

Appunti di Algebra Commutativa

(versione non completa)

Giovanni Cutolo

Indice

Notazioni e terminologia	iii
1 Anelli, Moduli, Algebre	1
1.1 Anelli ed Anelli unitari	1
1.1.1 L’anello degli endomorfismi di un gruppo abeliano	3
1.2 Moduli e premoduli	5
1.2.1 Alcuni esempi fondamentali	6
1.2.2 Omomorfismi, sotto(pre)moduli	7
1.2.3 Prodotti e somme tra parti; sotto(pre)moduli generati	9
1.2.4 Congruenze e quozienti, teoremi di omomorfismo e di corrispondenza	11
1.2.5 Annullatori; moduli fedeli	12
1.2.6 Cambio degli scalari	13
1.2.7 Premoduli finitamente generati	15
1.2.8 Moduli ciclici e premoduli semplici	17
1.3 Algebre	19
1.3.1 Immersione in un’algebra unitaria: accrescimento	21
1.3.2 Riduzione di premoduli a moduli	23
1.3.3 Idealizzazione di un (pre)modulo	24
2 Divisibilità in monoidi commutativi	27
2.1 Richiami	27
2.2 Una caratterizzazione dei monoidi fattoriali in termini di ordinamenti	28
2.2.1 Reticoli	28
2.2.2 Il preordinamento divisibilità	29
2.3 Parti sature e saturazioni	33
3 Ideali	35
3.1 Operazioni tra parti e ideali in un anello	35
3.2 Ideali primi e massimali	37
3.2.1 Primi	37
3.3 Nilradicale e radicale di Jacobson di un anello commutativo	40
3.3.1 Il nilradicale di un anello; varietà e radicale di un ideale	40
3.3.2 Il radicale di Jacobson	42
3.3.3 Versioni del Lemma di Nakayama	45
3.4 Divisibilità e ideali in anelli unitari	47
4 Costruzioni per moduli e per anelli	49
4.1 Prodotti e somme dirette di moduli	49
4.2 Prodotti e somme dirette di anelli e algebre	51
4.2.1 Idempotenti e decomposizioni dirette in anelli	55
4.2.2 Immersioni in prodotti diretti di quozienti	57
4.3 Costruzioni universali: oggetti liberi, prodotti e coprodotti	58
4.3.1 Moduli e premoduli liberi	59

Indice

4.3.2	Algebre unitarie libere: anelli di polinomi	63
4.3.3	Prodotti e coprodotti	67
5	Proprietà di anelli di polinomi e di serie formali di potenze	71
5.1	Due risultati elementari	71
5.2	Fattorialità di anelli di polinomi	72
5.3	Invertibili, nilpotenti, divisori dello zero	76
5.4	Serie formali di potenze	78
6	Condizioni di catena per moduli e anelli	81
6.1	Definizioni e prime proprietà	81
6.2	Caratterizzazioni di moduli e anelli noetheriani	85
6.3	Il teorema della base di Hilbert	87
7	Decomposizione primaria	90
7.1	Ideali primari	90
7.2	Decomposizioni primarie e decomposizioni primarie minimali	94
7.2.1	Ideali irriducibili per intersezione e decomposizioni primarie in anelli noetheriani	95
7.3	Teoremi di unicità	96
8	Anelli artiniani	101
8.1	Ideali primi e massimali	101
8.2	La struttura degli anelli artiniani unitari	102
8.3	Il teorema dell'intersezione di Krull e gli anelli locali noetheriani	104
9	Anelli di frazioni	107
9.1	Posizione del problema e costruzione	107
9.2	Ideali negli anelli di frazioni. Localizzazioni.	111
9.3	Decomposizioni primarie in anelli di frazioni	118
10	Ampliamenti interi ed anelli di valutazione	120
10.1	Interi su un anello	120
10.2	Anelli di Bézout ed anelli di valutazione	124
11	Funtori Hom e moduli proiettivi	129
11.1	Sequenze di moduli	129
11.2	I funtori Hom	132
11.3	Funtori esatti	134
11.4	Moduli proiettivi	136
12	Anelli di Dedekind	141
12.1	Ideali frazionari	141
12.2	Anelli di Dedekind	143
12.2.1	Alcune caratterizzazioni e loro conseguenze	145
12.3	Ideali in anelli di Dedekind	149
13	Argomenti vari	153
13.1	Condizioni minimale e condizione massimale per insiemi ordinati	153

