \{\alpha_1, \dots, \alpha_s\}$ è finita e I è radicale allora

$$I = \sqrt{I} = \mathbb{I}(\mathbb{V}(I)) = \mathbb{I}(\{\alpha_1, \dots, \alpha_s\}) = \bigcap_{i=1}^{s} \mathbb{I}(\{\alpha_i\}),$$

e quindi da **T.3.15** discende che $I = \bigcap_{i=1}^{s} \mathfrak{m}_{\alpha_i}$. Dato che tali ideali sono massimali distinti e dunque comassimali, avremo

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

cf. **T.1.21**. Il fatto che tale prodotto diretto abbia dimensione 0 segue dalla descrizione degli ideali in un prodotto diretto, cf. **E.8.34**. □

Dimostrazione T. 3.19. La prima uguaglianza è ovvia, la seconda è fornita da **T.3.18** e l'ultima disuguaglianza da **T.3.17**.

Per l'altra disuguaglianza, sia $>$ un ordinamento monomiale fissato. Grazie a **T.2.23** sappiamo che

$$\dim_K(A/\sqrt{I}) = \dim_K(A/\operatorname{Lt}(\sqrt{I})) \leq \dim_K(A/\operatorname{Lt}(I)) = \dim_K(A/I),$$

dove la disuguaglianza è dovuta al fatto che $\operatorname{Lt}(I) \subseteq \operatorname{Lt}(\sqrt{I})$. Inoltre, per **T.2.21** vale l'uguaglianza se e solo se I è radicale.

Per quanto riguarda la dimensione di Krull, da **T.1.14** discende che in generale $\dim(A/I) = \dim(A/\sqrt{I})$; pertanto I è 0-dimensionale se e solo se $\sqrt{I}$ è 0-dimensionale, e questo è dato da **T.3.18**. □

Dimostrazione T. 3.20. Tutto lo spazio $K^n = \mathbb{V}((0))$ e l'insieme vuoto $\emptyset = \mathbb{V}((1))$ sono chiusi. Inoltre è facile verificare che l'unione finita di chiusi è chiusa e che l'intersezione di una famiglia qualsiasi di chiusi è un chiuso, cf. la dimostrazione di **T.3.1**.5 e 6. □

Dimostrazione T. 3.21. 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 $\mathbb{I}(W) \subseteq \mathbb{I}(S)$, da cui segue che $W = \mathbb{V}(\mathbb{I}(W)) \supseteq \mathbb{V}(\mathbb{I}(S)) = \overline{S}$. Dunque $\overline{S}$ è l'intersezione di tutte le varietà affini che contengono S. □

Dimostrazione T. 3.24. 1. Chiaramente $\mathcal{X} = \mathcal{V}(\{0\})$ e $\emptyset = \mathcal{V}(A)$; quindi $\mathcal{X}$ e $\emptyset$ sono chiusi.

2. Ovvio.

3. Dato che (E) è il più piccolo ideale che contiene E, ogni primo che contiene E contiene anche (E) e $\sqrt{(E)} = \bigcap_{(E)\subset\mathfrak{p}\in\mathcal{X}} \mathfrak{p}$. Quindi si ha $\mathcal{V}(E) = \mathcal{V}((E)) = \mathcal{V}(\sqrt{(E)})$ per ogni sottoinsieme E di A.

4. Da $IJ \subseteq I \cap J \subseteq I, J$ segue che $\mathcal{V}(IJ) \supseteq \mathcal{V}(I \cap J) \supseteq \mathcal{V}(I) \cup \mathcal{V}(J)$.

Per le altre inclusioni, ricordiamo che se $I \cap J \subseteq \mathfrak{p}$ allora $I \subseteq \mathfrak{p}$ oppure $J \subseteq \mathfrak{p}$, cf. **T.1.12**.2, e che se $IJ \subseteq \mathfrak{p}$ allora $I \subseteq \mathfrak{p}$ oppure $J \subseteq \mathfrak{p}$ per definizione di ideale primo. Da ciò si deduce che

$$\mathcal{V}(I) \cup \mathcal{V}(J) \supseteq \mathcal{V}(I \cap J) \quad \text{e} \quad \mathcal{V}(I) \cup \mathcal{V}(J) \supseteq \mathcal{V}(IJ),$$

e abbiamo dimostrato le uguaglianze volute.
Notiamo che da questo punto segue immediatamente il fatto che l'unione finita di chiusi è un chiuso.

5. Osserviamo che $\mathfrak{p} \supseteq \bigcup_{\alpha\in\Lambda} I_\alpha$ se e solo se $\mathfrak{p} \supseteq I_\alpha$ per ogni α, cioè se e solo se $\mathfrak{p} \in \bigcap_{\alpha\in\Lambda} \mathcal{V}(I_\alpha)$. □

Dimostrazione T. 3.25. Bisogna verificare che ogni aperto $\mathcal{X} \setminus \mathcal{V}(I)$ si scrive come unione di $\mathcal{X}_f$ per certi $f \in A$. Da **T.3.24**.5 segue che $\mathcal{V}(I) = \bigcap_{f\in I} \mathcal{V}(\{f\})$, e dunque

$$\mathcal{X} \setminus \mathcal{V}(I) = \mathcal{X} \setminus \Big(\bigcap_{f\in I} \mathcal{V}(\{f\})\Big) = \bigcup_{f\in I} \big(X \setminus \mathcal{V}(\{f\})\big) = \bigcup_{f\in I} \mathcal{X}_f. \qquad \square$$

Dimostrazione T. 3.26. Uno spazio topologico $\mathcal{X}$ è compatto se e solo se da ogni ricoprimento di aperti della base si può estrarre un sottoricoprimento finito. Sia

$$\mathcal{X} = \bigcup_{\alpha\in\Lambda} \mathcal{X}_{f_\alpha} = \bigcup_{\alpha\in\Lambda} (\mathcal{X} \setminus \mathcal{V}(f_\alpha)) = \mathcal{X} \setminus \bigcap_{\alpha\in\Lambda} \mathcal{V}(f_\alpha) = \mathcal{X} \setminus \mathcal{V}(\bigcup_{\alpha\in\Lambda} \{f_\alpha\});$$

allora $\mathcal{V}(\bigcup_{\alpha\in\Lambda} \{f_\alpha\}) = \emptyset$, ossia $\{f_\alpha\}_{\alpha\in\Lambda}$ genera A. Pertanto esistono 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 $\mathcal{X} = \bigcup_{\lambda\in\Lambda'} \mathcal{X}_{f_\lambda}$, ossia $\{\mathcal{X}_{f_\lambda} : \lambda \in \Lambda'\}$ è un sottoricoprimento finito. □

Dimostrazione T. 3.27. Dato che $\overline{\mathcal{Y}}$ è chiuso, avremo che $\overline{\mathcal{Y}} = \mathcal{V}(I)$ con I ideale di A. Chiaramente si ha $\mathcal{Y} \subseteq \mathcal{V}(\bigcap_{\mathfrak{p}\in\mathcal{Y}} \mathfrak{p})$, perché se $\mathfrak{q} \in \mathcal{Y}$ allora $\mathfrak{q} \supseteq \bigcap_{\mathfrak{p}\in\mathcal{Y}} \mathfrak{p}$ e quindi $\mathfrak{q} \in \mathcal{V}(\bigcap_{\mathfrak{p}\in\mathcal{Y}} \mathfrak{p})$. Inoltre, $\mathcal{V}(I) \supseteq \mathcal{V}(\bigcap_{\mathfrak{p}\in\mathcal{Y}} \mathfrak{p})$; basta infatti verificare che $I \subseteq \bigcap_{\mathfrak{p}\in\mathcal{Y}} \mathfrak{p}$ e questo è vero perché $\mathfrak{p} \in \mathcal{Y} \subseteq \mathcal{V}(I)$ implica $\mathfrak{p} \supseteq I$.
Dunque $\mathcal{Y} \subseteq \mathcal{V}(\bigcap_{\mathfrak{p}\in\mathcal{Y}} \mathfrak{p}) \subseteq \mathcal{V}(I) = \overline{\mathcal{Y}}$ e passando alla chiusura si ha la tesi. □

Dimostrazione T. 3.28. Usando **T.3.27** 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 $\mathcal{X}$ non è T_1, in quanto sono chiusi alcuni punti di $\mathcal{X}$ ma non tutti, perché se tutti i primi fossero massimali A avrebbe dimensione 0. A fortiori, $\mathcal{X}$ non è T_2.
Proviamo che $\mathcal{X}$ è T_0. Consideriamo $\mathfrak{p}_1$ e $\mathfrak{p}_2$ due punti distinti di $\mathcal{X}$; allora esiste, ad esempio, $f \in \mathfrak{p}_1$ e $f \notin \mathfrak{p}_2$ e quindi $\mathcal{X}_f = \mathcal{X} \setminus \mathcal{V}(f)$ è un aperto che contiene $\mathfrak{p}_2$ e non $\mathfrak{p}_1$. □

Dimostrazione T. 3.29. Sappiamo che la contrazione di un ideale primo è un ideale primo e dunque la funzione ϕ^* è ben definita. Proviamo che la controimmagine di un aperto della base di $\mathcal{X}$ è aperta in $\mathcal{Y}$; basta verificare che se $f \in A$ allora $(\phi^*)^{-1}(\mathcal{X}_f) = \mathcal{Y}_{\phi(f)}$. Infatti, abbiamo che

$$\begin{aligned}(\phi^*)^{-1}(\mathcal{X}_f) &= \{\mathfrak{q} \in \mathcal{Y} \colon \phi^*(\mathfrak{q}) \in \mathcal{X}_f\} = \{\mathfrak{q} \in \mathcal{Y} \colon f \notin \phi^*(\mathfrak{q})\} \\ &= \{\mathfrak{q} \in \mathcal{Y} \colon f \notin \phi^{-1}(\mathfrak{q})\} = \{\mathfrak{q} \in \mathcal{Y} \colon \phi(f) \notin \mathfrak{q}\} = \mathcal{Y}_{\phi(f)}.\end{aligned}$$ □

Dimostrazione T. 3.30. Per il risultato precedente $\pi^* \colon \operatorname{Spec}(A/\mathcal{N}(A)) \longrightarrow \mathcal{X}$ indotta da $\pi \colon A \longrightarrow A/\mathcal{N}(A)$ 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 per ogni ideale I di $A/\mathcal{N}(A)$

$$\begin{aligned}\pi^*(\mathcal{V}(I)) &= \pi^*\left(\{\mathfrak{p} \in \operatorname{Spec}(A/\mathcal{N}(A)) \colon I \subseteq \mathfrak{p}\}\right) \\ &= \left\{\pi^{-1}(\mathfrak{p}) \colon \mathfrak{p} \in \operatorname{Spec}(A/\mathcal{N}(A)) \text{ e } I \subseteq \mathfrak{p}\right\} \\ &= \{\mathfrak{q} \in \mathcal{X} \colon I \subseteq \pi(\mathfrak{q})\} = \left\{\mathfrak{q} \in \mathcal{X} \colon \pi^{-1}(I) \subseteq \mathfrak{q}\right\} = \mathcal{V}(\pi^{-1}(I)),\end{aligned}$$

abbiamo che π^* è chiusa e quindi un omeomorfismo. □

16.4 Dimostrazioni del capitolo 4

Dimostrazione T. 4.1. 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. □

Dimostrazione T. 4.2. Le proprietà della struttura di A-modulo sono conseguenze immediate della definizione (verificarlo!).
Sia $\varphi \colon M \longrightarrow \operatorname{Hom}_A(A, M)$ la funzione definita da $\varphi(m) = f_m$, dove $f_m(a) = am$. Tale applicazione è A-lineare; infatti si verifica facilmente che

$$\varphi(\alpha m_1 + \beta m_2) = f_{\alpha m_1 + \beta m_2} = \alpha f_{m_1} + \beta f_{m_2}$$

per ogni $\alpha, \beta \in A$. È iniettiva perché $\varphi(m) = 0$ se e solo se $f_m = 0$, i.e. $am = 0$ per ogni $a \in A$; quindi con $a = 1$ si ottiene $m = 0$. È inoltre surgettiva perché ogni omomorfismo di A-moduli da A in M è individuato per A-linearità dall'immagine di 1; se $f \in \mathrm{Hom}_A(A, M)$ è tale che $f(1) = m$ allora $f = f_m = \varphi(m)$. □

Dimostrazione T. 4.3. I. La dimostrazione è analoga al corrispondente teorema per anelli; si dimostra facilmente che la mappa $\overline{f}\colon M/\operatorname{Ker} f \to \operatorname{Im} f$ definita da $\overline{f}(\overline{m}) = f(m)$ è ben definita ed è un isomorfismo.

II. Osserviamo 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 $(N + P)/P \simeq N/(N \cap P)$. □

Dimostrazione T. 4.4. Supponiamo che M sia libero; dato che S è un insieme di generatori di M, 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.

Viceversa 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. □

Dimostrazione T. 4.8. Sia $\{m_h\}_{h \in H}$ un insieme di generatori di M; consideriamo il modulo libero A^H e l'omomorfismo definito da $f(e_h) = m_h$, dove $\{e_h\}_{h \in H}$ è la base canonica di A^H. Tale f risulta essere surgettivo e dunque $M \simeq A^H/\operatorname{Ker} f$. □

Dimostrazione T. 4.9. Nella dimostrazione di **T.4.7** abbiamo visto che se M è libero con base S allora $M \simeq A^S$. □

Dimostrazione T. 4.12. Sia $N = \langle n_1, \ldots, n_k \rangle \subseteq M$ e consideriamo l'omomorfismo

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

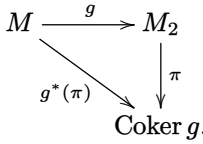
dove j è l'inclusione di N in M. Per ipotesi, $\pi \circ j$ è surgettivo; dunque $M = N + \mathfrak{m}M$. Infatti chiaramente $N + \mathfrak{m}M \subseteq M$.

Per l'altra inclusione, osserviamo che 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 $M = N$ per la terza forma del Lemma di Nakayama. □

Dimostrazione T. 4.15. Siano $S = \{m_1, \dots, m_r\}$ e $\{n_1, \dots, n_r\}$ 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 $i = 1, \dots, r$ induce per **T.4.7** un endomorfismo surgettivo $\tilde{f}$ di M. Per **T.4.14**, $\tilde{f}$ è un isomorfismo. Pertanto anche $\{n_1, \dots, n_r\}$ è un insieme libero. □

Dimostrazione T. 4.17. 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.

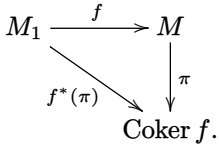
In M_2 Scegliamo $N = \operatorname{Coker} g = M_2/\operatorname{Im} g$ e proviamo che $N = 0$. Consideriamo il diagramma



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^* sia iniettiva per ogni A-modulo N.

In M Dal fatto che $(g \circ f)^* = f^* \circ g^* = 0$ segue immediatamente $\operatorname{Ker} g \supseteq \operatorname{Im} f$. Infatti, preso $N = M_2$, abbiamo $0 = (g \circ f)^*(\mathrm{id}_{M_2}) = \mathrm{id}_{M_2} \circ g \circ f = g \circ f$, ovvero $\operatorname{Im} f \subseteq \operatorname{Ker} g$.

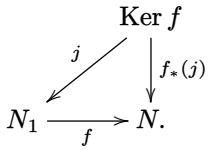
Per l'altra inclusione, scegliamo $N = \operatorname{Coker} f = M/\operatorname{Im} f$ e consideriamo il diagramma



Per costruzione abbiamo $\operatorname{Im} f = \operatorname{Ker} \pi$ e $f^*(\pi) = 0$; 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 $\operatorname{Im} f = \operatorname{Ker} \pi \supseteq \operatorname{Ker} g$.

2. Come nel punto precedente dimostriamo che la successione di partenza è esatta scegliendo degli opportuni moduli M per la successione degli Hom.

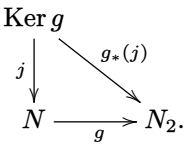
In N_1 Scegliamo $M = \operatorname{Ker} f$; consideriamo l'immersione $j\colon \operatorname{Ker} f \longrightarrow N_1$ e il diagramma



Per costruzione, $f_*(j) = 0$; dato che per ipotesi f_* è iniettiva per ogni M, si ottiene $j = 0$, cioè f è iniettiva.

In N 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 $\mathrm{id}_{N_1} \in \operatorname{Hom}_A(M, N_1)$, otteniamo $g \circ f = 0$, ovvero $\operatorname{Im} f \subseteq \operatorname{Ker} g$.

Per l'altra inclusione, 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 $\operatorname{Im} f \supseteq \operatorname{Im} j = \operatorname{Ker} g$, come volevamo.

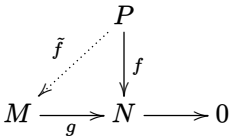
Alternativamente, la conclusione segue subito scegliendo $M = A$ e osservando che, per **T.4.2**, nel diagramma

$$\begin{array}{ccccccc} 0 & \longrightarrow & \operatorname{Hom}_A(A, N_1) & \xrightarrow{f_*} & \operatorname{Hom}_A(A, N) & \xrightarrow{g_*} & \operatorname{Hom}_A(A, N_2) \\ & & \downarrow \simeq & & \downarrow \simeq & & \downarrow \simeq \\ 0 & \longrightarrow & N_1 & \xrightarrow{f} & N & \xrightarrow{g} & N_2 \end{array}$$

le frecce verticali, tutte definite da $\varphi \mapsto \varphi(1_A)$, sono isomorfismi e i quadrati commutano. □

Dimostrazione T. 4.20. Supponiamo che α e β siano isomorfismi, 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. □

Dimostrazione T. 4.21. 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 $\hat{f}$ sugli elementi di $\mathcal{B}$, ponendo $\hat{f}(b) = m_b$ per ogni $b \in \mathcal{B}$. Da **T.4.7** otteniamo che $\hat{f}$ si estende in maniera unica ad un omomorfismo $\tilde{f}$ tale che $g \circ \tilde{f} = f$; dunque P è proiettivo. □

Dimostrazione T. 4.24. Supponiamo che M sia proiettivo; allora è addendo diretto di un modulo libero, cf. **T.4.22**, ed è dunque isomorfo ad un sottomodulo di un modulo libero, che è libero per **T.4.23**.1; quindi M è libero.

Il viceversa è sempre vero, cf. **T.4.21**. □

Dimostrazione T. 4.25. 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 combinazione lineare 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 $\Delta_i(RX) \subseteq \Delta_i(X)$.

Per l'altra inclusione, osserviamo che R è invertibile e dunque vale anche $\Delta_i(RX) \supseteq \Delta_i(R^{-1}RX) = \Delta_i(X)$, come volevamo. □

Dimostrazione T. 4.28. Per **T.4.25**, abbiamo che

$$\Delta_i(X) = \Delta_i(D) = (d_{11} \cdots d_{ii}),$$

dove la seconda uguaglianza è dovuta al fatto che D è diagonale e alle relazioni di divisibilità $d_{11} \mid d_{22} \mid \ldots \mid d_{tt}$ tra i d_{ii}; le due affermazioni seguono immediatamente. □

Dimostrazione T. 4.30. 1. Certamente $\overline{v_1}, \ldots, \overline{v_r}$ generano L/N; proviamo allora che la somma è diretta. Sia $a\overline{v_i} \in \sum_{j\neq i}\langle\overline{v_j}\rangle$ con $a \in A$ per qualche $i = 1, \ldots, r$; allora esistono $a_j \in A$ tali che $av_i - \sum_{i\neq j} a_j v_j \in N$. Esistono quindi $b_1, \ldots, b_s \in A$ 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 $\operatorname{Ann}\overline{v_i} = 0\colon \langle\overline{v_i}\rangle$. 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. □

Dimostrazione T. 4.31. Siano $M = \langle m_1, \ldots, m_r\rangle$ e $f\colon A^r \longrightarrow M$ 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 $\{d_1v_1, \ldots, d_sv_s\}$ è una base di $\operatorname{Ker} f$, cf. **T.4.29**. La tesi segue da **T.4.30**, dato che $M \simeq A^r/\operatorname{Ker} f$ e gli ideali $I_i = (d_i) = 0\colon \langle\overline{v_i}\rangle$ verificano le relazioni di contenimento, poiché $d_1 \mid d_2 \mid \ldots \mid d_s$ e $I_{s+1} = \ldots = I_r = 0$. □

Dimostrazione T. 4.33. 1. È un caso particolare di **T.4.23**.2.

2. Dal Teorema di struttura **T.4.31** sappiamo che esistono ideali principali $I_1 = (d_1) \supseteq I_2 = (d_2) \supseteq \ldots \supseteq I_r = (d_r)$ 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 $0 \colon T(M) = I_s = (d_s)$, e questo basta per concludere. □

Dimostrazione T. 4.34. Ricordiamo innanzitutto che in un PID gli ideali primari sono generati da potenze di elementi primi, cf. **E.8.63**.
Per il Teorema di struttura **T.4.31** esistono ideali principali $I_1 = (d_1) \supseteq I_2 = (d_2) \supseteq \ldots \supseteq I_r = (d_r)$ tali che $M \simeq \bigoplus_{i=1}^{r} A/I_i$. Dato che $M = M_{[p]}$ ogni ideale I_i contiene una potenza di p con esponente positivo, 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. 4.35. Per il Teorema di struttura **T.4.31** esistono ideali principali $I_1 = (d_1) \supseteq I_2 = (d_2) \supseteq \ldots \supseteq I_r = (d_r)$ tali che $M \simeq \bigoplus_{i=1}^{r} A/I_i$. Siano $d_1, \ldots, d_s \neq 0$, $d_{s+1} = \ldots = d_r = 0$ e $d_i = \prod_{j=1}^{h_i} p_{ij}^{e_{ij}}$ la decomposizione di d_i come prodotto di primi distinti, per $i = 1, \ldots, s$. Abbiamo allora $M \simeq \bigoplus_{i=1}^{s} A/I_i \oplus A^{r-s}$; inoltre, per il Teorema cinese del resto, si ha $A/I_i \simeq \bigoplus_{j=1}^{h_i} A/(p_{ij}^{e_{ij}})$ e quindi

$$M \simeq \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{h_i} A/(p_{ij}^{e_{ij}}) \oplus A^{r-s},$$

dove gli ideali $(p_{ij}^{e_{ij}})$ sono gli ideali primari cercati. □

Dimostrazione T. 4.37. 1. Per **T.4.36**.5 ogni insieme $\{v_i, \ldots, \varphi^{d_i - 1}(v_i)\}$ 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 $\langle v_1 \rangle, \ldots, \langle v_s \rangle$.

2. È una immediata conseguenza del punto precedente. □

16.5 Dimostrazioni del capitolo 5

Dimostrazione T. 5.3. 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

$$\begin{array}{ccc} M \times N & \xrightarrow{0} & M \otimes N/\langle L \rangle \\ {\scriptstyle \tau}\downarrow & \nearrow_{\varphi} & \\ M \otimes N. & & \end{array}$$

Senz'altro $\varphi = 0$ fa commutare il diagramma. Inoltre, sia $(m, n) \in M \times N$, dove $m = \sum_{i=1}^{h} a_i m_i$, con $m_i \in \mathcal{G}_1$ e $a_i \in A$ per ogni $i = 1, \dots, h$, e $n = \sum_{j=1}^{k} b_j n_j$ con $n_j \in \mathcal{G}_2$ e $b_j \in A$ per ogni $j = 1, \dots, k$; allora, indicando con π la proiezione $M \otimes N \to (M \otimes N)/\langle L \rangle$, si ha

$$\begin{aligned} \pi(\tau(m, n)) = \pi(m \otimes n) &= \pi\left(\sum_{i=i}^{h} a_i m_i \otimes \sum_{j=1}^{h} b_j n_j\right) \\ &= \sum_{i,j} a_i b_j \pi(m_i \otimes n_j) = 0, \end{aligned}$$

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. □

Dimostrazione T. 5.4. 1. L'applicazione $f\colon A \times M \longrightarrow M$, data da $f(a, m) = am$ è A-bilineare; per la proprietà universale esiste allora un omomorfismo $\tilde{f}\colon A \otimes M \longrightarrow M$ tale che $\tilde{f}(a \otimes m) = am$, che è chiaramente surgettivo. Consideriamo l'omomorfismo $g\colon M \longrightarrow A \otimes M$, definito da $g(m) = 1 \otimes m$. Abbiamo $g \circ \tilde{f}(a \otimes m) = g(am) = 1 \otimes am = a \otimes m$, 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

$$f_m\colon N \times P \longrightarrow (M \otimes N) \otimes P$$

$$f_m(n, p) = (m \otimes n) \otimes p$$

è bilineare e quindi risulta definito un omomorfismo $\widetilde{f_m} : N \otimes P \longrightarrow (M \otimes N) \otimes P$. Consideriamo poi 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

$$\tilde{g}\colon M \otimes (N \otimes P) \longrightarrow (M \otimes N) \otimes P$$

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

In modo analogo si può costruire un omomorfismo

$$\tilde{h}\colon (M \otimes N) \otimes P \longrightarrow M \otimes (N \otimes P)$$

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

che è l'inverso di $\tilde{g}$, da cui la tesi.

4. L'omomorfismo di A moduli

$$f\colon (M \oplus N) \times P \longrightarrow (M \otimes P) \oplus (N \otimes P)$$

$$f((m,n),p) = (m \otimes p, n \otimes p)$$

è bilineare e quindi induce un omomorfismo

$$\tilde{f}\colon (M \oplus N) \otimes P \longrightarrow (M \otimes P) \oplus (N \otimes P)$$

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

A partire dalle applicazioni bilineari

$$\begin{aligned} g\colon M \times P &\longrightarrow (M \oplus N) \otimes P, & g(m,p) &\mapsto (m,0) \otimes p, \\ h\colon N \times P &\longrightarrow (M \oplus N) \otimes P, & h(n,p) &\mapsto (0,n) \otimes p, \end{aligned}$$

costruiamo gli omomorfismi

$$\tilde{g}\colon M \otimes P \longrightarrow (M \oplus N) \otimes P \quad \text{e} \quad \tilde{h}\colon N \otimes P \longrightarrow (M \oplus N) \otimes P.$$

Per la proprietà universale della somma diretta, cf. **T.4.6**.1, otteniamo 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 $\tilde{f}$.

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 l'omomorfismo $M/IM \longrightarrow A/I \otimes M$ definito da $\overline{m} \longmapsto \overline{1} \otimes m$. È ben definito; infatti, se $\overline{m} = \overline{n}$ allora $m - n \in IM$ e dunque $m - n = \sum_i a_i m_i$, per certi $a_i \in I$, $m_i \in M$. Abbiamo

$$\overline{1} \otimes m - \overline{1} \otimes n = \overline{1} \otimes (m-n) = \overline{1} \otimes \sum_i a_i m_i = \sum_i \overline{a_i} \otimes m_i = 0.$$

È immediato verificare che i due omomorfismi sono uno l'inverso dell'altro.

6. 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 usiamo il punto 4. Siano $M \simeq A^m$ e $N \simeq A^n$; allora

$$\begin{aligned} M \otimes N &= A^m \otimes A^n = (A^{m-1} \oplus A) \otimes A^n \\ &\simeq (A^{m-1} \otimes A^n) \oplus (A \otimes A^n) \\ &\simeq A^{(m-1)n} \oplus A^n \simeq A^{mn}. \end{aligned}$$ □

Dimostrazione T. 5.5. Abbiamo già dimostrato il secondo isomorfismo in **T.5.1**.
Per ogni $f \in \mathrm{Bil}(M, N; P)$ esiste un unico omomorfismo $\tilde{f}$ tale che $\tilde{f}(m \otimes n) = f(m, n)$. Definiamo $\Phi\colon \mathrm{Bil}(M, N; P) \longrightarrow \mathrm{Hom}_A(M \otimes_A N, P)$ ponendo $\Phi(f) = \tilde{f}$. Siano $\tilde{f} = \Phi(f) = \Phi(g) = \tilde{g}$; allora $f(m, n) = \tilde{f}(m \otimes n) = \tilde{g}(m \otimes n) = g(m, n)$, per ogni $m \in M$ e $n \in N$, cioè Φ è iniettiva. L'omomorfismo Φ è anche surgettivo; dato $f \in \mathrm{Hom}_A(M \otimes_A N, P)$, definiamo $\underline{f}\colon M \times N \longrightarrow P$ ponendo $\underline{f}(m, n) = f(m \otimes n)$. Allora $\underline{f}$ 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 $m \in M$ e $n \in N$. Quindi $f = \widetilde{\underline{f}} = \Phi(\underline{f})$. □

Dimostrazione T. 5.7. Ponendo $N = A$, la tesi discende subito da **T.5.4**.1. □

16.6 Dimostrazioni del capitolo 6

Dimostrazione T. 6.1. 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 $vut(ar - cs) = 0$, e quindi $(a, s) \sim (c, r)$, dato che $vut \in S$. □

Dimostrazione T. 6.2. 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.
L'affermazione su σ_S è di verifica immediata. □

Dimostrazione T. 6.3. 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. Abbiamo $S^{-1}A = 0$ se e solo se $\frac{0}{1} = \frac{1}{1}$, ossia, per definizione, se e solo se $0 \in S$. Quindi, dato che S è moltiplicativo, se e solo se S contiene un elemento nilpotente. □

Dimostrazione T. 6.5. 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 $S^{-1}A$ abbiamo $\frac{a}{s} = 0$. □

Dimostrazione T. 6.6. L'insieme $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$ 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, $\mathfrak{m}$ è proprio perché se $\frac{a}{s} = \frac{1}{1}$ per qualche $a \in \mathfrak{p}$ allora esiste $u \in A\setminus\mathfrak{p}$ 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 $\mathfrak{m}$. □

Dimostrazione T. 6.7. 1a. È chiaro che $S^{-1}I \subset I^e$.

Per l'inclusione opposta, sia $i \in I^e$; allora

$$i = \sum_{h=1}^{k} \frac{a_h}{s_h}\frac{i_h}{1} \quad \text{per certi} \quad \frac{a_1}{s_1}, \dots, \frac{a_k}{s_k} \in S^{-1}A \ \text{ e } \ i_1, \dots, i_k \in I.$$

Possiamo 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 $i \in S^{-1}I$.

1b. 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 $\frac{a}{s} = \frac{1}{1}$. Dunque esiste $t \in S$ tale che $st = at \in I \cap S$.

1c. Sia $a \in \bigcup_{s\in S} I\colon(s)$; allora esiste $s \in S$ tale che $as \in I$. Dato che $\frac{a}{1} = \frac{as}{s}$, abbiamo $\frac{a}{1} \in S^{-1}I = I^e$ e quindi $a \in I^{ec}$.

Per l'altra inclusione, sia $b \in I^{ec}$; 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 $b \in I\colon(st)$ con $st \in S$.

2. Vale sempre che $J \supseteq J^{ce}$ per cui basta provare che $J \subseteq J^{ce}$.
Consideriamo $\frac{a}{s} \in J$; allora $\frac{a}{1} \in J$ e quindi $a \in J^c$ e $\frac{a}{s} = \frac{1}{s}\frac{a}{1} \in J^{ce}$. □

Dimostrazione T. 6.8. Vale sempre che $\mathfrak{p} \subseteq \mathfrak{p}^{ec}$.

Per l'altra inclusione, sia $a \in \mathfrak{p}^{ec}$; per **T.6.7**.1c esiste $s \in S$ tale che $a \in \mathfrak{p}\colon(s)$. Dal momento che $\mathfrak{p} \cap S = \emptyset$ si deve avere $a \in \mathfrak{p}$, e quindi $\mathfrak{p}^{ec} \subseteq \mathfrak{p}$.
Proviamo ora la seconda affermazione; dall'ipotesi e da **T.6.7**.1b abbiamo $\mathfrak{p}^e \subsetneq S^{-1}A$.
Siano $\frac{a}{s}, \frac{b}{t} \in S^{-1}A$ tali che $\frac{a}{s}\frac{b}{t} \in \mathfrak{p}^e$; allora, per **T.6.7**.1a, esistono $p \in \mathfrak{p}$ e $u \in S$ tali che $\frac{ab}{st} = \frac{p}{u}$, ed esiste $v \in S$ tale che $vuab = vstp \in \mathfrak{p}$. Dato che

$vu \in S$ e $\mathfrak{p} \cap S = \emptyset$ per ipotesi, otteniamo $ab \in \mathfrak{p}$. Quindi $\frac{a}{s} \in \mathfrak{p}^e$ oppure $\frac{b}{t} \in \mathfrak{p}^e$, come volevamo. □

Dimostrazione T. 6.9. I punti 1 e 2 seguono immediatamente dalle proprietà dell'estensione di ideali, cf. **E.8.46**.

3. Certamente $S^{-1}(I \cap J) \subseteq S^{-1}I \cap S^{-1}J$, ancora per **E.8.46**.

Per l'altra inclusione, sia $\alpha = \frac{i}{s} = \frac{j}{t} \in S^{-1}I \cap S^{-1}J$ con $i \in I$, $j \in J$ e $s, t \in S$; 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 segue $\alpha \in \sqrt{S^{-1}I}$.

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 $\beta^n = \frac{i}{s}$, per certi $i \in I$ e $s \in S$. Di conseguenza esiste $u \in S$ tale che $ua^n s = ut^n i \in I$, quindi $uas \in \sqrt{I}$ e $\beta = \frac{usa}{ust} \in S^{-1}\sqrt{I}$. □

Dimostrazione T. 6.10. Osserviamo che gli omomorfismi μ_s e μ_t commutano per ogni $s, t \in S$, e, se sono invertibili, chiaramente commutano anche i loro inversi.

Siano N dotato di una struttura di $S^{-1}A$-modulo compatibile con quella di A-modulo e $s \in S$; 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 per elementi di $S^{-1}A$ che sia compatibile con la struttura di A-modulo. In particolare 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 $\frac{a}{s} = \frac{b}{t}$ e $u \in S$ tali che $u(at - bs) = 0$; allora $u(at - bs)n = 0$ 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 questo prodotto esterno definisca su N l'unica struttura di $S^{-1}A$-modulo compatibile sono immediate. □

Dimostrazione T. 6.11. Osserviamo che se $\tilde{f}$ esiste allora è univocamente determinato; infatti per ogni $m \in M$ e $s \in S$ abbiamo

$$\tilde{f}\left(\frac{m}{s}\right) = \tilde{f}\left(\frac{1}{s}\sigma(m)\right) = \frac{1}{s}\tilde{f}(\sigma(m)) = \frac{1}{s}f(m) = \mu_s^{-1}(f(m)),$$

dove l'ultima uguaglianza è garantita da **T.6.10**.

Per verificare che $\tilde{f}$ è ben definito ed è un omomorfismo di $S^{-1}A$-moduli basta procedere come nella dimostrazione di **T.6.4**. □

Dimostrazione T. 6.12. Dato che $S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f) = 0$, si ha $\operatorname{Im} S^{-1}f \subseteq \operatorname{Ker} S^{-1}g$.

Per l'altra inclusione, sia $\frac{n}{s} \in \operatorname{Ker} S^{-1}g$; allora $\frac{g(n)}{s} = \frac{0}{1}$ ed 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

$$\frac{n}{s} = \frac{tn}{ts} = \frac{f(m)}{ts} = S^{-1}f(\tfrac{m}{ts}) \in \operatorname{Im} S^{-1}f. \qquad \square$$

Dimostrazione T. 6.14. 1. Definiamo $f\colon S^{-1}A \times M \longrightarrow S^{-1}M$ con $f\left(\frac{a}{s}, m\right) = \frac{am}{s}$. Tale f è ben definita e A-bilineare e quindi, per la proprietà universale del prodotto tensoriale, esiste un unico omomorfismo di A-moduli

$$\tilde{f}\colon S^{-1}A \otimes_A M \longrightarrow S^{-1}M, \text{ definito da } \tilde{f}\left(\frac{a}{s} \otimes_A m\right) = \frac{am}{s}.$$

Poiché f è surgettiva anche $\tilde{f}$ è surgettiva.
Osserviamo che se $\alpha \in S^{-1}A \otimes_A M$ allora $\alpha = \sum_{i=1}^{k} \frac{a_i}{s_i} \otimes m_i$ per certi $a_i \in A$, $s_i \in S$ e $m_i \in M$; quindi, ponendo $s = \prod_{i=1}^{k} s_i$, $t_i = \frac{s}{s_i}$ e $n = \sum_{i=1}^{k} t_i a_i m_i$, si può scrivere

$$\alpha = \sum_{i=1}^{k} \frac{t_i a_i}{t_i s_i} \otimes m_i = \frac{1}{s} \otimes \sum_{i=1}^{k} t_i a_i m_i = \frac{1}{s} \otimes n.$$

Proviamo che $\tilde{f}$ è iniettiva; se $\alpha \in \operatorname{Ker} \tilde{f}$ allora $0 = \tilde{f}(\alpha) = \tilde{f}\left(\frac{1}{s} \otimes n\right) = \frac{n}{s}$ ed esiste $u \in S$ tale che $un = 0$. Da ciò otteniamo

$$\alpha = \frac{1}{s} \otimes n = \frac{u}{us} \otimes n = \frac{1}{us} \otimes un = 0,$$

come volevamo.

2. Per il punto precedente e le proprietà del prodotto tensoriale **T.5.4** e **T.5.8**, si ha

$$\begin{aligned} S^{-1}M \otimes_{S^{-1}A} S^{-1}N &\simeq S^{-1}M \otimes_{S^{-1}A} (S^{-1}A \otimes_A N) \\ &\simeq (S^{-1}M \otimes_{S^{-1}A} S^{-1}A) \otimes_A N \simeq S^{-1}M \otimes_A N \\ &\simeq (S^{-1}A \otimes_A M) \otimes_A N \simeq S^{-1}A \otimes_A (M \otimes_A N) \\ &\simeq S^{-1}(M \otimes_A N). \end{aligned}$$ $\square$

Dimostrazione T. 6.15. 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 $\mathfrak{m}$ che contiene $\operatorname{Ann} m$. Per ipotesi $M_{\mathfrak{m}} = 0$, quindi $\frac{m}{1} = \frac{0}{1}$ ed esiste $u \in S = A \setminus \mathfrak{m}$ tale che $um = 0$, ma questo non è possibile perché $\operatorname{Ann} m \subseteq \mathfrak{m}$. $\square$

Dimostrazione T. 6.17. 1. Segue subito da $S^{-1}\mathcal{N}(A) = \mathcal{N}(S^{-1}A)$, cf. **T.6.9**.4, e da **T.6.15**.

2. Dal fatto che S^{-1} è un funtore esatto e da **T.6.14** segue che $S^{-1}A$ è piatto. Dato che il prodotto tensoriale di moduli piatti è piatto, cf. **E.11.9**.5, la piattezza di M implica la piattezza di $M_\mathfrak{p}$ per ogni primo $\mathfrak{p}$, ancora per **T.6.14**.

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, $(M \otimes_A N)_\mathfrak{p} \simeq M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p}$, abbiamo $(\mathrm{id}_M \otimes f)_\mathfrak{p} = \mathrm{id}_{M_\mathfrak{p}} \otimes f_\mathfrak{p}$. Pertanto $M_\mathfrak{p}$ piatto implica $0 = \mathrm{Ker}(\mathrm{id}_{M_\mathfrak{p}} \otimes f_\mathfrak{p}) = (\mathrm{Ker}(\mathrm{id}_M \otimes f))_\mathfrak{p}$ per ogni primo $\mathfrak{p}$. Dunque, per **T.6.15**, $\mathrm{Ker}(\mathrm{id}_M \otimes f) = 0$ e M è piatto. □

Dimostrazione T. 6.18. Consideriamo l'insieme $P = \{\mathfrak{p} \in \mathrm{Spec}A\colon \mathfrak{p} \cap S = \emptyset\}$; allora sicuramente $S \subseteq A \setminus \bigcup_{\mathfrak{p}\in P} \mathfrak{p}$.

Per l'altra inclusione, nel caso in cui S è saturato, supponiamo che $a \notin S$ e proviamo che esiste un primo $\mathfrak{p} \in P$ tale che $a \in \mathfrak{p}$. Dato che $a \notin S$ e S saturato, l'elemento $\frac{a}{1}$ non è invertibile in $S^{-1}A$ e quindi esiste un ideale massimale $\mathfrak{m} \subset S^{-1}A$ che lo contiene. Per **T.6.8** esiste $\mathfrak{p} \subset A$ 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 $t \in S$ ed esiste $u \in S$ tale che $uta = ub \in \mathfrak{p}$, da cui segue $a \in \mathfrak{p}$.

Viceversa, abbiamo già osservato che il complementare di un'unione di ideali primi è un insieme moltiplicativo. Inoltre se $st \in S$ allora $st \notin \mathfrak{p}$ per ogni $\mathfrak{p} \in P$, e quindi $s, t \in S$ per cui S è saturato. □

Dimostrazione T. 6.20. Se $S^{-1}A = T^{-1}A$ allora i loro elementi invertibili sono gli stessi e da **T.6.19**.5 discende che

$$\overline{S} = {\sigma_S}^{-1}((S^{-1}A)^*) = {\sigma_T}^{-1}((T^{-1}A)^*) = \overline{T}.$$

Viceversa, se $\overline{S} = \overline{T}$ allora per **T.6.19**.6 si ha

$$S^{-1}A = {\overline{S}}^{-1}A = {\overline{T}}^{-1}A = T^{-1}A.$$ □

16.7 Dimostrazioni del capitolo 7

Dimostrazione T. 7.1. $1 \Rightarrow 2$. Sia S un sottoinsieme non vuoto di Σ ed $s_1 \in S$. Se S non ammette elementi massimali allora 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 $\{s_\alpha\}_{\alpha\in\Lambda}$ una catena ascendente di elementi di Σ. L'insieme $\{s_\alpha\}_{\alpha\in\Lambda}$ è dunque un sottoinsieme non vuoto di Σ, quindi ammette un elemento massimale s_{α_0}, cioè tale che $s_\alpha = s_{\alpha_0}$ per ogni $\alpha \geq \alpha_0$. □

Dimostrazione T. 7.3. La dimostrazione è analoga a quella di **T.7.2**.2. □

Dimostrazione T. 7.5. Per **T.7.2**.1 l'ideale $\sqrt{I}$ è finitamente generato, diciamo da $f_1, \dots, f_r$. Allora esistono interi $k_1, \dots, k_r$ tali che $f_i^{k_i} \in I$ per ogni $i = 1, \dots, r$. Un qualsiasi intero $k \geq \sum_{i=1}^{r} k_i$ fa allora al caso nostro. □

Dimostrazione T. 7.7. Verifichiamo che l'ideale $\mathfrak{q}$ è primario. Sia $ab \in \mathfrak{q} \subseteq \mathfrak{q}_1$ con $a \notin \mathfrak{q}_1$; allora $b^n \in \mathfrak{q}_1$, da cui segue $b \in \sqrt{\mathfrak{q}_1} = \mathfrak{p} = \sqrt{\mathfrak{q}_2}$. Pertanto abbiamo $b^m \in \mathfrak{q}_2$ per qualche intero m e ciò implica $b^{n+m} \in \mathfrak{q}_1\mathfrak{q}_2 \subseteq \mathfrak{q}$. (E se $a \in \mathfrak{q}_1 \setminus \mathfrak{q}$?)
Inoltre $\sqrt{\mathfrak{q}} = \sqrt{\mathfrak{q}_1 \cap \mathfrak{q}_2} = \sqrt{\mathfrak{q}_1} \cap \sqrt{\mathfrak{q}_2} = \mathfrak{p}$. □

Dimostrazione T. 7.8. 1. Segue subito dal fatto che $1 \in \mathfrak{q} : (a)$.

2. Ricordiamo che $\mathfrak{q} : (a) \supseteq \mathfrak{q}$. Dimostriamo prima 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, abbiamo $b \in \sqrt{\mathfrak{q}} = \mathfrak{p}$. Dunque $\mathfrak{q} \subseteq \mathfrak{q} : (a) \subseteq \mathfrak{p}$. 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 $b \notin \mathfrak{p}$. Dato che $\mathfrak{q}$ è primario, $bca \in \mathfrak{q}$ implica $ca \in \mathfrak{q}$, i.e. $c \in \mathfrak{q} : (a)$ come volevamo.

3. Sia $b \in \mathfrak{q} : (a)$, i.e. $ab \in \mathfrak{q}$. Per ipotesi $a \notin \mathfrak{p}$, dunque $\mathfrak{q}$ primario implica che $b \in \mathfrak{q}$, e abbiamo verificato l'inclusione non banale $\mathfrak{q} : (a) \subseteq \mathfrak{q}$. □

Dimostrazione T. 7.10. Per **T.7.5** esiste un intero k tale che $\mathfrak{p}_i^k \subseteq \mathfrak{q}_i$; abbiamo allora $(\bigcap_{j \neq i} \mathfrak{q}_j)\mathfrak{p}_i^k \subseteq \bigcap_{j \neq i} \mathfrak{q}_j \cap \mathfrak{q}_i = I$. Scegliamo il più piccolo k per cui $(\bigcap_{j \neq i} \mathfrak{q}_j)\mathfrak{p}_i^k \subseteq I$ e sia $0 \neq a \in (\bigcap_{j \neq i} \mathfrak{q}_j)\mathfrak{p}_i^{k-1} \setminus I$.
Abbiamo allora $a\mathfrak{p}_i \subseteq I$, e dunque $\mathfrak{p}_i \subseteq I : (a)$.

Per l'altra inclusione, basta osservare che $a \in \bigcap_{j \neq i} \mathfrak{q}_j \setminus \mathfrak{q}_i$ e, dalla dimostrazione di **T.7.8**, discende che $I : (a) \subseteq \sqrt{I : (a)} = \mathfrak{p}_i$. □

Dimostrazione T. 7.11. 1. Vogliamo mostrare che

$$\operatorname{Min} I = \{\mathfrak{p}_i \in \operatorname{Ass} I : \mathfrak{p}_i \text{ minimale in } \operatorname{Ass} I\} = \{\mathfrak{p} \in \operatorname{Spec} A : \mathfrak{p} \supseteq I \text{ minimale}\}.$$

Sia $\mathfrak{p}$ un primo che contiene $I = \bigcap_{i=1}^{t} \mathfrak{q}_i$; allora $\mathfrak{p} \supseteq \sqrt{I} = \bigcap_{i=1}^{t} \mathfrak{p}_i$ e quindi $\mathfrak{p} \supseteq \bigcap_{\mathfrak{p}_i \in \operatorname{Min} I} \mathfrak{p}_i$. Dunque, dato che $\mathfrak{p}$ è primo, deve contenere qualche $\mathfrak{p}_{i_0} \in \operatorname{Min} I$, per **T.1.12**.2. Quindi $\mathfrak{p} \supseteq \mathfrak{p}_{i_0} \supseteq I$ e, se $\mathfrak{p}$ è minimale tra i primi che contengono I, deve essere necessariamente $\mathfrak{p} = \mathfrak{p}_{i_0}$. Abbiamo mostrato che vale l'inclusione $\supseteq$ e, in particolare, che l'insieme dei primi che contengono I e sono minimali è finito.

Per l'altra inclusione, sia $\sqrt{I} = \mathfrak{p}_{i_1} \cap \ldots \cap \mathfrak{p}_{i_k}$, con $\mathfrak{p}_{i_j} \in \operatorname{Min} I$ per $j = 1, \dots, k$ 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 $\mathfrak{p}_{i_1} \cap \ldots \cap \mathfrak{p}_{i_k} = \sqrt{I} \subseteq \mathfrak{p}'$ e, dato che $\mathfrak{p}'$ è primo, esiste i_j tale che $\mathfrak{p}_{i_1} \supseteq \mathfrak{p}' \supseteq \mathfrak{p}_{i_j}$, ancora per **T.1.12**.2. Per la minimalità, non si può avere $i_j \neq i_1$ e da ciò segue $\mathfrak{p}_{i_1} = \mathfrak{p}'$, come volevamo.

2. La prima uguaglianza discende subito dal punto 1, dato che $\mathcal{N}(A) = \sqrt{0}$. Per la seconda, da **E.8.29** sappiamo che $\mathcal{D}(A) = \bigcup_{0 \neq a \in A} \sqrt{0 \colon (a)}$.

Sia $\mathfrak{p}_i \in \operatorname{Ass}(0)$; allora $\mathfrak{p}_i = \sqrt{0 \colon (a_i)}$ per qualche $a_i \in A$ per il Teorema di unicità **T.7.9**, e questo dimostra l'inclusione $\supseteq$.

Per l'altra inclusione, se $0 \neq a \in \mathcal{D}(A)$ allora $a \notin \bigcap_{i=1}^{t} \mathfrak{q}_i$. Per **T.7.8**, abbiamo $\sqrt{0 \colon (a)} = \bigcap_{i=1}^{t} \sqrt{\mathfrak{q}_i \colon (a)} = \bigcap_{i \colon a \notin \mathfrak{q}_i} \mathfrak{p}_i$, che è contenuto in qualche $\mathfrak{p}_i$ per come abbiamo scelto a. □

Dimostrazione T. 7.12. 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.6.7** e da $S^{-1}\sqrt{\mathfrak{q}} = \sqrt{S^{-1}\mathfrak{q}}$, cf. **T.6.9**.4.
Supponiamo $S \cap \mathfrak{p} = \emptyset$ 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 $wua \notin \mathfrak{q}$, 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.6.9**.3 e dal punto 1.

3. È un caso particolare del punto 2. □

Dimostrazione T. 7.13. Sia $S_i = A \setminus \mathfrak{p}_i$ con $\mathfrak{p}_i \in \operatorname{Min} I$; allora $S_i \cap \mathfrak{p}_j \neq \emptyset$ per ogni $j \neq i$, altrimenti avremmo che $\mathfrak{p}_j \subset \mathfrak{p}_i$, contro la minimalità di $\mathfrak{p}_i$. Da **T.7.12**.1 segue allora $IA_{\mathfrak{p}_i} = S_i^{-1}I = S_i^{-1}\mathfrak{q}_i$ e $(IA_{\mathfrak{p}_i})^c = \mathfrak{q}_i$. □

Dimostrazione T. 7.15. 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.7.14**.1. Di conseguenza, $\mathcal{N}(A) = \mathfrak{m}$ e la tesi segue da **T.7.14**.3. □

Dimostrazione T. 7.17. Se A è un anello artiniano allora ogni ideale primo è massimale e dunque $\dim A = 0$. Per **T.7.14**, A possiede solo un numero finito di ideali massimali $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ ed esiste k tale che

$$0 = \mathcal{N}(A)^k = \Big(\bigcap_{i=1}^{s} \mathfrak{m}_i\Big)^k \supseteq \prod_{i=1}^{s} \mathfrak{m}_i^k.$$

Per **T.7.16**, A è dunque noetheriano.

Viceversa, se A è noetheriano con $\dim A = 0$ si ha che $\sqrt{0} = \bigcap_{i=1}^{s} \mathfrak{m}_i$ è intersezione finita di ideali massimali, cf. **T.7.11**; allora esiste un intero k tale che $\prod_{i=1}^{s} \mathfrak{m}_i^k \subseteq \sqrt{0}^{\,k} \subseteq 0$ per **T.7.5**. Quindi, ancora per **T.7.16**, A è artiniano. □

17

Soluzioni degli esercizi proposti

17.1 Soluzioni del capitolo 8

Soluzione E. 8.1. Sia I un ideale contenente S; allora abbiamo $as_1 + bs_2 \in I$ per ogni s_1, $s_2 \in S$ e a, $b \in A$. Pertanto $I \supseteq (S)$ e l'intersezione di tutti questi ideali contiene S.

Per l'altra inclusione, basta osservare che (S) è un ideale che contiene S per costruzione.

Soluzione E. 8.2. $1 \Rightarrow 2$. È ovvio che se $b = c$ allora $ab = ac$ per ogni $a \in A$.

Viceversa, sia $ab = ac$ con $a \neq 0$; allora, dato che $a \neq 0$ e A è un dominio, $a(b - c) = 0$ implica $b - c = 0$.

$2 \Rightarrow 3$. Siano $b, c \in A \setminus \{0\}$ e supponiamo per assurdo che $bc \notin A \setminus \{0\}$, ovvero $bc = 0$; allora $b = 0$ oppure, visto che $bc = 0 = b0$ con $b \neq 0$, dall'ipotesi discende che $c = 0$. In entrambi casi abbiamo una contraddizione.

$3 \Rightarrow 1$. Dire che per ogni $b, c \in A$ con $b, c \neq 0$ si ha $bc \neq 0$ è equivalente a dire che se $bc = 0$ allora $b = 0$ oppure $c = 0$, che è la definizione di dominio.

Soluzione E. 8.3. 1. L'anello A è finito e dunque, da **T.1.1**, 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

$$A^* = \{\overline{h} \colon h \in \mathbb{Z},\ (h, 24) = 1\} \quad \text{e} \quad \mathcal{D}(A) = \{\overline{h} \colon h \in \mathbb{Z},\ (h, 24) \neq 1\}.$$

Gli ideali di $\mathbb{Z}/(24)$ corrispondono agli ideali (a) di $\mathbb{Z}$ tali che $(a) \supseteq (24)$, ossia tali che $a \,|\, 24 = 8 \cdot 3$.
Gli unici ideali primi sono $(\overline{2})$ e $(\overline{3})$ che sono anche massimali.

2. Ragionando come al punto precedente, troviamo che

$$A^* = \{\overline{h} \colon h \in \mathbb{Z},\ (h, 17) = 1\} = A \setminus \{\overline{0}\} \quad \text{e} \quad \mathcal{D}(A) = \{\overline{0}\}.$$

Quindi $(\overline{0})$ è l'unico ideale primo ed è anche massimale.

3. Abbiamo che $A = \mathbb{Z}/(n)$ è un dominio se e solo se $\mathcal{D}(A) = \{\overline{0}\}$, cioè se e solo se $A^* = A \setminus \{\overline{0}\}$ che equivale a dire che 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. 8.4. Poiché a è nilpotente esiste $n \in \mathbb{N}_+$ tale che $a^n = 0$. Dunque $1 = 1 - a^n = (1-a)\sum_{i=0}^{n-1} a^i$, ossia la prima parte della tesi.
Sia ora $b \in A^*$ e proviamo che $b + a \in A^*$; basta osservare che $b + a = b(1 + ab^{-1})$. Dato che $-ab^{-1}$ è nilpotente, la conclusione segue dalla prima parte dell'esercizio, poiché il prodotto di invertibili è invertibile.

Soluzione E. 8.5. 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. $fg = \sum_{i=0}^{n+m} c_i x^i = 1$. 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

$$a_n^2 b_{m-1} = -a_n a_{n-1} b_m = 0.$$

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.8.4**, e argomentando nello stesso modo si ottiene la tesi.

Il viceversa discende immediatamente da **E.8.4**, visto che $f = a_0 + (a_1 x + \dots a_n x^n)$, a_0 è invertibile e la somma dei nilpotenti $a_i x^i$ per $i = 1, \dots, n$ è nilpotente.

2. Per quanto detto sopra, se $a_0, \dots, a_n$ sono nilpotenti, è immediato vedere che f è nilpotente.

Viceversa, se f è nilpotente allora xf è nilpotente e $1 + xf$ è invertibile. La tesi segue allora dal punto precedente.

3. Una implicazione è semplicemente la definizione di divisore di zero.

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

$$a_n b_i = 0 \quad \text{per ogni } i.$$

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 $a_i b_m = 0$ per ogni i. Prendendo $a = b_m$ si ha la tesi.

Soluzione E. 8.6. È sempre vero che il radicale di Jacobson contiene il nilradicale.

Per l'altra inclusione, sia $f \in \mathcal{J}(A[x])$; allora $1 + xf$ è invertibile per la caratterizzazione degli elementi nel radicale di Jacobson **T.1.15**. Quindi i

coefficienti di f sono nilpotenti per **E.8.5**.1 e da **E.8.5**.2 segue che f è nilpotente, come volevamo.

Soluzione E. 8.7. Sia $a \in I$ e 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 $-a$ entrambi i membri, otteniamo $b = -ba = ba^2 \in I^2$. Induttivamente abbiamo che $b \in I^n$ per ogni n e quindi $b = 0$, cioè la tesi.

Soluzione E. 8.8. La verifica del fatto che $I[x]$ è un ideale di $A[x]$ è immediata dato che I è un ideale di A.

Consideriamo la funzione $\varphi\colon A[x] \longrightarrow (A/I)[x]$ definita da $\varphi\left(\sum_i a_i x^i\right) = \sum_i \overline{a_i} x^i$. È facile verificare che φ è un omomorfismo ed è 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. Dunque 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.

Soluzione E. 8.9. Dato un polinomio $f = \sum_{i=0}^n f_i x^i \in A[x]$, denotiamo con $I(f) = (f_0, \dots, f_n)$ l'ideale di A generato dai coefficienti di f.
Se fg è primitivo allora $(1) = I(fg) \subseteq I(f)I(g)$, da cui $I(f) = I(g) = (1)$.

Viceversa, siano $f = \sum_{i=0}^n f_i x^i$ e $g = \sum_{j=0}^m g_j x^j$ polinomi primitivi e sia $h = fg = \sum_{l=0}^t h_l x^l$. Se $I(h)$ è un ideale proprio di A allora esiste un ideale massimale $\mathfrak{m} \supseteq I(h)$; d'altra parte, per ipotesi, esistono f_i e g_j che non appartengono a $\mathfrak{m}$. Siano r e 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 ottiene $f_r g_s \in \mathfrak{m}$, che è assurdo.

Alternativamente, si può argomentare nel seguente modo: se $\mathfrak{m} \supseteq I(h)$ allora $h \in \mathfrak{m}[x]$ e $\overline{fg} = \overline{h} = \overline{0}$ in $A[x]/\mathfrak{m}[x]$, che è un dominio perché isomorfo a $(A/\mathfrak{m})[x]$, cf. **E.8.8**. Pertanto si ha $\overline{f} = \overline{0}$ oppure $\overline{g} = \overline{0}$, cioè $\mathfrak{m} \supseteq I(f)$ oppure $\mathfrak{m} \supseteq I(g)$, che è contro l'ipotesi.

Soluzione E. 8.10. Per la caratterizzazione degli anelli locali **T.1.16**, 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 $(\mathcal{J}(A), a) = (b)$ dove $b \notin \mathcal{J}(A)$. Da questo segue che $x = by$ per qualche $y \in A$. Poiché $\mathcal{J}(A)$ è un ideale primo e $b \notin \mathcal{J}(A)$, deve essere $y \in \mathcal{J}(A)$; quindi $y = cx$ per qualche $c \in A$. Otteniamo dunque $x = by = bcx$ e pertanto $x(1 - bc) = 0$.
Usando iii) deduciamo che $1 - bc \in \mathcal{J}(A)$; di conseguenza $bc = 1 - (1 - bc)$ è invertibile per **T.1.15** e quindi anche b lo è. Allora $(\mathcal{J}(A), a) = (1)$ ed esiste dunque $s \in A$ tale che $1 - sa \in \mathcal{J}(A)$; ragionando come prima otteniamo che a è invertibile, come volevamo.

Soluzione E. 8.11. 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 $m=cd$ e supponiamo che c non sia invertibile. Se $(m)=(d)$ allora, per il punto precedente, esiste $u\in A^*$ tale che $d=um$ e quindi $m(1-uc)=0$; dato che $c\in\mathfrak{m}$, si ha $1-uc\in A^*$ e infine $m=0$, che contraddice l'ipotesi. Dunque $(m)\subsetneq(d)$ e dalla massimalità di (m) segue che $(d)=A$; abbiamo quindi mostrato che d è invertibile e m è irriducibile.

Soluzione E. 8.12. Siano $a\in I$ e $b\in J$ 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. 8.13. 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. 8.14. 1. Possiamo scrivere $2a=(2a)^2=4a^2=4a$, da cui $2a=0$.

2. Per ipotesi $A/\mathfrak{p}$ è un dominio e sia $\overline{a}\neq\overline{0}$ in $A/\mathfrak{p}$. Dato che $\overline{a}^2=\overline{a^2}=\overline{a}$, abbiamo $\overline{a}=\overline{1}$ 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 $b=b(a+b-ab)$. Quindi $(a,b)=(a+b-ab)$ e la tesi segue subito.

Soluzione E. 8.15. Chiaramente A è un dominio perché (0) è primo.
Sia $b\in A$ un elemento non invertibile; allora (b^2) è primo, dunque $b\in(b^2)$ e $b=ab^2$ per qualche $a\in A$. Dato che b non è invertibile, si ha $ab\neq1$ e da $b(1-ab)=0$ segue che $b=0$; ciò mostra che A è un campo.

Soluzione E. 8.16. 1. Per ogni $m,\,n\in\mathbb{Z}$ esistono $\alpha,\beta\in\mathbb{Z}$ tali che $\alpha m+\beta n=\gcd(m,n)$ e questo mostra che $(m,n)\supseteq(\gcd(m,n))$.

Per l'altra inclusione basta osservare che $\gcd(m,n)$ divide m e n, 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 $\operatorname{lcm}(m,n)\mid a$.

Per l'altra inclusione, basta osservare che m ed n dividono $\operatorname{lcm}(m,n)$, per cui $\operatorname{lcm}(m,n)\in I\cap J$.

3. Dato che $IJ=(ij\colon\ i\in I,\ j\in J)$ è l'ideale generato dai prodotti, avremo sicuramente che $mn\in IJ$.

Per l'altra inclusione, sia $a\in IJ$; allora $a=\sum_{h=1}^{r}a_h(\alpha_h m)(\beta_h n)$ per certi interi a_h, α_h e β_h. Pertanto possiamo scrivere a come $(\sum_{h=1}^{r}a_h\alpha_h\beta_h)mn\in(mn)$.

4. Osserviamo intanto che $I\colon J=(m)\colon(n)$ è l'insieme degli elementi $a\in A$ tali che $an\in(m)$. Chiaramente $n\cdot\frac{m}{\gcd(m,n)}$ è multiplo di m, per cui vale $\supseteq$.

Per l'altra inclusione scriviamo $m=m'\gcd(m,n)$ e $n=n'\gcd(m,n)$; allora $a\in I\colon J$ implica che an' è multiplo di m'.

5. Per il Teorema fondamentale dell'Aritmetica possiamo scrivere ogni $d \in \mathbb{Z}$ come $d = \pm \prod_{p \in \mathbb{N},\, p \text{ primo}} p^{d_p}$, dove $d_p = 0$ per quasi ogni p.
Usando i punti 1 e 2 si vede che la tesi è equivalente a provare 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 1, 2 e 3 abbiamo che

$$(I+J)(I \cap J) = (\gcd(m,n)\operatorname{lcm}(m,n)) = (mn) = IJ.$$

Soluzione E. 8.17. I punti 1 e 2 seguono immediatamente dalla definizione di ideale quoziente.

3. Si ha $a \in (I\colon J)\colon H$ se e solo se $aH \subseteq I\colon J$. Dunque se e solo se $aHJ \subseteq I$, ovvero 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 $a \in I_\alpha\colon J$ per ogni α.

5. Se $a\sum_\alpha I_\alpha \subseteq I$ allora $aI_\alpha \subseteq a\sum_\alpha I_\alpha \subseteq I$ per ogni α, il che prova $\subseteq$.
Per l'altra inclusione, se $aI_\alpha \subseteq I$ per ogni α allora, dato un qualsiasi $b = \sum_\alpha j_\alpha$, dove la somma è finita e $j_\alpha \in I_\alpha$ per ogni α, abbiamo $ab = \sum_\alpha aj_\alpha \subseteq I$ e anche l'altra inclusione è verificata.

Soluzione E. 8.18. Sia $g \in \frac{1}{f}(I \cap (f))$; allora $gf \in I$ ossia $g \in I\colon (f)$.
Viceversa, se $g \in I\colon (f)$ allora $gf \in I$ e quindi $gf \in I \cap (f)$. Dunque $g \in \frac{1}{f}(I \cap (f))$.

Soluzione E. 8.19. Per ipotesi $(\overline{f}, \overline{g}) = (\overline{1})$ in A/I e dunque $(\overline{fg}) = (\overline{f})(\overline{g}) = (\overline{f}) \cap (\overline{g})$ per **T.1.4**, che equivale alla tesi.

Soluzione E. 8.20. 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 $n \in \mathbb{N}$, abbiamo

$$1 = (ab+q)^n = abp + q^n \in I \cap J + H^n,$$

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 $j_1, j_2 \in H \cap J = I \cap J$ e $i \in I$ tali che $i + j_2 = h + j_1$. Dunque $h = i - j_1 + j_2 \in I$, come volevamo.

Soluzione E. 8.21. 1. Per induzione su n. L'affermazione è ovvia per $n = 1$.
Sia $n = 2$ e, 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 $n = 2$.

2. Basta prendere $H_i = J$ per ogni i e poi scambiare i ruoli di I e J.

Soluzione E. 8.22. 1. Sappiamo che $\sqrt{I} = (1)$ se e solo se $I = (1)$, cf. **T.1.6**.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 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. 8.23. 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 e b sono elementi tali che $a + b = 1$, con $a^m \in I$ e $b^n \in J$, allora

$$\begin{aligned} 1 &= (a+b)^{m+n} \\ &= a^m \sum_{i=0}^{n-1} \binom{m+n-i}{i} a^{n-i} b^i + b^n \sum_{i=n}^{m+n} \binom{m+n-i}{i} a^{m+n-i} b^{i-n} \in I + J \end{aligned}$$

e abbiamo concluso.

2. Dato che

$$I + \sqrt{J} \supseteq I + J,$$

passando ai radicali si ottiene la relazione $\supseteq$.

Per l'altra inclusione, sia $a \in \sqrt{I + \sqrt{J}}$; allora esiste $m \in \mathbb{N}$ tale che $a^m = i + j$, con $i \in I$ e $j \in \sqrt{J}$. Dato $n \in \mathbb{N}$ tale che $j^n \in J$ troviamo $a^{nm} = (i+j)^n = c + j^n$, con $c \in I$ e $j^n \in J$, e la conclusione segue subito.

Soluzione E. 8.24. Consideriamo gli ideali $I = (x^2 + y)$ e $J = (x^2 - y)$ in $\mathbb{Q}[x, y]$. Dato che $x^2 + y$ e $x^2 - y$ sono irriducibili in $\mathbb{Q}[x, y]$, si ha $\sqrt{I} = I$ e $\sqrt{J} = J$, quindi $\sqrt{I} + \sqrt{J} = (x^2, y)$, mentre $\sqrt{I + J} = (x, y)$.

Soluzione E. 8.25. Proviamo che $\sqrt{I} = (x)$, che è un ideale primo di A. Dato che $x^2 \in I$ abbiamo $(x) \subseteq \sqrt{I}$.

Per l'altra inclusione, se $a \in A$ è tale che $a^k \in I$ abbiamo $a^k = \alpha x^2 + \beta xy \in (x)$ per qualche $\alpha, \beta \in A$. Dalla primalità di (x) discende allora che $a \in (x)$. Rimane da mostrare che I non è primario; basta osservare che $x \notin I$ e $y^n \notin (x)$ per ogni $n \in \mathbb{N}$, mentre $xy \in I$.

Soluzione E. 8.26. L'inclusione $\mathcal{N}(A) \subseteq \mathcal{J}(A)$ è vera in generale.

Per l'altra inclusione, supponiamo per assurdo che $\mathcal{J}(A) \not\subseteq \mathcal{N}(A)$. Per ipotesi esiste allora un elemento $0 \neq a \in \mathcal{J}(A)$ idempotente, i.e. tale che $a(a-1) = 0$. Dato che $a \in \mathcal{J}(A)$, l'elemento $a - 1$ risulta invertibile e quindi $a = 0$, che fornisce la contraddizione cercata.

Soluzione E. 8.27. $1 \Rightarrow 2$. 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 $\overline{a} = \overline{0}$ 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. 8.28. Un elemento a appartiene a $\sqrt{\bigcup_\alpha E_\alpha}$ 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. 8.29. Dalle definizioni di divisore di zero e annullatore di un elemento si ha subito che

$$\mathcal{D}(A) = \bigcup_{0 \neq a \in A} \operatorname{Ann} a.$$

Visto che le operazioni di radicale e unione commutano per **E.8.28**, basta mostrare che $\mathcal{D}(A) = \sqrt{\mathcal{D}(A)}$.
Siano $0 \neq a \in \sqrt{\mathcal{D}(A)}$ e n il minimo intero tale che $a^n \in \mathcal{D}(A)$. Sia inoltre $b \neq 0$ tale che $a^n b = 0$. Dato che $a^{n-1} b \neq 0$ possiamo concludere che a è un divisore di zero.

Soluzione E. 8.30. 1. Indichiamo con π la proiezione $A \to A/\mathcal{J}(A)$. Se $a \in A$ è invertibile e b è il suo inverso allora $ab = 1$ e quindi $\overline{a}\overline{b} = \pi(a)\pi(b) = \pi(1) = \overline{1}$.

Viceversa, se $a \in A$ ed esiste $b \in A$ tale che $\overline{a}\overline{b} = \overline{1}$ allora si ha $1 - ab \in \mathcal{J}(A)$ e quindi $ab = 1 - (1 - ab)$ è invertibile in A, ovvero a è invertibile, come richiesto.

2. Sia $a \in \mathcal{J}(A)$ tale che $a^2 = a$; allora $1 - a$ è invertibile e quindi $a(1 - a) = 0$ implica che $a = 0$.

Soluzione E. 8.31. Per ipotesi $\overline{a}^2 = \overline{a}$ in A/I, ovvero $a(1 - a) \in I$. Poiché $a \in \mathcal{J}(A)$ si ha che $1 - a$ è invertibile e quindi $a \in I$.

Soluzione E. 8.32. Osserviamo che per ipotesi A non è un campo.
Supponiamo per assurdo che A possegga solo un numero finito di ideali massimali $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$. Per ogni $i = 1, \ldots, k$ sia a_i un elemento non nullo di $\mathfrak{m}_i$ e sia $a = \prod_i a_i$; allora $a \in \bigcap_i \mathfrak{m}_i = \mathcal{J}(A)$ e abbiamo che $1 - ab$ è invertibile per ogni $b \in A$. Ora, poiché A ha infiniti elementi ma solo un numero finito di invertibili, 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. 8.33. Ricordiamo che le operazioni in $A \times B$ sono definite componente per componente.
Dati I e J ideali di A e B rispettivamente, per ogni $(a, b) \in A \times B$ e per ogni $(i, j), (h, k) \in I \times J$, si ha

$$(i, j) - (h, k) = (i - h, j - k) \in I \times J \quad \text{e} \quad (a, b)(i, j) = (ai, bj) \in I \times J.$$

Questo implica che $I \times J$ è un 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 $H = I \times J$. 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 $(a,b) \in H$ allora $a = \pi_1(a,b) \in \pi_1(H)$ e $b = \pi_2(a,b) \in \pi_2(H)$, per cui $H \subseteq \pi_1(H) \times \pi_2(H)$.

Per l'altra inclusione, sia $(a,b) \in \pi_1(H) \times \pi_2(H)$; dunque esistono un $b_1 \in B$ tale che $(a,b_1) \in H$ e un $a_1 \in A$ tale che $(a_1,b) \in H$. Allora $(a,0) = (1,0)(a,b_1)$ e $(0,b) = (0,1)(a_1,b)$, e quindi anche $(a,b) = (a,0) + (0,b)$, sono elementi di H.

Notiamo che se $A, B \neq 0$ allora $A \times B$ non è un dominio visto che $(1_A,0)(0,1_B) = (0,0)$.

Sia $H = I \times J$ un ideale di $A \times B$ e consideriamo l'omomorfismo $f \colon A \times B \longrightarrow A/I \times B/J$ definito da $(a,b) \mapsto (\overline{a},\overline{b})$. 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, rispettivamente massimale, di A e J ideale primo, rispettivamente massimale, di B.

Soluzione E. 8.34. La prima affermazione è una semplice generalizzazione del caso $n = 2$, cf. **E.8.33**.
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, rispettivamente massimale, di A_j.

Soluzione E. 8.35. 1. Sia $A \simeq \prod_{i=1}^{n} K_i$ per qualche $n \in \mathbb{N}_+$ e con K_i campo per ogni i; allora per **E.8.34** 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 $\mathcal{J}(A) = \bigcap_{\mathfrak{m} \in \operatorname{Max} A} \mathfrak{m} = (0)$.

Viceversa, se A ha solo un numero finito di ideali massimali, 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 un prodotto diretto di campi.

2. Sia $A \simeq \prod_{i=1}^{n} K_i$ per qualche $n \in \mathbb{N}_+$ e con K_i campo per ogni i; allora un elemento nilpotente di A è del tipo $(a_1, \dots, a_n)$ 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. 8.36. Ricordiamo che la somma e il prodotto in una somma diretta di anelli sono definiti componente per componente, e che i suoi ideali sono tutti e soli somme dirette di ideali nelle singole componenti, cf. **E.8.34**.

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 $(a^2, \bar{b}^2, c^2) = (a, \bar{b}, c)$, quindi si deve avere $a, c \in \{0, 1\}$ 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 $\overline{0}$ e $\overline{1}$, 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 e H ideali di $\mathbb{Z}$, $\mathbb{Z}/(36)$ e $\mathbb{Q}$ rispettivamente e sono quindi tutti principali. Dunque A è a ideali principali, i.e. A è PIR, ma 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

i) $\mathfrak{p} = ((p, \overline{1}, 1))$, con p primo in $\mathbb{Z}$ o $p = 0$; oppure

ii) $\mathfrak{p} = ((1, \overline{q}, 1))$, con $\mathfrak{q} = (\overline{q})$ ideale primo di $\mathbb{Z}/(36)$, ossia con $q = 2$ o 3; oppure

iii) $\mathfrak{p} = ((1, \overline{1}, 0))$.

È immediato verificare che l'unico primo non massimale è quello generato da $(0, \overline{1}, 1)$.

Soluzione E. 8.37. 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 si ha

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} \in I \quad \text{e} \quad \frac{\alpha}{\beta}\frac{a}{b} = \frac{\alpha a}{\beta b} \in I, \quad \text{per ogni} \quad \frac{a}{b}, \frac{c}{d} \in I \quad \text{e} \quad \frac{\alpha}{\beta} \in A_{(p)}.$$

Inoltre $0 \in I$ e dunque I è un ideale di $A_{(p)}$.

Preso poi $\frac{\alpha}{\beta} \notin I$ abbiamo che $\alpha \not\equiv 0 \mod p$, 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.1.16**.

Infine, la mappa $f \colon A_{(p)} \longrightarrow \mathbb{Z}/(p)$ definita da $f\left(\frac{a}{b}\right) = \overline{a}\overline{b}^{-1}$ è un omomorfismo;

infatti

$$f\left(\frac{a}{b}+\frac{c}{d}\right)=f\left(\frac{ad+bc}{bd}\right)=\overline{(ad+bc)}\,\overline{bd}^{-1}=\overline{a}\overline{b}^{-1}+\overline{c}\overline{d}^{-1}=f\left(\frac{a}{b}\right)+f\left(\frac{c}{d}\right)$$

$$f\left(\frac{a}{b}\cdot\frac{c}{d}\right)=f\left(\frac{ac}{bd}\right)=\overline{ac}\,\overline{bd}^{-1}=\overline{a}\overline{b}^{-1}\overline{c}\overline{d}^{-1}=f\left(\frac{a}{b}\right)f\left(\frac{c}{d}\right),$$

per ogni $\frac{a}{b},\frac{c}{d}\in A_{(p)}$.
Per ogni $\overline{a}\in\mathbb{Z}/(p)$ si ha $f\left(\frac{a}{1}\right)=\overline{a}$, il che mostra che f è surgettivo.
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 gli insiemi

$$I_j=\left\{\frac{a}{b}\in A_{(p_1,\dots,p_n)}\colon\ a\equiv 0 \mod p_j\right\}$$

sono ideali di $A_{(p_1,\dots,p_n)}$ e che gli omomorfismi

$$f_j\colon A_{(p_1,\dots,p_n)}\longrightarrow\mathbb{Z}/(p_j),\qquad \frac{a}{b}\mapsto\overline{a}\overline{b}^{-1}$$

inducono isomorfismi

$$\widetilde{f_j}\colon A_{(p_1,\dots,p_n)}/I_j\longrightarrow\mathbb{Z}/(p_j),$$

al variare di $j\in\{1,\dots,n\}$.
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

$$\operatorname{Max} A_{(p_1,\dots,p_n)}=\{I_1,\dots,I_n\}.$$

Soluzione E. 8.38. Siano $A=\prod_{i=1}^n A_i$ con A_i anello semilocale per ogni i e $I=\prod_{i=1}^n I_i$ un ideale di A. Dato che $A/I=\prod_i A_i/I_i$, 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.8.37** è semilocale ma, essendo un dominio, non può essere un prodotto diretto non banale di anelli.

Soluzione E. 8.39. Proviamo la tesi dimostrando che se I è un ideale primo allora in A/I ogni elemento diverso da zero è invertibile.
Sia dunque $\overline{a}\in A/I\setminus\{\overline{0}\}$. Per ipotesi $\overline{a}(\overline{a}^{n-1}-1)=\overline{0}$; dato che A/I è un dominio, si ha subito la tesi.

Soluzione E. 8.40. 1. L'insieme Σ è non vuoto dato che $(0) \in \Sigma$.
Le catene di ideali di Σ sono superiormente limitate dall'unione degli ideali della catena, che è un ideale contenuto in $\mathcal{D}(A)$. Quindi, per il Lemma di Zorn, esiste in Σ un elemento massimale P.
Proviamo che P è primo. Siano $a, b \notin P$ e consideriamo gli ideali (P, a) e (P, b) che, per ipotesi, contengono propriamente P. Dunque 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. Osserviamo che se $a \neq 0$ allora $\operatorname{Ann} a \in \Sigma$. Dato che $\mathcal{D}(A) = \bigcup_{0 \neq a \in A} \operatorname{Ann} a$, possiamo scrivere $\mathcal{D}(A) \subseteq \bigcup_\alpha \mathfrak{p}_\alpha$, dove ogni $\mathfrak{p}_\alpha$ è un elemento massimale di Σ. Quindi, per il punto precedente, ogni $\mathfrak{p}_\alpha$ è un ideale primo.
Inoltre, tali $\mathfrak{p}_\alpha$ sono ideali di zero divisori; dunque ciascuno di essi è contenuto in $\mathcal{D}(A)$, e pertanto

$$\mathcal{D}(A) = \bigcup_{\mathfrak{p} \in \operatorname{Spec} A,\ \mathfrak{p} \text{ max in } \Sigma} \mathfrak{p}.$$

Soluzione E. 8.41. 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 (verificarlo!); pertanto dal Lemma di Zorn discende che Σ possiede un elemento massimale I.
Poiché I non è principale, I non è primo per ipotesi ed esistono $a, b \notin I$ 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'altra inclusione, sia $j \in I \subset (I, a) = (c)$; allora $j = ck$ con $k \in I \colon (c) = (d)$, i.e. $k = hd$ per qualche $h \in A$ e $j = hcd \in (cd)$, come volevamo.

Soluzione E. 8.42. 1. Se $a, b \in \operatorname{Ker} f$ allora $f(a) = f(b) = 0$; dunque $f(a-b) = f(a) - f(b) = 0$ e $f(ca) = f(c)f(a) = 0$ per ogni $c \in A$, i.e. $a - b$, $ca \in \operatorname{Ker} f$.
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, e questo è vero per la linearità di f. Lo stesso vale per il prodotto, dato che $f(a)f(b) = f(ab)$ per ogni $a, b \in A$. Infine $1_B = f(1_A) \in \operatorname{Im} f$.

Soluzione E. 8.43. Per definizione di omomorfismo dobbiamo avere $f(0) = 0$ e $f(1) = 1$. Se $n \in \mathbb{Z}_+$, abbiamo $f(n) = \underbrace{f(1) + \cdots + f(1)}_{n \text{ volte}} = nf(1) = n$, e se $n \in \mathbb{Z}_-$ allora $f(n) = f(-(-n)) = -f(-n) = -(-n) = n$.
In conclusione, per ogni $n \in \mathbb{Z}$, si ha $f(n) = n$, ovvero l'unico omomorfismo è l'identità.

Soluzione E. 8.44. 1. Consideriamo $\varphi_a \colon A[x] \longrightarrow A$, l'omomorfismo di sostituzione definito da $\varphi_a(f) = f(a)$; allora $J = \varphi_a^{-1}(I)$ ed è quindi un ideale di $A[x]$.

2. Componendo φ_a con la proiezione su A/I troviamo un omomorfismo surgettivo $\pi \circ \varphi_a \colon A[x] \longrightarrow A/I$ il cui nucleo è J. Allora $A[x]/J \simeq A/I$, da cui segue che J è primo se e solo se I lo è.

3. Si ha $\varphi_a(x-1) = \varphi_a(y-2) = y - 2 \in I$, quindi $(x-1, y-2) \subseteq J$. Dal momento che J è un ideale proprio, poiché ad esempio $x \notin J$, e $(x-1, y-2)$ è un ideale massimale, abbiamo $J = (x-1, y-2)$.

Soluzione E. 8.45. $1 \Rightarrow 2$. Sia A un campo e sia I un suo ideale. Se $I \neq 0$ allora esiste $0 \neq a \in I$ e tale elemento è invertibile. Pertanto $I = (a) = (1)$.

$2 \Rightarrow 1$. 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.

$2 \Rightarrow 3$. 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 $f(1_A) = 1_B$ implica $B = 0$, che abbiamo escluso. Deve quindi essere $\operatorname{Ker} f = (0)$.

$3 \Rightarrow 2$. 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 è iniettiva e dunque $\mathfrak{m} = \operatorname{Ker} \pi = 0$. Da ciò segue che (0) e (1) sono gli unici ideali di A.

Soluzione E. 8.46. 1. Il contenimento $\supseteq$ segue dal fatto che la somma di ideali contiene i suoi addendi.

Per l'altra inclusione, sia $a = \sum_{i=1}^n b_i f(a_i) \in (I_1 + I_2)^e$ con $b_i \in B$ e $a_i \in I_1 + I_2$ per ogni i. Per ogni i allora esistono $c_i \in I_1$ e $d_i \in I_2$ tali che $a_i = c_i + d_i$ e dunque

$$\begin{aligned} a &= \sum_{i=1}^n b_i f(c_i + d_i) = \sum_{i=1}^n b_i (f(c_i) + f(d_i)) \\ &= \sum_{i=1}^n b_i f(c_i) + \sum_{i=1}^n b_i f(d_i) \in I_1^e + I_2^e. \end{aligned}$$

2. Siano G e H insiemi di generatori di I_1 e I_2 rispettivamente. Allora

$$\begin{aligned} (I_1 I_2)^e &= (f(gh) \colon g \in G, h \in H) \\ &= (f(g)f(h) \colon g \in G, h \in H) \\ &= (f(g) \colon g \in G)(f(h) \colon h \in H) = I_1^e I_2^e. \end{aligned}$$

3. Segue immediatamente da $I_1 \cap I_2 \subseteq I_h$ per $h = 1, 2$.

4. Siano $a_1 \in J_1^c$ e $a_2 \in J_2^c$; allora $f(a_i) \in J_i$ per $i = 1, 2$ e, di conseguenza, $f(a_1 + a_2) = f(a_1) + f(a_2) \in J_1 + J_2$, cioè $a_1 + a_2 \in (J_1 + J_2)^c$.

5. Siano $a_1 \in J_1^c$ e $a_2 \in J_2^c$; allora $f(a_i) \in J_i$ per $i = 1, 2$ e, di conseguenza, $f(a_1 a_2) = f(a_1) f(a_2) \in J_1 J_2$, cioè $a_1 a_2 \in (J_1 J_2)^c$.

6. Il contenimento $\subseteq$ segue da $J_1 \cap J_2 \subseteq J_h$ per $h = 1, 2$.

Per l'altra inclusione, sia $a \in J_1^c \cap J_2^c$; allora $f(a) \in J_1$ e $f(a) \in J_2$, i.e. $f(a) \in J_1 \cap J_2$ e quindi $a \in (J_1 \cap J_2)^c$.

Vediamo adesso gli esempi.

Per 3 consideriamo l'omomorfismo di anelli $f\colon \mathbb{Z}[x, y] \longrightarrow \mathbb{Z}$ definito da $f(x) = 10$ e $f(y) = 15$; con $I_1 = (x)$ e $I_2 = (y)$ si ha

$$(I_1 \cap I_2)^e = (xy)^e = (150) \subsetneq (30) = (10) \cap (15) = I_1^e \cap I_2^e.$$

Per 4 consideriamo l'inclusione $\mathbb{Z} \longrightarrow \mathbb{Z}[x]$; con $J_1 = (x)$ e $J_2 = (x + 1)$ si ha

$$J_1^c + J_2^c = (0) + (0) = (0) \subsetneq \mathbb{Z} = (1)^c = (J_1 + J_2)^c.$$

Per 5 consideriamo l'inclusione $\mathbb{Z} \longrightarrow \mathbb{Z}[i]$ con i unità immaginaria e $J = (1 + i)$; allora $2i = (1 + i)^2$ e $i \in \mathbb{Z}[i]^*$, quindi $2 \in J^c$ e $J^2 = (2)$. Dato che (2) è massimale in $\mathbb{Z}$ e $J \subsetneq \mathbb{Z}[i]$, deve essere $J^c = (2)$. Quindi

$$J^c J^c = (2)(2) = (4) \subsetneq (2) = (2)^c = (JJ)^c.$$

Soluzione E. 8.47. 1. Dato che $I[x] \subseteq IA[x] = j(I)A[x]$, abbiamo $I[x] \subseteq I^e$.

Per l'altra inclusione, basta osservare che $I[x]$ è un ideale che contiene I; allora I^e, il più piccolo ideale di $A[x]$ che contiene I, è contenuto in $I[x]$.

2. Per **E.8.8** $A[x]/I[x] \simeq (A/I)[x]$, quindi $A[x]/I[x]$ è un dominio se e solo se A/I lo è.

3. In generale non è vero. Siano ad esempio $A = \mathbb{Z}$ e p primo; allora (p) è massimale in A, mentre

$$(p)[x] = (p)^e \subsetneq (p, x) \subsetneq A[x]$$

non è massimale.

Soluzione E. 8.48. 1. Sia $b \in f(\sqrt{I})$; allora $b = f(c)$ con $c^m \in I$ per qualche m. Dunque $b^m = f(c)^m = f(c^m) \in f(I)$, ossia $b \in \sqrt{f(I)}$. Quindi

$$(f(\sqrt{I})) \subseteq \sqrt{f(I)} \subseteq \sqrt{(f(I))},$$

come volevamo.

2. Per la surgettività di f si ha $f(I) = (f(I)) = I^e$ per ogni ideale I.

Abbiamo provato un'inclusione nel punto precedente; verifichiamo allora l'altra. Siano $b \in \sqrt{f(I)}$ e $m \in \mathbb{N}$ tali che $b^m = f(c)$ con $c \in I$. Per la surgettività di f, si ha $b = f(a)$ per qualche $a \in A$; dunque $f(a^m - c) = f(a^m) - f(c) = f(a)^m - f(c) = 0$, cioè $a^m - c \in \operatorname{Ker} f \subseteq I$. Allora $a^m \in I$, dunque $a \in \sqrt{I}$ e $b \in f(\sqrt{I})$.

3. Si ha $a \in \sqrt{f^{-1}(J)}$ se e solo se $a^m \in f^{-1}(J)$ per qualche $m \in \mathbb{N}$, cioè se e solo se $f(a)^m = f(a^m) \in J$ per qualche m. L'ultima affermazione equivale a $f(a) \in \sqrt{J}$, cioè $a \in f^{-1}(\sqrt{J})$.

Soluzione E. 8.49. Ricordiamo che $\mathbb{Z}[i]$ è un anello euclideo e quindi un PID. Sia p dispari; sappiamo che

$$p = a^2 + b^2 \quad \text{se e solo se} \quad p \equiv 1 \mod 4.$$

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 $a, b \in \mathbb{Z}$.

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.

Soluzione E. 8.50. Ovviamente $\frac{1-\zeta_p^a}{1-\zeta_p} = 1 + \zeta_p + \ldots + \zeta_p^{a-1} \in \mathbb{Z}[\zeta_p]$. Cerchiamo il suo inverso. Sia b tale che $ab \equiv 1 \mod p$; allora

$$\frac{1-\zeta_p}{1-\zeta_p^a} = \frac{1-\zeta_p^{ab}}{1-\zeta_p^a} = 1 + \zeta_p^a + \ldots + \zeta_p^{a(b-1)} \in \mathbb{Z}[\zeta_p].$$

Ricordiamo che gli elementi ζ_p^a con $a = 1, \ldots, p-1$ sono tutte e sole le radici del polinomio $1 + x + \ldots + x^{p-1}$, dunque $1 + x + \ldots + x^{p-1} = \prod_{a=1}^{p-1}(x - \zeta_p^a)$ e valutando in $x = 1$ otteniamo $p = \prod_{a=1}^{p-1}(1 - \zeta_p^a)$. Per quanto visto sopra $(1-\zeta_p) = (1-\zeta_p^a)$ per ogni $a = 1, \ldots, p-1$, dunque

$$(p)^e = p\mathbb{Z}[\zeta_p] = \left(\prod_{a=1}^{p-1}(1-\zeta_p^a)\right) = \prod_{a=1}^{p-1}(1-\zeta_p^a) = \prod_{a=1}^{p-1}(1-\zeta_p) = (1-\zeta_p)^{p-1}.$$

Soluzione E. 8.51. 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 quindi $f(\mathcal{N}(A)) \subseteq \mathcal{N}(B)$.

2. Sia $a \in \mathcal{J}(A)$; allora $1 - ba$ è invertibile per ogni $b \in A$. Ne segue 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 $A_{(2)} = \left\{\frac{a}{b} \in \mathbb{Q} \colon b \not\equiv 0 \mod 2\right\}$ abbiamo già verificato che è un sottoanello di $\mathbb{Q}$ e che l'ideale $(2) = \left\{\frac{a}{b} \in A_{(2)} \colon a \equiv 0 \mod 2\right\}$ è l'unico ideale massimale di $A_{(2)}$, cf. **E.8.37**.1. Consideriamo l'omomorfismo di inclusione di $A_{(2)}$ in $\mathbb{Q}$, che sicuramente è iniettivo e non surgettivo; allora $\mathcal{J}(\mathbb{Q}) = 0$ mentre $\mathcal{J}(A_{(2)}) = (2)$.

4. Consideriamo la proiezione $f \colon \mathbb{Z} \longrightarrow \mathbb{Z}/(4)$; in questo caso

$$f(\mathcal{J}(\mathbb{Z})) = (0) \subsetneq \mathcal{J}(\mathbb{Z}/(4)) = (2).$$

5. Siano A semilocale e $\mathfrak{m}_1, \dots, \mathfrak{m}_k$ i suoi ideali massimali. Osserviamo che, per **T.1.18**.3, $f(\mathfrak{m}_i)$ è un ideale massimale di B se $\mathfrak{m}_i \supseteq \operatorname{Ker} f$, altrimenti $f(\mathfrak{m}_i)$ è tutto B (verificarlo!). Dato che $\mathcal{J}(A) = \bigcap_{i=1}^k \mathfrak{m}_i = \prod_{i=1}^k \mathfrak{m}_i$ si ha

$$f(\mathcal{J}(A)) = f\left(\prod_{i=1}^k \mathfrak{m}_i\right) = \prod_{i=1}^k f(\mathfrak{m}_i) = \bigcap_{i=1}^k f(\mathfrak{m}_i) \supseteq \mathcal{J}(B).$$

Soluzione E. 8.52. 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.

Viceversa, supponiamo che A/I sia locale con ideale massimale $\overline{\mathfrak{m}}$ e sia $\mathfrak{m}$ la sua controimmagine in A. Preso $a \notin \mathfrak{m}$, dimostriamo che è a invertibile e quindi proviamo che A è locale con massimale $\mathfrak{m}$.
Dato che $\overline{a} \notin \overline{\mathfrak{m}}$, $\overline{a}$ è invertibile poiché A/I è locale. Esistono allora $b \in A$ e $i \in I$ tali che $ab = 1 + i$. Poiché $I \subseteq \mathcal{N}(A)$, da **E.8.4** segue che $1 + i$ è invertibile, da cui otteniamo la tesi.

Soluzione E. 8.53. 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 $1 - cd \in \mathcal{D}(A) \subseteq \mathcal{J}(A)$. Pertanto cd è invertibile, e, di conseguenza, lo è anche d.

Soluzione E. 8.54. Sia $(a, b) = (\delta)$; allora $\delta \mid a$, $\delta \mid b$ ed esistono $u, v \in A$ tali che $\delta = ua + vb$. Quindi, per ogni $c \in A$ che divide sia a che b, si ha $c \mid ua + vb = \delta$. Dunque, per definizione, $\delta = d$.

Sia adesso $A = \mathbb{Z}[x]$, 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 suo termine noto appartiene a $(3) \subsetneq (1)$.

Soluzione E. 8.55. È sempre vero che $I^2 + J^2 \subseteq (I + J)^2$.

Per l'altra inclusione, siano $I = (a)$, $J = (b)$ e $I + J = (d)$; abbiamo allora $\gcd(a, b) = d$ 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 $1 = \alpha a_1^2 + \beta b_1^2$, quindi

$$d^2 = d^2 \cdot 1 = \alpha a^2 + \beta b^2 \in I^2 + J^2.$$

Soluzione E. 8.56. Iniziamo osservando che l'ideale $\mathcal{J}(A)$ è primo. Infatti, se $ab \in \mathcal{J}(A)$ allora esiste $c \neq 0$ tale che $cab = 0$, da cui segue che a oppure b è un elemento di $\mathcal{D}(A) = \mathcal{J}(A)$.
Sia ora $\mathcal{J}(A) = (j)$, con $j \neq 0$; dimostriamo che $\mathcal{J}(A)$ è massimale. 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 $j = bc$ per qualche $c \in \mathcal{J}(A)$ poiché $\mathcal{J}(A)$ è primo. Possiamo scrivere $c = jd$ per qualche $d \in A$ ed ottenere $j(1 - bd) = bc - bc = 0$; quindi $1 - bd \in \mathcal{D}(A) = \mathcal{J}(A)$. Allora bd è invertibile e quindi b lo è, come volevamo.

Soluzione E. 8.57. 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 invertibili o elementi associati ad a, quindi gli unici ideali che contengono (a) sono (1) e (a). Dato che ogni ideale di A è 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. L'anello $K[x]$ è un PID per **T.1.27**. Dato che un elemento non nullo in un PID è primo se e solo se è irriducibile, la tesi segue dal punto 2, cf. anche **T.1.22** e **T.1.23**.

Soluzione E. 8.58. Sia $f = \prod_i f_i$ con f_i irriducibili e distinti e siano F_i i campi $K[x]/(f_i)$ per ogni i. Per il Teorema cinese del resto $A = K[x]/\prod_i (f_i) \simeq \prod_i F_i$; pertanto $\mathcal{N}(A) \simeq \prod_i \mathcal{N}(F_i) = (0)$.

Viceversa, sia $f = \prod_i f_i^{s_i}$ con $s_i > 1$ per qualche i; allora la classe dell'elemento $\prod_i f_i$ è un elemento non nullo di $\mathcal{N}(A)$ e dunque l'anello A non è ridotto.

Soluzione E. 8.59. 1. Se f non è libero da quadrati allora esiste f_1 irriducibile tale che $f = f_1^e h$ con $e > 1$; si ha $f' = f_1^{e-1}(e f_1' h + f_1 h')$ e quindi $\gcd(f, f') \neq 1$.

Viceversa, sia g 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 $g \mid g'h$. Se $g' \neq 0$, allora $\deg g' < \deg g$; quindi $g \mid h$ e, di conseguenza, $g^2 \mid f$ e f ha un fattore multiplo.
D'altra parte, dato che 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 $r = s^p$.

2. Si ha che $\gcd(f, f') = 1$ in $K[x]$ se e solo se esistono $h, g \in K[x] \subseteq L[x]$ tali che $hf + gf' = 1$ e quindi $\gcd(f, f') = 1$ anche in $L[x]$.

Il viceversa è ovvio.

Soluzione E. 8.60. Riordinando le variabili possiamo supporre che $i_j = j$ per ogni j.
Sia $r = 1$. Per **E.8.58** l'ideale (h_1) è radicale in $K[x_1]$ e da **E.8.8** otteniamo

$$K[x_1, \dots, x_n]/(h_1) \simeq (K[x_1]/(h_1))\,[x_2, \dots, x_n] \simeq \left(\prod\nolimits_i F_i\right)[x_2, \dots, x_n],$$

dove $K \subseteq F_i$ sono estensioni di campi. Quindi $K[x_1, \dots, x_n]/(h_1)$ non ha nilpotenti non banali per **E.8.5**.2.
Sia ora $r = 2$ e consideriamo $K[x_1, \dots, x_n]/(h_1, h_2)$; abbiamo allora che

$$\begin{aligned} K[x_1, \dots, x_n]/(h_1, h_2) &\simeq (K[x_1]/(h_1))\,[x_2, \dots, x_n]/(h_2) \\ &\simeq \left(\prod\nolimits_i (F_i[x_2]/(h_2))\right)[x_3, \dots, x_n]. \end{aligned}$$

Per **E.8.59**.2 il polinomio h_2 è ancora libero da quadrati in $F_i[x_2]$ per ogni i e dunque $F_i[x_2]/(h_2) \simeq \prod_j F_{ij}$ è un prodotto di estensioni di F_i. Quindi

$$K[x_1,\dots,x_n]/(h_1,h_2) \simeq \left(\prod\nolimits_{i,j} F_{ij}\right)[x_3,\dots,x_n]$$

è ridotto. Iterando questo procedimento otteniamo la tesi.

Soluzione E. 8.61. 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 $\dfrac{x-\alpha_i}{\alpha_j-\alpha_i} + \dfrac{x-\alpha_j}{\alpha_i-\alpha_j} = 1$. Quindi se definiamo

$$L_i = \prod_{j\neq i} \frac{x-\alpha_j}{\alpha_i-\alpha_j}$$

otteniamo che $L_i \equiv 0 \mod I_j$ se $j \neq i$ e $L_i \equiv 1 \mod I_i$. Il polinomio cercato allora è dato da

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

Soluzione E. 8.62. Sia $f = \prod_{i=1}^{n} f_i$ con $f_i \in A$ 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 omomorfismo di anelli. Per **T.1.21**, esiste un isomorfismo $F\colon B \longrightarrow \prod_{i=1}^{n} A/(f_i)$, dove gli $A/(f_i)$ sono campi finiti che contengono $\mathbb{Z}/(p)$ per ogni i.
1. Sia $\overline{g} \in \operatorname{Ker}(\varphi_p - \mathrm{id}_B)$ e scriviamo $F(\overline{g}) = (\overline{g}_1,\dots,\overline{g}_n)$, 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 $\overline{g} \in \operatorname{Ker}(\varphi_p - \mathrm{id}_B)$ 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 $\operatorname{Ker}(\varphi_p - \mathrm{id}_B) \simeq (\mathbb{Z}/(p))^n$.
2. Sia ancora $\overline{g} \in \operatorname{Ker}(\varphi_p - \mathrm{id}_B)$ e sia g un suo rappresentante in A. Sia $F(\overline{g}) = (a_1,\dots,a_n) \in (\mathbb{Z}/(p))^n$; 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 $F(\overline{g-a}) = F(\overline{g}) - F(a) = (a_1-a,\dots,a_n-a)$ è nulla, cioè se e solo se $a_i = a$. Quindi

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

e la formula finale segue immediatamente.

Soluzione E. 8.63. 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 $a \mid p^k$ e, dato che A è 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. 8.64. 1. Per **T.1.23**.1 l'elemento p è irriducibile. Ora, se $ab \in (p^i)$ e $a \notin (p^i)$ allora $p \mid b$ per l'unicità della fattorizzazione e dunque $b \in (p) = \sqrt{(p^i)}$.
2. Siano $A = K[x,y]$ e $\mathfrak{q} = (x, y^2)$; allora $\sqrt{\mathfrak{q}} = (x,y)$ è massimale e $\mathfrak{q}$ è primario. Chiaramente $(x,y)^2 \subsetneq \mathfrak{q} \subsetneq (x,y)$ e quindi $\mathfrak{q}$ non è una potenza di (x,y) né di un altro ideale primo.
3. Dato che $B/\mathfrak{p} \simeq A/(x,z) \simeq K[y]$ l'ideale $\mathfrak{p}$ è primo, però $\mathfrak{p}^2$ non è primario. Infatti $\overline{xy} = \overline{z}^2 \in (\overline{x}^2, \overline{xz}, \overline{z}^2) = \mathfrak{p}^2$, ma $\overline{x} \notin \mathfrak{p}^2$ e $\overline{y}^k \notin \mathfrak{p}^2$ per ogni intero k.

Soluzione E. 8.65. Se A è un campo allora $A[x]$ è un anello euclideo, che è un PID per **T.1.27**.

Viceversa, consideriamo l'omomorfismo di sostituzione $\varphi_0 \colon A[x] \longrightarrow A$ dato dalla valutazione in 0, i.e. $\varphi_0(f) = f(0)$. È facile verificare che φ_0 è surgettivo e che $\operatorname{Ker}\varphi_0 = (x)$, da cui discende che $A[x]/(x) \simeq A$. Dato che, per ipotesi, $A[x]$ è un dominio, lo è anche A; quindi l'ideale (x) è primo e x è un elemento primo. Dato che $A[x]$ è un PID, x è irriducibile; dunque (x) è massimale, per **E.8.57**, e A è un campo.

Soluzione E. 8.66. Ricordiamo che la norma del numero complesso $\alpha = a + b\sqrt{-5}$ è data da $N(\alpha) = a^2 + 5b^2$; inoltre, dati $\alpha,\ \beta \in \mathbb{Z}[\sqrt{-5}]$, si ha $N(\alpha\beta) = N(\alpha)N(\beta)$. 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 $a + b\sqrt{-5},\ c + d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ tali che $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 3$. Passando alle norme, abbiamo $(a^2 + 5b^2)(c^2 + 5d^2) = 9$, 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

$$(3, 1 + \sqrt{-5}) \cap (3, 1 - \sqrt{-5}) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) = (3).$$

Dal momento che la norma di 3 non divide la norma di $1 + \sqrt{-5}$ e di $1 - \sqrt{-5}$, abbiamo $(3) \subsetneq (3, 1 + \sqrt{-5})$ e $(3) \subsetneq (3, 1 - \sqrt{-5})$, dunque (3) non è irriducibile.