Notazioni e terminologia

Applicazioni e funzioni La principale avvertenza da fare è che, come di abitudine in algebra, in queste note la composizione (prodotto operativo) tra applicazioni è indicata nel verso naturale “da sinistra verso destra” anziché viceversa, come capita in altri contesti. Dunque, se $f: A \rightarrow B$ e $g: B \rightarrow C$ sono applicazioni, l’applicazione composta ottenuta eseguendo prima f e poi g si indica con fg , non con gf oppure $g \circ f$. L’immagine di un elemento $a \in A$ mediante f sarà di regola indicata con la notazione esponenziale e non con quella sinistra, vale a dire: con a^f piuttosto che con $f(a)$. Dunque, per le applicazioni f e g indicate sopra, per ogni $a \in A$ avremo $a^{fg} = (a^f)^g$.

Sempre con riferimento ad una applicazione $f: A \rightarrow B$, indichiamo con $\vec{f}: \mathcal{P}(A) \rightarrow \mathcal{P}(B)$ e $\overleftarrow{f}: \mathcal{P}(B) \rightarrow \mathcal{P}(A)$ le applicazioni immagine e antiimmagine definite da f .

Anelli, ideali, (pre)moduli

- 0_R : zero dell’anello (o del premodulo) R
- 1_R : unità dell’anello (o del monoide moltiplicativo) R
- 0 : indica spesso l’ideale nullo $\{0_R\}$ di un anello R
o il sottopremodulo nullo $\{0_M\}$ di un premodulo M
- $\mathcal{U}(R)$: gruppo degli invertibili dell’anello unitario (o del monoide moltiplicativo) R
- $H \triangleleft R$: H è un ideale di R
- $H \triangleleft\!\!\triangleleft R$: H è un ideale massimale di R
- $\text{Spec}(R)$: spettro (= insieme degli ideali primi) di R
- $Q(R)$: campo dei quozienti del dominio di integrità R
- $S^{-1}R$: anello di frazioni di R (definito dalla sua parte $S \neq \emptyset$)
- $\sqrt{H}, \sqrt[n]{H}$: radicale di H (in R)
- $\text{Var}(H), \text{Var}_R(H)$: varietà di H (in R)
- $N \leq_R M, N \leq M$: N è un sotto(pre)modulo di M
- $N <_R M, N < M$: N è un sotto(pre)modulo proprio di M
- $N \triangleleft_R M, N \triangleleft M$: N è un sotto(pre)modulo massimale di M
- R_R : (l’anello commutativo) R riguardato come premodulo su sé stesso
- $\text{Ann}_R(X)$: annullatore di X in R
- $(N : X)_R, (N : X)$: annullatore di X modulo N , cioè $\{r \in R \mid Xr \subseteq N\}$

La terminologia utilizzata nella letteratura matematica sugli anelli, moduli e algebre non è affatto uniforme. Riassumiamo alcune scelte qui adottate, che vengono comunque discusse anche nel testo.

- Gli anelli, qui, *non sono necessariamente unitari*. Fare attenzione alla distinzione tra sottoanelli e sottoanelli unitari e tra omomorfismi di anelli e di anelli unitari, discussa nella [sezione 1.1](#).
- Un anello *nullo* è un anello con un solo elemento, che è quindi lo zero e allo stesso tempo l’unità dell’anello.

Notazioni e terminologia

- Un *divisore dello zero* in un anello R è un elemento $a \in R$ per il quale esista $b \in R$ tale che $ab = 0_R \neq b$. Dunque, se (e solo se) R non è nullo, 0_R ne è un divisore dello zero e, in ogni caso, i divisori dello zero di un anello sono tutti e soli i suoi elementi non cancellabili.
- Un *dominio di integrità* è un anello R , unitario o meno, in cui 0_R sia l'unico divisore dello zero. Un *campo* è un anello commutativo unitario in cui 0_R sia l'unico elemento non invertibile.
- Gli anelli nulli sono qui considerati unitari e, in conseguenza delle definizioni precedenti, non sono domini di integrità né sono campi.

Altro

\mathbb{N}^+ è l'insieme dei numeri interi positivi, $\mathbb{N} = \mathbb{N}^+ \cup \{0\}$ quello dei numeri naturali.

1 Anelli, Moduli, Algebre

In questo capitolo introdurremo (o rivisiteremo) le strutture algebriche che hanno un ruolo predominante nell'algebra commutativa, che sono quelle richiamate nel titolo. Nel farlo fisseremo alcune notazioni e un po' di terminologia.

1.1 Anelli ed Anelli unitari

Sono comunemente in uso in matematica diverse definizioni di anello, non tutte equivalenti tra loro. Quella che adottiamo in queste note è la stessa che chi legge ha probabilmente incontrato nei primi corsi di algebra. Chiamiamo quindi anello una struttura algebrica $(R, +, \cdot, -, 0_R)$, dove $+$ e \cdot sono operazioni binarie (dette rispettivamente addizione e moltiplicazione dell'anello), $-$ è un'operazione unaria e 0_R un'operazione nullaria (cioè la selezione di una costante), tali che $(R, +, -, 0_R)$ sia un gruppo abeliano, \cdot sia associativa e distributiva (cioè distributiva sia da sinistra che da destra) rispetto a $+$. Rendiamo esplicito il fatto che un'operazione unaria in R è semplicemente un'applicazione $R \rightarrow R$; in questo caso l'applicazione che ad ogni elemento di R associa il suo opposto, cioè il simmetrico rispetto all'addizione. In accordo con la definizione di gruppo che stiamo dando per nota, la costante 0_R indica l'elemento neutro di R rispetto a $+$ e si chiama *zero* dell'anello R (con un abuso di notazione denotiamo con lo stesso simbolo, 0_R , sia lo zero dell'anello R che l'operazione nullaria che lo seleziona).

Utilizzeremo spesso, ma non sempre, questo modo di indicare strutture algebriche con una notazione che dia conto dell'intera segnatura della struttura, esplicitando quindi non solo le operazioni binarie ma anche quelle di altra arietà (nei casi che incontreremo, le operazioni unarie o nullarie). Questo tipo di notazione è quella usuale in un ambito dell'algebra chiamato algebra universale e, tra gli altri vantaggi, giustifica alcune scelte terminologiche che sembrerebbero altrimenti arbitrarie.

Con pochissime eccezioni—essenzialmente [una](#)—gli anelli considerati in queste note saranno sempre commutativi (cioè con moltiplicazione commutativa), e spesso anche unitari. Mentre la nozione di anello commutativo non richiede particolari commenti, va spesa qualche parola a proposito degli anelli unitari.

Un anello unitario può essere semplicemente definito come un anello che abbia elemento neutro rispetto alla moltiplicazione. In realtà conviene considerare quella degli anelli unitari come un tipo di struttura differente, già nella segnatura, da quella degli anelli. Diciamo quindi che un anello unitario è una struttura algebrica $(R, +, \cdot, -, 0_R, 1_R)$, dove $(R, +, \cdot, -, 0_R)$ è un anello e 1_R è l'operazione nullaria che seleziona l'elemento neutro rispetto a \cdot , chiamato *unità* di R ed anch'esso denotato da 1_R . Assumere questo punto di vista comporta alcune conseguenze; vediamole.

In accordo con definizioni date in algebra universale (o in teoria dei modelli), un omomorfismo tra due strutture algebriche dello stesso tipo è un'applicazione tra i sostegni delle due strutture che conservi *tutte* le operazioni che definiscono il tipo di struttura. Come è noto dai primi corsi di algebra, un'applicazione tra gruppi che conservi l'operazione binaria conserva necessariamente anche l'elemento neutro ed i simmetrici ed è quindi un omomorfismo nel senso che abbiamo qui appena specificato. Allo stesso modo, quindi, un'applicazione tra due anelli che conservi addizione e moltiplicazione è in senso proprio un omomorfismo perché conserva anche l'operazione

nullaria (cioè lo zero) e l'operazione unaria (cioè gli opposti) ed è così un omomorfismo di anelli. Se però R e S sono anelli, entrambi dotati di unità, rispettivamente 1_R e 1_S , ed $f: R \rightarrow S$ è un omomorfismo di anelli, non è detto che f mandi 1_R in 1_S ; in altri termini: non è detto che f conservi l'unità. Solo nel caso in cui lo faccia diciamo che f è un *omomorfismo di anelli unitari*, in accordo con la terminologia dell'algebra univale.

Ad esempio, sia X un insieme e Y una sua parte propria. Possiamo considerare l'anello (unitario) delle parti di X , ovvero $(\mathcal{P}(X), \Delta, \cap, \text{id}_{\mathcal{P}(X)}, \emptyset, X)$ ¹ e l'anello delle parti di Y , cioè $(\mathcal{P}(Y), \Delta, \cap, \text{id}_{\mathcal{P}(Y)}, \emptyset, Y)$. Evidentemente l'applicazione immersione $\iota: \mathcal{P}(Y) \hookrightarrow \mathcal{P}(X)$ tra questi anelli conserva addizione e moltiplicazione ma non l'unità; quindi è un omomorfismo di anelli (tra due anelli unitari), ma non un omomorfismo di anelli unitari.