Soluzione E. 8.67. Supponiamo per assurdo che esista un elemento $a_1 \in A$ non nullo e non invertibile 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 $a_2 b_1$, 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 $(a_1) \subsetneq (a_2) \subsetneq \dots$ che contraddice l'ipotesi.

Soluzione E. 8.68. 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 calcoli espliciti 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.
Alternativamente, possiamo osservare che $\overline{x}$ è irriducibile ma $(\overline{x})$ non è primo, cf. **T.1.25**, e lo stesso vale per $\overline{y}$, $\overline{z}$ e $\overline{t}$.

Soluzione E. 8.69. 1. Siano $b_1 = ax_1 - x_1$, $b_2 = ax_2 - x_2 \in I_a$ e $c \in A$; allora $0 \in I_a$, $b_1 + b_2 = a(x_1 + x_2) - (x_1 + x_2)$ 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 $a = ac - c$.

Viceversa, supponiamo $a = ac - c \in I_a$ e dobbiamo mostrare che per ogni $d \in A$ si ha $d \in I_a$. Abbiamo $ad \in I_a$ e, per definizione di I_a, anche $ad - d \in I_a$; dunque $d = ad - (ad - d) \in I_a$.

3. Se a è nilpotente allora $1 - a$ è invertibile e quindi a è quasi-regolare.

4. Sia $a \in A \setminus \{0, 1\}$; per ipotesi a è quasi regolare, allora $1 - a$ è invertibile. Dunque esiste $b \in A \setminus \{0\}$ tale che $b - ab = b(1 - a) = 1$, quindi $ab = b - 1$. Dato che $b \neq 1$ è quasi-regolare, $b - 1$ è invertibile, e da ciò discende che a invertibile, come volevamo.

Soluzione E. 8.70. 1. Dato che A non è un campo, ogni ideale massimale $\mathfrak{m}$ è non nullo; sia $a \in \mathfrak{m} \setminus \{0\}$. Per ipotesi, $(a) = \prod_{i=1}^{k} \mathfrak{m}_i^{s_i} = \bigcap_{i=1}^{k} \mathfrak{m}_i^{s_i}$ per certi ideali massimali distinti $\mathfrak{m}_i$ e interi positivi s_i, dove l'uguaglianza segue dal fatto che le potenze di ideali massimali distinti sono comassimali, cf. **E.8.21**.2. Dunque, $\bigcap_{i=1}^{k} \mathfrak{m}_i^{s_i} \subseteq \mathfrak{m}$; allora esiste i tale che $\mathfrak{m}_i^{s_i} \subseteq \mathfrak{m}$ e quindi, per la massimalità di $\mathfrak{m}$ e $\mathfrak{m}_i$, deve valere l'uguaglianza $\mathfrak{m}_i = \mathfrak{m}$. Ora basta porre

$$I = \mathfrak{m}_i^{s_i - 1} \cdot \prod_{j=1,\ j \neq i}^{k} \mathfrak{m}_j^{s_j}$$

per ottenere la tesi.

2. Per il punto 1, sia $I\mathfrak{m} = (a)$, con $a \neq 0$. Moltiplicando per J l'uguaglianza precedente, si ottiene che $J(a) = J\mathfrak{m}I = H\mathfrak{m}I = H(a)$. Dunque, 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 $J \subseteq H$. Scambiando i ruoli di J ed H si ottiene la tesi.

Soluzione E. 8.71. 1. Dato che $\sqrt{I} \subseteq \sqrt{I \colon J^m}$, basta provare l'altra inclusione.

Per ipotesi $J \not\subseteq \sqrt{I}$, pertanto esiste $j \in J$ tale che $j^n \notin I$ per ogni $n \in \mathbb{N}$. Sia $a \in \sqrt{I \colon J^m}$; allora $a^n j^m \in I$ per qualche $n \geq 1$. Visto che I è primario e $j^m \notin I$, si ha $a \in \sqrt{I}$, 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 $ah \in \sqrt{I} = I$, dunque $a \in I\colon h$.

Soluzione E. 8.72. 1. Se p è invertibile allora esiste q tale che $pq = 1$; quindi a_0 è invertibile.

Viceversa, supponiamo che a_0 sia invertibile e costruiamo l'elemento $q = \sum_{i\in\mathbb{N}} b_i x^i \in A[[x]]$ 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 $b_0 = {a_0}^{-1}$, $b_1 = -{a_0}^{-1} a_1 b_0$, …, $b_k = -{a_0}^{-1} \sum_{i=1}^{k} a_i b_{k-i}$. Abbiamo ottenuto una formula ricorsiva per il calcolo dei b_i in funzione dei coefficienti a_j, quindi 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 $p - a_0 = x \sum_{i\in\mathbb{N}_+} a_i x^{i-1}$ 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

$$p = (0,0,\ldots) + (0,2,0,\ldots)x + (0,0,2,\ldots)x^2 + \ldots \in A[[x]];$$

allora tutti i coefficienti di p sono nilpotenti e non è difficile verificare che p non è nilpotente.

3. Un elemento p appartiene a $\mathcal{J}(A[[x]])$ 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 ciò 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 ha $(\mathfrak{m}, x) = (1)$ ed esistono $f \in \mathfrak{m}$ e $h \in A[[x]]$ tali che $1 = f + xh = f_0$, dove 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 $\mathfrak{n} = \{a \in A\colon a \text{ termine noto di un elemento di } \mathfrak{m}\}$. È immediato verificare che $\mathfrak{n}$ è un ideale di A e, per quanto appena visto, $(\mathfrak{n}, x) \subseteq \mathfrak{m}$. Per definizione di $\mathfrak{n}$ si ha subito anche l'altra inclusione, dunque $\mathfrak{m} = (\mathfrak{n}, x)$. Da questo segue $\mathfrak{m}^c = \mathfrak{n}$. Infine $\mathfrak{n} = \mathfrak{m}^c$ è massimale perché l'omomorfismo di

sostituzione $\varphi_0 \colon A[[x]] \longrightarrow A$ definito da $x \mapsto 0$, composto con la proiezione $\pi \colon A \longrightarrow A/\mathfrak{n}$, è surgettivo e induce un isomorfismo

$$A[[x]]/\mathfrak{m} \simeq A/\mathfrak{n}.$$

Dunque $A/\mathfrak{n}$ è un campo.

Soluzione E. 8.73. 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 $i \in I$ e $h \in A$. Visto che $ig^m + hg^{2m} = ag^m \in I$, abbiamo $h \in I \colon (g^{2m})$. Per il punto precedente $h \in I \colon (g^m)$, e dunque $a \in I$.

Soluzione E. 8.74. 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 $\{\mathfrak{p}_\lambda\}_{\lambda \in \Lambda}$ una catena discendente di ideali primi. Se proviamo che $\mathfrak{p} = \bigcap_\lambda \mathfrak{p}_\lambda$ è un ideale primo la prima affermazione discende 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 $ab \in \mathfrak{p}_\lambda$ per ogni λ e supponiamo che $a, b \notin \mathfrak{p}$. Esistono allora $\alpha, \beta \in \Lambda$ tali che $a \notin \mathfrak{p}_\alpha$ e $b \notin \mathfrak{p}_\beta$. Possiamo supporre $\alpha \leq \beta$, cosicché $\mathfrak{p}_\alpha \supseteq \mathfrak{p}_\beta$ e $ab \notin \mathfrak{p}_\beta$, 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. 8.75. Sia $b \in A \setminus \{0\}$, 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 $a \in \mathfrak{p}$, come richiesto.

Soluzione E. 8.76. Dato che $63 = 3^2 7$, per **T.1.6**.7, possiamo scrivere $\sqrt{I} = \sqrt{(I, 9)} \cap \sqrt{(I, 7)}$. Abbiamo

$$(I, 9) = (9x^2 - y, 7y^2 + 2x + y, 9) = (y, 2x, 9) = (x, y, 9),$$

che è primario per **T.1.7**.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.1.6**.3 e 7, abbiamo anche

$$\begin{aligned}\sqrt{(I,7)} &= \sqrt{(x,2x+y,7)\cap(x+1,2x+y,7)}\\ &= \sqrt{(x,y,7)}\cap\sqrt{(x+1,y-2,7)}\\ &= (x,y,7)\cap(x+1,y-2,7),\end{aligned}$$

dove l'ultima uguaglianza segue dal fatto che gli ideali sotto il segno di radicale sono entrambi massimali.

1. Dalla discussione precedente, **T.1.14**, **E.8.74** e **T.1.12**.2 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) e (7) sono comassimali è facile vedere che $I=(I,7)(I,9)$. Visto che anche $(I,7)$ e $(I,9)$ sono comassimali 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 che anche (x) e $(x+1)$ sono comassimali, dunque $(x^2+x,2x+y,7) = (x,2x+y,7)(x+1,2x+y,7)$ e, nuovamente per il Teorema cinese del resto,

$$\begin{aligned}A/I &\simeq A/(x,y,9)\times A/(x+1,y-2,7)\times A/(x,y,7)\\ &\simeq \mathbb{Z}/(9)\times(\mathbb{Z}/(7))^2.\end{aligned}$$

3. Per quanto abbiamo visto nella discussione iniziale,

$$I\subseteq(x,y,9)\cap(x,y,7)\cap(x+1,y-2,7),$$

dove questi tre ideali sono primari e anche a due a due comassimali. Per **T.1.4**

$$(x,y,9)\cap(x,y,7)\cap(x+1,y-2,7) = (x,y,9)(x,y,7)(x+1,y-2,7)$$

ed è facile verificare che questo prodotto è contenuto in I, come volevamo.

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. 8.77. Ovviamente (0) è un ideale primo di $\mathbb{Z}[x]$. Sia $\mathfrak{p}\neq(0)$ un ideale primo di $\mathbb{Z}[x]$. Considerando l'inclusione $\mathbb{Z}\longrightarrow\mathbb{Z}[x]$, si ha che $\mathfrak{p}^c=\mathfrak{p}\cap\mathbb{Z}$ è ancora un ideale primo, dunque $\mathfrak{p}^c=(0)$ oppure $\mathfrak{p}^c=(p)$ per qualche primo p di $\mathbb{Z}$.
Se $\mathfrak{p}^c=(0)$ allora sia $f\in\mathfrak{p}\setminus\{0\}$ di grado minimo; dato che $\mathfrak{p}$ è primo, f deve essere irriducibile. Se esiste $g\in\mathfrak{p}\setminus(f)$ allora in $\mathbb{Q}[x]$ abbiamo che $\gcd(f,g)=1$ ed esistono r, $s\in\mathbb{Q}[x]$ tali che $rf+sg=1$. Moltiplicando per il minimo comune multiplo m dei denominatori dei coefficienti di r e s si ottiene $\tilde{r}f+\tilde{s}g=m$ per qualche $m\in\mathbb{Z}\setminus\{0\}$ e $\tilde{r}$, $\tilde{s}\in\mathbb{Z}[x]$, ma questo implica $m\in\mathfrak{p}\cap\mathbb{Z}=(0)$, contraddizione. Dunque, in questo caso, $\mathfrak{p}=(f)$ con f irriducibile in $\mathbb{Z}[x]$.

Se invece $\mathfrak{p}^c = (p)$ allora $\mathfrak{p} = (p)$ oppure esiste $g \in \mathfrak{p} \setminus (p)$ di grado minimo. Supponiamo che $\overline{g}$ sia riducibile in $\mathbb{Z}[x]/(p)$; allora esistono $f, h \in \mathbb{Z}[x]$ tali che $\overline{g} = \overline{f}\,\overline{h}$ e possiamo assumere che $\deg f = \deg \overline{f}$, $\deg h = \deg \overline{h}$ e che entrambi siano minori di $\deg \overline{g} = \deg g$. Dunque esiste $r \in \mathbb{Z}[x]$ tale che $fh = g + pr \in \mathfrak{p}$ e quindi $f \in \mathfrak{p}$ oppure $h \in \mathfrak{p}$, il che contraddice la minimalità del grado di g. Pertanto g deve essere irriducibile in $\mathbb{Z}[x]/(p)$; di conseguenza

$$\mathbb{Z}[x]/(p, g) \simeq (\mathbb{Z}/(p))[x]/(\overline{g})$$

è un campo e (p, g) è un ideale massimale contenuto in $\mathfrak{p}$, quindi uguale a $\mathfrak{p}$. Notiamo che questo è l'unico caso in cui si ottiene $\mathfrak{p}$ massimale.

17.2 Soluzioni del capitolo 9

Soluzione E. 9.1. Chiaramente una catena discendente non stazionaria è un sottoinsieme non vuoto di $\mathbb{N}^n$ che non ha minimo.

Viceversa, se $>$ non è un buon ordinamento, esiste un sottoinsieme non vuoto $V \subset \mathbb{N}^n$ che non ha elemento minimo. Quindi, dato un elemento $\mathbf{a}_1 \in V$, esiste $\mathbf{a}_2 \in V$ tale che $\mathbf{a}_1 > \mathbf{a}_2$ e, ragionando in questo modo, costruiamo una catena discendente infinita di elementi di $\mathbb{N}^n$.

Soluzione E. 9.2. Si tratta in tutti e tre i casi di ordinamenti totali su $\mathbb{N}^n$; infatti 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 $|\mathbf{a}| = |\mathbf{b}|$, ed 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 $\alpha_1 = \min\{a_1 \colon \mathbf{a} \in S\}$, cioè il minimo tra tutte le prime coordinate dei vettori di S. Definiamo $S_1 = \{\mathbf{a} \in S \colon a_1 = \alpha_1\}$ e consideriamo $\alpha_2 = \min\{a_2 \colon \mathbf{a} \in S_1\}$. Iterando il procedimento si arriva a trovare $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in S$ che è il minimo di S rispetto a lex.
Per deglex basta seguire lo stesso procedimento, con una riduzione preliminare da S a $S_0 = \{\mathbf{a} \in S \colon |\mathbf{a}| = \min\{|\mathbf{b}| \colon \mathbf{b} \in S\}\}$.
Per degrevlex usiamo la stessa riduzione precedente da S a S_0. Definiamo poi $\beta_n = \max\{c_n \colon \mathbf{c} \in S_0\}$, cioè il massimo tra le ultime coordinate dei vettori di S_0; tale massimo esiste perché il grado totale degli elementi di S_0 è fissato. Adesso definiamo $S_1' = \{\mathbf{a} \in S_0 \colon a_n = \beta_n\}$ e iteriamo il procedimento fino ad ottenere $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n)$ 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. 9.3. Per definizione di ordinamento monomiale, dobbiamo provare che $>$ è un buon ordinamento se e solo se $\mathbf{a} \geq 0$ per ogni $\mathbf{a} \in \mathbb{N}^n$. Se $>$ è un buon ordinamento allora esiste $\overline{\mathbf{a}}$ elemento minimo di $\mathbb{N}^n$. Se $0 > \overline{\mathbf{a}}$, allora abbiamo una catena discendente $0 > \overline{\mathbf{a}} > 2\overline{\mathbf{a}} > 3\overline{\mathbf{a}} > \dots$ infinita, contro l' ipotesi che $>$ sia un buon ordinamento, cf. **E.9.1**.

Viceversa, supponiamo che per ogni $\mathbf{a} \in \mathbb{N}^n$ valga $\mathbf{a} \geq 0$; siano $\Sigma \subset \mathbb{N}^n$ un sottoinsieme non vuoto e

$$E = \Sigma + \mathbb{N}^n = \{\mathbf{a} + \mathbf{b} \colon \mathbf{a} \in \Sigma, \mathbf{b} \in \mathbb{N}^n\}$$

l'$\mathcal{E}$-sottoinsieme generato dagli elementi di Σ. Dal Lemma di Dickson **T.2.3** segue che E ha una frontiera finita minimale $F = \{\mathbf{a}_1, \dots, \mathbf{a}_m\}$. Chiaramente $F \subseteq \Sigma$. Eventualmente riordinando gli elementi di F possiamo supporre che $\mathbf{a}_1 > \dots > \mathbf{a}_m$.
Dimostriamo ora che $\mathbf{a}_m$ è l'elemento minimo di Σ. Infatti, per ogni $\mathbf{b} \in E$ esistono $i \in \{1, \dots, m\}$ e $\mathbf{c} \in \mathbb{N}^n$ tali che $\mathbf{b} = \mathbf{a}_i + \mathbf{c}$; per ipotesi $\mathbf{c} \geq 0$, dunque $\mathbf{b} = \mathbf{a}_i + \mathbf{c} \geq \mathbf{a}_i \geq \mathbf{a}_m$, dove la prima disuguaglianza è data dall'ipotesi.

Soluzione E. 9.4. Fissiamo un ordinamento monomiale sull'insieme dei monomi nelle variabili $x_1, \dots, x_n$ e sia $G = \{g_1, \dots, g_s\}$ una base di Gröbner di $I \subseteq K[x_1, \dots, x_n]$ rispetto a tale ordinamento. Osserviamo che, per **T.2.10**, $g_1, \dots, g_s$ sono un insieme di generatori di I e, ovviamente, anche di I^e.
Vogliamo mostrare che $\mathrm{Lt}(I)^e = \mathrm{Lt}(I^e)$ sapendo che $\mathrm{Lt}(I)^e = \mathrm{Lt}(G)^e$.
Dato che ogni monomio di $\mathrm{Lt}(G)$ è certamente anche un elemento di $\mathrm{Lt}(I^e)$, si ha immediatamente $\mathrm{Lt}(I)^e \subseteq \mathrm{Lt}(I^e)$.

Per l'altra inclusione, fissiamo una base $\{e_\lambda\}_{\lambda \in \Lambda}$ di K' su K. Per ogni $f \in K'[x_1, \dots, x_n]$ possiamo scrivere $f = \sum_{\mathbf{a} \in \mathbb{N}^n} c_{\mathbf{a}} X^{\mathbf{a}}$, dove $X^{\mathbf{a}} = x_1^{a_1} \cdots x_n^{a_n}$ 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 $f_\lambda \in K[x_1, \dots, x_n]$. 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 $f_i \in K'[x_1, \dots, x_n]$ e $f_{i,\lambda} \in K[x_1, \dots, x_n]$; pertanto, per un certo λ_0, abbiamo $\mathrm{lt}(f) = \alpha h$, 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 abbia 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.

Alternativamente, per il Criterio di Buchberger tutti gli S-polinomi di $g_1, \dots, g_s$ riducono a 0; dunque anche gli S-polinomi di $g_1, \dots, g_s$, visti come elementi di $K'[x_1, \dots, x_n]$, riducono a 0. Ancora per il Criterio di Buchberger, questo implica che $\{g_1, \dots, g_s\}$ 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. 9.5. Dividendo f per $\{f_1, f_2\}$ si ottiene $f = x_1x_2f_1 + 0$ mentre dividendo per $\{f_2, f_1\}$ si ottiene $f = (x_1^2 + x_2)f_2 + x_2^3$; dunque il resto della divisione non è univocamente determinato.

Soluzione E. 9.6. 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 $f = f(x) = u_1(x, x, z)(z + x)$. Dunque $z + x$ divide f, che non è possibile, poiché f non contiene termini in cui è presente la z.

Per il secondo ordinamento, 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 $\mathrm{Lt}_{>_2}(I) \supsetneq (x, y) \supsetneq (x) = (\mathrm{lt}_{>_2}(g_1), \mathrm{lt}_{>_2}(g_2)) = \mathrm{Lt}_{>_2}(G)$.

Soluzione E. 9.7. 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.2.1**. Dunque, per ogni ordinamento $>$, $\mathrm{Lt}_>(I) = I$. Il suo insieme minimale di generatori $G(I)$ è una base di Gröbner minimale di I; dato che $G(I)$ costituito da monomi essa è chiaramente ridotta.

Viceversa, se vi è una base di Gröbner di I costituita da monomi, in particolare I possiede un insieme di generatori monomiale.

Soluzione E. 9.8. Verifichiamo che 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 $f_1 = x^2 - xy,\ f_2 = xz - y^2,\ f_3 = yz^2 - z^4$ 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 $G_1 = G_0 \cup \{f_4\}$.

$S_{14} = y^2f_1 - xf_4 = xy^3 - xy^3 = 0$.

$S_{24} = y^2f_2 - zf_4 = -y^4 + y^3z$,
che è ridotto rispetto a G_1. Poniamo $f_5 = y^4 - y^3z$ e $G_2 = G_1 \cup \{f_5\}$.

$S_{35} = y^3 f_3 - z^2 f_5 = y^3 z^3 - y^3 z^4 \xrightarrow{f_3} -z^{10} + z^9$,
che è ridotto rispetto a G_2. Poniamo $f_6 = z^{10} - z^9$ e $G_3 = G_2 \cup \{f_6\}$.

$S_{23} = yzf_2 - xf_3 = xz^4 - y^3 z \xrightarrow{f_2, f_3} yz^5 - y^3 z \xrightarrow{f_3} -y^3 z + z^7$,
che è ridotto rispetto a G_3. Poniamo $f_7 = y^3 z - z^7$ 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 $G_5 = (G_4 \cup \{f_{5'}\}) \setminus \{f_5\}$.
Continuiamo la costruzione con il criterio degli S-polinomi; possiamo osservare che sicuramente si ridurranno a 0 rispetto a G_5 tutti gli S-polinomi calcolati fino ad adesso e verificare che

$S_{26} = z^9 f_2 - x f_6 = xz^9 - y^2 z^9 \xrightarrow{f_2, f_3, f_6}_* 0$

$S_{27} = y^3 f_2 - x f_7 \xrightarrow{f_2, f_3, f_{5'}, f_3, f_6}_* 0.$

$S_{34} = xyf_3 - z^2 f_4 = -xyz^4 + y^3 z^2 \xrightarrow{f_2, f_3} z^9 - z^8 = f_{6'}$,
che è ridotto rispetto a G_5 e divide f_6. Poniamo $G_6 = (G_5 \cup \{f_{6'}\}) \setminus \{f_6\}$.
Dovremmo ripartire daccapo con il controllo degli S-polinomi; come osservato sopra, sicuramente S_{12}, S_{14}, S_{23}, S_{24}, S_3, $S_{27} \xrightarrow{G_6}_* 0$. Abbiamo poi

$S_{26'} \xrightarrow{f_2, f_3, f_{6'}}_* 0,$

$S_{35'} \xrightarrow{f_3, f_{6'}}_* 0,$

$S_{36'} \xrightarrow{f_3, f_{6'}}_* 0,$

$S_{37} \xrightarrow{f_3}_* 0,$

$S_{45'} \xrightarrow{f_2, f_{5'}, f_3, f_{6'}}_* 0,$

$S_{47} \xrightarrow{f_2, f_{5'}, f_3, f_{6'}}_* 0,$

$S_{5'7} \xrightarrow{f_3, f_{6'}}_* 0,$

$S_{6'7} \xrightarrow{f_3, f_{6'}}_* 0.$

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.2.16**. 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 $G_6 = G$ è la base cercata e, per costruzione, risulta già essere ridotta.

Soluzione E. 9.9. 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 $f \xrightarrow{G}_* -9z \neq 0$ si ha $f \notin I$.
Alternativamente, si può osservare che $(-2, 1, 1) \in \mathbb{V}(I)$ ma $f(-2, 1, 1) = -9$.

Soluzione E. 9.10. 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. 9.11. 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.2.24**. Sia dunque $H = G \cup \{f\}$; dato che

$$\begin{aligned}
S(f_1, f) \xrightarrow{G} x^2 + x &= -(f_1 - x^2 f + f_3) = g_1,\\
S(f_2, f) \xrightarrow{G\cup\{g_1\}} 2x + 1 &= f_2 - yf + 2xf - g_1 + f\\
&= f_2 - (y - 2x - 1)f - g_1 = g_2,\\
S(g_1, g_2) \xrightarrow{G\cup\{g_1,g_2\}} -\tfrac{1}{2} &= 2g_1 - xg_2 - \tfrac{1}{2}g_2\\
&= 2g_1 - (x + \tfrac{1}{2})g_2,
\end{aligned}$$

possiamo concludere che $1 \in (I, f)$ e $\overline{f}$ è invertibile in $\mathbb{Q}[x,y]/I$.

Per calcolare il suo inverso procediamo a ritroso, ottenendo

$$\begin{aligned}
1 &= (-2)\cdot\left(-\tfrac{1}{2}\right) = -2\left(2g_1 - \left(x + \tfrac{1}{2}\right)g_2\right)\\
&= -2\left[2\left(x^2 f - f_1 - f_3\right) - \left(x + \tfrac{1}{2}\right)\left((2x - y + 1)f + f_2 - g_1\right)\right] =\\
&= -2\left[f\left(2x^2 - \left(x + \tfrac{1}{2}\right)(2x - y + 1)\right) + \left(x + \tfrac{1}{2}\right)\left(x^2 f - f_1 - f_3\right) + h_1\right]\\
&= f(-2x^3 - 2xy - x^2 - y + 4x + 1) + h_2\\
&= f(-2xy - x^2 + y + 1) + h_3,
\end{aligned}$$

dove $h_1, h_2, h_3 \in I$ e, nell'ultima uguaglianza, abbiamo ridotto il coefficiente di f modulo I sommandogli $2f_3$. Dunque

$$\overline{f}^{-1} = \overline{-2xy - x^2 + y + 1}.$$

Soluzione E. 9.12. 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 relazioni

$$S(f_1, f_2) = zf_1 - xyf_2 = -f_3,$$

$$S(f_2, f_3) = y^2 f_2 - z f_3 = f_4 = y^2 f_2 + z^2 f_1 - xyz f_2 = z^2 f_1 + (-xyz + y^2) f_2.$$

Dunque la matrice M associata al passaggio tra i due insiemi di generatori tale che $M(f_1, f_2)^{\mathrm{t}} = (f_1, f_2, f_3, f_4)^{\mathrm{t}}$ è

$$M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ -z & xy \\ z^2 & -xyz + y^2 \end{pmatrix}.$$

3. Come è ben noto i coefficienti della divisione di f per G non sono unici. Osserviamo subito che $f = y^2 f_2 = 0f_1 + y^2 f_2 + 0f_3 + 0f_4 = 0f_1 + y^2 f_2$.
D'altra parte, possiamo anche scrivere $f = 0f_1 + 0f_2 + zf_3 + f_4$ e, per risalire ai coefficienti rispetto a f_1, f_2, basta usare la matrice di passaggio trovata al punto precedente:

$$M^{\mathrm{t}} \begin{pmatrix} 0 \\ 0 \\ z \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ y^2 \end{pmatrix}.$$

Una terza scrittura possibile (ne esistono infinite, perché?) è $f = yf_1 - zf_2 - (x - z)f_3 + f_4$, che fornisce coefficienti rispetto ai generatori iniziali dati da

$$M^{\mathrm{t}} \begin{pmatrix} y \\ -z \\ -x + z \\ 1 \end{pmatrix} = \begin{pmatrix} xz + y \\ -x^2 y + y^2 - z \end{pmatrix}.$$

Soluzione E. 9.13. 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.2.25** segue che $I \cap \mathbb{C}[y] = (y^3 - y)$.

Soluzione E. 9.14. Abbiamo delineato una strategia da seguire in **T.2.26**.2; per brevità scriviamo $g_1 = x(x + y)^2$, $g_2 = y$, $f_1 = x^2$ e $f_2 = x + y$. Per **E.8.17**.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.2.6**.3.
Per determinare $I : (f_2)$, grazie a **E.8.18**, possiamo calcolare $\frac{1}{f_2}(I \cap (f_2))$ utilizzando **T.2.26**.
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 questa base otteniamo

$$\frac{1}{x+y}(I \cap (f_2)) = \frac{1}{x+y}(x^3+y^3, xy+y^2) = (x^2-xy+y^2, y) = (x^2, y).$$

Pertanto $I : J = (x,y) \cap (x^2,y) = (x^2,y)$.

Soluzione E. 9.15. Usando due volte **T.1.6.7** 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 per l'ipotesi sulla caratteristica.
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 $f \neq 0$ è ridotto rispetto a tale base.

Soluzione E. 9.16. 1. 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 e scrivere $I = (f_1, f_2, f_3)$, con $f_1 = z^4, f_2 = x^2+y^2+z^2-1, f_3 = xy-2$.
Rispetto all'ordinamento lessicografico con $x > y > z$ 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

$$G = \{f_1, \tfrac{1}{2}f_4, f_5\}$$

è una base di Gröbner di I, che risulta essere ridotta.
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 $\mathbb{V}(I+J) = \emptyset$ risolvendo il sistema calcolato nel primo punto, i.e. $f_1 = f_4 = f_5 = 0$, e verificando che nessuna soluzione soddisfa le equazioni di J.
Alternativamente si può osservare che $z \in \sqrt{I+J}$, quindi il polinomio $g_1 = 3x^3 - 2 \in \sqrt{I+J}$. Allora anche $y^3g_1 = 3x^3y^3 - 2y^3 \in \sqrt{I+J}$. Usando il polinomio $xy-2$ si ottiene che $2y^3 - 24 \in \sqrt{I+J}$. Poichè $z \in \sqrt{I+J}$ abbiamo anche $1 = \gcd(y^3-12, f_5 - y^2z^2) \in (y^3-12, f_5-y^2z^2) \subseteq \sqrt{I+J}$ e la tesi segue.

Soluzione E. 9.17. Fissiamo l'ordinamento lessicografico con $x > y > a$ e scriviamo

$$I = (f_1 = x + y - a,\ \ f_2 = x^2 + y^2 - a^2,\ \ f_3 = x^3 + y^3 - a^5).$$

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

$$I = (f_1,\ f_4,\ f_3).$$

Riduciamo poi $f_3 \xrightarrow{f_1, f_4}_* -a^5 + a^3$ e poniamo $f_5 = a^5 - a^3$. Abbiamo che $I = (f_1, f_4, f_5)$; ora questi generatori formano una base di Gröbner perché i loro leading monomials x, y^2 e a^5 sono coprimi, cf. **T.2.16**.

Osserviamo 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.3.17**. Troviamo dunque le soluzioni del sistema triangolare superiore $f_1 = f_4 = f_5 = 0$, che è equivalente a quello originario, e otteniamo

a) se $a = 0$ esiste solo la soluzione $(0, 0)$;

b) se $a = -1$ esistono due soluzioni, $(-1, 0)$ e $(0, -1)$;

c) se $a = 1$ esistono due soluzioni, $(1, 0)$ e $(0, 1)$.

Soluzione E. 9.18. 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

$$\begin{aligned}\sqrt{I} &= \sqrt{(x^2y, z)} \cap \sqrt{(x^2y + xz + yz, xyz^2, xz^3 + yz^3, y^2)} \\ &= (xy, z) \cap (xz, y) = (x, z) \cap (y, z) \cap (x, y) = (xy, xz, yz).\end{aligned}$$

3. Dato che $x^2y^3, y^3z \xrightarrow{G}_* 0$, abbiamo $J = (x^2y^3, y^3z) \subseteq I$. Analogamente, per ogni $g \in G$, abbiamo $g \xrightarrow{x^2,\, z}_* 0$ e dunque $I \subseteq (x^2, z)$. Dato che

$$\begin{aligned}\mathrm{Lt}(J) = (x^2y^3, y^3z) &\subsetneq \mathrm{Lt}(I) = \mathrm{Lt}(G) \\ &= (x^2y, xyz^2, xz^3, y^2z) \subsetneq (x^2, z) \\ &= \mathrm{Lt}(x^2, z),\end{aligned}$$

le inclusioni sono strette, i.e. $J \subsetneq I \subsetneq (x^2, z)$.

Soluzione E. 9.19. 1. Siano $\alpha_1, \dots, \alpha_m \in \overline{K}$ le radici di f. Da **T.3.9** segue subito

$$\begin{aligned}\operatorname{Ris}(f, g_1\, g_2) &= a_m^{\deg g_1 + \deg g_2} \prod_{i=1}^{m} g_1(\alpha_i) g_2(\alpha_i) \\ &= \left(a_m^{\deg g_1} \prod_{i=1}^{m} g_1(\alpha_i) \right) \left(a_m^{\deg g_2} \prod_{i=1}^{m} g_2(\alpha_i) \right) \\ &= \operatorname{Ris}(f, g_1) \operatorname{Ris}(f, g_2).\end{aligned}$$

2. Ancora per **T.3.9**, si ha

$$\begin{aligned}\operatorname{Ris}(f, g_1 f + g_2) &= a_m^N \prod_{i=1}^{m} (g_1 f + g_2)(\alpha_i) \\ &= a_m^N \prod_{i=1}^{m} g_2(\alpha_i) = a_m^{N - \deg(g_2)} \operatorname{Ris}(f, g_2).\end{aligned}$$

Soluzione E. 9.20. Gli enunciati sono conseguenze di **T.3.9**.
Siano $f = a_m \hat{f}$ e $g = b_n \hat{g}$, con $\hat{f} = \prod_{i=1}^{m} (x - \alpha_i)$ e $\hat{g} = \prod_{j=1}^{n} (x - \beta_j)$.

1. $$\begin{aligned}\operatorname{Ris}_y(f(x-y), g(y)) &= (-1)^{mn} b_n^m \prod_{j=1}^{n} f(x - \beta_j) \\ &= (-1)^{mn} a_m^n b_n^m \prod_{j=1}^{n} \hat{f}(x - \beta_j) \\ &= (-1)^{mn} a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (x - (\alpha_i + \beta_j)).\end{aligned}$$

2. $$\begin{aligned}\operatorname{Ris}_y(f(x+y), g(y)) &= (-1)^{mn} a_m^n b_n^m \prod_{j=1}^{n} \hat{f}(x + \beta_j) \\ &= (-1)^{mn} a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (x - (\alpha_i - \beta_j)).\end{aligned}$$

3. $$\begin{aligned}\operatorname{Ris}_y\left(y^m f\left(\frac{x}{y}\right), g(y) \right) &= (-1)^{mn} b_n^m \prod_{j=1}^{n} \beta_j^m f\left(\frac{x}{\beta_j}\right) \\ &= (-1)^{mn} a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} \beta_j \left(\frac{x}{\beta_j} - \alpha_i\right) \\ &= (-1)^{mn} a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (x - \alpha_i \beta_j).\end{aligned}$$

4. $$\begin{aligned}\operatorname{Ris}_y(f(xy), g(y)) &= (-1)^{mn} b_n^m \prod_{j=1}^{n} f(x\beta_j) \\ &= (-1)^{mn} a_m^n b_n^m \prod_{i=1}^{m}\prod_{j=1}^{n}(x\beta_j - \alpha_i) \\ &= (-1)^{mn} a_m^n b_n^m \prod_{i=1}^{m}\prod_{j=1}^{n}\beta_j(x - \frac{\alpha_i}{\beta_j}),\end{aligned}$$

poiché $g(0) \neq 0$ implica $\beta_j \neq 0$ per ogni j.

Soluzione E. 9.21. Per **E.9.19**.1 si ha

$$\operatorname{Ris}(f, x^k g) = \operatorname{Ris}(f, x^k)\operatorname{Ris}(f, g) = (\operatorname{Ris}(f, x))^k \operatorname{Ris}(f, g).$$

D'altra parte abbiamo $\operatorname{Ris}(f, x) = (-1)^{\deg f} f(0)$ per **T.3.9**.1, e 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. 9.22. 1. Grazie a **T.3.7** sappiamo che $(p) \subseteq (f, g) \cap \mathbb{Z}$. Dato che (p) è massimale basta provare che $(f, g) \neq (1)$.
Supponiamo per assurdo che esistano $a, b \in A$ tali che $af + bg = 1$, allora $\overline{a}\,\overline{f} + \overline{b}\,\overline{g} = \overline{1}$ 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 $\operatorname{Syl}(f, g)$. Abbiamo dunque $\operatorname{Ris}(\overline{f}, \overline{g}) = \overline{\operatorname{Ris}(f, g)} = \overline{0}$ e questo contraddice $\gcd(\overline{f}, \overline{g}) = \overline{1}$ per **T.3.9**.4.

2. Calcoliamo

$$\operatorname{Ris}(f, g) = \det \begin{pmatrix} 1 & -4 & 1 & 0 \\ 0 & 1 & -4 & 1 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix} = -2.$$

Per il punto precedente allora $I \cap \mathbb{Z} = (2)$; inoltre $I = I + (2) = (x - 1, 2)$ e dunque $A/I \simeq \mathbb{Z}/(2)$.

Soluzione E. 9.23. Sia $r = \operatorname{Ris}(f, f') \in \mathbb{Z}$; dato che $\gcd(f, f') = 1$, da **T.3.9**.4 segue che $r \neq 0$ ed esistono polinomi $a, b \in \mathbb{Z}[x]$ tali che $af + bf' = r$, cf. **T.3.7**. Rileggendo questa ultima uguaglianza modulo p, con p primo di $\mathbb{Z}$ che non divide r, otteniamo $\overline{a}\,\overline{f} + \overline{b}\,\overline{f'} = \overline{r}$ in $(\mathbb{Z}/(p))[x]$, cioè $\gcd(\overline{f}, \overline{f}') = 1$. Quindi $(\mathbb{Z}/(p))[x]/(\overline{f})$ è ridotto per **E.8.58** e **E.8.59**.1.

Soluzione E. 9.24. La base di Gröbner ridotta rispetto all'ordinamento lessicografico con $x > y > z$ è

$$\{x - yz,\ yz^2 - y\};$$

quindi si ha $\sqrt{I} = (x, y) \cap (x + y, z + 1) \cap (x - y, z - 1)$ e

$$\mathbb{V}(I) = \mathbb{V}(\sqrt{I}) = \mathbb{V}(x, y) \cup \mathbb{V}(x + y, z + 1) \cup \mathbb{V}(x - y, z - 1).$$

Sia K infinito e sia $f \in \mathbb{I}(\mathbb{V}(x,y))$; allora possiamo scrivere

$$f = xg(x,y,z) + yh(y,z) + r(z)$$

e $f(0,0,a) = r(a) = 0$ per ogni $a \in K$ implica $r(z) = 0$, cioè $f \in (x,y)$. Dato che l'altra inclusione è ovvia, si ha che $\mathbb{I}(\mathbb{V}(x,y)) = (x,y)$ è primo e quindi $\mathbb{V}(x,y)$ è irriducibile per **T.3.3**.

Per le altre due componenti $\mathbb{V}(x \pm y, z \pm 1) = \{(a, \mp a, \mp 1) \colon a \in K\} \subset K^3$ la dimostrazione è analoga, osservando che ogni $f \in \mathbb{I}(\mathbb{V}(x \pm y, z \pm 1))$ si può scrivere $f = (z \pm 1)g(x,y,z) + (x \pm y)h(x,y) + r(y)$. Di nuovo $0 = f(a, \mp a, \mp 1) = r(\mp a)$ per infiniti valori di a implica $r = 0$.

Sia ora K finito; ovviamente $\mathbb{V}(x,y) = \{(0,0,a) \colon a \in K\} \subset K^3$ si decompone ulteriormente come unione finita di $|K|$ punti che sono le sue componenti irriducibili. Lo stesso vale per $\mathbb{V}(x \pm y, z \pm 1)$.

Soluzione E. 9.25. 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. Abbiamo

$$\begin{aligned}\sqrt{I} &= \sqrt{(x^2 - zt, y - zt, t)} \cap \sqrt{(x^2 - zt, y - zt, zt - 1)} \\ &= (x,y,t) \cap (x+1, y-1, zt-1) \cap (x-1, y-1, zt-1).\end{aligned}$$

Gli ideali di questa decomposizione sono primi e quindi determinano le componenti irriducibili di $\mathbb{V}(I)$, dato che $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$ per la forma forte del Nullstellensatz **T.3.14**.

2. Dato che, rispetto all'ordinamento fissato, $\mathrm{lt}(f) = xt \notin \mathrm{Lt}(I) = (x^2, y, zt^2)$, si ha $f \notin I$.

Soluzione E. 9.26. 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. Dato che l'ideale iniziale di I non contiene una potenza pura della z, la dimensione $\dim_{\mathbb{C}} \mathbb{C}[x,y,z]/I$ è infinita per **T.3.17**.

2. Sappiamo che $\mathbb{V}(I) \cap \mathbb{V}(z-1) = \mathbb{V}(I, z-1)$. Dato che

$$(x + y + z - 1, y^2 + yz - y + z^2 - z, z - 1) = (x + y, y^2, z - 1)$$

la varietà cercata è $\{(0,0,1)\}$.

Soluzione E. 9.27. 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.2.25** discende subito che $I_1 = (y^2 - z^2, z^4)$ e $I_2 = (z^4)$.

2. Dato che $\mathbb{V}(I) = \{(a, 0, 0) \colon a \in \mathbb{C}\}$ e $\mathbb{V}(I_1) = \{(0, 0)\}$ si ha che $\pi_1(\mathbb{V}(I)) = \mathbb{V}(I_1)$.

Soluzione E. 9.28. Per calcolare J usiamo l'ordinamento lessicografico con $z > t > x > y$. La base di Gröbner ridotta di I rispetto a questo ordinamento è

$$G = \{z - x^2,\, t^2 - x, tx - y, ty - x^2, x^3 - y^2\},$$

quindi $J = (x^3 - y^2)$ per **T.2.25**.
Dato che G contiene polinomi monici in t e z il Teorema di estensione **T.3.11** garantisce che ogni elemento di $\mathbb{V}(J)$ si estende ad un elemento di $\mathbb{V}(I)$.

Soluzione E. 9.29. Dato che $I \subseteq J$ è sufficiente vedere che $y^3z^2 - y^3 - y^2z \in I$. Calcolando una base di Gröbner di I rispetto all'ordinamento lessicografico con $x > y > z$, si trova

$$I = (x^2 - y^2 - yz,\, xy - y^2z,\, y^3z^2 - y^3 - y^2z) = J.$$

Dato che $\mathbb{C}$ è algebricamente chiuso, per il Nullstellensatz **T.3.14**, sappiamo che $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$; quindi è sufficiente verificare che I è radicale.
Prendiamo il polinomio $y^2(yz^2 - y - z) \in I$; 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 $I \subsetneq \mathbb{I}(\mathbb{V}(I))$.

Soluzione E. 9.30. La base di Gröbner ridotta di I rispetto all'ordinamento lessicografico con $x > y > z$ è

$$G = \{x + y + z,\, y^2 + yz + z^2,\, z^3 - 1\}.$$

1. Notiamo che α è una radice terza primitiva dell'unità, dunque $\alpha \cdot \overline{\alpha} = \alpha \cdot \alpha^2 = \alpha^3 = 1$ e $1 + \alpha + \alpha^2 = 0$. Pertanto è immediato verificare che l'insieme delle 6 permutazioni di $(1, \alpha, \alpha^2)$ è contenuto in $\mathbb{V}(I)$.
Inoltre, dato che $\mathrm{Lt}(I) = (x, y^2, z^3)$, l'ideale I è 0-dimensionale per **T.3.17**, e $|\mathbb{V}(I)| \leq \dim_{\mathbb{C}} \mathbb{C}[x, y, z]/I = 6$ per **T.3.19**. Quindi $|\mathbb{V}(I)| = 6$ e $\mathbb{V}(I)$ è l'insieme delle permutazioni descritte.

2. Per il punto 1 e **T.3.19** abbiamo

$$\dim_K(\mathbb{C}[x, y, z]/\sqrt{I}) = \dim_K(\mathbb{C}[x, y, z]/I) = 6,$$

quindi $\mathrm{Lt}(\sqrt{I}) = \mathrm{Lt}(I)$ e I è radicale per **T.2.21**.

Soluzione E. 9.31. 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 $\mathbb{V}(I)$ non è finita per **T**.3.17.

2. Abbiamo

$$\sqrt{I} = (x + y, z + 1) \cap (x + 1, y + z) \cap (x + z, y + 1)$$

e questi ideali sono primi. Dato che il campo è algebricamente chiuso,

$$\mathbb{V}(I) = \mathbb{V}(x + y, z + 1) \cup \mathbb{V}(x + 1, y + z) \cup \mathbb{V}(x + z, y + 1)$$

è una decomposizione in varietà irriducibili.

Soluzione E. 9.32. 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. Dato che I^c è il primo ideale di eliminazione di I, si ha $I^c = (y(y-z)(yz-1))$.

3. Si ha

$$\begin{aligned}\sqrt{I} &= \sqrt{(I, y)} \cap \sqrt{(I, y - z)} \cap \sqrt{(I, yz - 1)} \\ &= (x, y) \cap \sqrt{(x^2, xz^2 - x, y - z)} \cap \sqrt{(x^2 + y^2 - 1, yz - 1)}.\end{aligned}$$

Quindi $\mathbb{V}_{\mathbb{Q}}(I) = \mathbb{V}_{\mathbb{Q}}(\sqrt{I}) \supset \mathbb{V}_{\mathbb{Q}}((x, y))$ e $\mathbb{V}_{\mathbb{Q}}(I)$ è infinita.

4. Gli ideali (x, y) e $\sqrt{(x^2, xz^2 - x, y - z)} = (x, y - z)$ sono ovviamente primi. Inoltre $\sqrt{(x^2 + y^2 - 1, yz - 1)} = (x^2 + y^2 - 1, yz - 1)$; infatti

$$\mathbb{Q}[x, y, z]/(x^2 + y^2 - 1, yz - 1) \simeq \mathbb{Q}[y, y^{-1}][x]/(x^2 + y^2 - 1)$$

è un dominio, quindi l'ideale $(x^2 + y^2 - 1, yz - 1)$ è primo. Dato che non ci sono relazioni di contenimento tra i primi trovati abbiamo

$$\operatorname{Min} I = \{(x, y),\ (x, y - z),\ (x^2 + y^2 - 1,\ yz - 1)\}.$$

Soluzione E. 9.33. 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. Si ha

$$I = (x^2, yt^2, z^2) \cap (t^2, z^2) = (x^2, y, t^2) \cap (x^2, t^2, z^2) \cap (t^2, z^2)$$

e dunque la decomposizione richiesta 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 subito

$$\mathcal{N}(A) = (\overline{x}, \overline{y}, \overline{z}) \cap (\overline{z}, \overline{t}).$$

4. Dalla forma della base G si ricava immediatamente che

$$\mathbb{V}(I) = \{(a, b, 0, 0) \colon\ a, b \in K\} \cup \{(0, 0, 0, c) \colon\ c \in K\}$$

dunque $|\,\mathbb{V}(I)|$ è finita se e solo se è finito il campo K.

Soluzione E. 9.34. 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. Si ha $\mathbb{V}(I) = \mathbb{V}(\sqrt{I})$ e

$$\begin{aligned}\sqrt{I} &= \sqrt{(x^2 - yz, xz - yz, y)} \cap \sqrt{(x^2 - yz, xz - yz, y - z)} \\ &= (x, y) \cap (x - z, y - z).\end{aligned}$$

Infine $\mathbb{V}(I) = \mathbb{V}(x, y) \cup \mathbb{V}(x - z, y - z)$ è una decomposizione in componenti irriducibili, cf. **E.9.24**, e nessuna delle due componenti è finita.

2. Se $f \in \sqrt{I}$ allora $\mathbb{V}(f) \supseteq \mathbb{V}(I)$, ma $P = (1, 1, 1) \in \mathbb{V}(I) \setminus \mathbb{V}(f)$, quindi $f \notin \sqrt{I}$.

Soluzione E. 9.35. Dato che $(a, 0, 0) \in \mathbb{V}(I)$ per ogni $a \in \mathbb{C}$, $\mathbb{V}(I)$ non è finita. Se $I \subseteq (x^2, y + 1, z - 1)$ allora $P = (0, -1, 1) \in \mathbb{V}((x^2, y + 1, z - 1)) \subseteq \mathbb{V}(I)$. Dato che P non è soluzione di $y^2z^2 - yz$, questo non è possibile.

Soluzione E. 9.36. 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 $\operatorname{char} K \neq 2, 3$, otteniamo

$$G = \{x - y^2z,\ y^3 - 12,\ 6z^2 - 1\}.$$

1. Dato che $\mathbb{C}$ è algebricamente chiuso, la conclusione segue direttamente da **T.3.17**.

2. Se $p = 3$, allora $\mathbb{V}(I) = \emptyset$, mentre $\mathbb{V}(I)$ è chiaramente infinita se $p = 2$. Nei rimanenti casi $\mathbb{V}(I)$ è finita di nuovo per **T.3.17**.

Soluzione E. 9.37. La base di Gröbner ridotta G di I rispetto all'ordinamento lex con $x > y > z$ è

$$G = \left\{x + 2z^3 - 3z,\, y^2 - z^2 + 1,\, z^4 - \tfrac{3}{2}z^2 + \tfrac{1}{2}\right\}.$$

1. Abbiamo $\mathrm{Lt}(I) = \mathrm{Lt}(G) = (x, y^2, z^4)$ e $\mathcal{B} = \{1,\, y,\, yz,\, yz^2,\, yz^3,\, z,\, z^2,\, z^3\}$ è la base cercata, cf. **T.2.23**.1.

2. Riducendo f modulo 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 $\mathbb{V}(I)$, 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

$$|\,\mathbb{V}_{\mathbb{C}}(I)| = 6 < \dim_{\mathbb{Q}} A = 8.$$

4. Abbiamo

$$\begin{aligned}\sqrt{I} &= \sqrt{\left(I, (z+1)(z-1)\left(z^2 - \tfrac{1}{2}\right)\right)} \\ &= \sqrt{(I, z+1)} \cap \sqrt{(I, z-1)} \cap \sqrt{\left(I, z^2 - \tfrac{1}{2}\right)} \\ &= \sqrt{(x-1, y, z-1)} \cap \sqrt{(x+1, y, z+1)} \cap \sqrt{\left(x - 2z, y^2 + \tfrac{1}{2}, z^2 - \tfrac{1}{2}\right)}\end{aligned}$$

e gli ideali sotto il segno di radicale sono massimali in $\mathbb{Q}[x, y, z]$. Ciò è immediato per i primi due ideali mentre per vedere che il terzo ideale è massimale basta osservare che

$$\mathbb{Q}[x, y, z]/\left(x - 2z, y^2 + \tfrac{1}{2}, z^2 - \tfrac{1}{2}\right) \simeq \mathbb{Q}[y, z]/\left(y^2 + \tfrac{1}{2}, z^2 - \tfrac{1}{2}\right)$$

è isomorfo al campo $\mathbb{Q}(\sqrt{2}, i)$.

Soluzione E. 9.38. 1. Sia $I = (f_1, f_2, f_3)$. Rispetto all'ordinamento deglex con $y > x$ si ha $x^3,\ y^2 \in \mathrm{Lt}(I)$, quindi Σ ha un numero finito di soluzioni.

2. Usiamo ora l'ordinamento lex con $x > y$. Si ha

$$S(f_1, f_2) + 3f_3 = xy^2 - x = f \in I$$

e $I = (I, f)$. Pertanto

$$\begin{aligned}\mathbb{V}(I) &= \mathbb{V}(I, x) \cup \mathbb{V}(I, y^2 - 1) \\ &= \mathbb{V}(x, y) \cup \mathbb{V}(x^2 - 3x + 1, y - 1) \cup \mathbb{V}(x^2 + 3x + 1, y + 1)\end{aligned}$$

e l'unica soluzione razionale è $(0, 0)$.