Osserviamo comunque che una condizione apparentemente molto più debole garantisce che un omomorfismo di anelli tra anelli unitari sia un omomorfismo di anelli unitari:

Lemma 1.1. *Siano R ed A anelli unitari, e sia $\varphi: R \rightarrow A$. Allora φ è un omomorfismo di anelli unitari se e solo se l'immagine di φ contiene almeno un elemento cancellabile in A .*

Dimostrazione. Se φ è un omomorfismo di anelli unitari, allora $\text{im } \varphi$ ha come elemento 1_A , ovviamente cancellabile in A . Viceversa, se esiste $r \in R$ tale che r^φ sia cancellabile in A , allora da $(1_R)^\varphi r^\varphi = (1_R r)^\varphi = r^\varphi = 1_A r^\varphi$ deduciamo $(1_R)^\varphi = 1_A$. \square

Discorso analogo a quello fatto per gli omomorfismi vale per le sottostrutture. Una parte non vuota di una struttura algebrica ne costituisce una sottostruttura se e solo se è chiusa rispetto a tutte le operazioni della struttura. Nel caso degli anelli otteniamo così la consueta nozione di sottoanello, dato da una parte non vuota chiusa rispetto all'operazione di addizione, a quella di opposto e, di conseguenza, alla selezione dello zero (quindi un sottogruppo rispetto all'addizione), e chiusa anche rispetto all'operazione di moltiplicazione. Nel caso degli anelli unitari richiediamo in aggiunta la chiusura rispetto alla selezione dell'unità. Quindi in *sottoanello unitario* di un anello unitario R è un sottoanello di R a cui appartenga l'unità di R . Abbiamo così che se R è un anello unitario e S un suo sottoanello, sono possibili i seguenti casi:

- S non è un anello unitario;
- S è un anello unitario, ma la sua unità non è quella di R . La terminologia utilizzata in questo caso è davvero infelice e può essere fuorviante: S non è un sottoanello unitario di R , ma ne è un sottoanello che, come anello, è unitario;
- S è un anello unitario, e $1_S = 1_R$. In questo caso (e solo in questo) S è un sottoanello unitario di R .

Esempi per queste tre tipologie: $R = \mathbb{Z}$ e $S = 2\mathbb{Z}$ (l'anello dei numeri interi pari) per la prima, $R = \mathcal{P}(X)$ e $S = \mathcal{P}(Y)$, dove, come sopra, $Y \subset X$ per la seconda, $R = \mathbb{Q}$ e $S = \mathbb{Z}$ (o $S = \mathbb{Q}$) per la terza. Osserviamo anche che S è un sottoanello unitario di R precisamente quando l'immersione $S \hookrightarrow R$ è un omomorfismo di anelli unitari.

¹ Δ indica l'operazione di differenza simmetrica, che è l'addizione di questo anello, mentre la moltiplicazione è l'operazione di intersezione; l'opposto di ogni elemento di $\mathcal{P}(X)$ è l'elemento stesso, quindi $\text{id}_{\mathcal{P}(X)}$, l'applicazione identica di $\mathcal{P}(X)$, è l'operazione unaria di selezione dell'opposto e ovviamente \emptyset e X sono lo zero e l'unità dell'anello.

Osservazioni.

1.A.1. Come accennato, esistono nella letteratura matematica definizioni di anello diverse dalla nostra. Quella più generale tra quelle di uso frequente differisce dalla nostra solo nel non richiedere che l'operazione di moltiplicazione sia associativa. Chi adotta questa terminologia chiama anelli associativi quelli che noi abbiamo chiamato anelli. Sono esempi importanti di questi 'anelli non associativi' gli anelli di Lie, un tipo di struttura il cui studio ha numerose applicazioni sia in algebra che in altri settori della matematica.

Al contrario, moltissimi autori adottano una definizione di anello più restrittiva della nostra e richiedono nella definizione di anello l'esistenza di un elemento neutro per la moltiplicazione. In altri termini, questi autori chiamano anelli quelli che per noi sono gli anelli unitari. Occorre dunque verificare sempre, quando si consultano testi di algebra (o altre fonti), quale sia la definizione di anello lì utilizzata.