3. Raffinando la decomposizione di $\mathbb{V}(I)$ ottenuta al punto precedente, si ha

$$\begin{aligned}\mathbb{V}(I) = &\mathbb{V}(x, y) \cup \mathbb{V}\left(x - \tfrac{3-\sqrt{5}}{2}, y - 1\right) \cup \mathbb{V}\left(x - \tfrac{3+\sqrt{5}}{2}, y - 1\right) \\ &\cup \mathbb{V}\left(x - \tfrac{-3-\sqrt{5}}{2}, y + 1\right) \cup \mathbb{V}\left(x - \tfrac{-3+\sqrt{5}}{2}, y + 1\right).\end{aligned}$$

Dato che ognuna di queste 5 varietà è costituita esattamente da un punto di $\mathbb{R}^2$ la decomposizione trovata è quella richiesta.

Soluzione E. 9.39. La base di Gröbner ridotta di I rispetto all'ordinamento lex con $x > z > y$ è

$$\{x - y,\ z - y^2,\ y^4 - 1\}.$$

1. Otteniamo $I \cap \mathbb{Q}[y] = (y^4 - 1)$; pertanto $p(y) = y^4 - 1$ ha le proprietà richieste.

2. Per il Nullstellensatz, $\mathbb{V}_{\mathbb{C}}((q, I)) = \emptyset$ 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. 9.40. 1. Abbiamo che $\mathbb{I}(V) = \bigcap_{i=1}^{m} \mathfrak{m}_{\alpha_i}$; 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 $A \simeq \prod_i A/\mathfrak{m}_i \simeq \mathbb{C}^m$. Si verifica allora facilmente che le controimmagini $a_i \in A$ degli elementi e_i, $i = 1, \ldots, m$, della base canonica di $\mathbb{C}^m$ sono gli idempotenti cercati, cf. **T.1.19**.

2. Gli idempotenti di $\mathbb{C}^m$ sono tutti e soli i 2^m vettori con coordinate 0 oppure 1; per l'isomorfismo precedente essi corrispondono agli idempotenti di A che quindi sono tutti della forma $a = \sum_{i=1}^{m} b_i a_i$ dove $b_i \in \{0, 1\}$ per ogni i.

17.3 Soluzioni del capitolo 10

Soluzione E. 10.1. Una volta provata la buona definizione del prodotto esterno, la verifica della definizione della struttura di A/I-modulo segue immediatamente dalla definizione della struttura di A-modulo su M.
Se $\overline{a} = \overline{b}$ in A/I allora $a - b \in I$ e $\overline{am} - \overline{bm} = \overline{a}\,\overline{m} - \overline{b}\,\overline{m} = (\overline{a} - \overline{b})\overline{m} = \overline{(a - b)m} = \overline{0}$ in M/IM.

Soluzione E. 10.2. 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. 10.3. Per la somma non vi è nulla da verificare.
Sia I un ideale di B; allora, per ogni $a \in A$, si ha $a \cdot I = f(a)I \subseteq I$, 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. 10.4. Ovviamente $0 \in N : P$. Per ogni $a, b \in N : P$, $c \in A$ e $p \in P$, dalla definizione di $N : P$ e dal fatto che N è un sottomodulo di M, otteniamo immediatamente $(a-b)p = ap - bp \in N$ e $(ca)p = c(ap) \in N$.

Soluzione E. 10.5. Per i punti 1, 2 e 3 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.

4. Sia $A = K[x_i : i \in \mathbb{N}_+]$ 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 $I = (x_i : i \in \mathbb{N}_+)$ è un sottomodulo di A che non è finitamente generato.

5. Consideriamo lo $\mathbb{Z}$-modulo $N = \mathbb{Z}/(n)$, con $n \neq 0, \pm 1$; dato che $n \cdot m = 0$ per ogni $m \in N$, non esistono elementi linearmente indipendenti, e quindi non esistono basi di N su $\mathbb{Z}$.

6. 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 $\overline{3}P = 0$.

Soluzione E. 10.6. Il risultato è una conseguenza dei Teoremi di omomorfismo. Osserviamo 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. 10.7. 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 I Teorema di omomorfismo.

Soluzione E. 10.8. Se $n > m$ possiamo scrivere $A^n = A^m \oplus A^{n-m}$ e considerare l'omomorfismo surgettivo $f \circ \pi : A^n = A^m \oplus A^{n-m} \longrightarrow A^m \longrightarrow A^n$, dove π è la proiezione naturale. Per **T.4.14**, $f \circ \pi$ è un isomorfismo; dal momento che $0 = \mathrm{Ker}(f \circ \pi) \supseteq A^{n-m}$ si ha $A^{n-m} = 0$, dunque $A = 0$.

Soluzione E. 10.9. Siano $\{m_1, \ldots, m_r\}$ e $\{n_1, \ldots, n_s\}$ rispettivamente una base e un insieme di generatori di M con $s < r$. L'assegnazione $m_i \mapsto n_i$ per ogni $i = 1, \ldots, s$ e $m_i \mapsto 0$ per $i = s+1, \ldots, r$, induce un endomorfismo

surgettivo $\tilde{f}$ di M per **T.4.7**. Per **T.4.14**, $\tilde{f}$ è un isomorfismo, che non è possibile dato che $m_{s+1} \in \operatorname{Ker} \tilde{f}$.

Soluzione E. 10.10. Dall'ipotesi discende $N = \varphi(M) + IN$; infatti, per ogni $n \in N$ esiste $m \in M$ tale che $\overline{\varphi}(\overline{m}) = \overline{n}$, dunque $n = \varphi(m) + h$ con $h \in IN$, mentre l'altra inclusione è ovvia. Allora, dato che $I\varphi(M) \subset \varphi(M)$, abbiamo

$$N = \varphi(M) + I(\varphi(M) + IN) = \varphi(M) + I^2 N.$$

Iterando n volte, dove n è tale che $I^n = 0$, si ottiene $N = \varphi(M) + I^n N = \varphi(M)$; quindi φ è surgettivo.

Soluzione E. 10.11. Sia $\mathcal{B} = \{e_1, \dots, e_m\}$ la base canonica di A^m.

1. È l'esercizio **E.10.8**.
Alternativamente, si può osservare che f surgettivo implica che $f(\mathcal{B})$ è un insieme di generatori di A^n; da **E.10.9** segue allora che $m \geq \operatorname{rank} A^n = n$.

2. Supponiamo 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 $\varphi = i \circ f \in \operatorname{End}_A(A^m)$ e, per **T.4.10**, esistono $\alpha_i \in A$ tali che

$$\varphi^k + \alpha_{k-1}\varphi^{k-1} + \ldots + \alpha_1 \varphi + \alpha_0 = 0.$$

Possiamo supporre che tale k sia minimo e, in tal caso, osserviamo che $\alpha_0 \neq 0$; altrimenti $\varphi(\varphi^{k-1} + \alpha_{k-1}\varphi^{k-2} + \ldots + \alpha_1) = 0$ e l'iniettività di φ implica $\varphi^{k-1} + \alpha_{k-1}\varphi^{k-2} + \ldots + \alpha_1 = 0$, contraddicendo la minimalità di k. Valutando in e_m otteniamo

$$(\varphi^k + \alpha_{k-1}\varphi^{k-1} + \ldots + \alpha_1\varphi)(e_m) = -\alpha_0 e_m$$

ma, per come abbiamo definito φ, il membro a sinistra deve avere ultima coordinata 0, contraddizione.

3. Segue direttamente da 1 e 2.

Soluzione E. 10.12. 1. Se esiste un isomorfismo $\varphi\colon M/N \longrightarrow M$ allora, componendo con la proiezione, si ottiene un endomorfismo surgettivo $\varphi \circ \pi\colon M \longrightarrow M/N \longrightarrow M$. Per **T.4.14**, $\varphi \circ \pi$ è iniettivo; dunque $N \subseteq \operatorname{Ker}(\varphi \circ \pi) = 0$, che è contro le ipotesi.

2. Consideriamo $M = K[x_i\colon i \in \mathbb{N}]$ come K-modulo e sia $0 \neq N = \langle x_0 \rangle_K \subset M$. 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. 10.13. 1. Se $M \simeq A/\mathfrak{m}$ con $\mathfrak{m}$ massimale allora M è un campo, quindi 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; quindi, dato che M è semplice, $f(A) = M$, ovvero f è un omomorfismo surgettivo. Dal

I Teorema di omomorfismo otteniamo $M \simeq A/\operatorname{Ker} f$. Infine, dato che a ogni ideale proprio che contiene strettamente $\operatorname{Ker} f$ corrisponde un sottomodulo non banale di M, l'ideale $\operatorname{Ker} f$ 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 quest'ultimo caso $0 \neq \operatorname{Im}\varphi$ e quindi si deve avere $\operatorname{Im}\varphi = N$.

3. Dal punto 1 segue che $M = 0$, 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 volevamo.

Soluzione E. 10.14. 1. 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 $M \neq 0$ sia ciclico e sia $0 \neq N \subseteq M$ un sottomodulo di M. Per ogni $0 \neq n \in N$ abbiamo per ipotesi $\langle n\rangle = M$, quindi $N = M$, come volevamo.

2. Per quanto appena visto cerchiamo gli $\mathbb{Z}$-moduli ciclici in cui ogni elemento non nullo è un generatore. Pertanto i moduli cercati sono tutti e soli della forma $\mathbb{Z}/(p)$ con p primo, cf. anche con **E.10.13**.1.

Soluzione E. 10.15. Iniziamo dimostrando che $M = pM \oplus qM$ e, in seguito, che $N = qM$ e $P = pM$.
Siano $x, y \in \mathbb{Z}$ tali che $xp + yq = 1$; allora per ogni $m \in M$ si ha $m = (xp + yq)m = p(xm) + q(ym) \in pM + qM$. Inoltre $pM \cap qM = 0$; infatti, per ogni $m \in pM \cap qM$, dato che $\operatorname{Ann} M = (pq)$, abbiamo $\operatorname{Ann} m \supseteq (q) + (p) = (1)$ 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 $a \in \mathbb{Z}$. Dalle relazioni $apm = pn = 0$ segue che $ap \in \operatorname{Ann} M = (pq)$; di conseguenza $a = bq \in (q)$ per qualche $b \in \mathbb{Z}$, e abbiamo ottenuto $N \subseteq qM$.

Per l'inclusione opposta, dato che $\operatorname{Ann} N = (p)$, si deve avere $(b, p) = 1$ (perché?); 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 che $P = pM$.

Soluzione E. 10.16. Dimostriamo il primo isomorfismo, il secondo si ottiene in maniera del tutto analoga. Definiamo

$$\Phi\colon \operatorname{Hom}_A(M, P) \oplus \operatorname{Hom}_A(N, P) \longrightarrow \operatorname{Hom}_A(M \oplus N, P)$$

come $\Phi(\varphi_1, \varphi_2) = \lambda_{\varphi_1,\varphi_2}$ con $\lambda_{\varphi_1,\varphi_2}(m, n) = \varphi_1(m) + \varphi_2(n)$.
Siano $i_M\colon M \longrightarrow M \oplus N$ e $i_N\colon N \longrightarrow M \oplus N$ le inclusioni naturali; definiamo

$$\Psi\colon \operatorname{Hom}_A(M \oplus N, P) \longrightarrow \operatorname{Hom}_A(M, P) \oplus \operatorname{Hom}_A(N, P)$$

come $\Psi(\psi) = (\psi \circ i_M, \psi \circ i_N) = (i_M^*(\psi), i_N^*(\psi))$.

È facile verificare che Φ e Ψ sono due omomorfismi e che sono uno inverso dell'altro.

Alternativamente, possiamo considerare la successione esatta

$$0 \longrightarrow M \xrightarrow{i_M} M \oplus N \xrightarrow{\pi_N} N \longrightarrow 0$$

e applicare il funtore $\mathrm{Hom}_A(\bullet, P)$ per ottenere la successione esatta

$$0 \longrightarrow \mathrm{Hom}_A(N,P) \xrightarrow{\pi_N^*} \mathrm{Hom}_A(M \oplus N, P) \xrightarrow{i_M^*} \mathrm{Hom}_A(M,P).$$

Per ogni $\varphi \in \mathrm{Hom}_A(M,P)$ consideriamo l'omomorfismo nullo $N \longrightarrow P$ e applichiamo la proprietà universale della somma diretta **T.4.6**.1 per ottenere $\psi \in \mathrm{Hom}(M \oplus N, P)$ tale che $\psi \circ i_M = \varphi$, i.e. $i_M^*(\psi) = \varphi$. Quindi i_M^* è surgettiva.
Sia adesso $\pi_M \colon M \oplus N \longrightarrow M$; è facile verificare che

$$i_M^* \circ \pi_M^* = \mathrm{id}_{\mathrm{Hom}_A(M,P)}.$$

Dunque i_M^* ha una sezione, la successione esatta degli Hom spezza e la conclusione segue da **T.4.18**.

Soluzione E. 10.17. 1. Per ogni $f \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})$ 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 per ogni $b \in \mathbb{Z} \setminus \{0\}$ si ha $bf\left(\frac{1}{b}\right) = f(1)$, abbiamo che $f(1)$ 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 $f \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n),\mathbb{Z})$, allora $\mathrm{Im}\, f$ è generata da $f(\overline{1})$. Inoltre $nf(\overline{1}) = f(\overline{0}) = 0$ implica $f(\overline{1}) = 0$, 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 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n),\mathbb{Q}/\mathbb{Z})$.

Soluzione E. 10.18. Osserviamo innanzitutto che se $\pi \colon A \longrightarrow A/I$ è la proiezione canonica, ponendo $a\overline{b} = \pi(a)\overline{b} = \overline{a}\overline{b} = \overline{ab}$, risulta definita su A/I una struttura di A-modulo per restrizione di scalari, cf. **E.10.2**. Inoltre, con una dimostrazione simile a quella di **E.10.4**, è facile verificare che $0 :_M I$ è un sottomodulo di M.

1. Consideriamo la mappa $\Phi \colon 0 :_M I \longrightarrow \mathrm{Hom}_A(A/I, M)$ definita da $\Phi(m) = \varphi_m$, dove $\varphi_m(\overline{b}) = bm$.
Proviamo che Φ è ben definito, 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 $b_1 - b_2 \in I$; quindi $(b_1 - b_2)m = 0$ implica $\varphi_m(\overline{b_1}) = \varphi_m(\overline{b_2})$, 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 φ_m è un omomorfismo di A-moduli per ogni $m \in 0 :_M I$; 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 perché, se $\Phi(m) = \varphi_m = 0$ allora $0 = \varphi_m(\overline{1}) = m$. È surgettivo perché ogni $f \in \operatorname{Hom}_A(A/I, M)$ 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 è sufficiente mostrare che l'A-modulo $0 :_M I$ è un A/I-modulo. Basta notare che

$$I \subseteq 0 :_A (0 :_M I) = \operatorname{Ann}_A(0 :_M I)$$

e concludere grazie a **T.4.1**.

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 $a \mapsto \overline{a}$; è ben definita poiché se $aI \subseteq J$ allora $\overline{a}I = 0_{A/J}$. Chiaramente φ è un omomorfismo di A-moduli ed è surgettivo poiché se $\overline{a} \in 0 :_{A/J} I$ allora $aI \subseteq J$, i.e. $a \in J : I$. La conclusione segue ora dal fatto che $\operatorname{Ker}\varphi = J$.

Soluzione E. 10.19. Grazie all'esercizio precedente e al fatto che $I \subset J$, otteniamo $\operatorname{Hom}_A(A/I, A/J) \simeq (J : I)/J = A/J$.
Dato che (x^2, yz) è una base di Gröbner di J , il quoziente A/J è un K-spazio vettoriale di dimensione infinita; ad esempio, gli elementi di $\{\overline{y}^n : n \in \mathbb{N}\}$ sono linearmente indipendenti, cf. **T.2.23**.1.

Soluzione E. 10.20. Dato che A è locale e M è finitamente generato e non nullo, dal Lemma di Nakayama otteniamo $\mathfrak{m}M \neq M$ e $M/\mathfrak{m}M$ è un $A/\mathfrak{m}$-modulo, cioè uno spazio vettoriale, non nullo e di dimensione finita. Dunque esiste certamente una applicazione lineare $f : M/\mathfrak{m}M \longrightarrow A/\mathfrak{m}$ non nulla. Sia $\pi : M \longrightarrow M/\mathfrak{m}M$ la proiezione canonica; allora $f \circ \pi$ è un elemento non nullo di $\operatorname{Hom}_A(M, A/\mathfrak{m})$.

Soluzione E. 10.21. Ogni elemento non zero di B è invertibile in K; pertanto, indicato con $\mathfrak{m}$ l'ideale massimale di B, abbiamo $\mathfrak{m}K = K$. Se K fosse un B-modulo finitamente generato allora $K = 0$ per il Lemma di Nakayama, che non è possibile poiché $B \neq 0$.

Soluzione E. 10.22. 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 $a^n M = (b + i)M = 0 + iM \subset IM$, implica che $a^n \in \operatorname{Ann}(M/IM)$ e $a \in \sqrt{\operatorname{Ann}(M/IM)}$.

Per l'altra inclusione, sia $a \in \sqrt{\operatorname{Ann}(M/IM)}$ e sia $k \in \mathbb{N}$ tale che $a^k \in \operatorname{Ann}(M/IM)$, ovvero $a^k M \subseteq IM$. Consideriamo 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 **T.4.10** per ottenere $a_0, \ldots, a_{n-1} \in I$ tali che

$$\varphi^n + a_{n-1}\varphi^{n-1} + \ldots + a_0 = 0.$$

Ponendo $b = a^{kn} + a_{n-1}a^{k(n-1)} + \ldots + a_1 a^k + a_0$, otteniamo $bM = 0$, ossia $b \in \operatorname{Ann} M$. Inoltre $a^{kn} = b - \sum_{i=0}^{n-1} a_i a^{ki}$ e, dato che l'ultima sommatoria è un elemento di I, abbiamo $a \in \sqrt{\operatorname{Ann} M + I}$, come volevamo.

Soluzione E. 10.23. Sia $\{a_1, \ldots, a_n\}$ un insieme di generatori di $\mathcal{N}(A)$; allora per ogni $i = 1, \ldots, n$ esiste $r_i \in \mathbb{N}$ tale che $a_i^{r_i} = 0$. È facile verificare che esiste $s \in \mathbb{N}$ tale che $\mathcal{N}(A)^s = 0$. Dato che $\mathcal{N}(A)M = M$, abbiamo anche $0 = \mathcal{N}(A)^s M = M$, come volevamo.

Soluzione E. 10.24. Siano $A = K[x_i\colon i \in \mathbb{N}]$ un anello di polinomi in infinite variabili a coefficienti in K e $I \subset A$ l'ideale

$$I = (x_0^2, x_1^2 - x_0, x_2^2 - x_1, \ldots, x_n^2 - x_{n-1}, \ldots).$$

Dato che $\overline{x_0} \in \mathcal{N}(A/I)$ e $\overline{x_i}^{2^i} = \overline{x_0}$ per ogni i, abbiamo $\mathcal{N}(A/I) \supseteq (\overline{x_i} : i \in \mathbb{N})$. Inoltre $(\overline{x_i} : i \in \mathbb{N})$ è massimale, 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.

Soluzione E. 10.25. Chiamiamo $f_i\colon M_i \longrightarrow M_{i+1}$ gli omomorfismi della prima riga e $g_i\colon N_i \to N_{i+1}$ quelli della seconda.
1. Sia $m_3 \in M_3$ tale che $\alpha_3(m_3) = 0$ e verifichiamo che $m_3 = 0$. Abbiamo

$$0 = \alpha_3(m_3) = g_3(\alpha_3(m_3)) = \alpha_4(f_3(m_3))$$

e, dall'iniettività di α_4, discende $m_3 \in \operatorname{Ker} f_3 = \operatorname{Im} f_2$; 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 $\alpha_2(m_2) \in \operatorname{Ker} g_2 = \operatorname{Im} g_1$, quindi 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, per l'iniettività di α_2, abbiamo $m_2 = f_1(m_1)$. 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 surgettivo, 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. 10.26. Proviamo che esiste una retrazione di f, ossia un omomorfismo $\alpha\colon M \longrightarrow N$ tale che $\alpha \circ f = \mathrm{id}_N$. Dato che (p) e (q) sono comassimali, abbiamo $p' + q' = 1$ per certi $p', q' \in \mathbb{Z}$ multipli di p e q rispettivamente. Per ogni $m \in M$, si ha $m = p'm + q'm$ 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. 10.27. 1. Consideriamo la successione

$$0 \longrightarrow \mathbb{Z}/(2) \xrightarrow{f} \mathbb{Z}/(4) \xrightarrow{g} \mathbb{Z}/(2) \longrightarrow 0,$$

con f definita da $f(\overline{1}) = \overline{2}$ 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 $(2)\mathbb{Z}/(4)$, che è anche l'immagine di f.

2. Consideriamo la successione

$$0 \longrightarrow \mathbb{Z}/(2) \xrightarrow{f'} \mathbb{Z}/(2) \oplus \mathbb{Z}/(4) \xrightarrow{g'} \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \longrightarrow 0,$$

dove $f' = (0, f)$ e $g' = \mathrm{id}_{\mathbb{Z}/(2)} \oplus g$, con f e g definite come nel punto 1. Allora g' è surgettiva, perché le sue componenti lo sono, mentre f' è iniettiva perché f lo è. È chiaro che $\operatorname{Im} f' = 0 \oplus (2)\mathbb{Z}/(4) = \operatorname{Ker} g'$.

3. Consideriamo un omomorfismo $g_1\colon \mathbb{Z}/(8) \longrightarrow \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$; dato che $\operatorname{Im} g_1$ è generata da $g_1(\overline{1})$, deve essere uno $\mathbb{Z}$-modulo ciclico, quindi g_1 non può essere surgettiva.

Alternativamente possiamo osservare che un omomorfismo $f_1\colon \mathbb{Z}/(2) \longrightarrow \mathbb{Z}/(8)$ è determinato da $f_1(\overline{1})$ e che deve essere $2f_1(\overline{1}) = \overline{0}$. Dunque l'unico omomorfismo iniettivo manda $\overline{1}$ in $\overline{4}$, ha per immagine $(4)\mathbb{Z}/(8)$ e per conucleo $\mathbb{Z}/(4)$ e l'unica successione esatta possibile è

$$0 \longrightarrow M \longrightarrow P \longrightarrow N \longrightarrow 0.$$

Soluzione E. 10.28. Siano $n_1, \dots, n_r$ e $p_1, \dots, p_s$ insiemi di generatori di N e P rispettivamente; siano inoltre $m_1, \dots, m_s \in M$ tali che $g(m_i) = p_i$ per ogni i. Tali elementi esistono poiché g è surgettiva.
Sia ora $m \in M$; allora $g(m) = \sum_{i=1}^{s} a_i p_i = \sum_{i=1}^{s} a_i g(m_i)$.
Pertanto $g\left(m - \sum_{i=1}^{s} a_i m_i\right) = 0$, ovvero

$$m - \sum_{i=1}^{s} a_i m_i \in \operatorname{Ker} g = \operatorname{Im} f = \langle f(n_1), \dots, f(n_r) \rangle.$$

Possiamo dunque scrivere un qualsiasi elemento di M come combinazione lineare degli elementi $f(n_1), \dots, f(n_r), m_1, \dots, m_s$.

Soluzione E. 10.29. Sia $n \in N$ e scriviamo

$$n = (n - f(g(n))) + f(g(n));$$

dato che per ipotesi $g \circ f = \mathrm{id}_M$, si ha $n - f(g(n)) \in \operatorname{Ker} g$, mentre è ovvio che $f(g(n)) \in \operatorname{Im} f$. 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

$$N \simeq M \oplus \operatorname{Coker} f \simeq \operatorname{Im} f \oplus \operatorname{Ker} g;$$

infatti è facile vedere che $\pi_{|\operatorname{Ker} g} \colon \operatorname{Ker} g \longrightarrow \operatorname{Coker} f$ è un isomorfismo, cf. anche la dimostrazione di **T.4.18**.

Soluzione E. 10.30. 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, abbiamo $\operatorname{Ker}(g \circ f) = \operatorname{Ker} f = \operatorname{Im} \varphi$, mentre dalla surgettività di f discende che $\operatorname{Im}(g \circ f) = \operatorname{Im} g = \operatorname{Ker} \psi$.

Soluzione E. 10.31. Se $\mathbb{Z}/(n)$ fosse uno $\mathbb{Z}$-modulo proiettivo allora la successione $0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/(n) \longrightarrow 0$ spezzerebbe per **T.4.22**. Per **T.4.18** esisterebbe 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.10.17**.2.
Chiaramente, come $\mathbb{Z}/(n)$-modulo, $\mathbb{Z}/(n)$ è libero e dunque proiettivo.

Soluzione E. 10.32. Per il Teorema cinese del resto $A \simeq \mathbb{Z}/(4) \oplus \mathbb{Z}/(3)$ ed A è ovviamente libero come modulo su se stesso; quindi $\mathbb{Z}/(4)$ è un A-modulo proiettivo in quanto suo addendo diretto, cf. **T.4.22**.4.
Per motivi di cardinalità $\mathbb{Z}/(4) \not\simeq A^n$, per ogni n; pertanto non può essere libero.

Soluzione E. 10.33. In A l'unico sottomodulo non banale è $(\overline{2}) \simeq \mathbb{Z}/(2)$ e non è proiettivo perché, se lo fosse allora sarebbe un addendo diretto di $(\mathbb{Z}/(4))^n$ per qualche n, ma ciò è assurdo perché $\mathbb{Z}/(4) \not\simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.
Per quanto riguarda B gli unici sottomoduli non banali sono $(\overline{3}) \simeq \mathbb{Z}/(2)$ e $(\overline{2}) \simeq \mathbb{Z}/(3)$. Dato che $\mathbb{Z}/(6) \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(3)$ entrambi i sottomoduli sono proiettivi.

Soluzione E. 10.34. 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 $I + J = A$, si ha $I \cap J = IJ$ e possiamo scrivere

$$0 \longrightarrow IJ \xrightarrow{f} I \oplus J \xrightarrow{g} A \longrightarrow 0.$$

Visto che A è proiettivo la successione spezza e si ricava $I \oplus J \simeq IJ \oplus A$, come volevamo.

2. Sia $IJ = (d)$; se $d = 0$ allora $I \oplus J = A$. Altrimenti $d \neq 0$ e, dato che A è un dominio, $IJ = (d) \simeq A$; dal punto precedente abbiamo allora $I \oplus J \simeq A^2$.
In entrambi i casi I e J sono addendi diretti di un modulo libero e dunque sono proiettivi.

Soluzione E. 10.35. 1. Se $M \simeq N \simeq \mathbb{Z}$ e $f(1) = n$ con $n \neq 0$ allora $P \simeq \mathbb{Z}/(n)$; in particolare $P = 0$ se $n = \pm 1$.
Altrimenti $P \simeq \mathbb{Z}$ è proiettivo e la successione

$$0 \longrightarrow M \longrightarrow M \oplus \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow 0$$

spezza. Quindi se $M \simeq \mathbb{Z}$ allora $N \simeq \mathbb{Z}^2$; se invece $N \simeq \mathbb{Z} \simeq P$ allora $M = 0$.

2. Se $N \simeq \mathbb{Z}$ abbiamo $M = 0$ oppure $M \simeq \mathbb{Z}$, e possiamo utilizzare quanto visto nel punto precedente.
Se $P \simeq \mathbb{Z}$ la successione spezza e abbiamo $0 \longrightarrow M \longrightarrow M \oplus \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow 0$, con M qualsiasi.
Infine, se $M \simeq \mathbb{Z}$ nulla di rilevante si può dire sulla successione senza ipotesi aggiuntive.

3. Nell'analogo della prima parte del punto 1, i.e. con $M \simeq N \simeq A$ e $f(1_A) = a \neq 0$ abbiamo che $P \simeq A/(a)$; in particolare $P = 0$ se $a \in A^*$.
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 sono veri anche per un qualsiasi PID, cf. **T.4.23**, quindi anche le dimostrazioni restano valide.

Soluzione E. 10.36. 1. Per ipotesi M/N e M'/N' sono liberi e dunque proiettivi. Pertanto le successioni in questione spezzano.

2. Dal punto precedente abbiamo 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. 10.37. 1. Ogni elemento di M si può scrivere come $m = (m - \varphi(m)) + \varphi(m)$, quindi $M = (\mathrm{id}_M - \varphi)(M) + \varphi(M)$.
Verifichiamo che tale somma è diretta; se

$$m = \varphi(m_1) = m_2 - \varphi(m_2) \in \varphi(M) \cap (\mathrm{id}_M - \varphi)(M)$$

allora $m = \varphi^2(m_1) = \varphi(m_2) - \varphi(m_2) = 0$.

2. Dato che M è finitamente generato esistono $n \in \mathbb{N}_+$ e un omomorfismo $g\colon A^n \longrightarrow M$ surgettivo. Se M è proiettivo allora esiste una sezione $\sigma\colon M \longrightarrow A^n$ tale che $g \circ \sigma = \mathrm{id}_M$.
Definiamo $f\colon A^n \longrightarrow A^n$ come $f = \sigma \circ g$; è un omomorfismo tale che $f^2 = \sigma \circ g \circ \sigma \circ g = f$. Inoltre

$$f(A^n) = \sigma(g(A^n)) = \sigma(M) \simeq M,$$

dove 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 $f(A^n) \simeq M$. Per il punto 1

$$A^n \simeq f(A^n) \oplus (\mathrm{id}_{A^n} - f)(A^n) \simeq M \oplus (\mathrm{id}_{A^n} - f)(A^n);$$

dunque M è addendo diretto di un modulo libero e quindi è proiettivo.

Soluzione E. 10.38. Se A è 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 è la moltiplicazione per a ed è iniettiva, perché 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, $1 = g(a) = ag(1)$, quindi a è invertibile in A e A è un campo.

Soluzione E. 10.39. 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 fosse $I = J$ avremmo $1 \in I$, che non è possibile.
Supponiamo ora per assurdo che $\alpha = a + b\sqrt{-5} \in A$ sia un elemento che verifica $(\alpha) = I$; allora $\alpha \,|\, 3$ e $\alpha \,|\, 1 - \sqrt{-5}$.

Indicando con $\overline{\alpha}$ il complesso coniugato di α otteniamo che $\alpha\overline{\alpha} \in \mathbb{Z}$ è tale che $\alpha\overline{\alpha} \,|\, 9$ e $\alpha\overline{\alpha} \,|\, 6$, cioè $\alpha\overline{\alpha} = 1$ oppure $\alpha\overline{\alpha} = 3$. Dato che $\alpha\overline{\alpha} = a^2 + 5b^2$, il caso $\alpha\overline{\alpha} = 3$ non è possibile mentre $\alpha\overline{\alpha} = 1$ 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.10.34** inoltre I e J sono A-moduli proiettivi e tali che $I \oplus J \simeq A^2$.
Abbiamo già verificato al punto 1 che non sono principali, quindi non sono isomorfi ad A.
Infine tra i generatori di I, rispettivamente J, esiste la relazione $2 \cdot 3 - (1 + \sqrt{-5})(1 - \sqrt{-5}) = 0$ e dunque I, rispettivamente J, non è libero.

Soluzione E. 10.40. Se M è proiettivo e finitamente generato allora M è addendo diretto di A^n per qualche intero n; scriviamo $A^n \simeq M \oplus N$. Dato che A^n è finitamente generato, anche N lo è in quanto suo addendo diretto. Sia allora $\{r_1, \dots, r_m\}$ un insieme di generatori di N, possiamo costruire una successione

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & N \oplus M \simeq A^n & \longrightarrow & M & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle e_i \mapsto r_i} & \nearrow & & & & & \\ & & A^m, & & & & & & \end{array}$$

che risulta esatta in M ed in A^n, come volevamo.

È chiaro che il viceversa vale per qualunque A-modulo.

Soluzione E. 10.41. $1 \Leftrightarrow 2$. Dato che il funtore $\mathrm{Hom}_A(\bullet, E)$ è controvariante ed esatto a sinistra, cf. **T.4.16**.1, dire che è esatto equivale a dire 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, i.e. 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 immediata conseguenza di **T.4.18**.

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. nuovamente **T.4.18**.

$1 \Rightarrow 3$. Basta considerare il diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E & \xrightarrow{f} & M & \longrightarrow & N & \longrightarrow & 0 \\ & & {\scriptstyle \mathrm{id}_E}\downarrow & \swarrow_{g} & & & & & \\ & & E & & & & & & \end{array}$$

dove per ipotesi esiste g tale che $g \circ f = \mathrm{id}_E$. Tale g è una retrazione di f e la sua esistenza implica lo spezzamento della successione.

$3 \Rightarrow 1$. Siano $f\colon M \longrightarrow N$ e $g\colon M \longrightarrow E$ omomorfismi, con f iniettivo. Definiamo $U = (E \oplus N)/L$, dove L è il sottomodulo di $E \oplus N$ generato dalle coppie $(g(m), -f(m))$ al variare di $m \in M$, e consideriamo il diagramma

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{f} & N \\ & & {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle i_N} \\ 0 & \longrightarrow & E & \xrightarrow[i_E]{} & U, \end{array}$$

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

$$(e,0) = \sum_i a_i(g(m_i), -f(m_i)) = (g(m), -f(m)) \quad \text{con} \quad m = \sum_i a_i m_i \in M.$$

Dunque $0 = f(m)$; l'iniettività di f implica allora $m = 0$ e, di conseguenza, $e = g(m) = 0$.

Per ipotesi allora esiste un omomorfismo $r\colon U \longrightarrow E$ tale che $r \circ i_E = \mathrm{id}_E$; possiamo definire $\tilde{g}\colon N \longrightarrow E$ per composizione come $\tilde{g} = r \circ i_N$ ed ottenere il diagramma

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{f} & N \\ & & {\scriptstyle g}\downarrow & \swarrow_{\tilde{g}} & \downarrow{\scriptstyle i_N} \\ 0 & \longrightarrow & E & \xrightarrow[i_E]{} & U. \\ & & & \underset{r}{\nwarrow} & \end{array}$$

Per concludere proviamo che $\tilde{g}$ estende g, da cui discende che E è iniettivo; in effetti 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. 10.42. 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.10.41**.

Alternativamente, possiamo osservare che se esiste un omomorfismo iniettivo $f\colon M \longrightarrow N$ 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 che $(\cdot n)^*$ corrisponde ancora alla moltiplicazione per n. Quindi $\mathrm{Hom}_{\mathbb{Z}}(\bullet, \mathbb{Z})$ non è esatto e $\mathbb{Z}$ non è iniettivo per **E.10.41**.

Soluzione E. 10.43. L'implicazione $\Rightarrow$ è immediata dalla definizione di modulo iniettivo, dato che l'omomorfismo di inclusione $I \longrightarrow A$ è iniettivo.

Viceversa, siano M, N due A-moduli e consideriamo omomorfismi $f\colon M \longrightarrow N$ e $g\colon M \longrightarrow E$ con f iniettivo. Definiamo

$$S = \{(N', g')\colon N' \subseteq N \text{ e } g'\colon N' \longrightarrow E \text{ tali che } g' \circ f = g\},$$

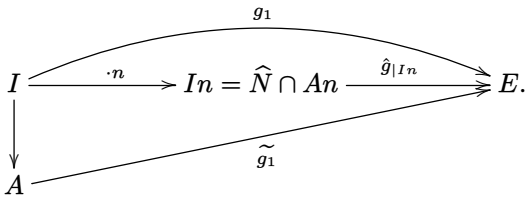
come l'insieme delle coppie di sottomoduli N' di N e omomorfismi g' che estendono g.
Osserviamo che S non è vuoto perché contiene la coppia $(f(M), \eta)$ dove $\eta(f(m)) = g(m)$ per ogni $m \in M$.
È facile vedere che S dotato della relazione d'ordine

$$(N', g') < (N'', g'') \iff N' \subseteq N'' \text{ e } g''_{|N'} = g'$$

verifica le ipotesi del Lemma di Zorn; dunque S ammette un elemento massimale $(\widehat{N}, \hat{g})$.
Se $\widehat{N} = N$ abbiamo finito.
Supponiamo allora che esista $n \in N \setminus \widehat{N}$ e consideriamo in A l'ideale $I = \widehat{N}\colon n$.
Abbiamo allora un omomorfismo

$$g_1\colon I \xrightarrow{\cdot n} \widehat{N} \xrightarrow{\hat{g}} E$$

che, per ipotesi, si estende a $\widetilde{g_1}\colon A \longrightarrow E$



Possiamo allora definire $\tilde{g}\colon \widehat{N} + An \longrightarrow E$ ponendo

$$\tilde{g}(\hat{n} + an) = \hat{g}(\hat{n}) + \widetilde{g_1}(a) \quad \text{per ogni } \hat{n} \in \widehat{N} \text{ e ogni } a \in A.$$

La mappa $\tilde{g}$ è ben definita perché, se $\hat{n}_1 + a_1 n = \hat{n}_2 + a_2 n$ allora $a_1 - a_2 \in \widehat{N}\colon n = I$ e

$$\begin{aligned}\tilde{g}(\hat{n}_1 + a_1 n) - \tilde{g}(\hat{n}_2 + a_2 n) &= \hat{g}(\hat{n}_1) + \widetilde{g_1}(a_1) - \hat{g}(\hat{n}_2) - \widetilde{g_1}(a_2)\\ &= \hat{g}(\hat{n}_1 - \hat{n}_2) + \widetilde{g_1}(a_1 - a_2)\\ &= \hat{g}(a_2 n - a_1 n) + g_1(a_1 - a_2)\\ &= g_1(a_2 - a_1) + g_1(a_1 - a_2) = 0,\end{aligned}$$

dove la penultima uguaglianza è data dalla definizione di g_1.
È facile vedere che $\tilde{g}$ è un omomorfismo e che $\tilde{g}_{|\widehat{N}} = \hat{g}$.

Abbiamo dunque trovato un elemento $(\widehat{N} + An, \tilde{g})$ di S strettamente maggiore di $(\widehat{N}, \hat{g})$, che però è massimale. Pertanto questo caso non si può verificare e abbiamo concluso.

Soluzione E. 10.44. Gli A-moduli proiettivi sono liberi, cf. **T.4.24**. Un sottomodulo N di un modulo libero M è libero per **T.4.23**, quindi proiettivo per **T.4.21**.

Soluzione E. 10.45. Siano $m_1, m_2 \in T(M)$ e $a_1, a_2 \in A \setminus \{0\}$ tali che $a_1 m_1 = a_2 m_2 = 0$; allora $a_1 a_2 (m_1 + m_2) = 0$ con $a_1 a_2 \neq 0$. Dato un qualunque $a \in A$ si ha poi $a_1(a m_1) = a(a_1 m_1) = 0$.

Soluzione E. 10.46. Siano m_1, $m_2 \in M_{[a]}$ e $b \in A$; allora esistono k_1, $k_2 \in \mathbb{N}$ tali che $a^{k_1} m_1 = a^{k_2} m_2 = 0$. Dunque $a^{\max\{k_1,k_2\}}(m_1 + m_2) = 0$ e $a^{k_1}(b m_1) = 0$, cioè $m_1 + m_2$, $b m_1 \in M_{[a]}$.

Soluzione E. 10.47. Visto che $M_{[a]}$, $M_{[b]}$ e $M_{[ab]}$ sono finitamente generati per **T.4.23**, esiste un opportuno intero k tale che

$$a^k M_{[a]} = b^k M_{[b]} = (ab)^k M_{[ab]} = 0.$$

Dato che $\gcd(a^k, b^k) = 1$ esistono inoltre s, $t \in A$ tali che $s a^k + t b^k = 1$. Poniamo ora $c = t b^k$ e $d = s a^k$.

È immediato verificare che

i) $cM_{[ab]} \subseteq M_{[a]}$ e $dM_{[ab]} \subseteq M_{[b]}$;

ii) $cM_{[b]} = 0$ e $dM_{[a]} = 0$;

iii) $cm_a = (c+d)m_a = m_a$ per ogni $m_a \in M_{[a]}$ e $dm_b = (c+d)m_b = m_b$ per ogni $m_b \in M_{[b]}$.

1. 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 interi k_1, k_2 tali che $a^{k_1}m_1 = b^{k_2}m_2 = 0$. Di conseguenza, $(ab)^{\max\{k_1,k_2\}}(m_1+m_2) = 0$.

Per l'altra inclusione, se $m \in M_{[ab]}$ si ha $m = 1\cdot m = (c+d)m \in M_{[a]} + M_{[b]}$ per i).
Inoltre la somma è diretta perché se $m \in M_{[a]} \cap M_{[b]}$ allora $m = (c+d)m = 0$ per ii).

2. Dal punto 1, applicando ii) e iii), otteniamo che 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 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 $cm = m_a$ e $dm = m_b$, e dunque $\langle m\rangle \subseteq M_{[ab]}$. Preso poi $m' \in M_{[ab]}$, abbiamo

$$m' = cm' + dm' = c'm_a + d'm_b = c'cm + d'dm = (c'c + d'd)m,$$

per qualche c', $d' \in A$, e dunque $\langle m\rangle = M_{[ab]}$.

Soluzione E. 10.48. Per ipotesi $M \simeq A/(d)$, con $d \notin A^* \cup \{0\}$. Osserviamo che M coincide con la sua d-componente $M_{[d]}$. Sia $d = \prod_{j=1}^{h} p_i^{e_i}$ la fattorizzazione di d in irriducibili distinti, ognuno contato con la sua molteplicità. Allora per **E.10.47**

$$M = M_{[d]} \simeq \bigoplus_{i=1}^{h} M_{[p_i^{e_i}]} = \bigoplus_{i=1}^{h} M_{[p_i]},$$

dove $M_{[p_i]} \simeq A/(p_i^{e_i})$ sono i moduli ciclici p_i-primari richiesti.

Soluzione E. 10.49. 1. Siano $\{m_\alpha : \alpha \in \Lambda\}$ una base di M, $m = \sum_{\alpha\in\Lambda} a_\alpha m_\alpha \in M$ non nullo e $a \in A$ tali che $am = 0$. Allora $\sum_{\alpha\in\Lambda} aa_\alpha m_\alpha = 0$ 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.4.33**.2.

3. Consideriamo $A = K[x,y]$ 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. 10.50. Chiaramente $M \simeq \operatorname{Coker} f$; la matrice associata a f rispetto alle basi canoniche

$$\begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & -3 \\ 1 & 3 & 1 \end{pmatrix} \quad \text{ha forma di Smith} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}.$$

Da questa forma deduciamo che

$$M \simeq \mathbb{Z} \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(4).$$

Soluzione E. 10.51. La forma di Smith della matrice associata a φ rispetto alle basi canoniche è

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x & 0 \\ 0 & 0 & 0 & x^2(x-1) \end{pmatrix}.$$

Dunque

$$\operatorname{Coker} \varphi \simeq 0 \oplus 0 \oplus \mathbb{Q}[x]/(x) \oplus \mathbb{Q}[x]/(x^2) \oplus \mathbb{Q}[x]/(x-1),$$

dove l'ultimo isomorfismo è dovuto al fatto che gli ideali (x^2) e $(x-1)$ sono comassimali. Pertanto

$$\operatorname{Coker} \varphi \simeq \mathbb{Q} \oplus \langle 1, x \rangle_{\mathbb{Q}} \oplus \mathbb{Q} \quad \text{e} \quad \dim_{\mathbb{Q}} \operatorname{Coker} \varphi = 4.$$

Alternativamente, se d_1, d_2 ,d_3 e d_4 sono i fattori invarianti nella forma di Smith della matrice M che rappresenta φ, si ha $\operatorname{Coker} \varphi \simeq \bigoplus_{i=1}^{4} \mathbb{Q}[x]/(d_i)$. Da ciò si deduce che $\dim_{\mathbb{Q}} \operatorname{Coker} \varphi = \sum \deg d_i = \deg(d_1 \cdots d_4) = 4$.

Soluzione E. 10.52. La matrice che rappresenta φ è $\begin{pmatrix} 6 & 2 & 4 \\ 0 & a & 4 \\ 2 & 2 & 2 \end{pmatrix}$. Per calcolare gli ideali Δ_i può essere utile semplificare la matrice con operazioni elementari consentite, ottenendo per esempio $\begin{pmatrix} 2 & 2 & 2 \\ 0 & 2 & 4 \\ 0 & 0 & a-8 \end{pmatrix}$.

i) Se $a = 2k+1$; allora $\Delta_1 = (1)$, $\Delta_2 = (2)$ e $\Delta_3 = (4(a-8))$, da cui segue $d_1 = 1$, $d_2 = 2$, $d_3 = 2(a-8)$ e

$$\operatorname{Coker} \varphi \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2a-16).$$

Quindi per ogni a dispari $\operatorname{Coker} \varphi$ è finito.

ii) Se $a = 2k$; allora $\Delta_1 = (2)$, $\Delta_2 = (4)$ e $\Delta_3 = (4(a-8))$, da cui segue $d_1 = d_2 = 2$, $d_3 = a - 8$ e

$$\operatorname{Coker}\varphi \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(a-8).$$

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. 10.53. Abbiamo $\Delta_1 = (\gcd(a,b,c))$, $\Delta_2 = (\gcd(a^2, ab, b^2 - ac))$ 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 $\gcd(a^2, ab) = a$; quindi $\Delta_1 = (1)$ e $\Delta_2 = (a, b^2) = (1)$, da cui $d_1 = d_2 = 1$.
Viceversa, sia $d = \gcd(a,b)$; allora $d \mid \gcd(a^2, ab, b^2 - ac) = 1$ e quindi $d = 1$.

Soluzione E. 10.54. Con alcune operazioni elementari possiamo ridurre la matrice e ottenere $\begin{pmatrix} a & 0 & 0 \\ -3 & 6 & 0 \\ 0 & 3 & 3 \end{pmatrix}$; abbiamo dunque $\Delta_1 = (a, 3)$, $\Delta_2 = (3a, 9)$ e $\Delta_3 = (18a)$.

1. Perché $\operatorname{Coker}\varphi$ sia finito si deve avere $\Delta_3 \neq (0)$ e questo accade se e solo se $a \neq 0$.

2. Abbiamo $d_1 = 1$ se $\gcd(a,3) = 1$ e $d_1 = 3$ altrimenti. Nel secondo caso sicuramente $\operatorname{Coker}\varphi$ non è ciclico. Se invece $\gcd(a,3) = 1$ otteniamo $\Delta_2 = (3a, 9) = (3(a,3)) = (3)$ e di nuovo $\operatorname{Coker}\varphi$ non è ciclico.

Soluzione E. 10.55. 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 $d_1 = 1$, $\Delta_2 = (b, 3a, 12)$ e $\Delta_3 = (12b)$. Quindi M è finito se e solo se $b \neq 0$.
Inoltre, M è ciclico se e solo se $\Delta_2 = (1)$. Dato che

$$\gcd(b, 3a, 12) = \gcd(b, 3\gcd(a,4)) = \gcd(b,3)\gcd(b, \gcd(a,4))$$

dobbiamo avere $b \not\equiv 0 \mod 3$ 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

i) $b \not\equiv 0 \mod 3$ e a dispari, oppure

ii) $b \not\equiv 0 \mod 3$, a pari e b dispari.

Soluzione E. 10.56. La forma di Smith della matrice le cui colonne sono i vettori m_1, m_2 e m_3 è $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 8 \end{pmatrix}$.
Quindi risulta

$$M \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(4) \oplus \mathbb{Z}/(8) \quad \text{e} \quad \operatorname{Ann}_{\mathbb{Z}} M = (8).$$

Soluzione E. 10.57. Dato che $\det A = 28$ le forme di Smith di A hanno sulla diagonale $1, 1, 28$ oppure $1, 2, 14$. Da $\det B = 7$, deduciamo che la forma di Smith di B è individuata dai fattori invarianti $1, 1, 7$.
Analogamente, dal momento che $\det D = \det A \det B = 196$, 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. 10.58. 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. 10.59. Dato che M è uno $\mathbb{Z}$-modulo finitamente generato, per **T.4.33**.2 si ha $M \simeq \mathbb{Z}^r \oplus T(M)$ con $r \geq 0$ e $T(M)$ di torsione. L'ipotesi implica però che M è tutto di torsione, dunque $r = 0$.
Dal Teorema di struttura **T.4.31** otteniamo $M \simeq \bigoplus_{i=1}^{n} \mathbb{Z}/I_i$, dove $I_i \neq 0$ per ogni i e $I_i = 0 \colon m_i$ per certi elementi $m_i \in M$, cf. anche la dimostrazione di **T.4.31**. Supponiamo che $I_1 = \ldots = I_s = \mathbb{Z}$ e $I_{s+1} \subsetneq \mathbb{Z}$.
Se $s = n$ allora $R\mathbb{Z}^n = \mathbb{Z}^n$, quindi R 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, generano ideali massimali, per cui $I_i = (p_{m_i})$ per ogni $i = s+1, \ldots, n$. Inoltre $I_h \subseteq I_k$ per ogni $h \geq k$, pertanto deve essere $I_i = I_{s+1} = (p_{m_{s+1}})$ per ogni $i = s+1, \ldots, n$. Sia $p = p_{m_{s+1}}$; allora $\det R$ è associato al determinante della sua forma di Smith D che, per quanto appena visto, è $\det D = p^{n-s} \neq 0$, con $n - s \leq n$.

Soluzione E. 10.60. 1. Consideriamo $\varphi \colon \mathbb{Z}^3 \longrightarrow M$ data da $\varphi(e_i) = m_i$, con $i = 1, 2, 3$; 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 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 $a \in \mathbb{Z}$;

$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 14 & 0 \\ 0 & 0 & 6+a \end{pmatrix}$ $a \equiv 8 \mod 14$ $M \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(14) \oplus \mathbb{Z}/(a+6)$	$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 7(6+a) \end{pmatrix}$ $a \equiv 0 \mod 2$ $a \not\equiv 1 \mod 7$ $M \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(7a+42)$
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 14 & 0 \\ 0 & 0 & 2(6+a) \end{pmatrix}$ $a \equiv 1 \mod 2$ $a \equiv 1 \mod 7$ $M \simeq \mathbb{Z}/(14) \oplus \mathbb{Z}/(2a+12)$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 14(6+a) \end{pmatrix}$ $a \equiv 1 \mod 2$ $a \not\equiv 1 \mod 7$ $M \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(14a+84)$.

2. L'unico caso in cui $\operatorname{Ann} M = 0$ si ha per $a = -6$.

Soluzione E. 10.61. Dato che G_1 e $G_2(\alpha)$ sono gruppi abeliani finitamente generati, quindi rappresentabili come somma diretta di gruppi ciclici, sono isomorfi se e solo hanno gli stessi fattori invarianti.
Consideriamo la matrice

$$R = \begin{pmatrix} 2 & 0 & -4 & 6 & 12 \\ 2 & -2 & 4 & 4 & 4 \\ 1 & 1 & -3 & 1 & 1 \\ 3 & 3 & -15 & 9 & 21 \end{pmatrix};$$

abbiamo $G_1 \simeq \operatorname{Coker} \psi$, dove $\psi \colon \mathbb{Z}^5 \longrightarrow \mathbb{Z}^4$ è l'omomorfismo associato ad R rispetto alle basi canoniche. Calcolando la forma di Smith di R 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 $G_1 \simeq \mathbb{Z} \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/6$.
Calcoliamo ora la forma di Smith associata alla matrice

$$S = \begin{pmatrix} 2 & 8 & -4 \\ \alpha & 6 & \alpha \\ -2 & -2 & 4 \end{pmatrix},$$

che rappresenta φ_α e dunque $G_2(\alpha)$. Per avere un isomorfismo i fattori invarianti di S devono essere $2, 6, 0$. Dato che $\Delta_3(S) = (\det S) = (36\alpha)$, l'unico valore possibile è $\alpha = 0$. Per $\alpha = 0$ si ha anche $\Delta_1(S) = 2$ e $\Delta_2(S) = 12$, da cui segue $d_1 = 2$, $d_2 = 6$; pertanto $G_1 \simeq G_2(0)$.

Soluzione E. 10.62. La forma di Smith della matrice $R - xI$ è una matrice diagonale $D = \operatorname{diag}(d_1, \ldots, d_6)$, dove $d_1 \,|\, d_2 \,|\, \ldots \,|\, d_6$ 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) può 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

$$\gamma_3 + \gamma_4 + \gamma_5 + \gamma_6 = \alpha \quad \text{e} \quad \gamma_3 \leq \gamma_4 \leq \gamma_5 \leq \gamma_6.$$

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 somma delle coordinate uguale a 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

$D_1 = \operatorname{diag}(1,1,1,1,1,(x-1)^2(x-2)^2(x^2+1))$;

$D_2 = \operatorname{diag}(1,1,1,1,(x-1),(x-1)(x-2)^2(x^2+1))$;

$D_3 = \operatorname{diag}(1,1,1,1,(x-2),(x-1)^2(x-2)(x^2+1))$;

$D_4 = \operatorname{diag}(1,1,1,1,(x-1)(x-2),(x-1)(x-2)(x^2+1))$.

Soluzione E. 10.63. Abbiamo $M \simeq \operatorname{Coker}\varphi$, 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

$$\Delta_1 = (3, a, b) = (1), \quad \Delta_2 = (9, 3a, 3b, ab), \quad \Delta_3 = (27).$$

Se $(3, ab) = 1$ allora $\Delta_2 = (1)$ e $\Delta_3 = (27)$; quindi

$$M \simeq \mathbb{Z} \oplus \mathbb{Z}/(27) \quad \text{e} \quad T(M) \simeq \mathbb{Z}/(27).$$

Se invece $(3, ab) = 3$ allora $\Delta_2 = (3)$ e $\Delta_3 = (27)$; quindi

$$M \simeq \mathbb{Z} \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(9) \quad \text{e} \quad T(M) \simeq \mathbb{Z}/(3) \oplus \mathbb{Z}/(9).$$

Soluzione E. 10.64. 1. Consideriamo la matrice $\begin{pmatrix} 2 & 2 & 0 \\ 2 & a & 4 \\ a & 0 & 2 \end{pmatrix}$ e calcoliamo

$$\Delta_1 = (2, a), \quad \Delta_2 = (4, 2a, a^2) \quad \text{e} \quad \Delta_3 = (4(2 - 3a)).$$

Abbiamo due casi

i) se $\gcd(2, a) = 1$ allora 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 $\gcd(2, a) = 2$ allora 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. Per **E.10.16** e **E.10.18**.3, il modulo $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(7), M)$ è non nullo se e solo se $2 - 3a \equiv 0 \mod 7$, cioè $a \equiv 3 \mod 7$.

Soluzione E. 10.65. Si ha $M \simeq \mathrm{Coker}\, f$, dove l'omomorfismo $f\colon \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ 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 $\varphi\colon \mathbb{Z}/(20) \longrightarrow \mathbb{Z}/(15)$ ponendo $\varphi(n) = 3n$.

2. Si ha

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(20), M) \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(20), \mathbb{Z}/(5a)) \simeq ((5a)\colon (20))/(5a),$$

cf. **E.10.18**.3. Se $a = 0$ allora $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(20), \mathbb{Z}) = 0$. Altrimenti $a \neq 0$ e

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(20), M) \simeq \begin{cases} \mathbb{Z}/(5) & \text{se } \gcd(a, 4) = 1; \\ \mathbb{Z}/(10) & \text{se } \gcd(a, 4) = 2; \\ \mathbb{Z}/(20) & \text{se } \gcd(a, 4) = 4. \end{cases}$$

Soluzione E. 10.66. 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

$$\Delta_1 = (2, a, b), \quad \Delta_2 = (2a, ab, 4(b-2)) \quad \text{e} \quad \Delta_3 = (2a(2-b)).$$

Per **E.10.14**, M è semplice se e solo se $d_1 = d_2 = 1$ e d_3 è primo, cioè $\gcd(2, a, b) = \gcd(2a, ab, 4(b-2)) = 1$ e $2a(b-2) = \pm 2$. Dunque

$$a = \pm 1 \quad \text{e} \quad b = 1 \ \text{ oppure } \ b = 3.$$

Alternativamente, riducendo con operazioni elementari consentite otteniamo $\begin{pmatrix} 2 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & b-2 \end{pmatrix}$. Quindi, per **E.10.14**, M è semplice se e solo se $M \simeq \mathbb{Z}/(2)$, i.e. se e solo se $a = \pm 1$ e $b - 2 = \pm 1$.

Soluzione E. 10.67. Ricordiamo che $K[x, y]$, e quindi A che è un suo quoziente, sono $K[x]$-moduli per restrizione di scalari tramite l'omomorfismo di immersione $K[x] \longrightarrow K[x, y]$.
Poniamo $g = y^3 - xy^2 - y + x$.

1. Proviamo che A è generato come $K[x]$-modulo da $\overline{1}$, $\overline{y}$ e $\overline{y}^2$. Infatti 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 $\overline{g} = \overline{0}$, in A possiamo scrivere $\overline{f} = \sum_{i=0}^{2} q_i(x)\,\overline{y}^i$ per certi $q_i \in K[x]$.

Alternativamente, possiamo osservare 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 abbiamo $\overline{f} = \overline{r} \in \langle 1, \overline{y}, \overline{y}^2 \rangle_{K[x]}$.

2. Da ora in poi, per semplificare le notazioni, omettiamo le barre per denotare le classi di equivalenza.
Siano $B = K[x, y]/(g)$ e $h = x^2 - xy + x - y$; allora $A \simeq B/(h)$ ed è facile vedere 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 $f(e_3) = y^2 h$; allora $\operatorname{Im} f = \langle h, yh, y^2 h \rangle_B$, quindi $\operatorname{Im} f \subseteq (h)$.

Per l'altra inclusione, 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, $s \in \operatorname{Im} f$.
Quindi $\operatorname{Im} f = (h)$ e $A \simeq B/(h) = \operatorname{Coker} f$.
La matrice che rappresenta f rispetto alle basi $\{e_1, e_2, e_3\}$ e $\{1, y, y^2\}$ è data da

$$\begin{pmatrix} x^2 + x & 0 & x^2 + x \\ -x - 1 & x^2 + x & -x - 1 \\ 0 & -x - 1 & 0 \end{pmatrix}.$$

Allora $\Delta_1 = (x+1)$, $\Delta_2 = (x+1)^2$ e $\Delta_3 = (0)$; possiamo concludere che $d_1 = d_2 = x+1$, $d_3 = 0$ e

$$A \simeq K^2 \oplus K[x].$$

Soluzione E. 10.68. Calcoliamo una base di Gröbner di I rispetto all'ordinamento lessicografico con $x > y > z$, ottenendo

$$\{x + y^3 - yz,\, y^4 - y^2 z + 1\}.$$

1. Risulta $A/I \simeq K[z][y]/(y^4 - y^2 z + 1)$ che è generato come $K[z]$-modulo da $\{\overline{1},\, \overline{y},\, \overline{y}^2,\, \overline{y}^3\}$.
2. Dato che $\overline{1}$, $\overline{y}$, $\overline{y}^2$ e $\overline{y}^3$ sono indipendenti modulo I, formano una base di A e quindi $A \simeq K[z]^4$.

Soluzione E. 10.69. 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.9.7**.

2. È immediato verificare che $M = \langle \overline{1},\, \overline{x},\, \overline{z},\, \overline{xz} \rangle_{K[y]}$.

3. Dato che $\overline{yx} = 0$ in M, abbiamo $0 \neq \overline{x} \in T(M)$, quindi M non è libero.

4. Da ora in poi omettiamo le barre per denotare le classi di equivalenza. Consideriamo l'omomorfismo $\varphi\colon K[y]^4 \longrightarrow M$ dato da

$$\varphi(e_1) = 1, \quad \varphi(e_2) = x, \quad \varphi(e_3) = z \quad \text{e} \quad \varphi(e_4) = xz.$$

Supponiamo che $(a_1, a_2, a_3, a_4) \in \operatorname{Ker}\varphi$; allora

$$0 = \varphi(a_1, a_2, a_3, a_4) = a_1(y) + a_2(y)x + a_3(y)z + a_4(y)xz,$$

i.e. $a_1(y) + a_2(y)x + a_3(y)z + a_4(y)xz \in I$. Dato che I è monomiale, si ha $a_1 = 0$, $a_2 = y a_2'$, $a_3 = y a_3'$ e $a_4 = y a_4'$. Pertanto otteniamo che

$$\operatorname{Ker}\varphi = \{(0,\, y b_2,\, y b_3,\, y b_4)\colon b_2,\, b_3,\, b_4 \in K[y]\}$$

è libero con base $\{v_1 = (0, y, 0, 0),\, v_2 = (0, 0, y, 0),\, v_3 = (0, 0, 0, y)\}$. Chiamiamo 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 $M \simeq \operatorname{Coker}\psi$. Infine, 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

$$M \simeq K^3 \oplus K[y].$$

Soluzione E. 10.70. 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 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 esistono $f(x)$, $g(x) \in K[x]$ tali che $f(x)\overline{1} + g(x)\overline{y} = \overline{0}$ allora abbiamo $f(x) + g(x)y \in (x^2-y^2)$, 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; dunque l'uguaglianza è possibile solo per $q(x,y) = 0$. Quindi $f(x) + g(x)y = 0$ e infine $f(x) = g(x) = 0$.
Pertanto A è isomorfo a $K[x]^2$ come $K[x]$-modulo.

2. In questo caso

$$A \simeq K[x,y,y^{-1}]/(y^2 - y^{-1} + x^2).$$

In A si ha $\overline{y}^{-1} = \overline{y}^2 + \overline{x}^2$, ovvero $\overline{1} = \overline{y}^3 + \overline{y}\overline{x}^2$ e quindi gli elementi $\overline{1}$, $\overline{y}$, $\overline{y}^2$ generano A come $K[x]$-modulo. Tale insieme di generatori è libero da relazioni; infatti, se $f(x)$, $g(x)$, $h(x) \in K[x]$ sono tali che $f(x)\overline{1} + g(x)\overline{y} + h(x)\overline{y}^2 = \overline{0}$ allora $f(x)+g(x)y+h(x)y^2 = (y^2-y^{-1}+x^2)q(x,y,y^{-1})$ per qualche polinomio $q(x,y,z) \in K[x,y,z]$. Dunque

$$f(x)y + g(x)y^2 + h(x)y^3 = (y^3 - 1 + x^2 y)q(x,y,y^{-1}).$$

Dato che nel membro di sinistra y^{-1} non compare, non può comparire neanche a destra, quindi possiamo scrivere $q(x,y,y^{-1}) = q(x,y)$. Inoltre il grado in y del membro di sinistra è al più 3. Se $\deg_y q(x,y) \geq 1$ allora il grado in y a destra è almeno 4, dunque y non compare in $q(x,y)$ e possiamo scrivere $q(x,y) = q(x)$. Ne segue che

$$f(x)y + g(x)y^2 + h(x)y^3 = (y^3 - 1 + x^2 y)q(x)$$

e pertanto $h = q$, $g = 0$, $f = x^2 q$ e $0 = -q$; quindi $f = g = h = 0$, come volevamo.
Possiamo concludere che, come $K[x]$-modulo, A è isomorfo a $K[x]^3$.

3. L'anello A è il quoziente dell'anello B definito sopra modulo l'ideale generato dall'elemento $a = \overline{x}^4 - \overline{x}^3\,\overline{y} + \overline{y}$. Come visto al punto 1, B è un $K[x]$-modulo libero generato da $\{\overline{1}, \overline{y}\}$; quindi un generico elemento di (a) si può scrivere come $ap(x,y) = ap_0(x) + ap_1(x)\overline{y}$. Dunque (a), come $K[x]$-modulo, è generato da

$$a = \overline{x}^4 - \overline{x}^3\,\overline{y} + \overline{y} = x^4\,\overline{1} + (1-x^3)\overline{y} \quad \text{e} \quad a\overline{y} = (-x^5 + x^2)\overline{1} + x^4\,\overline{y}.$$

Pertanto A è il conucleo dell'omomorfismo di $K[x]$-moduli $\varphi\colon K[x]^2 \longrightarrow K[x]^2$, definito da $\varphi(e_1) = x^4 e_1 + (1-x^3)e_2$ e $\varphi(e_2) = (-x^5+x^2)e_1 + x^4 e_2$, 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 $\Delta_2 = (2x^5 - x^2)$, abbiamo 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 $A \simeq K[x]/(2x^5 - x^2)$.

17.4 Soluzioni del capitolo 11

Soluzione E. 11.1. 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 $1_A b = b$ è ovvia, mentre per ogni $\alpha, \beta \in A$ e $b, b' \in \mathrm{Bil}(M, N; P)$, le uguaglianze

$$(\alpha + \beta)b = \alpha b + \beta b, \quad \alpha(b + b') = \alpha b + \alpha b' \quad \text{e} \quad (\alpha\beta)b = \alpha(\beta b)$$

seguono dal fatto che P è un A-modulo. Infatti, per ogni $m \in M$ e $n \in N$, si ha

$$\begin{aligned}
((\alpha + \beta)b)(m, n) &= (\alpha + \beta)b(m, n) = \alpha b(m, n) + \beta b(m, n) = (\alpha b + \beta b)(m, n);\\
(\alpha(b + b'))(m, n) &= \alpha((b + b')(m, n)) = \alpha(b(m, n) + b'(m, n))\\
&= \alpha b(m, n) + \alpha b'(m, n) = (\alpha b + \alpha b')(m, n);\\
((\alpha\beta)b)(m, n) &= (\alpha\beta)b(m, n) = \alpha(\beta b(m, n))\\
&= \alpha(\beta b)(m, n) = (\alpha(\beta b))(m, n).
\end{aligned}$$

Soluzione E. 11.2. Per ipotesi esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha a + \beta b = 1$. 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 tesi segue da **T.5.3**.2.

Soluzione E. 11.3. Da **T.5.4**.5 otteniamo $A/I \otimes_A A/J \simeq (A/I)/J(A/I)$. Quest'ultimo è $(A/I)/(J + I/I)$ e quindi isomorfo a $A/I + J$ per il II Teorema di omomorfismo, cf. **T.4.3**.

Alternativamente si può dimostrare la tesi usando la proprietà universale del prodotto tensoriale **T.5.2**. Costruiamo il diagramma

$$\begin{array}{ccc} A/I \times A/J & \xrightarrow{f} & A/(I+J) \\ {\scriptstyle\tau}\downarrow & \nearrow_{\tilde{f}} & \\ A/I \otimes A/J, & & \end{array}$$

dove $f(\overline{x},\overline{y}) = \overline{xy}$; tale f è ben definita e A-bilineare. La bilinearità di f è immediata; 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 $x_1y_1 - x_2y_2 = x_1(y_1-y_2) + y_2(x_1-x_2) \in x_1J + y_2I \subseteq I + J$. 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 dimostrare l'iniettività osserviamo che un elemento α di $A/I \otimes A/J$ si può scrivere come somma finita

$$\alpha = \sum_{i=1}^{k} \overline{x_i} \otimes \overline{y_i} = \Big(\sum_{i=1}^{k} \overline{x_iy_i}\Big) \otimes \overline{1} = \overline{\beta} \otimes \overline{1},$$

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 $\beta = x + y$ per qualche $x \in I$ e $y \in J$, e

$$\overline{\beta}\otimes\overline{1} = \overline{x+y}\otimes\overline{1} = \overline{y}\otimes\overline{1} = \overline{1}\otimes\overline{y} = \overline{1}\otimes\overline{0} = 0.$$

Soluzione E. 11.4. Siano $\{e_i\}_{i\in I}$ e $\{e'_j\}_{j\in J}$ basi di M e N rispettivamente. Sappiamo già che $\{e_i \otimes e'_j : i \in I,\ j \in J\}$ è un insieme di generatori di $M \otimes N$, cf. **T.5.3**.4. Vogliamo dunque provare che tale insieme è libero.
Supponiamo di avere una combinazione lineare finita $\sum_{i\in I_0,\, j\in J_0} c_{ij}(e_i \otimes e'_j) = 0$ e dimostriamo che i coefficienti c_{ij} sono tutti nulli; basta vedere che fissata una qualunque coppia di indici i_0 e j_0, il coefficiente corrispondente $c_{i_0j_0}$ è 0.
Sia $f\colon M \times N \longrightarrow A$ la mappa bilineare definita da $f(m,n) = a_{i_0}b_{j_0}$, per ogni $m = \sum_i a_ie_i$ e $n = \sum_j b_je'_j$. Consideriamo il diagramma

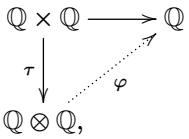
$$\begin{array}{ccc} M \times N & \xrightarrow{f} & A \\ {\scriptstyle\tau}\downarrow & \nearrow_{\tilde{f}} & \\ M \otimes N, & & \end{array}$$

che è commutativo e dunque $\tilde{f}(m\otimes n) = a_{i_0}b_{j_0}$, per ogni tensore elementare $m\otimes n$. In particolare abbiamo $\tilde{f}(e_{i_0}\otimes e'_{j_0}) = 1$ e $\tilde{f}(e_i\otimes e'_j) = 0$ se $(i,j) \neq (i_0,j_0)$. In conclusione abbiamo

$$0 = \tilde{f}(0) = \tilde{f}\Big(\sum_{i,j} c_{ij}(e_i\otimes e'_j)\Big) = c_{i_0j_0},$$

come volevamo.

Soluzione E. 11.5. 1. Consideriamo il diagramma



dove la mappa orizzontale è l'usuale moltiplicazione in $\mathbb{Q}$ che è $\mathbb{Z}$-bilineare. Esiste dunque un unico omomorfismo φ che fa commutare il diagramma, i.e. tale che $\varphi(x\otimes y)=xy$. Vogliamo dimostrare che φ è un isomorfismo.
Dato che $\varphi(x\otimes 1)=x$ per ogni $x\in\mathbb{Q}$, abbiamo che φ è surgettivo.
Per dimostrare l'iniettività, osserviamo che

$$L=\{x\otimes 1\colon x\in\mathbb{Q}\}$$

è un insieme di generatori di $\mathbb{Q}\otimes\mathbb{Q}$. Infatti, se consideriamo un tensore elementare $m\otimes n$ con $n=a/b$, abbiamo

$$m\otimes\frac{a}{b}=\frac{mb}{b}\otimes\frac{a}{b}=\frac{m}{b}\otimes a=\frac{am}{b}\otimes 1\quad\text{con}\quad\frac{am}{b}\in\mathbb{Q},$$

e l'osservazione è provata. Ogni elemento di $\mathbb{Q}\otimes\mathbb{Q}$ è combinazione lineare finita a coefficienti in $\mathbb{Z}$ di tensori elementari e dunque si può scrivere come $x\otimes 1$, per un opportuno $x\in\mathbb{Q}$. Quindi, se $\varphi(x\otimes 1)=0$ allora $x=0$ da cui $x\otimes 1=0$.

2. Osserviamo che $\mathbb{C}$ è dotato della usuale struttura di $\mathbb{R}$-spazio vettoriale ed è un $\mathbb{R}$-modulo libero con base $\{1,i\}$. Un tensore elementare in $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ è del tipo

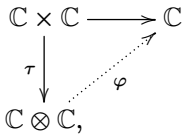
$$\begin{aligned}x\otimes y&=(a+ib)\otimes(c+id)\\&=a\otimes c+a\otimes id+ib\otimes c+ib\otimes id\\&=ac(1\otimes 1)+ad(1\otimes i)+bc(i\otimes 1)+bd(i\otimes i),\end{aligned}$$

per certi $a,b,c,d\in\mathbb{R}$. Gli elementi $1\otimes 1,\ 1\otimes i,\ i\otimes 1$ e $i\otimes i$ formano una base di $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$, cf. la soluzione di **E.11.4**. Consideriamo ora l'elemento

$$1\otimes 1+i\otimes i\in\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}.$$

Affinché sia un tensore elementare $(a+ib)\otimes(c+id)$, deve essere $ac=1,\ ad=0$, $bc=0$ e $bd=1$, che non ha soluzioni in $\mathbb{R}$.

3. Non è possibile. Se consideriamo l'analogo del diagramma precedente



abbiamo che, per ogni tensore elementare $x \otimes_{\mathbb{R}} y$, $0 = \varphi(x \otimes y) = xy$ implica $x = 0$ oppure $y = 0$. 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.5.4**.6.

Soluzione E. 11.6. Costruiamo il diagramma

$$\begin{array}{ccc} M \times N & \xrightarrow{\varphi} & M' \otimes N' \\ {\scriptstyle\tau}\downarrow & \nearrow_{\tilde{\varphi}} & \\ M \otimes N, & & \end{array}$$

dove $\varphi(m, n) = f(m) \otimes g(n)$ 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. 11.7. Per ogni tensore elementare $m \otimes n$ abbiamo

$$\begin{aligned} \big((f' \circ f) \otimes (g' \circ g)\big)(m \otimes n) &= (f' \circ f)(m) \otimes (g' \circ g)(n) \\ &= f'(f(m)) \otimes g'(g(n)) \\ &= (f' \otimes g')(f(m) \otimes g(m)) \\ &= (f' \otimes g')((f \otimes g)(m \otimes n)) \\ &= \big((f' \otimes g') \circ (f \otimes g)\big)(m \otimes n), \end{aligned}$$

come volevamo.

Soluzione E. 11.8. Basta controllare che tutti i tensori elementari $q \otimes_{\mathbb{Z}} \overline{a}$ sono nulli. Infatti

$$q \otimes_{\mathbb{Z}} \overline{a} = \frac{nq}{n} \otimes_{\mathbb{Z}} \overline{a} = \frac{q}{n} \otimes_{\mathbb{Z}} n\overline{a} = \frac{q}{n} \otimes_{\mathbb{Z}} \overline{0} = 0.$$

Soluzione E. 11.9. 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 $F_1 \simeq M_1 \oplus N_1$ e $F_2 \simeq M_2 \oplus N_2$, cf. **T.4.22**. Quindi

$$(M_1 \oplus M_2) \oplus (N_1 \oplus N_2) \simeq (M_1 \oplus N_1) \oplus (M_2 \oplus N_2) \simeq F_1 \oplus F_2,$$

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

$$F \simeq (N_1 \oplus N_2) \oplus M \simeq (M \oplus N_1) \oplus N_2 \simeq (M \oplus N_2) \oplus N_1;$$

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.5.4**.4, abbiamo

$$\begin{aligned} F_1 \otimes F_2 &\simeq (N_1 \oplus M_1) \otimes (N_2 \oplus M_2) \\ &\simeq (N_1 \otimes N_2) \oplus (N_1 \otimes M_2) \oplus (M_1 \otimes N_2) \oplus (M_1 \otimes M_2), \end{aligned}$$

dove $F_1 \otimes F_2$ è libero grazie a **E.11.4**.

3. Considerando $\mathbb{Z}/(n)$ come $\mathbb{Z}$-modulo si ha, per esempio, $\mathbb{Z}/(2) \otimes \mathbb{Z}/(3) = 0$, cf. **E.11.3**. È chiaro che 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 tensoriale è esatto a destra, cf. **T.5.6**, basta controllare che cosa succede tensorizzando le applicazioni iniettive.
Sia dunque $f\colon M \longrightarrow N$ un omomorfismo iniettivo e consideriamo il seguente diagramma

$$\begin{array}{ccc} M \otimes (N_1 \oplus N_2) & \xrightarrow{f\otimes(\mathrm{id}_{N_1},\mathrm{id}_{N_2})} & N \otimes (N_1 \oplus N_2) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ (M \otimes N_1) \oplus (M \otimes N_2) & \xrightarrow{(f\otimes\mathrm{id}_{N_1},f\otimes\mathrm{id}_{N_2})} & (N \otimes N_1) \oplus (N \otimes N_2), \end{array}$$

dove α e β sono gli isomorfismi dati da **T.5.4**.4. Si ha che $f \otimes (\mathrm{id}_{N_1}, \mathrm{id}_{N_2})$ è iniettiva se e solo se $f \otimes \mathrm{id}_{N_1}$ e $f \otimes \mathrm{id}_{N_2}$ sono iniettive.

5. Sia $f\colon M \longrightarrow N$ un omomorfismo iniettivo; allora $M \otimes N_1 \xrightarrow{f\otimes\mathrm{id}_{N_1}} N \otimes N_1$ è iniettivo e quindi è iniettivo anche

$$(M \otimes N_1) \otimes N_2 \xrightarrow{(f\otimes\mathrm{id}_{N_1})\otimes\mathrm{id}_{N_2}} (N \otimes N_1) \otimes N_2,$$

dove, chiaramente, $(f \otimes \mathrm{id}_{N_1}) \otimes \mathrm{id}_{N_2} = f \otimes (\mathrm{id}_{N_1} \otimes \mathrm{id}_{N_2})$.

6. Si consideri nuovamente $\mathbb{Z}/(2) \otimes \mathbb{Z}/(3) = 0$, dove 0 è piatto ma né $\mathbb{Z}/(2)$ né $\mathbb{Z}/(3)$ lo sono.

Soluzione E. 11.10. 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.4.13** e **T.5.4**.5; calcoliamo dunque $\mu(M \otimes_A N) = \dim_K((M \otimes_A N) \otimes_A K)$. Utilizzando le proprietà del prodotto tensoriale e **T.5.8** abbiamo che

$$\begin{aligned} (M \otimes_A N) \otimes_A K &\simeq M \otimes_A (N \otimes_A K) \simeq M \otimes_A (K \otimes_A N) \\ &\simeq M \otimes_A ((K \otimes_K K) \otimes_A N) \simeq M \otimes_A (K \otimes_K (K \otimes_A N)) \\ &\simeq (M \otimes_A K) \otimes_K (N \otimes_A K) \simeq K^{\mu(M)} \otimes_K K^{\mu(N)} \\ &\simeq K^{\mu(M)\mu(N)}, \end{aligned}$$

come volevamo.

Soluzione E. 11.11. Dall'esercizio precedente segue che $\mu(M) = 0$ oppure $\mu(N) = 0$. Quindi $M = \mathfrak{m}M$ oppure $N = \mathfrak{m}N$, e la conclusione discende dal Lemma di Nakayama.

Soluzione E. 11.12. La verifica del fatto che M è un $\mathbb{Z}$ modulo è lasciata al lettore.
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 $m, n \in \mathbb{N}$; abbiamo

$$\begin{aligned}\alpha \otimes \beta &= \frac{ap^n}{p^{n+m}} \otimes \beta = p^n \frac{a}{p^{n+m}} \otimes \beta = \frac{a}{p^{n+m}} \otimes p^n \beta \\ &= \frac{a}{p^{n+m}} \otimes \overline{\frac{bp^n}{p^n}} = \frac{a}{p^{n+m}} \otimes \overline{\frac{b}{1}} = \frac{a}{p^{n+m}} \otimes \overline{0} = 0.\end{aligned}$$

Soluzione E. 11.13. 1. Per **E.11.3** si ha

$$\mathbb{Q}[x]/(x) \otimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/(x^2+1) \simeq \mathbb{Q}[x]/(x, x^2+1) = 0;$$

quindi la dimensione è zero.

2. Abbiamo $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[x]/(x^5-3)$, quindi $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}[\alpha] \simeq \mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}[x]/(x^5-3)$. Inoltre, da **T.5.4**.5 segue che $\mathbb{C} \simeq \mathbb{C}[x]/(x) \simeq \mathbb{C}[x] \otimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/(x)$. Dato che $\mathbb{Q}[x]/(x)$ è un $(\mathbb{Q}[x], \mathbb{Q})$-bimodulo, per **T.5.8** 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 $\mathbb{Q}[\alpha] \simeq \mathbb{Q}^5$ come $\mathbb{Q}$-spazio vettoriale; pertanto $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}[\alpha] \simeq \mathbb{C}^5$.

Soluzione E. 11.14. Siano M un A-modulo proiettivo finitamente generato e $\{m_1, \dots, m_n\}$ un suo insieme minimale di generatori. Consideriamo l'omomorfismo $\phi\colon A^n \longrightarrow M$ definito da $e_i \mapsto m_i$, dove $\{e_1, \dots, e_n\}$ è la base canonica di A^n. Abbiamo allora una successione esatta corta

$$0 \longrightarrow N = \operatorname{Ker}\phi \longrightarrow A^n \longrightarrow M \longrightarrow 0.$$

Visto che M è proiettivo per ipotesi, la successione spezza e $A^n \simeq M \oplus N$. Tensorizzando con $A/\mathfrak{m}$, otteniamo $K^n \simeq M/\mathfrak{m}M \oplus N/\mathfrak{m}N$ come K-spazi vettoriali. Dato che $\dim_K M/\mathfrak{m}M = \dim_K K^n = n$ per **T.4.13**, abbiamo $N/\mathfrak{m}N = 0$, cioè $N = \mathfrak{m}N$. Il modulo N è finitamente generato in quanto addendo diretto di un modulo finitamente generato; quindi, applicando il Lemma di Nakayama, deduciamo che $N = 0$ e che $M \simeq A^n$ è libero.

Soluzione E. 11.15. Sia H un qualsiasi ideale di A; tensorizzando la successione esatta $0 \longrightarrow H \longrightarrow A \longrightarrow A/H \longrightarrow 0$ con B, che è A-piatto, si ottiene il diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H \otimes_A B & \longrightarrow & A \otimes_A B & \longrightarrow & A/H \otimes_A B & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \simeq & & \downarrow \simeq & & \\ 0 & \longrightarrow & HB & \longrightarrow & B & \longrightarrow & B/HB & \longrightarrow & 0. \end{array}$$

Dal Lemma del serpente segue dunque che

$$H \otimes_A B \simeq HB \quad \text{per ogni ideale } H \text{ di } A.$$

Tensorizzando con B la successione esatta corta di A-moduli

$$0 \longrightarrow I \cap J \xrightarrow{f} I \oplus J \xrightarrow{g} I + J \longrightarrow 0,$$

dove $f(a) = (a, -a)$ e $g(a, b) = a + b$, essa rimane esatta. Otteniamo dunque

$$0 \longrightarrow (I \cap J)B \longrightarrow IB \oplus JB \longrightarrow IB + JB \longrightarrow 0$$

e confrontando con

$$0 \longrightarrow IB \cap JB \longrightarrow IB \oplus JB \longrightarrow IB + JB \longrightarrow 0$$

si ottiene la tesi.

Soluzione E. 11.16. 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.4.18**. Dato che $a \in (a^2)$, esiste $c \in A$ tale che $a = ca^2$. Definiamo $r(b) = ca \cdot b$ per ogni $b \in A$. Abbiamo allora $r \circ j(a) = ca^2 = a$, da cui segue che $r \circ j = \mathrm{id}_{(a)}$.

$2 \Rightarrow 3$. Dato che A è libero, e dunque piatto, anche i suoi addendi diretti lo sono per **E.11.9**.4. Per ipotesi esiste un A-modulo M tale che $A \simeq (a) \oplus M$; dunque $M \simeq A/(a)$ è piatto.

$3 \Rightarrow 1$. 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 l'omomorfismo indotto $(a)/(a^2) \simeq (a) \otimes A/(a) \longrightarrow A/(a)$ è iniettivo ed è anche l'omomorfismo nullo. L'unica possibilità è che $(a)/(a^2) = 0$, cioè la tesi.

Soluzione E. 11.17. 1. Sia $I \neq A$ un ideale; allora esiste $\mathfrak{m}$ massimale tale che $I \subseteq \mathfrak{m}$. Quindi $IM \subseteq \mathfrak{m}M \subsetneq M$ da cui la tesi.

2. Siano $n \in N \setminus \{0\}$ e $N_1 = \langle n \rangle \simeq A/\operatorname{Ann} n$.
Consideriamo l'omomorfismo di inclusione $f\colon N_1 \longrightarrow N$ e tensorizziamo con M. Visto che M è piatto, si ottiene un omomorfismo iniettivo $f \otimes \mathrm{id}_M\colon N_1 \otimes M \longrightarrow N \otimes M$. Abbiamo

$$N_1 \otimes M \simeq A/\operatorname{Ann} n \otimes M \simeq M/(\operatorname{Ann} n)M,$$

e basta provare che $M/(\operatorname{Ann} n)M \neq 0$. Dato che $n \neq 0$, l'ideale $\operatorname{Ann} n$ è proprio; la tesi segue ora dal punto 1.

Soluzione E. 11.18. 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 un omomorfismo iniettivo $\cdot a \otimes \mathrm{id}_N\colon A \otimes_A N \longrightarrow A \otimes_A N$. L'omomorfismo indotto $\varphi\colon N \longrightarrow N$ definito da $\varphi(n) = an$ è quindi iniettivo, come volevamo.

Soluzione E. 11.19. 1. Dire che I, rispettivamente J e $I \cap J = IJ$, sono liberi equivale a dire che non esiste $a \neq 0$ tali che ax, rispettivamente ay e axy, sia nullo, e ciò è banalmente vero visto che siamo in un dominio.

2. Chiaramente anche $I + J = (x, y)$ non ha torsione.
Consideriamo l'omomorfismo $\varphi\colon I/IJ \oplus J/IJ \longrightarrow A/IJ$ dato da $\varphi(\overline{f}, \overline{g}) = \overline{f - g}$; è facile vedere che φ è ben definito e iniettivo. Tensorizzando con $I + J$ e ricordando **T.5.4**.4 e 5, si ottiene un omomorfismo

$$\widehat{\varphi}\colon (I/IJ \otimes (I + J)) \oplus (J/IJ \otimes (I + J)) \longrightarrow (I + J)/IJ,$$

dove

$$\widehat{\varphi}(\overline{x} \otimes y, \overline{y} \otimes x) = \overline{xy} - \overline{yx} = 0.$$

Notiamo che se $\overline{x} \otimes y = 0$, allora si ha $I/IJ \otimes J = \langle \overline{x} \otimes y \rangle = 0$, cf. **T.5.3**.3; ma $I/IJ \otimes J \simeq I/IJ \otimes A \neq 0$ e quindi $\overline{x} \otimes y \neq 0$. Pertanto $\widehat{\varphi}$ non è iniettivo e $I + J$ non è piatto.

Soluzione E. 11.20. Ricordiamo che $\operatorname{Hom}_A(A, M) \simeq M$ per **T.4.2**. Usando **E.10.16** e **T.5.4** si ottiene

$$\begin{aligned}\operatorname{Hom}(M, M) \otimes \operatorname{Hom}(N, N) &\simeq \operatorname{Hom}(A^r, A^r) \otimes \operatorname{Hom}(A^s, A^s) \\ &\simeq \operatorname{Hom}(A, A^r)^r \otimes \operatorname{Hom}(A, A^s)^s \\ &\simeq A^{r^2} \otimes A^{s^2} \simeq A^{r^2 s^2}\end{aligned}$$

per qualche $r, s \in \mathbb{N}_+$. Quest'ultimo modulo è isomorfo a

$$\begin{aligned}\operatorname{Hom}(A^r \otimes A^s, A^r \otimes A^s) &\simeq \operatorname{Hom}(A^{rs}, A^{rs}) \\ &\simeq \operatorname{Hom}(A, A^{rs})^{rs} \simeq A^{(rs)^2}.\end{aligned}$$

Soluzione E. 11.21. 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 $\operatorname{Coker}\varphi \simeq \mathbb{Z} \oplus \mathbb{Z}/(4) \oplus \mathbb{Z}/(12)$. Da **T.5.4**.4 e **E.11.3** si ottiene allora

$$\mathbb{Z}/(15) \otimes_{\mathbb{Z}} (\mathbb{Z}/(4) \oplus \mathbb{Z}/(12)) \simeq \mathbb{Z}/(15,4) \oplus \mathbb{Z}/(15,12) \simeq \mathbb{Z}/(3).$$

Soluzione E. 11.22. 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

$$M_a \otimes \mathbb{Z}/(n) \neq 0 \quad \text{se e solo se} \quad \gcd(2a+1, n) \neq 1.$$

17.5 Soluzioni del capitolo 12

Soluzione E. 12.1. Consideriamo la localizzazione A_a; si ha $A_a \neq 0$ poiché se fosse $\frac{1}{1} = \frac{0}{1}$ allora esisterebbe $n \geq 1$ tale che $a^n = 1a^n = 0$, che è contro l'ipotesi. Quindi esiste un ideale massimale in A_a e, per la corrispondenza biunivoca tra gli ideali primi di A e quelli di A_a, 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.1.14**.1.

Soluzione E. 12.2. In generale vale che $\sigma_S(A^*) \subseteq (S^{-1}A)^*$.
Se σ_S è un isomorfismo allora $\sigma_S(s) = \frac{s}{1} \in (S^{-1}A)^* = \sigma_S(A^*)$ per ogni $s \in S$. Dunque $s \in \sigma_S^{-1}((S^{-1}A)^*) = A^*$ e $S \subseteq A^*$.

Viceversa, se $S \subseteq A^*$ allora, per la proprietà universale dell'anello delle frazioni **T.6.4**, l'omomorfismo identità id_A si fattorizza tramite un omomorfismo $\varphi\colon S^{-1}A \longrightarrow A$ che è ovviamente surgettivo.
L'iniettività di φ 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. 12.3. Ricordiamo che A finito implica $A = A^* \sqcup \mathcal{D}(A)$, cf. **T.1.1**. Dato che σ_S è iniettivo, $S \cap \mathcal{D}(A) = \emptyset$ per **T.6.3**.1 e quindi $S \subseteq A^*$. La conclusione segue da **E.12.2**.

Soluzione E. 12.4. 1. Sia $A_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \colon\ b \not\equiv 0 \mod p \right\}$; è facile verificare che è un sottoanello di $\mathbb{Q}$, cf. **E.8.37**.
Definiamo $f \colon \mathbb{Z} \longrightarrow A_{(p)}$ tramite $f(a) = \frac{a}{1}$, allora $f(S) \subseteq A_{(p)}^*$ e, per la proprietà universale, otteniamo un omomorfismo $\tilde{f} \colon S^{-1}\mathbb{Z} \longrightarrow A_{(p)}$ 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 $a = 0$. Quindi $S^{-1}\mathbb{Z} \simeq A_{(p)}$.

2. Sia $B = \left\{ \frac{a}{b} \in \mathbb{Q} \colon\ b \not\equiv 0 \mod p_i \text{ per ogni } i \right\}$. Partendo dall'omomorfismo $f \colon \mathbb{Z} \longrightarrow B$ 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 con $0, \dots, 11$ gli elementi di A. Abbiamo $S = \{1, 2, 4, 8\}$ e $\frac{2}{s}$, $\frac{4}{s}$, $\frac{8}{s}$ sono elementi invertibili di $S^{-1}A$ per ogni $s \in S$. Inoltre

$$\frac{0}{s} = \frac{3}{s} = \frac{6}{s} = \frac{9}{s}, \quad \frac{1}{s} = \frac{4}{s} = \frac{7}{s} = \frac{10}{s} \quad \text{e} \quad \frac{2}{s} = \frac{5}{s} = \frac{8}{s} = \frac{11}{s} \quad \text{per ogni } \ s \in S.$$

Infine, abbiamo anche $\frac{1}{2^k} = \frac{2^k}{1}$ 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 con tre elementi, quindi isomorfo a $\mathbb{Z}/(3)$.

4. In questo caso $S = \{1, 3, 5, 7, 9, 11\}$ e si verifica facilmente che $\frac{a}{s} = \frac{b}{s}$, rispettivamente $\frac{a}{s} = \frac{a}{t}$, se e solo se $4 \,|\, a - b$, rispettivamente $4 \,|\, s - t$.
Dunque è sufficiente considerare numeratori $0, 1, 2, 3$ e denominatori $1, 3$. 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 dunque 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 $0, 1, 2$ e denominatori $1, 2$ 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, i.e. $S^{-1}A \simeq \mathbb{Z}/(3)$.

Alternativamente, 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.12.5**.1, e semplificare le dimostrazioni usando l'isomorfismo $S^{-1}A \simeq A/\operatorname{Ker}\sigma_S$.

Soluzione E. 12.5. 1. Sia $\frac{a}{s} \in S^{-1}A$ e proviamo che esiste $b \in A$ tale che $\frac{a}{s} = \frac{b}{1} = \sigma_S(b)$. Dato che S è un insieme finito, per ogni $s \in S$ esistono $r, k \in \mathbb{N}$ tali che $k > r$ e $s^k = s^r$. 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 $\operatorname{Ker}\sigma_S = \{a \in A \colon\ as = 0 \text{ per qualche } s \in S\} = (3)/(24)$, quindi, per il punto precedente, $S^{-1}A \simeq A/\operatorname{Ker}\sigma_S \simeq \mathbb{Z}/(3)$.

Soluzione E. 12.6. 1. Dato che I è un ideale, $0 \in I$ e dunque $1 \in S$. Presi due elementi $1 + i$, $1 + j \in S$, il loro prodotto $(1 + i)(1 + j) \in 1 + I + I^2 \subseteq 1 + I = S$; pertanto S è un insieme moltiplicativo.

Per la caratterizzazione del radicale di Jacobson **T.1.15** basta dimostrare che ogni elemento $\frac{x}{s} \in S^{-1}I$ è tale che $1 + \frac{x}{s}\frac{y}{t} \in (S^{-1}A)^*$, per ogni $\frac{y}{t} \in S^{-1}A$. È sufficiente osservare che $1 + \frac{x}{s}\frac{y}{t} = \frac{st+xy}{st}$ è invertibile in quanto $st + xy \in 1 + I$ per **T.6.7**.1a.

2. Indichiamo per semplicità con $0, \ldots, 59$ gli elementi di A.
Gli ideali non banali distinti di A sono (2), (3), (4), (5), (6), (10), (12), (15), (20) e (30). Abbiamo $-3 = 1 - 4 \in S$ e $5 = 1 + 4 \in S$. Pertanto $\frac{3}{1}$, $\frac{5}{1}$ 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 $\frac{4}{1} = 0$ implica $(0) = S^{-1}(4) = S^{-1}(12) = S^{-1}(20)$. Quindi in $S^{-1}A$ ci sono solo due ideali propri (0) e $S^{-1}(2)$. Dunque che $S^{-1}A$ è locale con ideale massimale generato da $\frac{2}{1}$.
In particolare $\operatorname{Ker}\sigma_S = (4)$ e $S^{-1}A \simeq \mathbb{Z}/(4)\mathbb{Z}$, per **E.12.5**.1.

3. Ricordiamo che i primi di $T^{-1}A$ sono in corrispondenza biunivoca con i primi di A che non intersecano T, cf. **T.6.8**. Si ha $(p) \cap T \neq \emptyset$ 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 come m un prodotto di almeno due primi divisori di 60, ad esempio $m = 6$ oppure 15, per ottenere un anello non locale $T^{-1}A$.

Soluzione E. 12.7. 1. Consideriamo l'omomorfismo $f\colon A \times B \longrightarrow A$ dato da $f(a, b) = a$ e notiamo che

i) per ogni $s \in S$, $f(s) = 1$ è invertibile;

ii) se $f(a, b) = a = 0$ allora $(1, 0)(a, b) = (0, 0)$ con $(1, 0) \in S$;

iii) per ogni $a \in A$, si ha $a = f(a, b)f(1, 0)^{-1}$.

Allora f si estende ad un isomorfismo $\tilde{f}\colon S^{-1}C \longrightarrow A$ per **T.6.5**.

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 $((1, b), (1, 1)) \sim ((1, 0), (1, 0))$. 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. 12.8. Poniamo $B = A[x]/(1 - fx)$.
Se f è nilpotente allora esiste $n \in \mathbb{N}$ tale che $f^n = 0$. Quindi $A_f = 0$ e $1 = (1 - (fx)^n) = (1 - fx)(1 + fx + \ldots + (fx)^{n-1}) \in (1 - fx)$ implica che anche $B = 0$.
Sia ora $f^n \neq 0$ per ogni n; definiamo $\varphi\colon A \xrightarrow{\mathrm{i}} A[x] \xrightarrow{\pi} B$ ponendo $\varphi(a) = \overline{a}$. Dato che $\overline{f}\overline{x} = \overline{1}$ in B, $\overline{f^k}$ è invertibile in B per ogni k; quindi φ si fattorizza attraverso A_f ed esiste $\psi\colon A_f \longrightarrow B$ definito da

$$\psi\left(\frac{a}{f^k}\right) = \varphi(a)\varphi(f^k)^{-1}.$$

Proviamo che ψ è un isomorfismo utilizzando **T.6.5**. 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 intero 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 $a = p(x)(1 - xf)$. Dunque $b_0 = a$, $b_1 = fb_0 = fa$, ..., $b_h = fb_{h-1} = f^h a$ e $fb_h = f^{h+1}a = 0$.
Infine, ogni $\overline{b} \in B$ si scrive come $\overline{b} = \sum_{i=0}^{k} \overline{b_i}\overline{x}^i = \frac{1}{\overline{f}^k} \sum_{i=0}^{k} \overline{b_i\ f^{k-i}}$. Quindi $\overline{b}$ è della forma $\varphi(a)\varphi(f^k)^{-1}$, come volevamo.

Soluzione E. 12.9. 1. Si ha certamente

$$\mathbb{Z}\left[\tfrac{2}{3}\right] \subseteq \mathbb{Z}\left[\tfrac{1}{3}\right] \simeq \mathbb{Z}[x]/(1-3x) \simeq \mathbb{Z}_3$$

per l'esercizio precedente.

Per l'altra inclusione, dato che $1 - \frac{2}{3} = \frac{1}{3}$, possiamo scrivere ogni elemento $\frac{1}{3^n}$ come somma finita di potenze di $\frac{2}{3}$ a coefficienti interi.

2. Sia $A \subsetneq \mathbb{Q}$; 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 insieme 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 $bm + cp = 1$. Si ha $\frac{1}{p} = bsa + c \in A$ e questo implica $S^{-1}\mathbb{Z} \subseteq A$.

L'altra inclusione segue direttamente dalla definizione di S.

Soluzione E. 12.10. Abbiamo visto in **E.9.9** 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). Dunque l'immagine di $f = x^3z - y^2$ è un elemento di J.

Soluzione E. 12.11. Abbiamo visto in **E.9.13** 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

$$I = (x^2 - 3, y) \cap (x - 1, y - 1) \cap (x + 1, y + 1).$$

Dunque $I \subset \mathfrak{p}_1$ e $I_{\mathfrak{p}_1} \cap \mathbb{C}[x,y] \neq (1)$. Dato che $y^3 - y = (y^2 + y)(y-1)$ e $y^2 + y$ è invertibile in $\mathbb{C}[x,y]_{\mathfrak{p}_1}$, 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 $x - 1 \in I_{\mathfrak{p}_1}$. Quindi $I_{\mathfrak{p}_1} \cap \mathbb{C}[x,y] = \mathfrak{p}_1$.
Invece $I \not\subset (x,y)$ e così $I_{\mathfrak{p}_2} \cap \mathbb{C}[x,y] = (1)$.

Soluzione E. 12.12. Abbiamo visto in **E.9.15** che $\sqrt{I} = (x,y) \cap (x^4 + 1, x^3 + y)$. Quindi, per **T.6.9**.4, $\sqrt{I_{(x,y)}} = (\sqrt{I})_{(x,y)} = (x,y)_{(x,y)}$. Dato che $f = x^2 + 5x$, abbiamo $\frac{f}{1} \in \sqrt{I_{(x,y)}}$.

Soluzione E. 12.13. Da **E.9.18**.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.9.18**.3 segue che $I_{(x,z)} = (x^2, z)_{(x,z)}$. 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. 12.14. Da **E.9.24** segue che $I = (x - yz, yz^2 - y)$. Dato che $z^2 - 1$ è invertibile in $S^{-1}A$, si ha

$$S^{-1}(A/I) \simeq K[x,y,z]_{(x,y)}/I_{(x,y)} \simeq K[x,y,z]_{(x,y)}/(x,y)_{(x,y)} \simeq K(z).$$

Soluzione E. 12.15. Da **E.9.34** segue che $I = (x^2 - yz, xz - yz, y^2 - yz)$. Dato che $\overline{z}, \overline{y - z}$ sono invertibili in $S^{-1}A$, da $\overline{z}(\overline{x - y}) = (\overline{y - z})\overline{y} = \overline{0}$ in A, otteniamo $\frac{x}{1} = \frac{y}{1} = 0$. Quindi $S^{-1}A \simeq \mathbb{Q}(z)$.

Soluzione E. 12.16. 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

$$\frac{a}{p^n} \otimes \overline{\frac{b}{p^m}} = \frac{ap^m}{p^{n+m}} \otimes \overline{\frac{b}{p^m}} = \frac{a}{p^{n+m}} \otimes \overline{\frac{p^m b}{p^m}} = \frac{a}{p^{n+m}} \otimes \bar{b} = 0,$$

perché $b \in \mathbb{Z}$.

Soluzione E. 12.17. Per definizione $\mathbb{Z}_2 = \{\frac{a}{2^n} \in \mathbb{Q} \colon a \in \mathbb{Z},\ n \in \mathbb{N}\} = S^{-1}\mathbb{Z}$, dove S è l'insieme moltiplicativo delle potenze di 2. Se $p \neq 2$ allora $(p) \cap S = \emptyset$ e quindi $S^{-1}(p) = (p)\mathbb{Z}_2$ è un ideale primo di $\mathbb{Z}_2$. Dato che $2 \in \mathbb{Z}_2 \setminus (p)\mathbb{Z}_2$ possiamo definire

$$f \colon \mathbb{Z}_2 \times \mathbb{Z}_{(p)} \longrightarrow (\mathbb{Z}_2)_{(p)\mathbb{Z}_2}, \qquad f\left(\frac{a}{2^n}, \frac{c}{d}\right) = \frac{ac}{2^n d},$$

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

$$\begin{array}{ccc} \mathbb{Z}_2 \times \mathbb{Z}_{(p)} & \xrightarrow{f} & (\mathbb{Z}_2)_{(p)\mathbb{Z}_2} \\ \downarrow & \nearrow_{\tilde{f}} & \\ \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}. & & \end{array}$$

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 surgettivo, è un isomorfismo.
Se $p = 2$ possiamo considerare il diagramma commutativo

$$\begin{array}{ccc} \mathbb{Z}_2 \times \mathbb{Z}_{(2)} & \xrightarrow{g} & \mathbb{Q} \\ \downarrow & \nearrow_{\tilde{g}} & \\ \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_{(2)}, & & \end{array}$$

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. 12.18. 1. Sia $a \in A$ tale che $\sigma_S(a) = 0$; allora esiste $s \in S$ tale che $as = 0$. Dato che $s \notin \mathcal{D}(A)$ otteniamo subito $a = 0$.

D'altra parte, se $T \supsetneq S$, allora T contiene un divisore di zero b tale che $bc = 0$ per qualche $c \neq 0$. Quindi $\sigma_T(c) = \frac{c}{1} = \frac{0}{1}$ e σ_T non è iniettiva.

2. Sia $\frac{a}{s} \in S^{-1}A$ e supponiamo che non sia un divisore di zero; allora $\frac{a}{1}$ non è un divisore di zero e vogliamo dimostrare che $a \notin \mathcal{D}(A)$. Se $ab = 0$, per qualche $b \in A$ allora $\frac{a}{1} \cdot \frac{b}{1} = 0$, quindi $\sigma_S(b) = \frac{b}{1} = 0$ e l'iniettività di σ_S implica $b = 0$. 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 $\sigma_S(as^{-1}) = \frac{as^{-1}}{1} = \frac{a}{s}$ per ogni $\frac{a}{s} \in S^{-1}A$. Dunque σ_S è surgettiva e la conclusione segue dal punto 1.

4. Quando $\mathcal{D}(A) = \{0\}$ e $S = A \setminus \{0\}$, per il punto 2 ogni elemento non nullo di $Q(A)$ è invertibile; 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.

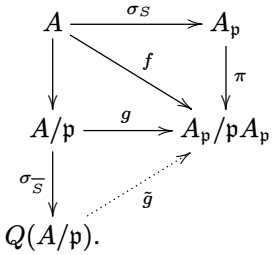
Soluzione E. 12.19. Sia $S = A \setminus \mathfrak{p}$ e consideriamo l'omomorfismo definito da

$$f\colon A \xrightarrow{\sigma_S} A_{\mathfrak{p}} \xrightarrow{\pi} A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}.$$

È facile vedere che $\operatorname{Ker} f = \mathfrak{p}$, quindi f induce un omomorfismo iniettivo

$$g\colon A/\mathfrak{p} \longrightarrow A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}\,, \quad \overline{a} \mapsto \frac{a}{1} + \mathfrak{p}A_{\mathfrak{p}}.$$

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 g induce un omomorfismo $\tilde{g}\colon Q(A/\mathfrak{p}) = \overline{S}^{-1}(A/\mathfrak{p}) \longrightarrow A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$



Ogni elemento di $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ si scrive come $\frac{a}{s} + \mathfrak{p}A_{\mathfrak{p}} = g(\overline{a})g(\overline{s})^{-1}$; inoltre g è iniettiva, pertanto la conclusione segue da **T.6.5**.

Soluzione E. 12.20. Dato un qualsiasi $a \neq 0$, in generale abbiamo $A_a \subseteq Q(A)$. Siano ora $(0) = \mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_k$ gli ideali primi distinti di A. Se $k = 0$, allora A è un campo e $A_a = A = Q(A)$ per ogni $a \neq 0$.
Sia allora $k > 0$ e consideriamo $\bigcap_{i=1}^{k} \mathfrak{p}_i$; se questa intersezione è zero allora, per **T.1.12**.1, $\bigcap_{i=1}^{k} \mathfrak{p}_i = \mathfrak{p}_0$ implica $\mathfrak{p}_i = \mathfrak{p}_0$ per qualche $i > 0$ e ciò contraddice

l'ipotesi. Possiamo dunque considerare $0 \neq a \in \bigcap_{i=1}^{k} \mathfrak{p}_i$ e l'anello A_a. Dato che $\mathfrak{p}_i A_a = A_a$ per ogni $i > 0$, l'anello A_a non ha ideali primi diversi da zero, quindi è un campo che contiene A. Essendo $Q(A)$ il più piccolo campo che contiene A, abbiamo $Q(A) \subseteq A_a$ e di conseguenza la tesi.

Alternativamente, possiamo provare l'inclusione non banale nel seguente modo. Sia $\frac{b}{c} \in Q(A)$ e consideriamo $\sqrt{(c)}$. Si ha $a \in \bigcap_{i=1}^{k} \mathfrak{p}_i \subseteq \bigcap_{i:\, c \in \mathfrak{p}_i} \mathfrak{p}_i = \sqrt{(c)}$, quindi esiste 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. 12.21. 1. Prima di tutto osserviamo che $\mathcal{D}(A) = \bigcup_{i=1}^{n} \overline{\mathfrak{p}}_i$. Infatti per ipotesi $\mathcal{D}(A) \supseteq \overline{\mathfrak{p}}_i$ per ogni i.

Per 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 $a \in \mathfrak{p}_i$.
Ponendo $S = A \setminus \bigcup_{i=1}^{n} \overline{\mathfrak{p}}_i$, si ha $Q(A) = S^{-1}A$ e gli ideali massimali di $Q(A)$ sono esattamente gli ideali $S^{-1}\overline{\mathfrak{p}}_i$ per $i = 1, \dots, n$. Da **T.6.13**.3 segue che $S^{-1}(A/\overline{\mathfrak{p}}_i) \simeq S^{-1}A/S^{-1}\overline{\mathfrak{p}}_i$ è un campo che contiene $A/\overline{\mathfrak{p}}_i$ per ogni $i = 1, \dots, n$. Inoltre, dato che $A/\mathfrak{p}_i$ è un dominio e $S \subseteq A \setminus \overline{\mathfrak{p}}_i$, possiamo considerare $S^{-1}(A/\overline{\mathfrak{p}}_i)$ come un sottoanello di $Q(A/\overline{\mathfrak{p}}_i)$, cf. la dimostrazione di **T.6.19**.6. Per **E.12.18**.4 abbiamo dunque

$$S^{-1}(A/\overline{\mathfrak{p}}_i) = Q(A/\overline{\mathfrak{p}}_i).$$

Da **T.6.13**.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 $S^{-1}A$; dunque, per il Teorema cinese del resto, si ha

$$\begin{aligned} Q(A) = S^{-1}A &\simeq \bigoplus_{i=1}^{n} S^{-1}A/S^{-1}\overline{\mathfrak{p}}_i \simeq \bigoplus_{i=1}^{n} S^{-1}(A/\overline{\mathfrak{p}}_i) \\ &\simeq \bigoplus_{i=1}^{n} Q(A/\overline{\mathfrak{p}}_i) \simeq \bigoplus_{i=1}^{n} Q(B/\mathfrak{p}_i), \end{aligned}$$

e ciò conclude la dimostrazione.

2. In questo caso $A \simeq \mathbb{C}[x,y]/(x) \cap (y)$ e $\mathcal{D}(A) = (x) \cup (y)$. Per il punto 1, $S^{-1}A \simeq \mathbb{C}(x) \oplus \mathbb{C}(y)$.

3. È facile verificare che l'ideale $(x^2 - y^3)$ è primo; di conseguenza $\mathcal{D}(A) = (0)$ e $S^{-1}A = Q(A)$ è il campo dei quozienti di A.

Soluzione E. 12.22. Abbiamo già visto in **E.10.21** 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 per **E.10.21**.

Soluzione E. 12.23. L'anello A è un dominio e la struttura di A-modulo di $Q(A)$ è definita per restrizione di scalari tramite l'omomorfismo canonico.

1. Abbiamo $Q(A) = K(x)$. Inoltre $Q(A) = (x)Q(A)$; infatti $m = x\frac{m}{x}$ per ogni $m \in Q(A)$, quindi $Q(A)/(x)Q(A) = 0$ che è ovviamente finitamente generato.

2. Supponiamo che $Q(A)$ sia finitamente generato. Dato che A è locale con ideale massimale (x) e $Q(A) = (x)Q(A)$, applicando il Lemma di Nakayama, si ha $Q(A) = 0$, contraddizione.

Soluzione E. 12.24. 1. Sia $s \in \operatorname{Ann} M \cap S$; allora, per ogni $\frac{m}{t} \in S^{-1}M$, si ha $\frac{m}{t} = \frac{0}{s}$ e dunque $S^{-1}M = 0$.

2. Sia $M = \langle m_1, \dots, m_r \rangle$; dato 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 $s \in \operatorname{Ann} M \cap S$.

3. Siano $A = \mathbb{Z}$ e $S = \{2^n : n \in \mathbb{N}\}$; consideriamo l'$A$-modulo

$$M = \bigoplus_{n \in \mathbb{N}} \mathbb{Z}/(2^{n+1}).$$

È facile verificare che $\operatorname{Ann} M = 0$, dunque $S \cap \operatorname{Ann} M = \emptyset$.
Ogni elemento $\alpha \in S^{-1}M$ si può scrivere come

$$\alpha = \left(\frac{\overline{a_0}}{s_0}, \dots, \frac{\overline{a_m}}{s_m}, 0, \dots, 0, \dots \right), \quad \text{con } \overline{a_i} \in \mathbb{Z}/(2^{i+1}) \text{ e } s_i \in S \text{ per ogni } i,$$

per qualche intero m. Ovviamente $2^{m+1}\alpha = 0$ e dunque $S^{-1}M = 0$.

Soluzione E. 12.25. Osserviamo che $(1) = (f_h : h \in H) \subseteq \sqrt{(f_h^{n_h} : h \in H)}$, per ogni scelta degli interi n_h, ovvero anche $\{f_h^{n_h} : h \in H\}$ è un insieme di generatori di A.
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. Per quanto appena osservato, possiamo scrivere 1 come somma finita di certi $a_i f_i^{n_i}$ con $a_i \in A$. Abbiamo allora $m = 1m = \sum a_i f_i^{n_i} m = 0$, come volevamo.

Soluzione E. 12.26. 1. Discende da **E.12.24**.1 e 2.

2. Per **T.6.12** la successione

$$0 \longrightarrow M'_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \longrightarrow M''_{\mathfrak{p}} \longrightarrow 0$$

è esatta per ogni $\mathfrak{p} \in \operatorname{Spec} A$; dunque $M_{\mathfrak{p}} \neq 0$ se e solo se $M'_{\mathfrak{p}} \neq 0$ oppure $M''_{\mathfrak{p}} \neq 0$.

3. Sia $\mathfrak{p} \in \operatorname{Spec} A$. Per **T.6.14**.2, abbiamo $(M \otimes_A N)_{\mathfrak{p}} = M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}}$. 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.11.11**, e la tesi segue immediatamente.

Soluzione E. 12.27. 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 $p = 2, 3, 5$.

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 $(\mathbb{Z}/(12))_{(3)} \simeq \mathbb{Z}/(3)$ come abbiamo visto in **E.12.4**.5.

Soluzione E. 12.28. 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 l'S-polinomio di $y^4 - 4$ e yz è $-4z$. Quindi M ha dimensione 4 su $\mathbb{Q}$.
2. Dato che M è un A-modulo finitamente generato, $S^{-1}M = 0$ se e solo se $S \cap \operatorname{Ann} M \neq \emptyset$, cf. **E.12.24**. Dunque $M_\mathfrak{p} \neq 0$ se e solo se $A \setminus \mathfrak{p} \subset A \setminus \operatorname{Ann} M$, ossia $\mathfrak{p} \supseteq \operatorname{Ann} M$, cf. **E.12.26**.1. 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. 12.29. Sia $\mathfrak{m} \subset A$ massimale. Se $I_\mathfrak{m} = 0$ allora $\operatorname{Ann} I \not\subset \mathfrak{m}$ per **E.12.26**.1. Se invece $I_\mathfrak{m} = A_\mathfrak{m}$ allora $I \not\subset \mathfrak{m}$; quindi $I + \operatorname{Ann} I \not\subset \mathfrak{m}$ per ogni ideale massimale $\mathfrak{m}$ di A. Dunque $I + \operatorname{Ann} I = A$ ed esistono $i \in I$ e $j \in \operatorname{Ann} I$ tali che $i + j = 1$. Notiamo che deve essere $i \neq 0$, altrimenti $j = 1$ e $I = 0$, contro l'ipotesi; inoltre $i = i(i + j) = i^2$ è idempotente.
Infine, per ogni $a \in I$, si ha $a = a(i + j) = ai$ e quindi $I = (i)$.

Soluzione E. 12.30. 1. Ovviamente $1 \in S$; inoltre, se $(q_1, p) = (q_2, p) = 1$ anche $(q_1 q_2, p) = 1$, dunque 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 quelle di **E.12.4**.1 e **E.12.4**.2 otteniamo

$$A = \left\{ \frac{f}{g} \in \mathbb{Q}(x) \colon (g, p) = 1 \right\}.$$

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 di A sono $\mathfrak{p}_1 = (0)$, $\mathfrak{p}_2 = (x - 1)$ e $\mathfrak{p}_3 = (x^2 + 2)$; solo $\mathfrak{p}_2$ e $\mathfrak{p}_3$ 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

$$A/(x - 1)A \simeq S^{-1}\mathbb{Q} \simeq \mathbb{Q} \quad \text{e} \quad A/(x^2 + 2)A \simeq S^{-1}\left(\mathbb{Q}[x]/(x^2 + 2)\right) \simeq \mathbb{Q}(\sqrt{-2}).$$

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. 12.31. Denotiamo $\overline{A} = A/I$, $\overline{M} = M/IM$ e $\overline{\mathfrak{m}} = \mathfrak{m}/I$, con $\mathfrak{m} \in \operatorname{Max} A$ contenente I. Basta provare che l'$\overline{A}$-modulo $\overline{M}$ è 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 $\mathfrak{m} \supseteq I$, cf. **T.6.15**. 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 prendere $m \in M \setminus IM$. Allora $I \subseteq IM : m \neq A$. Sia $\mathfrak{m}$ un ideale massimale tale che $IM : m \subseteq \mathfrak{m}$. Dato che $M_{\mathfrak{m}} = 0$ per ipotesi, abbiamo in particolare $\frac{m}{1} = 0$; quindi esiste $a \in A \setminus \mathfrak{m}$ tale che $am = 0$, che contraddice la scelta di $\mathfrak{m}$.

Soluzione E. 12.32. 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 $A_{\mathfrak{p}}$. 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 $sa^n = 0$ per qualche intero n. Scegliendo il minimo n con questa proprietà, otteniamo $sa^{n-1} \neq 0$ e quindi a è un divisore di zero, come volevamo.

3. Per **T.6.17**.1 essere ridotto è una proprietà locale, quindi $A_{\mathfrak{p}}$ è ridotto. Allora $\mathfrak{p}A_{\mathfrak{p}} = \mathcal{N}(A_{\mathfrak{p}}) = 0$ per il punto 1. Dunque l'ideale nullo è l'unico ideale massimale di $A_{\mathfrak{p}}$, che risulta essere un campo.

Soluzione E. 12.33. 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 $a \in A$, e quindi $(at)s = (as)t \in S$ implica $s, t \in \overline{S}$.

Soluzione E. 12.34. 1. Ovviamente $1 \in f^{-1}(T)$; inoltre $a, b \in f^{-1}(T)$ implica $f(ab) = f(a)f(b) \in T$, quindi $ab \in f^{-1}(T)$.

Viceversa, osserviamo che $1 \in T$ per ipotesi. Inoltre, 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 $st = f(ab) \in T$.

2. Sia $a \in \overline{f^{-1}(T)}$; allora esiste $b \in A$ tale che $ba \in f^{-1}(T)$, cioè $f(b)f(a) = f(ba) \in T$. Dato che T è saturato, si ha $f(a) \in T$ e quindi $a \in f^{-1}(T)$, come volevamo.

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 $ab \in f^{-1}(T)$; di conseguenza $a, b \in \overline{f^{-1}(T)} = f^{-1}(T)$ e $s = f(a) \in T$.

Soluzione E. 12.35. 1. Se $a, b \in I^S$ allora esistono $s, t \in S$ tali che $as, bt \in I$; quindi $(a + b)st \in I$. Inoltre $cas \in I$ per ogni $c \in A$, cioè $a + b, ac \in I^S$.

Alternativamente, possiamo osservare che **T.6.7**.1c implica $I^S = I^{ec}$ rispetto a σ_S, per ogni ideale I di A.

2a. Si ha $\sigma_S(a) = \frac{a}{1} = 0$ se e solo se esiste $u \in S$ tale che $au = 0$, cioè se e solo se $a \in (0)^S$.

2b. Segue immediatamente dal fatto che $1 \in S$.

2c. Sia $a \in I^S$; allora esiste $s \in S$ tale che $as \in I \subset J$ quindi $a \in J^S$.

2d. Per la parte b si ha $I^S \subseteq (I^S)^S$.

Per l'altra inclusione, se $a \in (I^S)^S$ esiste $s \in S$ tale che $as \in I^S$, quindi esiste $t \in S$ tale che $ast \in I$. Dato che $st \in S$, si ha $a \in I^S$.

2e. Per la parte b abbiamo che $IJ \subseteq I^S J^S$; quindi $(IJ)^S \subseteq (I^S J^S)^S$ per il punto c.

Per l'altra inclusione, 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 $t_i b_i \in J$. Poniamo $u = \prod_i s_i t_i$; 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 i punti c e d.

Soluzione E. 12.36. Le dimostrazioni di 1 e 2a sono del tutto analoghe a quelle di **E.12.35**.1, 2b e 2c.

2b. Dal punto precedente abbiamo $\sigma_S^{-1}(Q) \subseteq \sigma_S^{-1}(Q)^S$.

Per l'altra inclusione, sia $q \in \sigma_S^{-1}(Q)^S$; allora esiste $s \in S$ tale che $\frac{sq}{1} = \sigma_S(sq) \in Q$. Dunque $\frac{q}{1} \in Q$ e $q \in \sigma_S^{-1}(Q)$.

2c. 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.

2d. La dimostrazione è del tutto analoga a quella di **E.12.35**.2d.

2e. Discende immediatamente dal punto c e da **T.6.13**.2.

2f. Segue dal punto c e dal fatto che $\sigma_S^{-1}(N) + \sigma_S^{-1}(P) \subseteq \sigma_S^{-1}(N + P)$.

Soluzione E. 12.37. Siano $S_A = \{\overline{18}^n : n \in \mathbb{N}\}$ e $S_B = \{\overline{6}^n : n \in \mathbb{N}\}$ entrambi contenuti in $\mathbb{Z}/(200)$; per **T.6.19**.3

$$\overline{S}_B = (\mathbb{Z}/(200)) \setminus \bigcup_{\mathfrak{p} \cap S_B = \emptyset} \mathfrak{p} = (\mathbb{Z}/(200)) \setminus \bigcup_{\overline{2}, \overline{3} \notin \mathfrak{p}} \mathfrak{p} = \overline{S}_A.$$

Dunque

$$\begin{aligned}(\mathbb{Z}/(200))_{\overline{18}} &= S_A^{-1}(\mathbb{Z}/(200)) = \overline{S}_A^{-1}(\mathbb{Z}/(200)) \\ &= \overline{S}_B^{-1}(\mathbb{Z}/(200)) = S_B^{-1}(\mathbb{Z}/(200)) = (\mathbb{Z}/(200))_{\overline{6}}\end{aligned}$$

per **T.6.19**.6.

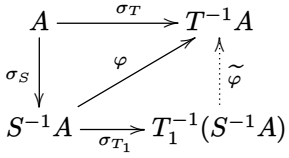
Inoltre $\overline{S}_B^{-1}(\mathbb{Z}/(200)) \simeq \overline{S}_B^{-1}(\mathbb{Z}/(8)) \times \overline{S}_B^{-1}(\mathbb{Z}/(25))$; dato che $\overline{2} \in \overline{S}_B$, si ha $\overline{S}_B^{-1}(\mathbb{Z}/(8)) = 0$. Infine l'omomorfismo $\sigma_{\overline{S}_B} : \mathbb{Z}/(25) \longrightarrow \overline{S}_B^{-1}(\mathbb{Z}/(25))$ è surgettivo, cf. **E.12.5**, ed iniettivo perché $5 \notin \overline{S}_B$, cf. **E.12.35**.2a.

Pertanto

$$S_A^{-1}(\mathbb{Z}/(200)) \simeq S_B^{-1}(\mathbb{Z}/(200)) \simeq \mathbb{Z}/(25).$$

Da **E.11.3** segue che $C \simeq \mathbb{Z}/(25,40) \simeq \mathbb{Z}/(5)$; dunque $A \simeq B \not\simeq C$.
Adesso consideriamo l'omomorfismo $\varphi\colon \mathbb{Z}_{(3)}[x] \longrightarrow (\mathbb{Z}_{(3)})_6$ 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.12.8**.
Infine, $\mathbb{Z}_{(3)}$ è un anello locale con unico ideale massimale generato dall'immagine di 3. In $(\mathbb{Z}_{(3)})_6$ si ha $\frac{1}{3} = \frac{2}{6}$, cioè 3 invertibile; quindi $(\mathbb{Z}_{(3)})_6 \subseteq \mathbb{Q}$ è un campo contenente $\mathbb{Z}$. Pertanto $D \simeq \mathbb{Q} \not\simeq A, B, C$.

Soluzione E. 12.38. 1. L'omomorfismo $\varphi\colon S^{-1}A \longrightarrow T^{-1}A$ dato da $\varphi\left(\frac{a}{s}\right) = \frac{a}{s}$ è ben definito e verifica $\varphi(T_1) \subseteq (T^{-1}A)^*$ per ipotesi; per la proprietà universale φ induce 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 $\sigma_S(t) \in T_1$. Inoltre, 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.6.5**.
2. Sia $U = \{st\colon s \in S \text{ e } t \in T\}$; è facile vedere che U è un insieme moltiplicativo che contiene S e T. Dal punto 1 otteniamo allora

$$\sigma_S(U)^{-1}(S^{-1}A) \simeq U^{-1}A \simeq \sigma_T(U)^{-1}(T^{-1}A).$$

Dimostriamo l'isomorfismo $\sigma_S(U)^{-1}(S^{-1}A) \simeq \sigma_S(T)^{-1}(S^{-1}A)$.
Consideriamo l'omomorfismo

$$\psi\colon S^{-1}A \longrightarrow \sigma_S(T)^{-1}(S^{-1}A), \qquad \text{definito da } \psi\left(\frac{a}{s}\right) = \frac{\frac{a}{s}}{1};$$

per ogni $\frac{u}{1} = \frac{st}{1} \in \sigma_S(U)$ si ha

$$\psi\left(\frac{st}{1}\right) \cdot \frac{\frac{1}{s}}{\frac{t}{1}} = \frac{\frac{st}{1}}{1} \cdot \frac{\frac{1}{s}}{\frac{t}{1}} = \frac{\frac{st}{s}}{\frac{t}{1}} = \frac{\frac{t}{1}}{\frac{t}{1}} = 1,$$

e dunque $\sigma_S(U) \subset (\sigma_S(T)^{-1}(S^{-1}A))^*$. Per la proprietà universale, abbiamo un omomorfismo indotto

$$\widetilde{\psi}\colon \sigma_S(U)^{-1}(S^{-1}A) \longrightarrow \sigma_S(T)^{-1}(S^{-1}A)$$

che è ovviamente surgettivo.

Per l'iniettività osserviamo che se $\psi\left(\frac{a}{s}\right) = 0$ allora esiste $t \in T$ tale che $\frac{t}{1} \cdot \frac{a}{s} = \frac{ta}{s} = 0$ in $S^{-1}A$, cioè esiste $s_1 \in S$ tale che $s_1 ta = 0$ in A. Dunque $\sigma_S(s_1 t)\frac{a}{s} = 0$ con $s_1 t \in U$ e la tesi segue ancora da **T.6.5**.

La dimostrazione di $\sigma_T(U)^{-1}(T^{-1}A) \simeq \sigma_T(S)^{-1}(T^{-1}A)$ è del tutto analoga; quindi possiamo concludere che

$$\sigma_S(T)^{-1}(S^{-1}A) \simeq U^{-1}A \simeq \sigma_T(S)^{-1}(T^{-1}A).$$

Soluzione E. 12.39. Se $\mathfrak{p}$ è un primo non minimale, allora $\mathfrak{p}$ contiene propriamente un certo $\mathfrak{q} \in \operatorname{Min} A$. Dunque $S = A \setminus \mathfrak{p} \subsetneq A \setminus \mathfrak{q} = T$ non è massimale.

Viceversa, siano $\mathfrak{p}$ un primo minimale di A e $S = A \setminus \mathfrak{p}$; supponiamo che T sia un insieme moltiplicativo con $T \supsetneq S$. Per **T.6.19**.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. 12.40. Da **T.6.19**.3 segue che $V = \{2^n 3^m\}_{n,m \in \mathbb{N}}$ è la saturazione sia di S che di T; allora

$$S^{-1}\mathbb{Z} = V^{-1}\mathbb{Z} = T^{-1}\mathbb{Z}$$

per **T.6.19**.6.

Soluzione E. 12.41. 1. Per **T.6.19**.3 è sufficiente dimostrare che

$$A \setminus \overline{S} = \bigcup_{\mathfrak{q} \cap S = \emptyset} \mathfrak{q} = \bigcup_{\mathfrak{p} \in \mathcal{V}(I)} \mathfrak{p}.$$

Ovviamente se $\mathfrak{p} \in \mathcal{V}(I)$ allora $\mathfrak{p} \cap S = \emptyset$, altrimenti $1 \in \mathfrak{p}$; quindi abbiamo l'inclusione $\supseteq$.

Per l'altra inclusione, sia $\mathfrak{q}$ un primo che non interseca S; allora $(I, \mathfrak{q}) \neq 1$, 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 $\mathfrak{q} \subseteq \mathfrak{q}' \in \mathcal{V}(I)$, come volevamo.

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

$$\overline{S}_f = A \setminus \bigcup_{f \notin \mathfrak{p}} \mathfrak{p} \subseteq A \setminus \bigcup_{g \notin \mathfrak{q}} \mathfrak{q} = \overline{S}_g$$

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.1.12**.1 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 dire che 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. 12.42. 1. I primi di $A_\mathfrak{q}$ sono in corrispondenza 1:1 con gli ideali primi di A contenuti in $\mathfrak{q}$; questi ultimi corrispondono ai primi I in $K[x,y]$ tali che $(x,y)\supseteq I\supseteq(x^2-y^2)$, i.e. 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 $K[x,y]/(x\pm y)\simeq K[x]$, $(x,y)/(x\pm y)\simeq(x)$, e, in $K[x]$, 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 $\operatorname{char}K\neq2$, abbiamo $x-y\notin(x+y)$ e $\frac{x-y}{1}\in S$. Infine, l'ideale massimale $S^{-1}(\mathfrak{p}A_\mathfrak{q})=\left(\frac{x+y}{1}\right)=\left(\frac{0}{x-y}\right)$ di $S^{-1}A_\mathfrak{q}$ è nullo, e quindi $S^{-1}A_\mathfrak{q}$ è un campo.
Per descriverlo, osserviamo che $(A_\mathfrak{q})_{\mathfrak{p}A_\mathfrak{q}}\simeq A_\mathfrak{p}$ per **E.12.38**.1. Inoltre,

$$S^{-1}((x^2-y^2)_\mathfrak{q})=S^{-1}((x+y)_\mathfrak{q}).$$

Quindi

$$\begin{aligned}(A_\mathfrak{q})_{\mathfrak{p}A_\mathfrak{q}}&\simeq A_\mathfrak{p}\simeq S^{-1}(K[x,y]/(x^2-y^2))\\&\simeq S^{-1}K[x,y]/S^{-1}(x^2-y^2)\simeq S^{-1}K[x,y]/S^{-1}(x+y)\\&\simeq S^{-1}(K[x,y]/(x+y))\simeq K(x).\end{aligned}$$

17.6 Soluzioni del capitolo 13

Soluzione E. 13.1. 1. Basta osservare che, dati due ideali $(a),(b)\subseteq\mathbb{Z}$, si ha $(a)\subseteq(b)$ 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 $a\neq0,\pm1$ di $\mathbb{Z}$ si può ottenere una catena discendente infinita $(a)\supsetneq(a^2)\supsetneq\ldots\supsetneq(a^k)\supsetneq\ldots$.
2. È sufficiente osservare che l'anello A è un campo isomorfo a $\mathbb{R}(\sqrt{-2})\simeq\mathbb{C}$.

Soluzione E. 13.2. È ovvio che $1\Rightarrow2$ e $1\Rightarrow3$ dato che $V\simeq K^n$.
Vediamo che $2\Rightarrow1$ e $3\Rightarrow1$. Supponiamo che la dimensione di V non sia finita; allora esiste un insieme $\{v_i\}_{n\in\mathbb{N}}$ 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.

Soluzione E. 13.3. Siano M noetheriano e N' un sottomodulo di N; allora $N' \simeq f(N')$ è un sottomodulo di M e quindi è finitamente generato. Analogamente, dato P' sottomodulo di P, il sottomodulo $g^{-1}(P)$ di M è finitamente generato e dunque anche $P' = g(g^{-1}(P))$ lo è.

Viceversa, supponiamo che N e P siano noetheriani e consideriamo un sottomodulo M' di M; allora $g(M')$ e $f^{-1}(M' \cap f(N))$ sono sottomoduli di P ed N rispettivamente, e quindi sono finitamente generati. Dunque

$$M' \cap f(N) = f(f^{-1}(M' \cap f(N))) \simeq f^{-1}(M' \cap f(N))$$

è finitamente generato e la tesi segue applicando **E.10.28** alla successione esatta $0 \longrightarrow M' \cap f(N) \xrightarrow{i} M' \xrightarrow{g_{|M'}} g(M') \longrightarrow 0$.

Soluzione E. 13.4. 1. Consideriamo gli ideali $\operatorname{Ker} \varphi^i$; dato che A è noetheriano, la catena di ideali $\operatorname{Ker} \varphi \subseteq \operatorname{Ker} \varphi^2 \subseteq \dots$ si stabilizza ed esiste un intero n tale che $\operatorname{Ker} \varphi^n = \operatorname{Ker} \varphi^{n+1}$.
Sia $a \in \operatorname{Ker} \varphi$; vogliamo provare che $a = 0$. Dato che φ è surgettivo, lo è anche φ^n ed esiste $b \in A$ tale che $\varphi^n(b) = a$. Dunque $\varphi^{n+1}(b) = \varphi(a) = 0$, ossia $b \in \operatorname{Ker} \varphi^{n+1} = \operatorname{Ker} \varphi^n$ e pertanto $a = 0$, come volevamo.

2. Dato che φ è surgettivo, $\varphi(I)$ è un ideale di A per ogni ideale $I \subset A$. Inoltre 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 $j \in J$. Dunque $\varphi(i - j) = 0$ e, 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 $A = K[x_i \colon i \in \mathbb{N}]$ e φ definita da $\varphi(x_1) = 0$ e $\varphi(x_i) = x_{i-1}$ per $i > 1$. È immediato verificare 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. 13.5. Dato che A è noetheriano, I è un A-modulo finitamente generato. Applicando il Lemma di Nakayama otteniamo un elemento $b \in A$ tale che $b \equiv 1 \mod I$ e $bI = 0$. 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 $0 = ab = a(1 - a)$, abbiamo che a è idempotente.

Soluzione E. 13.6. Consideriamo la successione

$$0 \longrightarrow N_1 \cap N_2 \longrightarrow M \xrightarrow{f} M/N_1 \oplus M/N_2,$$

dove il primo omomorfismo è l'inclusione ed f è dato dalle proiezioni naturali; è immediato verificare che è esatta. Allora $M/(N_1 \cap N_2) \simeq \operatorname{Im} f \subseteq M/N_1 \oplus M/N_2$, e tutti questi moduli sono noetheriani, cf. **T.7.2.**2 e 3.

Soluzione E. 13.7. Sia M noetheriano; allora tutti i suoi quozienti sono noetheriani, cf. **T.7.2**.2.

Viceversa, supponiamo che $M/\overline{f}M$ e $M/\overline{g}^2M$ siano A-moduli noetheriani. Per **E.13.6** basta dimostrare che $\overline{f}M \cap \overline{g}^2M = (\overline{f}\overline{g}^2)M = 0$. Osserviamo che l'inclusione $\supseteq$ è ovvia e per ipotesi esistono $r, s \in K[x]$ tali che $rf + sg^2 = 1$. Sia ora $m \in \overline{f}M \cap \overline{g}^2M$; allora $m = \overline{a}\overline{f}m_1 = \overline{b}\overline{g}^2 n_1$, con $a, b \in K[x]$ e $m_1, n_1 \in M$. Pertanto

$$m = (\overline{rf + sg^2})m = \overline{r}\,\overline{f}(\overline{b}\overline{g}^2 n_1) + \overline{s}\,\overline{g}^2(\overline{a}\overline{f}m_1) = (\overline{rb}\,\overline{fg^2})n_1 + (\overline{sa}\overline{fg^2})m_1$$

appartiene a $(\overline{f}\overline{g}^2)M$, come volevamo.

Soluzione E. 13.8. Osserviamo che per ipotesi d è necessariamente non nullo.

1. Dato che $(d) = IJ$, si ha $d = \sum_{i=1}^k f_i g_i$ per certi $f_i \in I$, $g_i \in J$ e qualche intero k. Sia allora $\tilde{J} = (g_1, \dots, g_k)$; abbiamo $(d) \subseteq I\tilde{J} \subseteq IJ = (d)$.

2. Proviamo la tesi dimostrando che ogni ideale I di A è finitamente generato. Sia $\tilde{J}$ l'ideale finitamente generato costruito al punto 1. Per ogni $f \in I$ e per ogni i, si ha $fg_i \in IJ = (d)$ e dunque $fg_i = h_i d$ per qualche $h_i \in A$. Inoltre $fd \in I\tilde{J}$; 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 $f = \sum_{i=1}^k f_i h_i$ e $I = (f_1, \dots, f_k)$.

Soluzione E. 13.9. 1. La verifica è facile e discende dalla linearità di f e g.

2. Siano $\pi_A \colon A \times_C B \longrightarrow A$ e $\pi_B \colon A \times_C B \longrightarrow B$ gli omomorfismi di proiezione sulle componenti. Tali proiezioni sono surgettive perché f e g lo sono. Infatti dato $a \in A$ abbiamo $f(a) = c$ per qualche $c \in C$ e 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 $\pi_A(a, b) = a$. L'altra verifica è del tutto analoga.
Per **E.10.3** gli ideali di A e di B sono $(A \times_C B)$-sottomoduli di A e B rispettivamente; dato che A e B sono noetheriani come anelli, A e B sono noetheriani come $(A \times_C B)$-moduli. Dunque $A \times B$ è noetheriano come $(A \times_C B)$-modulo e $A \times_C B$, che è sottomodulo di un $(A \times_C B)$-modulo noetheriano, è a sua volta un $(A \times_C B)$-modulo noetheriano per **T.7.2**.2. In conclusione $(A \times_C B)$ è noetheriano come anello.

Soluzione E. 13.10. 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 e otteniamo $\mathfrak{m}^k \subseteq (a) \subseteq \mathfrak{m}^n \subseteq \mathfrak{m}^k$ per ogni $n > k$. Pertanto, per un tale n, abbiamo $\mathfrak{m}^n = \mathfrak{m}^k$, 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.1.15**, si ha $m^k = 0$ 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 $a = um^k$ per qualche $u \notin \mathfrak{m}$; poiché A è locale, u 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 $a = um^k = um^{k-h}m^h \in \mathfrak{m}^h$, come volevamo.

3. Per il punto precedente è sufficiente provare che se A è noetheriano valgono le condizioni equivalenti del punto 1.
Sia dunque $0 \neq a = b_1 m \in \mathfrak{m}$. 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 $(b_1) \subsetneq (b_2) \subsetneq \ldots \subsetneq (b_n) \subsetneq \ldots$ di ideali di A generati da elementi tali che $b_i m^i = a$ per ogni i. Se tutti i b_i sono non invertibili allora la catena è infinita il che non è possibile visto che A è noetheriano; dunque esiste b_k invertibile tale che $a = b_k m^k$, come volevamo.

Soluzione E. 13.11. Ogni ideale di una catena ascendente $\mathcal{C}$ di ideali primi di A è contenuto in un ideale massimale $\mathfrak{m}_\mathcal{C}$ che è principale per ipotesi. Localizzando A in $\mathfrak{m}_\mathcal{C}$ e applicando **E.13.10**.2 e 3, otteniamo che ogni ideale di $A_{\mathfrak{m}_\mathcal{C}}$ è del tipo $\mathfrak{m}_\mathcal{C}^k$; dunque la lunghezza della catena $\mathcal{C}_{\mathfrak{m}_\mathcal{C}}$ dei primi localizzati è uguale a 1 se $A_{\mathfrak{m}_\mathcal{C}}$ è un dominio, altrimenti è uguale a 0. Abbiamo dunque dimostrato 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. 13.12. Per ipotesi M è noetheriano quindi finitamente generato, diciamo da $m_1, \ldots, m_n$. Consideriamo l'omomorfismo $\varphi\colon A \longrightarrow M^n$ dato da $\varphi(a) = (am_1, \ldots, am_n)$ e proviamo che $\operatorname{Ker}\varphi = I$.
L'inclusione $I \subseteq \operatorname{Ker}\varphi$ è ovvia.

Per l'altra inclusione, basta osservare che se $a \in \operatorname{Ker}\varphi$ allora $am_i = 0$ per ogni $i = 1, \ldots, n$.
Dunque $A/I \simeq \operatorname{Im}\varphi \subseteq M^n$ è isomorfo ad un sottomodulo di M^n, che è un A-modulo noetheriano; quindi è noetheriano come A-modulo e anche come A/I-modulo.

Soluzione E. 13.13. 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 è contenuto in I e in J, per ipotesi 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 **T.7.5**. Pertanto esiste $n \in N$ tale che $(IJ)^n \subseteq \mathcal{N}(A)^n = 0$, come richiesto.

Soluzione E. 13.14. 1. Sia $\{g_1, \dots, g_n\}$ un insieme minimale di generatori di I, dove $n = \mu(I) > 1$ per ipotesi. Allora I^2 è generato da tutti i prodotti distinti $g_i g_j$, che sono $\frac{n(n+1)}{2} < n^2$; quindi $\mu(I^2) < n^2$, 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 $0 \longrightarrow I \otimes J \longrightarrow J \longrightarrow J/IJ \longrightarrow 0$, che è ancora esatta. Consideriamo il diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I \otimes J & \longrightarrow & J & \longrightarrow & J/IJ & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & IJ & \longrightarrow & J & \longrightarrow & J/IJ & \longrightarrow & 0, \end{array}$$

dove β e γ sono isomorfismi. Dal Lemma del serpente, o direttamente da **T.4.20**, deduciamo che $I \otimes J \simeq IJ$.
Sia ora $J = I$; per **E.11.10** si ha $\mu(I)^2 = \mu(I \otimes I) = \mu(I^2)$, di conseguenza il punto 1 implica $\mu(I) \leq 1$ 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 $(a) \otimes (b) \simeq (a)(b) = 0$. Dato che A è locale, da **E.11.11** si deduce che $(a) = 0$ oppure $(b) = 0$, come volevamo.

Soluzione E. 13.15. 1. Dato che A è noetheriano, $\sqrt{I} = \bigcap_{\mathfrak{p}_i \in \operatorname{Min} I} \mathfrak{p}_i$ e $\sqrt{J} = \bigcap_{\mathfrak{q}_j \in \operatorname{Min} J} \mathfrak{q}_j$, cf. **T.7.11**.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 $\sqrt{J} = \bigcap_{\mathfrak{q}_j \in \operatorname{Min} J} \mathfrak{q}_j = \sqrt{I} \subseteq \mathfrak{p}$, e quindi, dato che $\operatorname{Min} J$ è finito, esiste un ideale $\mathfrak{q}_j \in \operatorname{Min} J$ tale che $\mathfrak{q}_j \subseteq \mathfrak{p}$, cf. **T.1.12**.2. Per lo stesso motivo esiste $\mathfrak{p}_i \in \operatorname{Min} I$ tale che $\mathfrak{p}_i \subseteq \mathfrak{q}_j \subseteq \mathfrak{p}$; allora, per la minimalità di $\mathfrak{p}$, si ha $\mathfrak{p} = \mathfrak{q}_j$. In questo modo abbiamo dimostrato 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 1 e dalle definizioni di altezza e dimensione. Basta osservare che, per ogni ideale I, si ha $\operatorname{ht} I = \min\{\operatorname{ht} \mathfrak{p} \colon \mathfrak{p} \in \operatorname{Min} I\}$ 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. 13.16. Sia $\bigcap_{i=1}^{n} \mathfrak{q}_i$ una decomposizione primaria minimale di $\operatorname{Ann} M$. Dato che $\operatorname{Ann} M$ è 0-dimensionale, per ogni i abbiamo che $\mathfrak{m}_i = \sqrt{\mathfrak{q}_i}$ è un ideale massimale. Per il primo Teorema di finitezza **T.7.5**, esistono s_i tali che $\mathfrak{m}^{s_i} \subseteq \mathfrak{q}_i$; 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 $J \not\subset \operatorname{Ann} M$ e dunque $0 \neq JM \subseteq M$ e $\operatorname{Ann}(JM) = \mathfrak{m}_1$. Dimostriamo che se $0 \neq m \in JM$ allora il sottomodulo $\langle m \rangle \subseteq M$ è semplice; infatti l'omomorfismo da A in $\langle m \rangle$ definito da $1 \mapsto m$

è surgettivo e il suo nucleo è l'ideale proprio $\operatorname{Ann} m \supseteq \operatorname{Ann}(JM) = \mathfrak{m}_1$. La conclusione segue da **E.10.13**.1.

Soluzione E. 13.17. Sia $\mathfrak{p} \in \operatorname{Min} A$ un primo minimale e consideriamo la decomposizione del nilradicale $\mathcal{N}(A) = \sqrt{(0)} = \mathfrak{p} \cap \bigcap_i \mathfrak{p}_i$ come intersezione finita di primi minimali, cf. **T.7.11**.2. 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 $a = b^n$ 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 $a\mathfrak{p} \subseteq \mathcal{N}(A)$. Sia $\mathcal{N}(A) = \bigcap_i \mathfrak{p}_i$, con $\mathfrak{p}_i$ primi minimali di A; dato che $a \notin \mathcal{N}(A)$, esiste $\mathfrak{p}_j$ tale che $a \notin \mathfrak{p}_j$, 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. 13.18. Sia I un ideale radicale contenuto in J e 0-dimensionale; allora possiamo scrivere $I = \sqrt{I} = \bigcap_i \mathfrak{m}_i$ come intersezione finita di ideali massimali distinti. Dunque

$$J = \Big(\bigcap\nolimits_i \mathfrak{m}_i\Big) + J = \Big(\prod\nolimits_i \mathfrak{m}_i\Big) + J = \prod\nolimits_i (\mathfrak{m}_i + J) = \bigcap\nolimits_i (\mathfrak{m}_i + J),$$

dove $\mathfrak{m}_i + J$ è uguale a $\mathfrak{m}_i$ oppure a (1), a seconda che $J \subseteq \mathfrak{m}_i$ oppure no. Dalla precedente uguaglianza otteniamo che, se $\mathfrak{m}_i + J = (1)$ per ogni i, allora $J = (1)$, altrimenti abbiamo $J = \bigcap_{i\colon J \subseteq \mathfrak{m}_i} \mathfrak{m}_i$, e dunque J è radicale.
Concludiamo osservando che A/J è isomorfo ad un quoziente di A/I, dunque, se $J \neq (1)$, allora è 0-dimensionale.

Soluzione E. 13.19. È sufficiente trovare una decomposizione del radicale di I, che è l'ideale $(xzt,\, yt,\, xyzt,\, xz) = (yt, xz)$. Si ha $\sqrt{I} = (x,y) \cap (y,z) \cap (x,t) \cap (z,t)$; quindi

$$\operatorname{Min} I = \{(x,y), (y,z), (x,t), (z,t)\}.$$

Soluzione E. 13.20. 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.2.6**.2, troviamo $I = (x) \cap (x^2,\, t^2) \cap (x^2,\, z,\, t^2) \cap (y^3,\, z,\, t^2)$. Dunque è facile verificare che $(x) \cap (x^2,\, t^2) \cap (y^3,\, z,\, t^2)$ è una decomposizione primaria minimale di I, con

$$\operatorname{Ass} I = \{(x), (x,t), (y,z,t)\} \quad \text{e} \quad \operatorname{Min} I = \{(x), (y,z,t)\}.$$

3. Dato che i divisori di zero e i nilpotenti sono dati rispettivamente dall'unione dei primi associati a $(\overline{0})$ e dall'intersezione dei primi minimali di A/I, cf. **T.7.11**.2, per quanto visto al punto 2 abbiamo

$$\mathcal{D}(A/I) = (\overline{x},\, \overline{t}) \cup (\overline{y},\, \overline{z},\, \overline{t}) \quad \text{e} \quad \mathcal{N}(A/I) = (\overline{y},\, \overline{z},\, \overline{t}) \cap (\overline{x}) = (\overline{xy},\, \overline{xz},\, \overline{xt}).$$

Soluzione E. 13.21. 1. Si ha $(x^5-3x^2)=(x^2)\cap(x^3-3)$; 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

$$\mathfrak{p}_1=(\overline{x})\oplus(\overline{1}),\quad \mathfrak{p}_2=\left(\overline{x^3-3}\right)\oplus(\overline{1}),\quad \mathfrak{p}_3=(\overline{1})\oplus(\overline{2})\quad\text{e}\quad \mathfrak{p}_4=(\overline{1})\oplus(\overline{3}),$$

e sono tutti primi associati a (0_A) (perché?). Dunque per **T.7.11**.2

$$\mathcal{N}(A)=\bigcap_i \mathfrak{p}_i=\left(\overline{x^4-3x}\right)\oplus(\overline{6})\quad\text{e}\quad \mathcal{D}(A)=\bigcup_{i=1}^{4}\mathfrak{p}_i.$$

2. Per $i=1,\dots,4$ 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; in particolare $(\overline{1},\overline{0})\in S_1$ implica $(\overline{a},\overline{b})=(\overline{a},\overline{0})$ in $S_1^{-1}A$, ed è sufficiente considerare le coppie con seconda coordinata $\overline{0}$. Dunque

$$\begin{aligned}S_1^{-1}A&\simeq(\mathbb{Q}[x]/(x^5-3x^2))_{\mathfrak{q}_1}\oplus\overline{0}\\&\simeq(\mathbb{Q}[x]/(x^2))_{\mathfrak{q}_1}\oplus(\mathbb{Q}[x]/(x^3-3))_{\mathfrak{q}_1}\simeq(\mathbb{Q}[x]/(x^2))_{(x)}\simeq\mathbb{Q}[x]/(x^2).\end{aligned}$$

In particolare $S_1^{-1}A$ contiene l'elemento nilpotente non banale x, quindi non è un dominio.
Analogamente abbiamo che

$$S_2^{-1}A\simeq(\mathbb{Q}[x]/(x^5-3x^2))_{\mathfrak{q}_2}\oplus\overline{0}\simeq\big(\mathbb{Q}[x]/(x^3-3)\big)_{(x^3-3)}\simeq\mathbb{Q}(\sqrt[3]{3}\,)$$

è un campo.
Infine per $i=3,4$ si ottiene

$$S_i^{-1}A\simeq\overline{0}\oplus(\mathbb{Z}/(12))_{\mathfrak{t}_i}\simeq(\mathbb{Z}/(4))_{\mathfrak{t}_i}\oplus(\mathbb{Z}/(3))_{\mathfrak{t}_i}.$$

Dunque

$$S_3^{-1}A\simeq(\mathbb{Z}/(4))_{(2)}\simeq\mathbb{Z}/(4)\quad\text{e}\quad S_4^{-1}A\simeq(\mathbb{Z}/(3))_{(3)}\simeq\mathbb{Z}/(3)$$

e solo il secondo è un campo.

Soluzione E. 13.22. 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 $(I,5)=(x^2-4,(x+y)^3,5)$. Siano $\mathfrak{m}_1=(x+2,y-2,3)$, $\mathfrak{m}_2=(x+2,y-2,5)$ e $\mathfrak{m}_3=(x-2,y+2,5)$; tali ideali sono massimali e dunque a due a due comassimali. Osserviamo che $\sqrt{(I,3)}=\mathfrak{m}_1$; inoltre

$$\begin{aligned}(I,5)&=(x+2,(x+y)^3,5)\cap(x-2,(x+y)^3,5)\\&=(x+2,(y-2)^3,5)\cap(x-2,(y+2)^3,5),\end{aligned}$$

e gli ideali di questa intersezione sono primari, dato che i loro radicali sono $\mathfrak{m}_2$ e $\mathfrak{m}_3$ rispettivamente. Per **T.7.11**.2

$$\mathcal{D}(A) = \mathfrak{m}_1 \cup \mathfrak{m}_2 \cup \mathfrak{m}_3.$$

2. Dato che (9) e (5) sono comassimali, sono a due a due comassimali anche gli ideali $\mathfrak{q}_1 = (I, 9)$, $\mathfrak{q}_2 = (x+2, (y-2)^3, 5)$ e $\mathfrak{q}_3 = (x-2, (y+2)^3, 5)$. Abbiamo allora 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. 13.23. $1 \Rightarrow 2$. Dato che I è 0-dimensionale possiamo scrivere $\sqrt{I} = \bigcap_i \mathfrak{m}_i$ come intersezione finita di ideali massimali distinti. Quindi $\mathbb{V}(I)$ è un'unione finita di punti e, per **T.3.17**, $d = \dim_K A/I < \infty$.
Per ogni i esiste allora una combinazione K-lineare non banale $\sum_{j=0}^{d} a_{ij}\overline{x_i}^j = \overline{0}$.
Dunque gli $h_i(x_i) = \sum_{j=0}^{d} a_{ij}x_i^j$ sono polinomi non nulli di $I \cap K[x_i]$.
$2 \Rightarrow 1$. Siano $0 \neq h_i(x_i) \in I \cap K[x_i]$ con $\deg(h_i) = m_i$; allora

$$\{x_1^{t_i} \cdots x_n^{t_n} : t_i < m_i \text{ per ogni } i\}$$

è un insieme di generatori del K-spazio vettoriale A/I. Per **T.3.17** la varietà associata $\mathbb{V}(I)$ è finita e la conclusione segue da **T.3.18**.

Soluzione E. 13.24. Osserviamo che, dato che l'ideale I è 0-dimensionale, i polinomi h_i esistono sempre per **E.13.23** e possono essere effettivamente calcolati grazie a **T.2.25**.
L'ideale $(\sqrt{h_1}, \ldots, \sqrt{h_n})$ è 0-dimensionale ancora per **E.13.23**; inoltre è radicale per **E.8.60**. Per ogni i, si ha $\sqrt{h_i} \in \sqrt{I} \subsetneq A$; quindi

$$(\sqrt{h_1}, \ldots, \sqrt{h_n}) \subseteq (I, \sqrt{h_1}, \ldots, \sqrt{h_n}) \subseteq \sqrt{I} \subsetneq A.$$

La tesi segue ora facilmente da **E.13.18**.

Soluzione E. 13.25. 1. Siano $0 \neq m \in M$ tale che $\operatorname{Ann} m$ è massimale in Σ e a, b in A tali che $ab \in \operatorname{Ann} m$. 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 non vuoto $\Sigma = \{\operatorname{Ann} m \colon 0 \neq m \in M\}$ ha elementi massimali che, per il punto precedente, sono elementi di $\operatorname{Ass} M$.

Soluzione E. 13.26. Siano $\mathfrak{p} = \operatorname{Ann} m$ e $f \colon A \longrightarrow M$ definita da $f(1) = m$; allora $\operatorname{Ker} f = \operatorname{Ann} m = \mathfrak{p}$ e dal I Teorema di omomorfismo si ottiene 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 $\mathfrak{p} \subseteq \operatorname{Ann} m$.

Per l'altra inclusione, sia $a \in \operatorname{Ann} m$; allora $0 = am = j(\overline{a})$ e, dall'iniettività di j, segue $a \in \mathfrak{p}$. Perciò $\operatorname{Ann} m \subseteq \mathfrak{p}$, come volevamo.

Soluzione E. 13.27. 1. Sia $\mathfrak{p} \in \operatorname{Ass} N$; allora esiste $j \colon A/\mathfrak{p} \longrightarrow N$ iniettiva per **T.13.26**. Dato che $f \circ j \colon A/\mathfrak{p} \longrightarrow M$ è ancora iniettiva, $\mathfrak{p} \in \operatorname{Ass} M$, sempre per **T.13.26**.
Sia $\mathfrak{p} = \operatorname{Ann} m \in \operatorname{Ass} M$; allora esiste $j \colon A/\mathfrak{p} \longrightarrow M$ iniettiva con $\overline{1} \mapsto m$. Ci sono due casi; se $j(A/\mathfrak{p}) \cap \operatorname{Ker} g = 0$, allora $g \circ j \colon A/\mathfrak{p} \longrightarrow P$ rimane iniettiva e $\mathfrak{p} \in \operatorname{Ass} P$.
Altrimenti, $j(A/\mathfrak{p}) \cap \operatorname{Ker} g \neq 0$ ed 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 $\mathfrak{p} = \operatorname{Ann} m = \operatorname{Ann}(am)$. Infatti, certamente $\operatorname{Ann} m \subseteq \operatorname{Ann}(am)$.

Per l'altra inclusione, sia b tale che $bam = 0$; allora $ba \in \mathfrak{p}$, per cui $b \in \mathfrak{p}$. Per l'iniettività di f, possiamo allora concludere che $\operatorname{Ann} n = \operatorname{Ann} f(n) = \operatorname{Ann}(am) = \mathfrak{p}$ e quindi $\mathfrak{p} \in \operatorname{Ass} N$.

2. Dato che $M \neq 0$, abbiamo $\operatorname{Ass} M \neq \emptyset$ per **T.13.25**.2. Sia $\mathfrak{p}_1 = \operatorname{Ann} m_1 \in \operatorname{Ass} M$; allora esiste $j \colon A/\mathfrak{p}_1 \longrightarrow M$ iniettiva per **T.13.26**. Poniamo $M_0 = 0$ e $M_1 = j(A/\mathfrak{p}_1) = \langle m_1 \rangle \subset M$; allora $M_1 \simeq M_1/M_0 \simeq A/\mathfrak{p}_1$.
Se $M_1 = M$ abbiamo concluso.
Altrimenti $\operatorname{Ass}(M/M_1) \neq \emptyset$; siano dunque $\mathfrak{p}_2 = \operatorname{Ann}(\overline{m_2}) \in \operatorname{Ass}(M/M_1)$, $M_2 = \langle m_1, m_2 \rangle \supsetneq M_1$ e $j \colon A/\mathfrak{p}_2 \longrightarrow M/M_1$ iniettiva. Se j è surgettiva allora $M_2 = M$ e abbiamo concluso; altrimenti iterando il ragionamento troviamo una catena ascendente di sottomoduli con la proprietà richiesta e il processo termina con $M_t = M$ perché M è noetheriano.

3. Siano $0 = M_0 \subset M_1 \subset \ldots \subset M_t = M$ come nel punto precedente e mostriamo la tesi per induzione su t. Se $t = 1$ allora $M \simeq A/\mathfrak{p}$, con $\mathfrak{p} \in \operatorname{Spec} A$ e quindi $\operatorname{Ass} M = \operatorname{Ass}(A/\mathfrak{p}) = \{\mathfrak{p}\}$.
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 otteniamo $\operatorname{Ass} M_i \subseteq \operatorname{Ass} M_{i-1} \cup \{\mathfrak{p}_i\}$ e, dall'ipotesi induttiva, segue che $\operatorname{Ass} M_i$ è finito.

Soluzione E. 13.28. Basta osservare che $N \subseteq M$ implica $I \subseteq \operatorname{Ann} M \subseteq \operatorname{Ann} N$ e che N è un A-sottomodulo se e solo se N è un A/I-sottomodulo.

Soluzione E. 13.29. Consideriamo la catena discendente di sottomoduli $\operatorname{Im} \varphi \supseteq \operatorname{Im} \varphi^2 \supseteq \ldots \supseteq \operatorname{Im} \varphi^n \supseteq \ldots$. Dato che M è artiniano, la catena è stazionaria ed esiste un intero k tale che $\operatorname{Im} \varphi^k = \operatorname{Im} \varphi^{k+1}$. Per ogni $m \in M$ esiste allora

$n \in M$ tale che $\varphi^k(m) = \varphi^{k+1}(n)$, ossia $\varphi^k(m - \varphi(n)) = 0$. La tesi segue dall'iniettività di φ, che implica quella di φ^k.

Soluzione E. 13.30. 1. Sia $a \in A \setminus A^*$ e dimostriamo che a è un divisore di zero. Consideriamo la catena $(a) \supseteq (a^2) \supseteq \ldots$; per d.c.c. esiste un intero k tale che $(a^k) = (a^{k+1})$, quindi esiste $b \in A$ tale che $a^k(ab - 1) = 0$. Dato che a non è invertibile, si ha $ab - 1 \neq 0$; dunque a^k è zero divisore e, di conseguenza, lo è anche a.

2. Sia $(A, \mathfrak{m})$ locale; consideriamo i due casi $S \cap \mathfrak{m} \neq \emptyset$ e $S \cap \mathfrak{m} = \emptyset$, tenendo a mente che, per la parte 1, ogni elemento di A è invertibile oppure un divisore di zero.
Se S contiene un elemento di $\mathfrak{m} = \mathcal{N}(A)$, cf. **T.7.14**.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 invertibile e quindi $S^{-1}A \simeq A$.
In entrambi i casi σ_S è ovviamente surgettiva.

Soluzione E. 13.31. Dimostriamo la tesi 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 uno spazio vettoriale. Per **E.13.2**, come $(A/\mathfrak{m}_1)$-modulo M è noetheriano se e solo se è artiniano; la conclusione discende allora da **T.7.2**.6 e **E.13.28**.
Sia ora $n > 1$ e consideriamo la successione esatta

$$0 \longrightarrow \mathfrak{m}_n M \longrightarrow M \longrightarrow M/\mathfrak{m}_n M \longrightarrow 0.$$

Come sopra, $M/\mathfrak{m}_n M$ è un $A/\mathfrak{m}_n$-spazio vettoriale, quindi artiniano se e solo se noetheriano. Dato che $(\mathfrak{m}_1 \cdots \mathfrak{m}_{n-1})\mathfrak{m}_n M = 0$, dall'ipotesi induttiva abbiamo che $\mathfrak{m}_n M$ è noetheriano se e solo se artiniano. Dato che la successione è esatta, la tesi segue da **T.7.2**.2 e **T.7.3**.

17.7 Soluzioni del capitolo 14

Soluzione VoF. 14.1. Vero. Un elemento $a \in A$ non è divisore di zero in A/I se e solo se per ogni $b \in A$ tale che $ab \in I$ si ha $b \in I$. Questo vuol dire che se $b \in A$ è tale che $ab \in I$ allora $b \in I$. Dunque $b \in I : a$ implica $b \in I$ e, dato che I è sempre contenuto in $I : a$, abbiamo dimostrato la tesi.

Soluzione VoF. 14.2. Vero. Il prodotto $(p, q) \mapsto pq$ in $Q[x]$ è $A[x]$-bilineare, dunque induce un omomorfismo definito da $p \otimes q \mapsto pq$ per ogni $p, q \in Q[x]$. Esso è chiaramente surgettivo. Per dimostrarne l'iniettività è utile osservare che, se $p \in Q[x]$ allora esiste $0 \neq d \in A$ tale che $dp = p' \in A[x]$; quindi se $p, q \in Q[x]$, allora

$$p \otimes q = \frac{p'}{d} \otimes q = \frac{1}{d} \otimes p'q = 1 \otimes pq.$$

Soluzione VoF. 14.3. 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 PID, dunque è massimale, cf. **T.1.23** e **E.8.57**. In quest'ultimo caso, B è un campo.

Soluzione VoF. 14.4. Le prime due uguaglianze sono vere, cf. **T.1.6**.7 e **E.8.23**.2, mentre la terza è falsa, cf. **E.8.24**.

Soluzione VoF. 14.5. Falso. Si veda la discussione che segue **T.1.5**.

Soluzione VoF. 14.6. Falso. Ad esempio $\mathcal{N}(\mathbb{Z}/(6)) = (\overline{0})$, ma (6) non è primo in $\mathbb{Z}$.

Soluzione VoF. 14.7. Vero. Il modulo è isomorfo a $\mathbb{Q}[x]/(x^2-1, x^2+1)$ per **E.11.3**, e quest'ultimo è chiaramente nullo.

Soluzione VoF. 14.8. Vero. L'anello A è quoziente di $A[x]$ ed è dunque noetheriano per **T.7.2**.2.

Soluzione VoF. 14.9. Vero. Ricordiamo che se $\operatorname{Lt}_>(I)$ è primo allora un insieme minimale di generatori è dato da un sottoinsieme delle indeterminate per **T.2.7**.1. Eventualmente rinominando le variabili possiamo supporre che $\operatorname{Lt}_>(I) = (x_1, \dots, x_k)$; quindi la base di Gröbner ridotta di I è della forma

$$G = \{x_1 - f_1(x_{k+1}, \dots, x_n), \dots, x_k - f_k(x_{k+1}, \dots, x_n)\}$$

per certi $f_1, \dots, f_k$. Dunque $K[X]/I \simeq K[x_{k+1}, \dots, x_n]$ è un dominio ossia I è primo.

Soluzione VoF. 14.10. Vero. Sia $b \in \sqrt{I\colon J}$; 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, abbiamo $b^n c^m \in I$. Se $n \geq m$, moltiplicando per c^{n-m}, si ottiene $(bc)^n \in I$, da cui segue $bc \in \sqrt{I}$. Se $n < m$ si conclude in maniera analoga.

Soluzione VoF. 14.11. Vero. Se $I = J$ allora (0) è massimale e A è un campo. Altrimenti, dato che I e 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. Quindi A è artiniano perché in A vale d.c.c.

Soluzione VoF. 14.12. Falso. Consideriamo gli $\mathbb{Z}$-moduli $M = \mathbb{Z}/(4)$ e $N = \mathbb{Z}$; allora M è di torsione mentre N è libero da torsione. Dunque $T(M \otimes_{\mathbb{Z}} N) \simeq T(M) = M = \mathbb{Z}/(4)$, mentre $T(M) \otimes T(N) = \mathbb{Z}/(4) \otimes 0 = 0$.

Soluzione VoF. 14.13. Vero. Se $\gcd(f,g) = 1$, allora i polinomi $p(x) = \operatorname{Ris}_y(f,g)$ e $q(y) = \operatorname{Ris}_x(f,g)$ sono diversi da zero ed appartengono a I, cf. **T.3.7**. Dunque, qualunque sia l'ordinamento monomiale fissato, $\operatorname{Lt}(I)$ contiene potenze di entrambe le variabili e la conclusione segue da **T.3.17**.

Viceversa, sia $h = \gcd(f,g) \neq 1$; scriviamo $f = f_1 h$ e $g = g_1 h$, per certi $f_1, g_1 \in \mathbb{C}[x,y]$. Allora $\mathbb{V}_{\mathbb{C}}(I) = \mathbb{V}(h) \cup \mathbb{V}(f_1, g_1)$ per **T.3.1**.6 e basta provare

che $\mathbb{V}_{\mathbb{C}}(h)$ è infinita. Questo segue da **T.3.17**, dato che (h) ovviamente non verifica la condizione 2.

Soluzione VoF. 14.14. Vero. Basta considerare l'omomorfismo $\varphi\colon A^n \longrightarrow (A/I)^n$ definito da $\varphi(a_1,\dots,a_n) = (\overline{a_1},\dots,\overline{a_n})$, che è banalmente surgettivo e il cui nucleo è IA^n.

Soluzione VoF. 14.15. 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 VoF. 14.16. Falso. Siano $A = \mathbb{Z}/(4)$, $M = A$ e $N = (2)A \simeq \mathbb{Z}/(2)$; allora M è libero, quindi proiettivo, ma N non è proiettivo. Per esempio possiamo osservare che $0 \longrightarrow \mathbb{Z}/(2) \xrightarrow{\cdot 2} \mathbb{Z}/(4) \longrightarrow N \longrightarrow 0$ non spezza, perché $\mathbb{Z}/(4) \not\simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.

Soluzione VoF. 14.17. Vero. Se I è massimale e $J \not\subseteq I$, allora 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 $\overline{0} \neq \overline{a} \in A/I$; dato che $(a) \not\subseteq I$, per ipotesi $I + (a) = A$ e quindi esistono $i \in I$ e $b \in A$ tali che $i + ba = 1$, i.e. $\overline{a}\overline{b} = \overline{1}$ e $\overline{a}$ è invertibile.

Soluzione VoF. 14.18. Vero. $A/\mathfrak{p}$ è un dominio finito, dunque è un campo, cf. **T.1.1**.

Soluzione VoF. 14.19. 1. Vero. Basta provare che, se $I + J = A$, allora, per ogni $n \in \mathbb{N}$, $I^n + J^n = A$; 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

$$1 = (i+j)^{2n-1} = i^n \sum_{k=0}^{n-1} \binom{2n-1}{k} i^{n-1-k} j^k + j^n \sum_{k=n}^{2n-1} \binom{2n-1}{k} i^{2n-1-k} j^{k-n}$$

appartiene a $I^n + J^n$.

2. Vero. Sia $a \in \sqrt{I\colon J}$; allora esiste m tale che $a^m j \in I$ per ogni $j \in J$. Quindi $(aj)^m \in I$ e $aj \in \sqrt{I}$ per ogni j, cioè $a \in \sqrt{I}\colon J$.

3. Falso. Basta considerare gli ideali $I = (8)$ e $J = (6)$ in $\mathbb{Z}$; infatti si ha $\sqrt{I}\colon J = (2)\colon(6) = \mathbb{Z}$, mentre $\sqrt{I\colon J} = \sqrt{(4)} = (2)$, cf. **E.8.16**.4.

4. Falso. Consideriamo gli ideali $I = (12)$ e $J = (8)$ in $\mathbb{Z}$; si ha $I\colon J = (3)$, mentre $I\colon \sqrt{J} = (12)\colon(2) = (6)$.

Soluzione VoF. 14.20. 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

$$\{x,\, y^2+1\}.$$

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 essere isomorfi come anelli. Infatti, supponiamo che esista un isomorfismo di anelli $\varphi\colon A_1 \longrightarrow A_2$; allora $\varphi_{|\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ e gli elementi $\varphi(1)$, $\varphi(x)$, $\varphi(y)$, $\varphi(xy)$ sono linearmente dipendenti su $\mathbb{Q}$. Dunque esistono $a_1, \dots, a_4 \in \mathbb{Q}$ non tutti nulli tali che

$$0 = a_1\varphi(1) + a_2\varphi(x) + a_3\varphi(y) + a_4\varphi(xy) = \varphi(a_1 + a_2x + a_3y + a_4xy);$$

da ciò si deduce che $1, x, y, xy$ sono linearmente dipendenti in A_1, che è la contraddizione cercata.

Soluzione VoF. 14.21. Vero. Se $I = I^{ec}$ e I^e è primo, allora I è primo per **T.1.17**.7.

Viceversa, osserviamo che $K(x)[y] = S^{-1}(K[x,y])$, con $S = K[x] \setminus 0$ ed 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 $I \longrightarrow I^e$ e tale che $I^{ec} = I$, cf. **T.6.8**.

Soluzione VoF. 14.22. Vero. Basta provare che $\sqrt{(f,g)} \subseteq \sqrt{(f^2, g^3)}$, dato che l'altro contenimento è ovvio. Dato che $(f,g) \subseteq \sqrt{(f^2,g^3)}$, passando ai radicali si ottiene la tesi.

Soluzione VoF. 14.23. Vero. Dato che A è locale si ha $A^* = A \setminus \mathfrak{m}$ e $A/\mathfrak{m}$ 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 VoF. 14.24. Vero. È un caso particolare di **T.4.12**.

Soluzione VoF. 14.25. Falso. Consideriamo $A = K[x_n : n \in \mathbb{N}]$; allora A è un dominio non noetheriano ma A è contenuto nel suo campo dei quozienti che è noetheriano.

Soluzione VoF. 14.26. 1. Vero. È facile verificare che $A = (\overline{2}) \oplus (\overline{9})$, pertanto M_1 è proiettivo come addendo diretto del modulo libero A.

Le affermazioni 2, 3 e 4 sono false. La successione esatta

$$0 \longrightarrow (\overline{6}) \longrightarrow A \xrightarrow{\cdot 3} (\overline{3}) \longrightarrow 0$$

non spezza perché $\mathrm{Ann}_A\big((\overline{3}) \oplus (\overline{6})\big) = (\overline{6}) \neq (\overline{0}) = \mathrm{Ann}_A A$. Quindi il modulo M_2 non è proiettivo e tantomeno libero.
Infine $\mathrm{Ann}_A M_1 = (\overline{9})$, dunque M_1 non è libero.

Soluzione VoF. 14.27. Falso. Dato che $\mathrm{Ann}_{K[x]} K \neq (0)$, il campo K è un $K[x]$-modulo di torsione, quindi non può essere addendo diretto del modulo libero $K[x]$.

Soluzione VoF. 14.28. Vero. Dato che M è finitamente generato, si ha $\mathfrak{p} \in \mathrm{Supp}\, M$ se e solo se $\mathrm{Ann}\, M \subseteq \mathfrak{p}$, cf. **E.12.26**.1. Inoltre $M = \mathbb{Z}/(12) \otimes_{\mathbb{Z}} \mathbb{Z}/(30) \simeq \mathbb{Z}/(6)$, quindi il suo annullatore è (6) e $\mathrm{Supp}\, M = \{(2), (3)\}$.

Soluzione VoF. 14.29. Falso. L'anello A è noetheriano, quindi $\mathcal{D}(A)$ è uguale all'unione dei primi associati a (0), cf. **T.7.11**.2. Dunque $\mathcal{D}(A) = (\overline{x}) \cup (\overline{y})$ ma l'elemento $a = \overline{x} + \overline{y}$ non appartiene a $\mathcal{D}(A)$ e nemmeno a K.

Soluzione VoF. 14.30. Vero. Dato che f è irriducibile e $K[X]$ è UFD, (f) è primo per **T.1.25** e **T.1.22**.5. Per la forma forte del Nullstellensatz e **T.3.1**.4, si ha $\sqrt{(g)} = \mathbb{I}(\mathbb{V}(g)) \subseteq \mathbb{I}(\mathbb{V}(f)) = (f)$, da cui discende la tesi.

Soluzione VoF. 14.31. Vero. Dato che Q è proiettivo, la successione esatta

$$0 \longrightarrow \operatorname{Ker}\varphi \longrightarrow P \longrightarrow Q \longrightarrow 0$$

spezza e $P \simeq \operatorname{Ker}\varphi \oplus Q$. Dunque $\operatorname{Ker}\varphi$ è addendo diretto di un modulo proiettivo ed è proiettivo per **E.11.9**.1.

Soluzione VoF. 14.32. Falso. Si ha $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}[x]/(f) \simeq \mathbb{C}[x]/(f)$, cf. la dimostrazione di **E.11.13**.2. Dato che f è libero da quadrati, in $\mathbb{C}[x]$ abbiamo $f(x) = a\prod_{i=1}^{k}(x-\alpha_i)$, con $a \in \mathbb{Q}$ e $\alpha_i \neq \alpha_j$ se $i \neq j$. 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 VoF. 14.33. 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 VoF. 14.34. Vero. Da **T.5.4**.2, 3 e 5 abbiamo

$$\begin{aligned} M/\mathfrak{m}M \otimes M/\mathfrak{n}M &\simeq (A/\mathfrak{m} \otimes M) \otimes (A/\mathfrak{n} \otimes M) \simeq M \otimes (A/\mathfrak{m} \otimes A/\mathfrak{n}) \otimes M \\ &\simeq (A/(\mathfrak{m}+\mathfrak{n})) \otimes M \otimes M \end{aligned}$$

che è nullo perché $\mathfrak{m} + \mathfrak{n} = A$.

Soluzione VoF. 14.35. Falso. Consideriamo l'ideale $(x^2-1) = (x+1)\cap(x-1) \subset K[x]$ che non è primario in quanto intersezione di due primi distinti. Chiaramente $\operatorname{Lt}(I) = (x^2)$ è primario.

Soluzione VoF. 14.36. Vero. La matrice è già in forma diagonale, dunque

$$\operatorname{Coker}\varphi \simeq \mathbb{Q}[x]/(x-1) \oplus \mathbb{Q}[x]/(x) \oplus \mathbb{Q}[x]/(x(x-1)^3)$$

che ha dimensione 6 su $\mathbb{Q}$.

Soluzione VoF. 14.37. 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 $I = \operatorname{Ann}(A/I) = 0$. Dunque non esistono ideali non banali in A e A deve essere un campo per **T.1.2**.3.

Soluzione VoF. 14.38. 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 $\operatorname{Ann} m \subseteq \mathfrak{m}$. 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 $\frac{a}{1}\frac{m}{1} = \frac{am}{1} = 0$, cioè $\frac{m}{1}$ è un elemento di torsione non banale di $M_{\mathfrak{m}}$, che è contro l'ipotesi.

Soluzione VoF. 14.39. Vero. Se M è libero di rango k allora $M \simeq A^k$; quindi $M \otimes_A B \simeq A^k \otimes_A B \simeq B^k$ per **T.5.4**.1 e 4.

Soluzione VoF. 14.40. Vero. Se $f \in I$ allora $IA_f \cap A = A$ e la tesi è verificata. Supponiamo quindi che $f \notin I$.
Dato che $I \subsetneq (I, f)$ e $I \subseteq IA_f \cap A$ per **T.1.17**.3, l'inclusione $\subseteq$ è verificata.

Per 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 $f^m j \in I$; quindi

$$bf^{m+1} = (j - i)f^m = f^m j - f^m i \in I.$$

Allora $a^{n(m+1)} = (i + bf)^{m+1} \in I$ e $a \in \sqrt{I}$.

Soluzione VoF. 14.41. Vero. Sia $0 \neq a \in A$. La catena discendente $(a) \supseteq (a^2) \supseteq \ldots \supseteq (a^n) \supseteq \ldots$ 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, dato che A è un dominio, $1 = ba$, ossia a è invertibile.

Alternativamente, dato che A è un dominio, l'ideale (0) è primo e quindi massimale per **T.7.14**.1, cioè A è un campo.

Soluzione VoF. 14.42. 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.6.7**.2, dunque A è PID. Infine A è locale per **T.6.6** e $\mathcal{J}(A) = (p)A \neq 0$.

Soluzione VoF. 14.43. Vero. Consideriamo $\varphi\colon \mathbb{Q} \times \mathbb{R} \longrightarrow \mathbb{R}$ data da $\varphi(x, y) = xy$. La mappa 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

$$\frac{a}{b} \otimes_{\mathbb{Z}} y = \frac{a}{b} \otimes_{\mathbb{Z}} \frac{by}{b} = a \otimes_{\mathbb{Z}} \frac{y}{b} = 1 \otimes_{\mathbb{Z}} \frac{ay}{b} \quad \text{per ogni} \quad \frac{a}{b} \in \mathbb{Q} \quad \text{e} \quad y \in \mathbb{R},$$

ogni elemento di $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{R}$ è della forma $1 \otimes y$ con $y \in \mathbb{R}$. Pertanto $0 = \tilde{\varphi}(1 \otimes y) = y$, implica $y = 0$, ossia $\tilde{\varphi}$ è anche iniettivo.

Soluzione VoF. 14.44. Vero. Consideriamo l'A-modulo $N'/(N' \cap N)$ e localizziamo in un ideale $\mathfrak{m} \in \operatorname{Max} A$. Utilizzando **T.6.13**.2 e 3 otteniamo

$$(N'/(N' \cap N))_{\mathfrak{m}} \simeq N'_{\mathfrak{m}}/(N' \cap N)_{\mathfrak{m}} \simeq N'_{\mathfrak{m}}/(N'_{\mathfrak{m}} \cap N_{\mathfrak{m}}).$$

Dato che, per ipotesi, $N'_{\mathfrak{m}} \subseteq N_{\mathfrak{m}}$, abbiamo dimostrato che $(N'/(N' \cap N))_{\mathfrak{m}} = 0$ per ogni $\mathfrak{m} \in \operatorname{Max} A$. La tesi segue immediatamente da **T.6.15**.

Soluzione VoF. 14.45. Falso. Consideriamo 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.

Soluzione VoF. 14.46. Vero. Il modulo M è libero con base $\{1, x\}$, quindi è piatto.

Soluzione VoF. 14.47. Falso. Consideriamo $\mathbb{Q}$, che è uno $\mathbb{Z}$-modulo non finitamente generato. È sicuramente libero da torsione, 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, cf. **E.10.49**.

Soluzione VoF. 14.48. Vero. Da **T.6.19**.3 segue che S è il saturato di T; si conclude grazie a **T.6.19**.6.

Soluzione VoF. 14.49. Vero. La tesi è ovvia se uno dei due moduli è nullo; supponiamo allora $M \neq 0$ e $N \neq 0$. Ricordiamo che la tesi è vera se A è locale per **E.11.11**.
Supponiamo per assurdo che $J = \operatorname{Ann} M + \operatorname{Ann} N \subsetneq A$; allora esiste un ideale massimale $\mathfrak{m}$ che contiene J. Localizzando in $\mathfrak{m}$ otteniamo

$$0 = (M \otimes_A N)_{\mathfrak{m}} \simeq M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} N_{\mathfrak{m}};$$

quindi $M_{\mathfrak{m}} = 0$ 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.12.24**; questo è assurdo, perché $\operatorname{Ann} M \subseteq J \subseteq \mathfrak{m}$. Si conclude analogamente se $N_{\mathfrak{m}} = 0$.

Soluzione VoF. 14.50. Vero. Chiaramente $\mathfrak{m} \subseteq \operatorname{Ann}(M/\mathfrak{m}M)$.

Per l'altra inclusione, notiamo che $\operatorname{Ann}(M/\mathfrak{m}M) \neq A$ perché $M = \mathfrak{m}M$ implica $M = 0$ per il Lemma di Nakayama, contro le ipotesi. Allora $\operatorname{Ann}(M/\mathfrak{m}M) = \mathfrak{m}$ e ovviamente $\mathcal{V}(\mathfrak{m}) = \{\mathfrak{m}\}$.

Soluzione VoF. 14.51. Vero. La dimostrazione è analoga alla prima parte della dimostrazione di **E.11.15**.

Soluzione VoF. 14.52. Vero. Si veda la dimostrazione di **E.13.4**.1.

Soluzione VoF. 14.53. Falso. Sia $A = \prod_{n\in\mathbb{N}} K$ un prodotto diretto di campi. Gli elementi di A sono successioni di elementi di K e le operazioni sono definite componente per componente. Sia $S \subset A$ l'insieme

$$\{s_0 = (0, 1, \ldots, 1, \ldots), (1, \ldots, 1, \ldots) = 1_A\}.$$

L'insieme S è chiaramente moltiplicativamente chiuso e l'omomorfismo di anelli $\tau\colon A \longrightarrow A$ definito da $(a_0, a_1, a_2, \ldots) \mapsto (a_1, a_2, \ldots)$ verifica

i) $\tau(S) = \{1_A\} \subset A^*$;

ii) $\tau(a) = 0$ implica $a = (a_0, 0, \ldots, 0, \ldots)$ e dunque $as_0 = 0$;

iii) ogni $a = (a_0, a_1, \ldots) \in A$ si può scrivere come $\tau((0, a_0, a_1, \ldots,))\tau(1_A)^{-1}$.

Per **T.6.5** possiamo concludere che $A \simeq S^{-1}A$, ma $S \not\subseteq A^*$ poiché s_0 non è invertibile in A.

Soluzione VoF. 14.54. Vero. Dato che A è libero su se stesso, 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 possiamo prendere a_1 e a_2 elementi distinti di un insieme di generatori di I ed ottenere $a_1a_2 = a_2a_1$,

ovvero una relazione di dipendenza non banale, contraddicendo il fatto che I deve essere libero.

Soluzione VoF. 14.55. Vero. Basta considerare $B = A$ e prendere come $\mathfrak{p}$ l'ideale massimale di A.

Soluzione VoF. 14.56. Vero. Sia $A = \mathbb{Z}/(540)$; per **E.8.5**.1 basta osservare che $\overline{7} \in A^*$ e $\overline{30}, \overline{60}, \overline{90} \in \mathcal{N}(A)$.

Soluzione VoF. 14.57. 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

$$\mathbb{Z}_{(2)}[x]/(2x+1) \simeq (\mathbb{Z}_{(2)})_2 \simeq \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_{(2)} \simeq \mathbb{Q},$$

per **E.12.8**, **T.6.14**.1 e **E.12.17**.

Soluzione VoF. 14.58. Falso. $M = (\mathbb{Z}/(15) \oplus \mathbb{Z}/(18))_{(3)} \simeq \mathbb{Z}/(3) \oplus \mathbb{Z}/(9)$ che non è ciclico.

Soluzione VoF. 14.59. 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 otteniamo $M \simeq \mathbb{Z}/(2a+1)$. Se $a > 0$ allora $2a+1 \neq \pm 1$, quindi, per ogni n tale che $\gcd(2a+1, n) \neq 1$, $M \otimes_{\mathbb{Z}} \mathbb{Z}/(n) \neq 0$.

Soluzione VoF. 14.60. Falso. Consideriamo $I = (12) = (3) \cap (4) \subset \mathfrak{p} = (2) \subset \mathbb{Z}$. Allora I non è primario, $\mathfrak{p}$ è primo e $I_{(2)} = (4)_{(2)}$ è primario.

Soluzione VoF. 14.61. Vero. Sia $ax + by + c = 0$ l'equazione di ℓ. Per **T.3.1**.5 abbiamo $\mathcal{C} \cap \ell = \mathbb{V}(f, ax+by+c)$; quindi $\mathcal{C} \cap \ell = \mathbb{V}(f(x, -\frac{ax+c}{b}))$ se $b \neq 0$, oppure $\mathcal{C} \cap \ell = \mathbb{V}(f(-\frac{c}{a}, y))$. Dato che $\ell \not\subseteq \mathcal{C}$ per ipotesi, in entrambi i casi la varietà che ci interessa è definita da un polinomio non nullo univariato di grado $\leq n$ che ha al più n radici.

Soluzione VoF. 14.62. Vero. Sia $m \in T(M)$ e sia $a \in A \setminus \{0\}$ tale che $am = 0$; consideriamo la successione esatta

$$0 \longrightarrow A \xrightarrow{\cdot a} A \longrightarrow A/(a) \longrightarrow 0.$$

Tensorizzando con M otteniamo

$$M \xrightarrow{\cdot a} M \longrightarrow M/(a) \longrightarrow 0$$

dove l'omomorfismo di moltiplicazione non è iniettivo, il che contraddice la piattezza di M.

Soluzione VoF. 14.63. Vero. Per ogni $a \in A \setminus \{0\}$ si ha $Q(A) \otimes_A A/(a) = 0$; infatti

$$\frac{b}{c} \otimes_A \overline{d} = \frac{ab}{ac} \otimes_A \overline{d} = \frac{b}{ac} \otimes_A a\overline{d} = 0.$$

Per **T.5.4**.1 e 4 abbiamo

$$Q(A) \otimes_A M \simeq Q(A) \otimes_A A^n \simeq Q(A)^n.$$

Soluzione VoF. 14.64. 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 $N = \langle xe_0, xe_1 - e_0, xe_2 - e_1, \ldots, xe_{i+1} - e_i, \ldots\rangle$. Chiaramente $\mathcal{J}(A) = (x)$ è finitamente generato. Consideriamo ora il modulo quoziente $M = F/N$; non è difficile verificare che

$$M \neq 0 \quad \text{e} \quad (x)M = (\langle xe_i : i \in \mathbb{N}\rangle + N)/N = M.$$

Si confronti l'enunciato con quello di **E.10.23**.

Soluzione VoF. 14.65. Falso. Consideriamo l'ideale $I = (x^2, 2x) = (x^2, 2) \cap (x)$; si ha $\sqrt{I} = (x)$ ma I non è primario.

Soluzione VoF. 14.66. Vero. Sia $M = N \oplus P$, con M finitamente generato; se $M = \langle (n_1, p_1), \ldots, (n_h, p_h)\rangle$ allora $N = \langle n_1, \ldots, n_h\rangle$ è finitamente generato.

Soluzione VoF. 14.67. Falso. Per calcolare $\sqrt{I}$ utilizziamo la decomposizione

$$\begin{aligned}\sqrt{I} &= \sqrt{(y - z, x^3y^3 - y^2)} \cap \sqrt{(y + z, x^3y^3 + y^2)} \\ &= \sqrt{(y - z, y^2)} \cap \sqrt{(y - z, x^3y - 1)} \cap \sqrt{(y + z, y^2)} \cap \sqrt{(y + z, x^3y + 1)} \\ &= (y, z) \cap (y - z, x^3y - 1) \cap (y + z, x^3y + 1),\end{aligned}$$

dove l'ultima uguaglianza dipende dal fatto che $x^3y \pm 1$ sono irriducibili in $\mathbb{Q}[x, y]$ e dunque gli ideali $(y \pm z, x^3y \pm 1)$ sono primi.
I generatori indicati nella decomposizione formano già basi di Gröbner ridotte rispetto all'ordinamento deglex con $x > z > y$ e $f = (x^3y + 1)(y + z)$ non appartiene a $(y - z, x^3y - 1)$.

Soluzione VoF. 14.68. Vero. Ricordiamo che $I \otimes A/I \simeq I/I^2$, consideriamo l'inclusione $I \longrightarrow A$ e tensorizziamo con A/I; per l'ipotesi di piattezza otteniamo l'omomorfismo iniettivo $I \otimes A/I \longrightarrow A \otimes A/I$. L'immagine in $A \otimes A/I$ di un elemento $i \otimes \overline{a} \in I \otimes A/I$ è $i \otimes \overline{a} = 1 \otimes \overline{ia} = 0$; dunque $I \otimes A/I = 0$ e $I = I^2$ come volevamo.

Soluzione VoF. 14.69. 1. Le affermazioni sono vere. Sia $a \in \operatorname{Ann} N$; allora si ha $0 = af(m) = f(am)$ e l'iniettività di f implica $am = 0$ per ogni $m \in M$, i.e. $a \in \operatorname{Ann} M$.
Inoltre, per ogni $\ell \in L$ esiste $n \in N$ tale che $g(n) = \ell$, quindi $a\ell = ag(n) = g(an) = g(0) = 0$ e $a \in \operatorname{Ann} L$.
Infine siano $b \in \operatorname{Ann} M$ e $c \in \operatorname{Ann} L$; dato che g induce un isomorfismo $L \simeq \operatorname{Coker} f = N/\operatorname{Im} f$, per ogni $n \in N$ si ha $cn \in \operatorname{Im} f$. Quindi $cn = f(m)$ per

qualche $m \in M$ e $bcn = bf(m) = f(bm) = f(0) = 0$, i.e. $bc \in \operatorname{Ann} N$. Questo basta per concludere visto che l'ideale prodotto è generato dai prodotti bc.

2. Vero. In generale se $\varphi\colon M_1 \longrightarrow M_2$ è un omomorfismo di A-moduli allora $\varphi(T(M_1)) \subseteq T(M_2)$. Infatti se $m \in T(M_1)$ allora esiste $a \in A \setminus \{0\}$ tale che $am = 0$, quindi $a\varphi(m) = \varphi(am) = 0$ e $\varphi(m) \in T(M_2)$.

3. Falso. Per un controesempio basta considerare la successione di $\mathbb{Z}$-moduli

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

con $T(M) = T(N) = 0$ e $T(L) = \mathbb{Z}/2\mathbb{Z}$.

4. Vero. Ovviamente f iniettiva implica $f_{|T(M)}$ iniettiva e $g_{|T(N)} \circ f_{|T(M)} = 0$ segue immediatamente da $g \circ f = 0$; quindi $\operatorname{Im} f_{|T(M)} \subseteq \operatorname{Ker} g_{|T(N)}$.

Per l'altra inclusione, sia $n \in \operatorname{Ker} g_{|T(N)}$; allora $g(n) = 0$ implica $n = f(m)$ per qualche $m \in M$ e vogliamo verificare che $m \in T(M)$. Dato che n è di torsione, esiste $a \in A \setminus \{0\}$ tale che $an = 0$; dunque $f(am) = af(m) = 0$ e l'iniettività di f implica $am = 0$, cioè $m \in T(M)$, come volevamo.

Soluzione VoF. 14.70. Vero. Sia $\varphi_5\colon \mathbb{Z}[x] \longrightarrow \mathbb{Z}$ l'omomorfismo di valutazione definito da $p(x) \mapsto p(5)$; allora

$$I = (p(x) \in \mathbb{Z}[x]\colon \varphi_5(p(x)) \in (2)) = (2)^c \supseteq (2, x-5).$$

Dato che $1 \notin (2)^c$ e $(2, x-5)$ è massimale, possiamo concludere che $I = (2, x-5)$ e $\mathbb{Z}[x]/(2, x-5) \simeq \mathbb{Z}/(2)$.

Soluzione VoF. 14.71. Falso. Ricordiamo che per ogni omomorfismo di anelli $\varphi\colon A \longrightarrow B$ si ha $\varphi(-1_A) = -1_B$. Sia $\varphi\colon \mathbb{C} \longrightarrow \mathbb{R}$ un omomorfismo di anelli; allora abbiamo $\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -1$, che non è possibile per nessun $\varphi(i) \in \mathbb{R}$. Dunque non esistono omomorfismi di anelli da $\mathbb{C}$ in $\mathbb{R}$.

Soluzione VoF. 14.72. Vero. Si ha $M = \mathfrak{p}M$; allora, per il Lemma di Nakayama, esiste $a \equiv 1 \mod \mathfrak{p}$ tale che $aM = 0$. Dunque $\operatorname{Ann} M \not\subset \mathfrak{p}$ e otteniamo $M_{\mathfrak{p}} = 0$, cf. **E.12.26**.1.

Soluzione VoF. 14.73. Vero. Se esistono $a, b \in A \setminus I$ tali che $ab \in I$ allora

$$(I, a), (I, b) \supsetneq I \quad \text{e} \quad (I, a) \cap (I, b) \supseteq I.$$

Per l'altra inclusione osserviamo che

$$(I, a) \cap (I, b) \subseteq \sqrt{(I, a) \cap (I, b)} = \sqrt{(I, ab)} \subseteq \sqrt{I} = I.$$

L'uguaglianza $(I, a) \cap (I, b) = I$ contraddice l'irriducibilità di I.

Soluzione VoF. 14.74. Vero. Siano $a, b \in A$ tali che $ab \in I$; allora, per ogni j, si ha $a \in I_j$ oppure $b \in I_j$. Se $a \in I_j$ per ogni j allora $a \in I$; altrimenti sia h il primo indice per cui $a \notin I_h$. Dato che $I_h \supset I_k$ e $ab \in I_k$ per ogni $k \geq h$, si deve avere che $b \in I_k$ per ogni k. Pertanto $b \in I$.

Soluzione VoF. 14.75. Vero. Per $n = 0$ l'affermazione è ovvia e per $n = 1$ è data da **E.8.72**.4.
Procediamo dunque per induzione supponendo che $(K[[x_1, \dots, x_n]], (x_1, \dots, x_n))$ sia locale.
Un elemento $f \in K[[x_1, \dots, x_{n+1}]] = K[[x_1, \dots, x_n]][[x_{n+1}]]$ si scrive come

$$f = \sum_{i \in \mathbb{N}} f_i(x_1, \dots, x_n) x_{n+1}^i$$

ed è invertibile se e solo se $f_0(x_1, \dots, x_n) \in K[[x_1, \dots, x_n]]^*$ e dunque, per l'ipotesi induttiva, $f_0 \notin (x_1, \dots, x_n)$. Allora possiamo scrivere $f = f_0 + x_{n+1} g$ per qualche g e osservare che $f \notin (x_1, \dots, x_{n+1})$ perché, altrimenti $f_0 \in (x_1, \dots, x_{n+1}) \cap K[[x_1, \dots, x_n]] = (x_1, \dots, x_n)$.
Abbiamo quindi provato che ogni elemento invertibile è contenuto nel complementare di $(x_1, \dots, x_{n+1})$, dunque $K[[x_1, \dots, x_{n+1}]]$ è locale con ideale massimale $(x_1, \dots, x_{n+1})$.

Soluzione VoF. 14.76. Vero. Dato che i $\mathfrak{p}_i$ sono minimali, abbiamo $\dim A_{\mathfrak{p}_i} = 0$ per ogni i. Inoltre, $\dim A \geq \dim A/\mathfrak{p}_i$ per ogni i.

Per l'altra disuguaglianza, basta osservare che ogni catena di ideali primi $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ tale che $\mathfrak{q}_1 \neq \mathfrak{p}_i$ per ogni i può essere estesa con un primo minimale $\mathfrak{p}_j \subsetneq \mathfrak{q}_1$.

Soluzione VoF. 14.77. Vero. Sia $0 \neq a \in A$; dato che $(a^2) = (a)(a) = (a) \cap (a) = (a)$, si ha $a = ba^2$ per qualche $b \in A$. Pertanto $a(1 - ba) = 0$ da cui segue che $ab = 1$.

Soluzione VoF. 14.78. Vero. Sappiamo che in generale vale che libero implica piatto. Sia allora A un PID e M un A-modulo piatto finitamente generato. Per il Teorema di struttura **T.4.35**, possiamo scrivere $M = A^k \oplus T(M)$, con $T(M) \simeq \bigoplus_i A/(d_i)$ la parte di torsione e $d_i \neq 0$ per ogni i. Dato che M è piatto, la successione esatta

$$0 \longrightarrow A \xrightarrow{d_i} A \longrightarrow A/(d_i) \longrightarrow 0$$

tensorizzata con M deve rimanere esatta. L'unica possibilità è che $T(M) = 0$, ovvero che M sia libero.

Soluzione VoF. 14.79. Falso. Gli ideali $\mathfrak{p} \subset \mathfrak{q} \subset A$ sono primi; di conseguenza $A \setminus \mathfrak{q} \subset A \setminus \mathfrak{p}$ sono insiemi moltiplicativi di A uno contenuto nell'altro, ma non è possibile trovare un omomorfismo iniettivo tra le corrispondenti localizzazioni. Infatti, dato che $xy = 0$ in A, in $A_{\mathfrak{p}}$ si ha $\frac{x}{1} = \frac{0}{1}$; quindi l'ideale massimale di $A_{\mathfrak{p}}$ è 0 e $A_{\mathfrak{p}}$ è un campo.
Invece in $A_{\mathfrak{q}}$ si ha $\frac{x}{1} \neq 0$ e $\frac{y}{1} \neq 0$, ma $\frac{x}{1}\frac{y}{1} = \frac{0}{1}$; quindi $A_{\mathfrak{q}}$ contiene divisori di zero e una sua immagine omomorfa non può essere contenuta nel campo $A_{\mathfrak{p}}$.

Soluzione VoF. 14.80. Vero. Per la caratterizzazione dei moduli proiettivi, M è proiettivo se e solo se esistono A-moduli N e F tali che $F \simeq M \oplus N$ è

libero. Tensorizzando su A con l'A-modulo piatto $S^{-1}A$ otteniamo $S^{-1}F \simeq S^{-1}M \oplus S^{-1}N$. La conclusione segue dalla stessa caratterizzazione, una volta osservato che se $F \simeq A^H$ per qualche insieme H allora $S^{-1}F \simeq \left(S^{-1}A\right)^H$ è un $S^{-1}A$-modulo libero.

Soluzione VoF. 14.81. Falso. Prendiamo $f = x^2 + 1$ e $g = y^2 + 1$; allora

$$\begin{aligned}\mathbb{Q}[x,y]/(f) \otimes_{\mathbb{Q}[x,y]} \mathbb{Q}[x,y]/(g) &\simeq \mathbb{Q}[x,y]/(x^2+1, y^2+1) \\ &\simeq \mathbb{Q}(i)[y]/(y^2+1) \simeq \mathbb{Q}(i)^2,\end{aligned}$$

che ha dimensione 4 come $\mathbb{Q}$-spazio vettoriale.

Soluzione VoF. 14.82. Falso. L'anello $K[x,y]/(xy-1)$ è isomorfo a $K[x]_x = S^{-1}K[x]$ con $S = \{x^k \colon k \in \mathbb{N}\}$, cf. **E.12.8**.
Sia $\mathfrak{p}$ un primo tale che $\mathfrak{p}^c = (x)$; allora abbiamo $K[x]_x = S^{-1}(x) = \mathfrak{p}^{ce} = \mathfrak{p}$ ma un ideale primo è proprio.

Soluzione VoF. 14.83. Vero. L'implicazione non banale è un caso particolare di quanto visto in **VoF.14.44**.

Soluzione VoF. 14.84. Vero. È vero in generale che un modulo libero è anche proiettivo.

Il viceversa è fornito da **E.11.14**.

Soluzione VoF. 14.85. Vero. Ogni omomorfismo $\varphi \colon \mathbb{Z}/(n) \longrightarrow \mathbb{Q}/\mathbb{Z}$ è completamente determinato da $\varphi(\overline{1})$ che deve verificare $n\varphi(\overline{1}) = \varphi(\overline{n}) = 0$; dunque $\varphi(\overline{1}) \in \left\{\frac{a}{n} + \mathbb{Z} \colon\ a = 0, \dots, n-1\right\}$. La mappa

$$\mathbb{Z}/(n) \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Q}/\mathbb{Z}), \quad \overline{a} \mapsto \varphi_a \quad \text{con} \quad \varphi_a(\overline{1}) = \frac{a}{n} + \mathbb{Z}$$

è ben definita e fornisce l'isomorfismo richiesto.

Soluzione VoF. 14.86. Falso. È immediato vedere che

$$\begin{aligned}M &\simeq A/(x-1) \oplus A/(x^3-1) \oplus A/(x^2-1) \\ &\simeq (A/(x-1))^3 \oplus A/(x+1) \oplus A/(x^2+x+1) \simeq \mathbb{Q}^4 \oplus A/(x^2+x+1).\end{aligned}$$

L'A-modulo $A/(x^2+x+1)$ ha annullatore (x^2+x+1); quindi non può essere isomorfo a $\mathbb{Q}^2$, perché $\operatorname{Ann}_A \mathbb{Q} = (x-a)$ con $a \in \mathbb{Q}$.

Soluzione VoF. 14.87. Falso. Sia $n = 1$, $K = \mathbb{Q}$ e $S = \mathbb{Z} \subset \mathbb{Q}$. Dato che ogni polinomio $0 \neq p \in \mathbb{Q}[x]$ ha solo un numero finito di zeri, $\mathbb{I}(S) = (0)$ e $\mathbb{V}(\mathbb{I}(S)) = \mathbb{Q} \neq S$.

Soluzione VoF. 14.88. Vero. Sia $P_0 \subsetneq \ldots \subsetneq P_m$ una catena di primi in $S^{-1}A$; per la corrispondenza biunivoca tra primi di $S^{-1}A$ e primi di A che non intersecano S, esistono primi $\mathfrak{p}_0, \dots, \mathfrak{p}_m$ di A tali che

$$S^{-1}\mathfrak{p}_i = P_i \quad \text{e} \quad \mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_m.$$

Per definizione $\dim A = n \geq m$; dato che la disuguaglianza vale per ogni catena in $S^{-1}A$, si ha $\dim A \geq \dim S^{-1}A$.
Sia adesso $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ una catena di primi di A; prendendo $T = A - \mathfrak{p}_n$ si ottiene una catena di primi distinti $T^{-1}\mathfrak{p}_0 \subsetneq \ldots \subsetneq T^{-1}\mathfrak{p}_n$ in $T^{-1}A$. Dunque $\dim T^{-1}A \geq n$ e otteniamo l'uguaglianza.

Soluzione VoF. 14.89. Vero. Se φ è un omomorfismo surgettivo allora $\operatorname{Ker}\varphi$ è un ideale massimale di $\mathbb{Z}[x]$; dunque $\operatorname{Ker}\varphi = (p, f)$ con $p \in \mathbb{Z}$ primo e $f \in \mathbb{Z}[x]$ irriducibile modulo p, cf. **E**.8.77. Quindi

$$K \simeq \mathbb{Z}[x]/(p, f) \simeq (\mathbb{Z}/(p))[x]/(\overline{f})$$

è un campo finito con $p^{\deg \overline{f}}$ elementi.

Soluzione VoF. 14.90. Vero. Dato che P è finitamente generato e proiettivo, esistono un intero n e un A-modulo M tali che $A^n \simeq P \oplus M$. Dunque

$$\begin{aligned} A^n &\simeq \operatorname{Hom}_A(A, A)^n \simeq \operatorname{Hom}_A(A^n, A) \simeq \operatorname{Hom}_A(P \oplus M, A) \\ &\simeq \operatorname{Hom}_A(P, A) \oplus \operatorname{Hom}_A(M, A) \end{aligned}$$

e $\operatorname{Hom}_A(P, A)$ è proiettivo in quanto addendo diretto di un A-modulo libero.

Soluzione VoF. 14.91. Falso. Dato che $nm \equiv 0 \mod (n)$ per ogni $m \in \mathbb{Z}/(n)$, si ha $S^{-1}(\mathbb{Z}/(n)) = 0$ per ogni $n \in \mathbb{N}_+$. Invece l'elemento $\dfrac{(1, 1, \ldots, 1, \ldots)}{1}$ è diverso da zero in $S^{-1}\left(\prod_{n\in\mathbb{N}_+} \mathbb{Z}/(n)\right)$, dato che, per ogni n, la componente k-esima di $n(1, 1, \ldots, 1, \ldots)$ è non nulla per $k > n$.

Soluzione VoF. 14.92. Falso. Consideriamo gli $\mathbb{Z}$-moduli $\mathbb{Z}/(n)$ per $n \in \mathbb{N}_+$ e sia $N = \mathbb{Q}$; allora $\mathbb{Z}/(n) \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ per ogni $n \in \mathbb{N}_+$ per **E**.11.8, quindi

$$\prod_{n\in\mathbb{N}_+} (\mathbb{Z}/(n) \otimes_{\mathbb{Z}} \mathbb{Q}) = 0.$$

Invece $\left(\prod_{n\in\mathbb{N}_+} \mathbb{Z}/(n)\right) \otimes_{\mathbb{Z}} \mathbb{Q} \neq 0$; infatti consideriamo il sottomodulo ciclico generato da $m = (\overline{1}_{\mathbb{Z}/(n)})_{n\in\mathbb{N}_+} \in \prod_{n\in\mathbb{N}_+} \mathbb{Z}/(n)$. 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 per **T**.6.12 e **T**.6.14, si ottiene l'inclusione

$$\begin{array}{ccccc} 0 & \longrightarrow & \langle m \rangle_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q} & \longrightarrow & \left(\prod_{n\in\mathbb{N}_+} \mathbb{Z}/(n)\right) \otimes_{\mathbb{Z}} \mathbb{Q} \\ & & \downarrow \simeq & & \\ & & \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \neq 0. & & \end{array}$$

17.8 Soluzioni del capitolo 15

Soluzione E. 15.1. Siano $m_1 = x_{i_1}^{a_1} \cdots x_{i_r}^{a_r}$, con $a_1 > 0$, e $m_2 = x_{j_1}^{b_1} \cdots x_{j_s}^{b_s}$ e supponiamo per assurdo che per ogni coppia di indici i, j esista un intero positivo $k = k(i,j)$ tale che $x_i^k > x_j$. Per ogni $h = 1, \ldots, s$ esistono per ipotesi $k_h \geq 1$ tali che $x_{i_1}^{k_h} > x_{j_h}$, e dunque $x_{i_1}^{k_h b_h} > x_{j_h}^{b_h}$. Definendo $k_0 = \sum_{h=1}^{s} k_h b_h$ otteniamo

$$m_1^{k_0} \geq x_{i_1}^{a_1 k_0} \geq x_{i_1}^{k_0} = x_{i_1}^{k_1 b_1} \cdots x_{i_1}^{k_s b_s} > m_2,$$

che fornisce la contraddizione cercata.

Soluzione E. 15.2. 1. Definiamo φ ponendo $\varphi(x^a y^b z^c) = t^{a+2b+3c}$ per ogni $x^a y^b z^c \in \operatorname{Mon} A$ ed estendendo per linearità. Allora φ risulta essere l'omomorfismo di sostituzione $p(x,y,z) \mapsto p(t, t^2, t^3)$ per ogni $p(x,y,z) \in A$, ed è surgettivo perché ogni $q(t) \in B$ è immagine di $q(x)$.

2. È immediato verificare che $f_1 = y - x^2$, $f_2 = z - x^3 \in \operatorname{Ker} \varphi$. Fissiamo l'ordinamento lessicografico con $z > y > x$ e calcoliamo la riduzione completa $r = r(x,y,z) \in A$ di un qualsiasi elemento $f = f(x,y,z) \in A$ rispetto a $F = \{f_1, f_2\}$. Dato che nessun monomio di r appartiene a $(\operatorname{lt}(f_1), \operatorname{lt}(f_2)) = (y, z)$, possiamo scrivere $r = r(x)$. Sia ora $f = g_1 f_1 + g_2 f_2 + r \in \operatorname{Ker} \varphi$; allora $0 = \varphi(f) = 0 + r(t)$. Quindi $r = 0$ e $f \in (f_1, f_2)$; pertanto $\operatorname{Ker} \varphi = (y - x^2, z - x^3)$.
Alternativamente, calcoliamo $\operatorname{Ker} \varphi$ con una tecnica che può essere generalizzata e applicata all'eliminazione di parametri da un sistema di equazioni polinomiali. Consideriamo $\varphi\colon K[x,y,z] \longrightarrow K[t]$ come composizione di omomorfismi

$$K[x,y,z] \longrightarrow K[x,y,z,t] \xrightarrow{\psi} K[t],$$

dove il primo è dato dall'inclusione e ψ è definito da

$$\psi(x) = p_1(t), \quad \psi(y) = p_2(t), \quad \psi(z) = p_3(t) \quad \text{e} \quad \psi_{|K[t]} = \mathrm{id}_{K[t]}$$

con p_1, p_2, p_3 polinomi di $K[t]$ dati da

$$p_1(t) = t, \quad p_2(t) = t^2, \quad p_3(t) = t^3.$$

Chiaramente $\psi_{|K[x,y,z]} = \varphi$ e $\operatorname{Ker} \varphi = \operatorname{Ker} \psi \cap K[x,y,z]$.
Inoltre non è difficile vedere che

$$\operatorname{Ker} \psi = (x - p_1(t),\, y - p_2(t),\, z - p_3(t)).$$

Il contenimento $\supseteq$ è ovvio; l'altra inclusione si ottiene facilmente dividendo un generico $f(x,y,z,t) \in \operatorname{Ker} \psi$ per l'insieme $\{x - p_1(t),\, y - p_2(t),\, z - p_3(t)\}$, fissato su $K[x,y,z,t]$ un qualsiasi ordinamento monomiale per cui $t^k < x$, $t^k < y$, $t^k < z$ per ogni $k \in \mathbb{N}$, ad esempio l'ordinamento lex con $x > y > z > t$.

Grazie al Teorema di eliminazione possiamo calcolare $\operatorname{Ker}\varphi$ trovando una base di Gröbner G di $\operatorname{Ker}\psi$ rispetto all'ordinamento lex con $t > x > y > z$. Calcoliamo G e otteniamo

$$G = \{t - x,\, x^2 - y,\, xy - z,\, xz - y^2,\, y^3 - z^2\};$$

quindi

$$\operatorname{Ker}\varphi = (x^2 - y,\, xy - z,\, xz - y^2,\, y^3 - z^2) = (x^2 - y,\, x^3 - z).$$

Soluzione E. 15.3. 1. Procediamo per induzione su n; la tesi è ovvia per $n = 1$. Grazie all'ipotesi induttiva e alla distributività di Hom e del prodotto tensoriale rispetto alla somma diretta abbiamo

$$\begin{aligned}
\operatorname{Hom}(A^n, M) \otimes N &\simeq \big(\operatorname{Hom}(A^{n-1}, M) \oplus \operatorname{Hom}(A, M)\big) \otimes N \\
&\simeq \big(\operatorname{Hom}(A^{n-1}, M) \otimes N\big) \oplus (\operatorname{Hom}(A, M) \otimes N) \\
&\simeq \operatorname{Hom}(A^{n-1}, M \otimes N) \oplus \operatorname{Hom}(A, M \otimes N) \\
&\simeq \operatorname{Hom}(A^n, M \otimes N).
\end{aligned}$$

2. Sia Q un A-modulo; osserviamo che l'applicazione

$$\varphi_Q \colon \operatorname{Hom}_A(Q, M) \times N \longrightarrow \operatorname{Hom}_A(Q, M \otimes N)$$

definita da $(\varphi_Q(f, n))(q) = f(q) \otimes n$ per ogni $q \in Q$, è bilineare e dunque induce un unico omomorfismo $\widetilde{\varphi}_Q \colon \operatorname{Hom}(Q, M) \otimes N \longrightarrow \operatorname{Hom}_A(Q, M \otimes N)$. In particolare, per $Q = A^n$, abbiamo visto al punto 1 che tale applicazione è un isomorfismo.
Per ipotesi esiste una successione esatta

$$0 \longrightarrow H \longrightarrow A^n \longrightarrow L \longrightarrow 0$$

per un certo $n \in \mathbb{N}$. Applicando il funtore controvariante $\operatorname{Hom}(\bullet, M)$, si ottiene una successione esatta

$$0 \longrightarrow \operatorname{Hom}(L, M) \longrightarrow \operatorname{Hom}(A^n, M) \longrightarrow \operatorname{Hom}(H, M)$$

che rimane esatta anche tensorizzando con N, perché N è piatto.
Applicando invece $\operatorname{Hom}(\bullet, M \otimes N)$, si ottiene una successione esatta

$$0 \longrightarrow \operatorname{Hom}(L, M \otimes N) \longrightarrow \operatorname{Hom}(A^n, M \otimes N) \longrightarrow \operatorname{Hom}(H, M \otimes N).$$

Le ultime due successioni formano un diagramma commutativo

$$\begin{array}{ccccccc}
0 & \longrightarrow & \operatorname{Hom}(L, M) \otimes N & \longrightarrow & \operatorname{Hom}(A^n, M) \otimes N & \longrightarrow & \operatorname{Hom}(H, M) \otimes N \\
 & & \downarrow{\scriptstyle \widetilde{\varphi}_L} & & \downarrow{\scriptstyle \widetilde{\varphi}_{A^n}} & & \downarrow{\scriptstyle \widetilde{\varphi}_H} \\
0 & \longrightarrow & \operatorname{Hom}(L, M \otimes N) & \longrightarrow & \operatorname{Hom}(A^n, M \otimes N) & \longrightarrow & \operatorname{Hom}(H, M \otimes N).
\end{array}$$

Dato che $\widetilde{\varphi}_{A^n}$ è un isomorfismo, si ha $\operatorname{Ker}\widetilde{\varphi}_L = 0$.

Soluzione E. 15.4. 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 un elemento massimale P.
Poiché P non è finitamente generato, P è un ideale proprio e non primo, per cui esistono a, $b \notin P$ con $ab \in P$. Per la massimalità di P, l'ideale (P, a) è finitamente generato dunque esistono 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 l'ideale $J = P\colon (a)$ che contiene propriamente P dato che $b \in J \backslash P$. Di nuovo per la massimalità di P abbiamo che J 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 $\supseteq$.

Per l'altra inclusione, sia $c \in P \subseteq (P, a)$, con

$$c = \sum_i c_i d_i = \sum_i c_i (p_i + s_i a) = \sum_i c_i p_i + ja \quad \text{per certi } c_i, j \in A;$$

visto che $c - \sum_i c_i p_i \in P$, abbiamo

$$j \in J \quad \text{e} \quad c \in (p_1, \ldots, p_k) + aJ,$$

come volevamo.

Soluzione E. 15.5. 1. Si vede facilmente che $I \subsetneq (x) \subsetneq (x, z) \subsetneq (x, y, z)$; la corrispondenza tra ideali di A contenenti I e ideali di A/I mostra che la catena di ideali primi $(\overline{x}) \subsetneq (\overline{x}, \overline{z}) \subsetneq (\overline{x}, \overline{y}, \overline{z})$ ha lunghezza 2 e quindi $\dim A/I \geq 2$.

2. La base di Gröbner ridotta rispetto a entrambi gli ordinamenti è

$$G = \{x^2 z - x^2,\ xyz + xz,\ x^2 y + x^2\}$$

quindi anche gli escalier sono gli stessi.

3. Dal Teorema di eliminazione e dal punto 2 segue direttamente che $I \cap \mathbb{Q}[y, z] = 0$. Consideriamo ora l'ordinamento lex con $z > x > y$ e calcoliamo la base di Gröbner, che rimane invariata. Possiamo allora concludere che

$$I \cap \mathbb{Q}[x, y] = (x^2 y + x^2).$$

4. Usando ripetutamente la relazione $\sqrt{(J, fg)} = \sqrt{(J, f)} \cap \sqrt{(J, g)}$ si ottiene

$$\begin{aligned}\sqrt{I} &= \sqrt{(x^2,\, xyz + xz)} \cap \sqrt{(z-1,\, xy + x)} \\ &= \sqrt{(x)} \cap \sqrt{(y+1, x^2)} \cap \sqrt{(z, x^2)} \cap \sqrt{(x, z-1)} \cap \sqrt{(y+1, z-1)} \\ &= (x) \cap (y+1, x) \cap (z, x) \cap (x, z-1) \cap (y+1, z-1).\end{aligned}$$

Infine $\mathbb{V}(I) = \mathbb{V}(\sqrt{I})$ implica

$$\mathbb{V}(I) = \mathbb{V}(x) \cup \mathbb{V}(y+1, x) \cup \mathbb{V}(z, x) \cup \mathbb{V}(x, z-1) \cup \mathbb{V}(y+1, z-1).$$

Pertanto $\mathbb{V}(I) = \mathbb{V}(x) \cup \mathbb{V}(y+1, z-1)$ è una decomposizione di $\mathbb{V}(I)$ in componenti irriducibili.

5. Dato che $(A/I)_{\mathfrak{p}} \simeq A_{\mathfrak{p}}/I_{\mathfrak{p}}$, si ha $(A/I)_{\mathfrak{p}} \neq 0$ se e solo se $I_{\mathfrak{p}} \neq A_{\mathfrak{p}}$, i.e. se e solo se $I \subseteq \mathfrak{p}$. Da ciò segue che per ogni primo associato, dunque per ogni primo minimale, la localizzazione di A/I in $\mathfrak{p}$ è non nulla, mentre il viceversa non è vero. Ad esempio, $\mathfrak{m} = (x, y, z^2+1) \supsetneq I$ e $\mathfrak{m} \notin \operatorname{Ass}(I)$.

6. I primi minimali sono $\mathfrak{p}_1 = (x)$ e $\mathfrak{p}_2 = (y+1, z-1)$ e le relative componenti primarie corrispondono a $(I_{\mathfrak{p}_i})^c$ per $i = 1, 2$. Quindi

$$(I_{\mathfrak{p}_1})^c = ((x^2z - x^2,\, xyz + xz)_{\mathfrak{p}_1})^c = ((x^2,\, x)_{\mathfrak{p}_1})^c = (x),$$

$$(I_{\mathfrak{p}_2})^c = ((x^2z - x^2,\, xyz + xz)_{\mathfrak{p}_2})^c = ((z-1, y+1)_{\mathfrak{p}_2})^c = (y+1, z-1).$$

Soluzione E. 15.6. Sia $I_1 I_2 = \bigcap_{i=1}^n \mathfrak{q}_i$ una decomposizione primaria di $I_1 I_2$. Eventualmente riordinando gli indici, possiamo supporre che esista un intero $r \leq n$ tale che $I_1 \subseteq \sqrt{\mathfrak{q}_i}$ per $i = 1, \ldots, r$ e $I_1 \nsubseteq \sqrt{\mathfrak{q}_i}$ per $i = r+1, \ldots, n$.
Definiamo $J = \bigcap_{i=1}^r \mathfrak{q}_i$ e $J' = \bigcap_{i=r+1}^n \mathfrak{q}_i$. Per ogni $i = 1, \ldots, r$ esiste $t_i \in \mathbb{N}$ tale che $I_1^{t_i} \subseteq \mathfrak{q}_i$ e quindi esiste t tale che $I_1^t \subseteq J$.
Per ogni $i = r+1, \ldots, n$ esiste $a_i \in I_1 \setminus \sqrt{\mathfrak{q}_i}$; dato che $a_i b \in I_1 I_2 \subseteq \mathfrak{q}_i$ per ogni $b \in I_2$, otteniamo che $b \in \mathfrak{q}_i$, i.e. $I_2 \subseteq J'$. Adesso per concludere basta osservare che

$$I_1 I_2 = I_1 I_2 \cap I_2 = (J \cap J') \cap I_2 = J \cap I_2.$$

Soluzione E. 15.7. Per ogni A-modulo N la successione

$$N \otimes M_1 \xrightarrow{\mathrm{id}_N \otimes \varphi} N \otimes M_2 \xrightarrow{\mathrm{id}_N \otimes \psi} N \otimes M_3 \longrightarrow 0$$

è esatta e dobbiamo dimostrare che $\mathrm{id}_N \otimes \varphi$ è iniettivo.
Consideriamo una successione esatta di A-moduli

$$0 \longrightarrow L \xrightarrow{g} F \xrightarrow{f} N \longrightarrow 0$$

con F libero e quindi piatto. Tensorizzando tale successione con M_2 e M_3 otteniamo un diagramma commutativo

$$\begin{array}{ccccccccc} & & L\otimes M_2 & \xrightarrow{g\otimes \mathrm{id}_{M_2}} & F\otimes M_2 & \xrightarrow{f\otimes \mathrm{id}_{M_2}} & N\otimes M_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_L\otimes\psi} & & \downarrow{\scriptstyle \mathrm{id}_F\otimes\psi} & & \downarrow{\scriptstyle \mathrm{id}_N\otimes\psi} & & \\ 0 & \longrightarrow & L\otimes M_3 & \xrightarrow[g\otimes \mathrm{id}_{M_3}]{} & F\otimes M_3 & \xrightarrow[f\otimes \mathrm{id}_{M_3}]{} & N\otimes M_3 & \longrightarrow & 0 \end{array}$$

dove gli omomorfismi verticali sono surgettivi e la prima riga è esatta per le proprietà del prodotto tensoriale, mentre la seconda è esatta perché M_3 è piatto per ipotesi. Il Lemma del serpente fornisce una successione esatta

$$\mathrm{Ker}(\mathrm{id}_L\otimes\psi)\longrightarrow \mathrm{Ker}(\mathrm{id}_F\otimes\psi)\longrightarrow \mathrm{Ker}(\mathrm{id}_N\otimes\psi)\longrightarrow 0$$

dove gli omomorfismi sono dati dalle opportune restrizioni di $g\otimes\mathrm{id}_{M_2}$ e $f\otimes\mathrm{id}_{M_2}$. Dato che F è piatto, $\mathrm{Ker}(\mathrm{id}_F\otimes\psi)=\mathrm{Im}(\mathrm{id}_F\otimes\varphi)\simeq F\otimes M_1$. Tensorizzando la successione esatta $0\longrightarrow L\longrightarrow F\longrightarrow N\longrightarrow 0$ con M_1, otteniamo un diagramma commutativo con righe esatte

$$\begin{array}{ccccccccc} & & L\otimes M_1 & \xrightarrow{g\otimes \mathrm{id}_{M_1}} & F\otimes M_1 & \xrightarrow{f\otimes \mathrm{id}_{M_1}} & N\otimes M_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_L\otimes\varphi} & & \downarrow{\scriptstyle \mathrm{id}_F\otimes\varphi}\ \simeq & & \downarrow{\scriptstyle \mathrm{id}_N\otimes\varphi} & & \\ 0 & \longrightarrow & \mathrm{Ker}(\mathrm{id}_L\otimes\psi) & \longrightarrow & \mathrm{Ker}(\mathrm{id}_F\otimes\psi) & \longrightarrow & \mathrm{Ker}(\mathrm{id}_N\otimes\psi) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

dove le mappe verticali sono surgettive perché, per le proprietà del prodotto tensoriale, $\mathrm{Im}(\mathrm{id}_*\otimes\varphi)=\mathrm{Ker}(\mathrm{id}_*\otimes\psi)$, con $*$ uno qualsiasi tra L, F e N.
Il fatto che $\mathrm{id}_N\otimes\varphi$ sia un omomorfismo iniettivo segue da una caccia al diagramma.

Soluzione E. 15.8. 1. È chiaro dalla definizione che $\mathfrak{p}^{(n)}=(\mathfrak{p}^n)^{ec}$ rispetto all'omomorfismo canonico $A\longrightarrow A_\mathfrak{p}$, dunque $\mathfrak{p}^n\subseteq\mathfrak{p}^{(n)}$.

Per l'altra inclusione, sia $a\in\mathfrak{p}^{(n)}$; allora $\frac{a}{1}=\frac{b}{s}\in\mathfrak{p}^nA_\mathfrak{p}$, con $b\in\mathfrak{p}^n$ e $s\notin\mathfrak{p}$. Quindi esiste $u\notin\mathfrak{p}$ tale che $bu=asu$ e $asu\in\mathfrak{p}^n$, con $\mathfrak{p}^n$ primario. Dato che $su\notin\mathfrak{p}$, otteniamo $a\in\mathfrak{p}^n$, come volevamo.

2. Siano $A=K[x,y,z]/(xy-z^2)$ e $\overline{\mathfrak{p}}=(\overline{x},\overline{z})\subset A$; allora $\overline{\mathfrak{p}}$ è primo e $\overline{\mathfrak{p}}^2=(\overline{x}^2,\overline{z}^2,\overline{xz})$ non è primario
Dato che $\frac{1}{\overline{y}}\in A_{\overline{\mathfrak{p}}}$ e $\overline{xy}\in\overline{\mathfrak{p}}^2$, si ha $\frac{\overline{x}}{\overline{1}}=\overline{xy}\cdot\frac{1}{\overline{y}}\in\overline{\mathfrak{p}}^2A_{\overline{\mathfrak{p}}}$. Dunque $\overline{x}\in\overline{\mathfrak{p}}^{(2)}\setminus\overline{\mathfrak{p}}^2$ e la generalizzazione non vale.

Soluzione E. 15.9. Denotiamo con φ l'endomorfismo di A^4 associato alla matrice

$$X = \begin{pmatrix} x^2-1 & 0 & x^2-1 & x^2-1 \\ 3x+3 & x^2+x & x+1 & 2x+2 \\ 3x+3 & x+1 & x+1 & 2x+2 \\ 3x+3 & x+1 & x+1 & 2x+2 \end{pmatrix},$$

in modo che $M \simeq \operatorname{Coker}\varphi$. La forma di Smith di X è la matrice diagonale $\operatorname{diag}(x+1, x^2-1, x^2-1, 0)$.

1. Dalla forma di Smith segue che la parte libera di M è isomorfa ad A,

$$T(M) \simeq A/(x+1) \oplus (A/(x^2-1))^2$$

e $\operatorname{Ann}_A M = 0$; notiamo inoltre che $\operatorname{Ann}_A T(M) = (x^2-1)$.

2. Abbiamo

$$M \otimes_A A/(x-1) \simeq A/(x+1, x-1) \oplus (A/(x^2-1, x-1))^2 \oplus A/(x-1),$$

che è isomorfo a $(A/(x-1))^3 \simeq \mathbb{C}^3$, mentre

$$M \otimes_A A/(x-i) \simeq A/(x+1, x-i) \oplus (A/(x^2-1, x-i))^2 \oplus A/(x-i),$$

è isomorfo a $A/(x-i) \simeq \mathbb{C}$.

3. Abbiamo

$$\operatorname{Hom}_A(M, N) \simeq \operatorname{Hom}_A(A, N) \oplus \operatorname{Hom}_A(T(M), N) \simeq N \oplus \operatorname{Hom}_A(T(M), N),$$

pertanto è sufficiente trovare un A-modulo N tale che $\operatorname{Hom}_A(T(M), N) = 0$. Basta prendere $N = A/(f)$ ciclico tale che $(f)\colon (x+1)/(f) = (f)\colon (x^2-1)/(f) = 0$; quindi qualsiasi f coprimo con x^2-1 verifica la richiesta.

Soluzione E. 15.10. 1. Scriviamo $\mathfrak{p}_1 = (a)$, $\mathfrak{p}_2 = (ab)$ e $\mathfrak{q} = (ac)$; per ipotesi b non è invertibile e $a \notin \mathfrak{p}_2$. Dato che $ab \in \mathfrak{p}_2$ e $\mathfrak{p}_2$ è primo, si ha $b \in \mathfrak{p}_2$ e dunque $b = abb_1$ per qualche $b_1 \in A$. Da ciò segue che $b(1-ab_1) = 0 \in \mathfrak{q}$; dato che $\mathfrak{q}$ è primario e $1-ab_1 \notin \sqrt{\mathfrak{q}}$ poiché non sta in $\mathfrak{p}_1$, otteniamo $b \in \mathfrak{q}$ e, di conseguenza, $\mathfrak{p}_2 \subseteq \mathfrak{q}$, come volevamo.

2. Segue immediatamente da 1.

3. Sia I l'intersezione di tutti gli ideali primari contenuti in $\mathfrak{p}_1$; allora $\mathfrak{p}_2 \subseteq I$ per il punto 1.

Per l'altra inclusione, basta osservare che $\mathfrak{p}_2$ è primario, ed è dunque compreso nell'insieme degli ideali la cui intersezione è I.

4. Per ipotesi esiste un ideale massimale $\mathfrak{m}$ che contiene sia $\mathfrak{p}_1$ che $\mathfrak{p}_2$. Se $\mathfrak{p}_1 \subsetneq \mathfrak{m}$ allora, per il punto 3, $\mathfrak{p}_1$ è l'intersezione di tutti gli ideali primari contenuti in $\mathfrak{m}$ e lo stesso vale per $\mathfrak{p}_2$. Dunque $\mathfrak{p}_1 = \mathfrak{p}_2$ oppure uno dei due coincide con $\mathfrak{m}$ e quindi contiene l'altro.

Soluzione E. 15.11. 1. Se $x > y$ si ha $\mathrm{lt}(g_1) = x^2y$ e $\mathrm{lt}(g_2) = x^3$; se invece $y > x$ si ha $\mathrm{lt}(g_1) = -y^2$ e $\mathrm{lt}(g_2) = -yx$. In entrambi i casi quindi $S(g_1, g_2) = xg_1 - yg_2 = 0$ e G è una base di Gröbner rispetto a tutti gli ordinamenti lessicografici.
Osserviamo che G è ridotta rispetto all'ordinamento con $x > y$ mentre non lo è rispetto all'ordinamento con $y > x$; infatti $yx \,|\, yx^2$ e $\mathrm{lc}(g_1) = \mathrm{lc}(g_2) = -1$. La base ridotta in questo ultimo caso è $G' = \{y^2 - x^4,\, yx - x^3\}$.

2. Si ha

$$\sqrt{I} = \sqrt{(x^2 - y)} \cap \sqrt{(y, x^3)} = (x^2 - y) \cap (x, y) = (x^2 - y).$$

Da ciò segue subito che $I \neq \sqrt{I}$; infatti $x^2 - y \notin I$ perché in ogni caso x^2 non appartiene a $\mathrm{Lt}(I)$.

3. Dato che $\mathbb{V}_{\mathbb{R}}(I) = \mathbb{V}_{\mathbb{R}}(\sqrt{I})$, dal punto 2 segue che $\mathbb{V}_{\mathbb{R}}(I) = \{(a, a^2) \colon a \in \mathbb{R}\}$. Dato che $(a, a^2, 0) \in \mathbb{V}_{\mathbb{R}}(J)$ per ogni $a \in \mathbb{R}$, l'affermazione è vera.

Soluzione E. 15.12. La base di Gröbner ridotta di I rispetto all'ordinamento lessicografico con $x > y$ è

$$G = \left\{x^2 - y^2,\, xy + y^2,\, y^4 + \tfrac{1}{2}y\right\}.$$

1. Si ha

$$\begin{aligned}\sqrt{I} &= \sqrt{(I, y)} \cap \sqrt{(I, y^3 + \tfrac{1}{2})} \\ &= \sqrt{(x^2, y)} \cap \sqrt{(x + y, y^3 + \tfrac{1}{2})} \cap \sqrt{(x - y, 2y^2, y^3 + \tfrac{1}{2})} \\ &= (x, y) \cap (x + y, y^3 + \tfrac{1}{2})\end{aligned}$$

e questi ideali sono entrambi massimali.

2. Dato che $(I, y) + (I, y^3 + \frac{1}{2}) = 1$, si ha

$$I = (I, y) \cap (I, y^3 + \tfrac{1}{2}) = (x^2, y) \cap (x + y, y^3 + \tfrac{1}{2}) = \mathfrak{q}_1 \cap \mathfrak{q}_2.$$

Poiché $\sqrt{\mathfrak{q}_1} = (x, y)$ è massimale, l'ideale (x^2, y) è primario, inoltre l'ideale $(x + y, y^3 + \frac{1}{2})$ è massimale e quindi primario.

3. Nella decomposizione minimale di I ci sono due ideali primari e i primi associati sono entrambi minimali, quindi $\mathcal{D}(A/I) = (\overline{x}, \overline{y}) \cup (\overline{x + y}, \overline{y^3 + \frac{1}{2}})$. Inoltre, dato che gli ideali nel punto 1 sono comassimali, si ha

$$\sqrt{I} = (x, y)(x + y,\, y^3 + \tfrac{1}{2}) = (x^2 + xy,\, xy^3 + \tfrac{1}{2}x,\, xy + y^2,\, y^4 + \tfrac{1}{2}y).$$

Riducendo i generatori rispetto a G osserviamo che l'unico che non appartiene ad I è

$$xy^3 + \tfrac{1}{2}x \xrightarrow{G}_* \tfrac{1}{2}(x + y);$$

dunque $\mathcal{N}(A/I) = (\overline{x+y})$.

4. Dato che $\mathfrak{p} = \sqrt{\mathfrak{q}_1}$ e $(A \setminus \mathfrak{p}) \cap (x+y, y^3+\frac{1}{2}) \neq \emptyset$, si ha

$$I_{\mathfrak{p}} \cap A = \big((x^2,y)_{\mathfrak{p}} \cap A\big) \cap \big((x+y,y^3+\tfrac{1}{2})_{\mathfrak{p}} \cap A\big) = (x^2,y).$$

Inoltre, dato che entrambi i radicali $\sqrt{\mathfrak{q}_1}$ e $\sqrt{\mathfrak{q}_2}$ intersecano $A \setminus \mathfrak{q}$, si ha

$$I_{\mathfrak{q}} \cap A = A_{\mathfrak{q}} \cap A = A.$$

5. Dai punti precedenti segue che

$$(A/I)_{\mathfrak{p}} \simeq (A/\mathfrak{q}_1 \oplus A/\mathfrak{q}_2)_{\mathfrak{p}} \simeq (A/\mathfrak{q}_1)_{\mathfrak{p}} \simeq A/\mathfrak{q}_1 = \mathbb{Q}[x]/(x^2),$$

mentre $(A/I)_{\mathfrak{q}} \simeq A_{\mathfrak{q}}/I_{\mathfrak{q}} = 0$.

Soluzione E. 15.13. 1. Il modulo $\operatorname{Coker}\varphi_{ab}$ è ciclico se e solo se nella forma di Smith di B_{ab} abbiamo $d_1 = d_2 = 1$. Si ha $(d_1) = \Delta_1 = (x-a, 1-x, b, a-x^2)$ e possiamo distinguere due casi.

i) $b \neq 0$; in questo caso certamente $d_1 = 1$ e dobbiamo calcolare d_2. Dato che $\Delta_2 = (x-a, 1-x)$, abbiamo $\Delta_2 = (1)$ se e solo se $a \neq 1$.

ii) $b = 0$; in questo caso $\Delta_1 = (x-a, 1-x, a-x^2) = (1)$ se e solo se $a \neq 1$. Abbiamo $\Delta_2 = (x-a)$ e dunque $\operatorname{Coker}\varphi_{ab}$ non può essere ciclico.

Pertanto $\operatorname{Coker}\varphi_{ab}$ è ciclico per $b \neq 0$ e $a \neq 1$.

2. Per $b \neq 0$ e $a = 1$ otteniamo $d_1 = 1$, $d_2 = x-1$ e $\Delta_3 = ((x-1)^2(1-x^2)) = ((x-1)^3(x+1))$. Quindi $d_3 = (x-1)^2(x+1)$ e

$$\operatorname{Coker}\varphi_{1b} \simeq \mathbb{Q}[x]/(x-1) \oplus \mathbb{Q}[x]/(x-1)^2 \oplus \mathbb{Q}[x]/(x+1) \simeq \mathbb{Q}^2 \oplus \mathbb{Q}[x]/(x-1)^2.$$

Per $b = 0$ e $a \neq 1$ otteniamo $d_1 = 1$, $d_2 = x-a$ e $\Delta_3 = ((x-a)^2(a-x^2))$. Quindi

$$d_3 = \begin{cases} (x-a)(x+c)(x-c)) & \text{se } a = c^2 \text{ per qualche } c \in \mathbb{Q}, \\ (x-a)(x^2-a) & \text{altrimenti} \end{cases}$$

e

$$\begin{aligned} \operatorname{Coker}\varphi_{a0} &\simeq \mathbb{Q}[x]/(x-a) \oplus \mathbb{Q}[x]/(x-a) \oplus \mathbb{Q}[x]/(x^2-a) \\ &\simeq \begin{cases} \big(\mathbb{Q}[x]/(x-a)\big)^2 \oplus \mathbb{Q}[x]/(x-c) \oplus \mathbb{Q}[x]/(x+c) \simeq \mathbb{Q}^4 & \text{se } a = c^2, \\ \big(\mathbb{Q}[x]/(x-a)\big)^2 \oplus \mathbb{Q}[x]/(x^2-a) \simeq \mathbb{Q}^2 \oplus \mathbb{Q}[x]/(x^2-a) & \text{altrimenti.} \end{cases} \end{aligned}$$

Infine per $b = 0$ e $a = 1$ otteniamo

$$B_{10} = \begin{pmatrix} x-1 & 0 & 0 \\ 0 & 1-x & x-1 \\ 0 & 1-x^2 & 0 \end{pmatrix};$$

quindi $\Delta_1 = (x-1)$, $\Delta_2 = (x-1)^2$, $\Delta_3 = ((x-1)^3(x+1))$ e

$$\operatorname{Coker}\varphi_{10} \simeq \mathbb{Q}[x]/(x-1) \oplus \mathbb{Q}[x]/(x-1) \oplus \mathbb{Q}[x]/(x-1) \oplus \mathbb{Q}[x]/(x+1) \simeq \mathbb{Q}^4.$$

Soluzione E. 15.14. La base di Gröbner ridotta di I rispetto all'ordinamento lex con $x > y > z$ è

$$\{x - yz, y^2 z\}.$$

Calcoliamo l'intersezione $\mathfrak{q}_1 \cap \mathfrak{q}_2$ come $((t-1)\mathfrak{q}_1, t\mathfrak{q}_2) \cap K[x,y,z]$. Abbiamo

$$((t-1)\mathfrak{q}_1, t\mathfrak{q}_2) = (f_1 = tx - x, f_2 = tz - z, f_3 = ty^2, f_4 = tx - tyz)$$

e

$$\begin{array}{lll}
S(f_1,f_2) = 0, & S(f_2,f_3) = -y^2z = -f_7, & S(f_4,f_5) \xrightarrow{f_7} 0, \\
S(f_1,f_3) = -x^2z = -f_5, & S(f_2,f_4) \xrightarrow{f_2,f_6} 0, & S(f_4,f_6) = 0, \\
S(f_1,f_4) \xrightarrow{f_2} -x + yz = -f_6, & S(f_2,f_7) \xrightarrow{f_7} 0, & S(f_5,f_6) \xrightarrow{f_7} 0, \\
S(f_1,f_5) \xrightarrow{f_5} 0, & S(f_3,f_4) \xrightarrow{f_7} 0, & S(f_5,f_7) = 0, \\
S(f_1,f_6) \xrightarrow{f_2,f_6} 0, & S(f_3,f_5) = S(f_3,f_7) = 0, & S(f_6,f_7) \xrightarrow{f_7} 0.
\end{array}$$

Dato che le coppie (f_2,f_5), (f_2,f_6), (f_3,f_6), (f_4,f_7), (f_6,f_7) e (f_1,f_7) hanno termini di testa coprimi, i corrispondenti S-polinomi riducono a zero; quindi $\{f_1,\dots,f_7\}$ è una base di Gröbner di $((t-1)\mathfrak{q}_1, t\mathfrak{q}_2)$ e

$$\mathfrak{q}_1 \cap \mathfrak{q}_2 = (x^2z, x - yz, y^2z) = (x - yz, y^2z) = I.$$

Sicuramente $\mathfrak{q}_1$ è primo e quindi primario. Inoltre osserviamo che i divisori di zero di $K[x,y,z]/\mathfrak{q}_2 \simeq K[y,z]/(y^2)$ sono nilpotenti; quindi anche $\mathfrak{q}_2$ è primario. Infine $\sqrt{\mathfrak{q}_1} = (x,z) \neq \sqrt{\mathfrak{q}_2} = (x,y)$ e la decomposizione trovata è minimale.

Soluzione E. 15.15. Se $I = 0$ chiaramente I è finitamente generato; altrimenti esiste $0 \neq x \in I$ e se $\mathfrak{m} \in \operatorname{Max} A$ è tale che $\mathfrak{m} \supseteq I$ allora $\mathfrak{m} \in \mathcal{M}_x$. Quindi ogni $I \neq 0$ è contenuto in un numero finito di ideali massimali.
Consideriamo ora una catena ascendente $\{I_\alpha\}_{\alpha\in\Lambda}$ di ideali di A, e indichiamo con $I_{\overline{\alpha}}$ il primo elemento non nullo della catena. Siano $\mathfrak{m}_1,\dots,\mathfrak{m}_s$ gli ideali massimali di A che contengono $I_{\overline{\alpha}}$. Dato che $A_{\mathfrak{m}_i}$ è noetheriano, per ogni $i = 1,\dots,s$ esiste un indice β_i tale che la catena $\{I_\alpha A_{\mathfrak{m}_i}\}_{\alpha\in\Lambda}$ si stabilizza in β_i. Inoltre, se $\mathfrak{m} \in \operatorname{Max} A$ e $I_{\overline{\alpha}} \not\subset \mathfrak{m}$ allora $I_{\overline{\alpha}} A_{\mathfrak{m}} = A_{\mathfrak{m}}$. Esiste quindi $\beta = \max_i\{\beta_i\} \geq \overline{\alpha}$ tale che $I_\beta A_{\mathfrak{m}} = I_\gamma A_{\mathfrak{m}}$, i.e.

$$(I_\gamma/I_\beta)_{\mathfrak{m}} \simeq I_\gamma A_{\mathfrak{m}}/I_\beta A_{\mathfrak{m}} = 0,$$

per ogni $\gamma \geq \beta$ e per ogni $\mathfrak{m} \in \operatorname{Max} A$. Questo implica che $I_\gamma/I_\beta = 0$; quindi la catena è stazionaria e A è noetheriano.

Soluzione E. 15.16. Dalla definizione abbiamo immediatamente $I^{[n]} \subseteq I^n$.

1. L'ideale I^2 è generato dagli elementi fg al variare di $f, g \in I$; dato che $2fg = (f+g)^2 - f^2 - g^2 \in I^{[2]}$ per ogni $f, g \in I$, abbiamo $I^2 \subseteq I^{[2]}$, come volevamo.

2. Siano $B = \mathbb{Z}/(2)[x,y]$ e $I = (x,y)$. Abbiamo $I^2 = (x^2, xy, y^2) \supsetneq I^{[2]} = (x^2, y^2)$ perché non esiste elemento di I che elevato al quadrato dia xy. Infatti un generico elemento di I si scrive come $ax + by$ con $a, b \in \mathbb{Z}/(2)[x,y]$; per la fattorizzazione unica l'uguaglianza $(ax+by)^2 = a^2x^2 + b^2y^2 = xy$ implica $x \mid b$, quindi $x^2 \mid b^2$ e infine $x^2 \mid (ax+by)^2 = xy$ che è una contraddizione.

3. L'ideale I^n è generato da tutti i monomi di grado n, ovvero $x^n, x^{n-1}y, \dots, y^n$. Se consideriamo $(x + a_i y)^n = \sum_j \binom{n}{j} a_i^j y^j x^{n-j}$ per valori distinti $a_1, \dots, a_{n+1}$ in $\mathbb{Q}$, otteniamo $n+1$ relazioni che possiamo scrivere come

$$M \begin{pmatrix} \binom{n}{0} x^n \\ \binom{n}{1} x^{n-1} y \\ \vdots \\ \binom{n}{n} y^n \end{pmatrix} = \begin{pmatrix} (x + a_1 y)^n \\ (x + a_2 y)^n \\ \vdots \\ (x + a_{n+1} y)^n \end{pmatrix},$$

dove $M = \begin{pmatrix} 1 & a_1 & a_1^2 & \dots & a_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_{n+1} & a_{n+1}^2 & \dots & a_{n+1}^n \end{pmatrix}$ è una matrice di Vandermonde. Dato che $\det M = \prod_{i \neq j} (a_i - a_j) \neq 0$, la matrice è invertibile e quindi $I^n \subseteq I^{[n]}$.

Soluzione E. 15.17. 1. Dalla catena $J \supseteq J^2 \supseteq \dots \supseteq J^k \supseteq \dots$ otteniamo la catena ascendente $I \colon J \subseteq I \colon J^2 \subseteq \dots \subseteq I \colon J^k \subseteq \dots$, e quindi $I \colon J^\infty = \bigcup_{n=1}^\infty I \colon J^n$ è un ideale di A.

2. Iniziamo calcolando $I \colon J^\infty$ nel caso in cui I è $\mathfrak{p}$-primario per qualche primo $\mathfrak{p}$.

Se J è un ideale non contenuto in $\mathfrak{p}$ allora un elemento $j \in J \setminus \mathfrak{p}$ è tale che $I \colon (j) = I$. Dunque

$$I \colon J = I \colon (J, j) = (I \colon J) \cap (I \colon (j)) = (I \colon J) \cap I = I$$

e $I \colon J^\infty = I$.

Se invece $J \subseteq \mathfrak{p}$ allora, dato che A è noetheriano, esiste k tale che $J^k \subseteq I$ da cui otteniamo $A = I \colon J^k \subseteq I \colon J^\infty \subseteq A$.

Siano ora $a, b \in A$ e $I = \bigcap_{i \in \Lambda} \mathfrak{q}_i$ una decomposizione primaria minimale di I. Denotiamo con $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$, $\Lambda_b = \{i \in \Lambda \colon b \notin \mathfrak{p}_i\}$ e $\Lambda_{a,b} = \{i \in \Lambda \colon a \notin \mathfrak{p}_i \text{ oppure } b \notin \mathfrak{p}_i\}$. Dalle precedenti osservazioni otteniamo

$$I \colon (b)^\infty = \bigcap_{i \in \Lambda} \mathfrak{q}_i \colon (b)^\infty = \bigcap_{i \in \Lambda_b} \mathfrak{q}_i \quad \text{e} \quad I \colon (a,b)^\infty = \bigcap_{i \in \Lambda_{a,b}} \mathfrak{q}_i.$$

Per la minimalità della decomposizione da ciò segue che $I\colon (b)^\infty = I\colon (a,b)^\infty$ se e solo se $\Lambda_b = \Lambda_{a,b}$, ossia se e solo se ogni primo associato di I che contiene b contiene anche a.

Soluzione E. 15.18. 1. Si ha $y^3 - 1 = (y-1)(y-\alpha)(y-\alpha^2)$ con α radice terza primitiva dell'unità.
L'unico valore possibile di y per un punto $(x,y) \in \mathbb{Q}^2$ nella varietà di I è $y = 1$, ma per $y = 1$ il valore di x deve soddisfare la relazione $x^2 + x + 1 = 0$ che non ha radici in $\mathbb{Q}$; quindi $\mathbb{V}_{\mathbb{Q}}(I) = \emptyset$.
Possiamo decomporre $I \subseteq \mathbb{Q}[x,y]$ nel seguente modo

$$\begin{aligned} I &= (x^2 + xy + y^2, y-1) \cap (x^2 + xy + y^2, y^2 + y + 1) \\ &= (x^2 + x + 1, y-1) \cap (x^2 + xy + (-y-1), y^2 + y + 1) \\ &= (x^2 + x + 1, y-1) \cap (x - 1, y^2 + y + 1) \cap (x + y + 1, y^2 + y + 1) \\ &= \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3, \end{aligned}$$

con $\mathfrak{p}_i \in \operatorname{Spec}(\mathbb{Q}[x,y])$ per $i = 1,2,3$.
Possiamo decomporre ulteriormente $I \subseteq \mathbb{C}[x,y]$ come intersezione degli ideali massimali $I = (x-\alpha, y-1) \cap (x-\alpha^2, y-1) \cap (x-1, y-\alpha) \cap (x-1, y-\alpha^2) \cap (x+\alpha+1, y-\alpha) \cap (x+\alpha^2+1, y-\alpha^2)$, da cui segue che

$$\mathbb{V}_{\mathbb{C}}(I) = \{\alpha, 1), (\alpha^2, 1), (1, \alpha), (1, \alpha^2), (\alpha^2, \alpha), (\alpha, \alpha^2)\}.$$

2. Nella decomposizione $I = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3$ tutti gli ideali sono primi; quindi $I = \sqrt{I}$,

$$\mathcal{N}(\mathbb{Q}[x,y]/I) = (\overline{0}) \quad \text{e} \quad \mathcal{D}(\mathbb{Q}[x,y]/I) = \overline{\mathfrak{p}}_1 \cup \overline{\mathfrak{p}}_2 \cup \overline{\mathfrak{p}}_3.$$

3. Per i punti precedenti i primi associati di I sono tutti massimali; dunque $\overline{\mathfrak{p}}_1$, $\overline{\mathfrak{p}}_2$ e $\overline{\mathfrak{p}}_3$ sono gli unici primi di $\mathbb{Q}[x,y]/I$.

4. Localizzando in uno degli ideali primi $\overline{\mathfrak{p}}_i$ otteniamo $(\overline{\mathfrak{p}}_i)_{\overline{\mathfrak{p}}_i} = (0)$, perché per ogni elemento $\overline{a} \in \overline{\mathfrak{p}}_i$ esiste $\overline{s} \in (\mathbb{Q}[x,y]/I) \setminus \overline{\mathfrak{p}}_i$ tale che $\overline{as} = \overline{0}$. Quindi, per ognuno dei tre ideali primi, $(\mathbb{Q}[x,y]/I)_{\overline{\mathfrak{p}}_i}$ è un campo.

Soluzione E. 15.19. 1. Dato che $I\,I^{-1} = A$, esistono $i_j \in I$ e $m_j \in I^{-1}$ tali che $1 = \sum_{j=1}^n i_j m_j$ per qualche intero positivo n. Per ogni $i \in I$ si ha $i = \sum_{j=1}^n (i m_j) i_j$ dove $i m_j \in A$ per ogni j; quindi I è un A-modulo generato dagli i_j.

2. Consideriamo la successione esatta corta di A-moduli

$$0 \longrightarrow \operatorname{Ker}\pi \longrightarrow A^n \xrightarrow{\pi} I \longrightarrow 0,$$

dove l'omomorfismo π è definito sugli elementi della base canonica da $\pi(e_j) = i_j$ con $j = 1, \ldots, n$ ed è surgettivo per il punto 1. È sufficiente mostrare che la

successione spezza. Consideriamo la mappa $s\colon I \longrightarrow A^n$ definita da $s(i) = \sum_{j=1}^{n} im_j e_j$. È facile verificare che s è un omomorfismo di A-moduli tale che $\pi \circ s = \mathrm{id}_I$, cioè s è una sezione di π.

Soluzione E. 15.20. Dato che $I = \sqrt{I}$, si ha

$$m = |\,\mathbb{V}(I)| = \dim_{\mathbb{C}} \mathbb{C}[x_1, \ldots, x_n]/I.$$

Per ipotesi $\overline{1}, \overline{x_n} \ldots, \overline{x_n}^{m-1}$ sono una base di $\mathbb{C}[x_1, \ldots, x_n]/I$; quindi per ogni $i < n$ esistono $b_{ij} \in \mathbb{C}$ tali che $\overline{x_i} = \sum_{j=0}^{m-1} b_{ij} \overline{x_n}^{j}$. Dunque i polinomi

$$x_i - \sum_{j=0}^{m-1} b_{ij} x_n^j = x_i - p_i(x_n)$$

appartengono a I e $(x_1 - p_1, \ldots, x_{n-1} - p_{n-1}, p_n) \subseteq I$.

Per l'altra inclusione, osserviamo che tramite l'algoritmo di divisione ogni $f \in \mathbb{C}[x_1, \ldots, x_n]$ si può scrivere come

$$f = \sum_{i=1}^{n-1} a_i(x_i - p_i) + r(x_n) \qquad \text{per qualche } a_i \in \mathbb{C}[x_1, \ldots, x_n].$$

Se $f \in I$ allora $r(x_n) \in I \cap \mathbb{C}[x_n]$ e quindi $I \subseteq (x_1 - p_1, \ldots, x_{n-1} - p_{n-1}, p_n)$. Infine, dato che $p_i \in \mathbb{C}[x_n]$ per ogni i e $\deg p_i < \deg p_n$ per ogni $i \neq n$, l'insieme $\{x_1 - p_1, \ldots, x_{n-1} - p_{n-1}, p_n\}$ è la base di Gröbner ridotta di I.

Soluzione E. 15.21. 1. Consideriamo il diagramma commutativo

$$\begin{array}{ccccc} P & \xrightarrow{\psi} & M & & \\ {\scriptstyle f}\,\vdots & & \downarrow{\scriptstyle \mathrm{id}_M} & & \\ P' & \xrightarrow[\psi']{} & M & \longrightarrow & 0 \end{array}$$

in cui l'omomorfismo f esiste perché ψ' è surgettivo e P è proiettivo. Se $p = \varphi(n) \in \operatorname{Im}\varphi = \operatorname{Ker}\psi$ allora

$$0 = (\mathrm{id}_M \circ \psi)(p) = (\psi' \circ f)(p)\,, \quad \text{i.e. } f(p) \in \operatorname{Ker}\psi' = \operatorname{Im}\varphi'.$$

Dunque $f_{|\varphi(N)}$ è a valori in $\varphi'(N')$ e possiamo definire l'omomorfismo $g\colon N \longrightarrow N'$ che associa ad ogni $n \in N$ l'unico elemento $g(n) \in N'$ tale che $f(\varphi(n)) = \varphi'(g(n))$. La buona definizione di g discende dall'iniettività di φ'. La tesi segue immediatamente dal Lemma del serpente applicato al diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{\varphi} & P & \xrightarrow{\psi} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}_M} & & \\ 0 & \longrightarrow & N' & \xrightarrow{\varphi'} & P' & \xrightarrow{\psi'} & M & \longrightarrow & 0. \end{array}$$

2. Definiamo una successione

$$0 \longrightarrow N \xrightarrow{\lambda} P \oplus N' \xrightarrow{\eta} P' \longrightarrow 0$$

con $\lambda(n) = (\varphi(n), g(n))$ e $\eta(p, n') = f(p) - \varphi'(n')$. Ovviamente λ e η sono omomorfismi e λ è iniettiva perché φ lo è.
Inoltre

$$(\eta \circ \lambda)(n) = \eta(\varphi(n), g(n)) = f(\varphi(n)) - \varphi'(g(n)) = 0$$

e quindi $\operatorname{Im}\lambda \subseteq \operatorname{Ker}\eta$.

Per l'altra inclusione, sia $(p, n') \in \operatorname{Ker}\eta$; allora

$$f(p) = \varphi'(n') \quad \text{e} \quad 0 = \psi'(\varphi'(n')) = \psi'(f(p)) = \mathrm{id}_M(\psi(p)).$$

Quindi $p \in \operatorname{Ker}\psi = \operatorname{Im}\varphi$ e, dato che φ è iniettiva, esiste un unico $n \in N$ tale che $\varphi(n) = p$. Ne segue che

$$\varphi'(n') = f(p) = f(\varphi(n)) = \varphi'(g(n)) \quad \text{e} \quad n' = g(n)$$

per l'iniettività di φ'; dunque $(p, n') = (\varphi(n), g(n)) = \lambda(n) \in \operatorname{Im}\lambda$.
Infine, sia $p' \in P'$; allora $\psi'(p') \in M$ ed esiste $p \in P$ tale che $\psi(p) = \psi'(p')$. Di conseguenza $\psi'(f(p)) = \psi(p) = \psi'(p')$ e $f(p) - p' \in \operatorname{Ker}\psi' = \operatorname{Im}\varphi'$. Dunque esiste $n' \in N'$ tale che $f(p) - p' = \varphi'(n')$, cioè $p' = f(p) - \varphi'(n') = \eta(p, n')$ e η è surgettiva.
Abbiamo dimostrato che la successione è esatta; dato che P' è proiettivo, ciò implica l'esistenza di un isomorfismo $P \oplus N' \simeq N \oplus P'$, come volevamo.

Bibliografia

[1] W. W. Adams e P. Loustaunau. *An introduction to Gröbner bases.* Vol. 3. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 1994.

[2] A. Altman e S. Kleiman. *A term of commutative algebra.* Worldwide Center of Mathematics, 2013.

[3] M. F. Atiyah e I. G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, 1969.

[4] H. Cartan e S. Eilenberg. *Homological algebra.* Princeton Landmarks in Mathematics. Princeton University Press, Princeton, NJ, 1956.

[5] D. A. Cox, J. Little e D. O'Shea. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra.* Fourth edition. Undergraduate Texts in Mathematics. Springer, Cham, 2015.

[6] S. Lang. *Algebra.* Revised third edition. Vol. 211. Graduate Texts in Mathematics. Springer-Verlag, New York, 2002.

[7] R. Mines, F. Richman e W. Ruitenburg. *A course in constructive algebra.* Universitext. Springer New York, NY, 1988.

[8] M. Reid. *Undergraduate commutative algebra.* Vol. 29. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 1995.

Indice analitico