1.A.2. Abbiamo insistito sui vantaggi nell'indicare la segnatura completa delle strutture algebriche che vengono introdotte, ma, naturalmente, è del tutto lecito riferirsi ad esse esplicitando solo alcune delle loro operazioni, che determinino univocamente le rimanenti. Ad esempio, si usano spesso scritte come "l'anello $(R, +, \cdot)$ ", in cui sono specificate solo le due operazioni binarie; questo non dà luogo ad ambiguità perché sia l'operazione unaria di opposto che quella nullaria di selezione dello zero sono univocamente determinate dall'operazione di addizione. Allo stesso modo, e per l'analogo motivo, potremmo scrivere "l'anello unitario $(R, +, \cdot)$ ", sottintendendo l'unità dell'anello.

Il caso estremo è quello in cui le operazioni vengono omesse del tutto e si scrive, ad esempio, "l'anello R " piuttosto che "l'anello $(R, +, \cdot)$ "; lo si può fare solo se il contesto chiarisce, senza ambiguità, quali siano le operazioni $+$ e \cdot .

1.A.3. È appena il caso di notare che talvolta lo stesso simbolo $(-)$ usato per l'operazione unaria di opposto in un anello viene anche usato per l'operazione binaria di differenza (generalmente non associativa e di non particolare interesse). Questo è implicito in scritte come $a - b$, comunemente usata come abbreviazione di $a + (-b)$.

Fissiamo un po' di terminologia (che non è del tutto universale). In queste note considereremo, tra gli anelli unitari, gli *anelli nulli*, quelli cioè con un solo elemento, che è, quindi, allo stesso tempo lo zero e l'unità dell'anello. Dovrebbe essere chiaro che gli anelli nulli sono tutti isomorfi tra loro e sono tutti e soli gli anelli unitari in cui lo zero è un elemento invertibile. A proposito dello zero, stabiliamo anche che, in queste note, se R è un anello non nullo lo zero di R è considerato un divisore dello zero in R ; dunque, in ogni anello, i divisori dello zero sono tutti e soli gli elementi non cancellabili (rispetto alla moltiplicazione). Inoltre, poiché lo troviamo vantaggioso, chiamiamo domini di integrità gli anelli commutativi in cui lo zero sia l'unico divisore dello zero; in questo modo stabiliamo che gli anelli nulli *non* sono domini di integrità.

1.1.1 L'anello degli endomorfismi di un gruppo abeliano

Iniziamo da qualcosa di molto elementare. Siano X un insieme e $*$ un'operazione binaria definita in un insieme S . Allora si definisce un'operazione binaria $*^X$ nell'insieme S^X delle applicazioni da X a S ponendo, per ogni $f, g \in S^X$,

$$f *^X g: x \in X \mapsto x^f * x^g \in S.$$

L'operazione $*^X$ viene abitualmente chiamata operazione puntuale definita da $*$ in S^X . È facilissimo verificare che, se $*$ è associativa, o commutativa, $*^X$ ha la stessa proprietà che se $t \in S$ è elemento neutro per $*$ l'applicazione costante t (in S^X) è neutra rispetto a $*^X$, inoltre, se $(S, *)$ è un gruppo anche $(S^X, *^X)$ lo è: il simmetrico di un'applicazione $f \in S^X$ sarà l'applicazione

che ad ogni $x \in X$ associa il simmetrico di x^f rispetto a $*$:

$$f^{-1}: x \in X \mapsto (x^f)^{-1} \in S,$$

usando $^{-1}$ per indicare simmetrici. Abitualmente si indica l'operazione puntuale $*^X$ con lo stesso simbolo usato per indicare l'operazione $*$.

Sia ora $(A, +, -, 0_A)$ un gruppo abeliano. Nell'insieme A^A delle applicazioni da A ad A sono definite due applicazioni associative: l'addizione puntuale (cioè l'operazione puntuale definita dall'addizione $+$ del gruppo), che indichiamo ancora con $+$, e il prodotto operativo (o composizione) tra applicazioni. L'insieme $\text{End}(A, +)$ degli endomorfismi del gruppo A è chiuso rispetto ad entrambe le operazioni, e le operazioni indotte lo strutturano come anello unitario:

Proposizione 1.2. *Con le notazioni appena fissate, $\text{End}(A, +)$, munito dell'operazione di addizione puntuale e quella di composizione tra applicazioni, è un anello unitario, il cui zero è l'endomorfismo nullo (l'applicazione costante 0_A) e la cui unità è l'applicazione identica id_A di A .*

La dimostrazione di queste affermazioni (inclusa quella che precede la proposizione) è lasciata per esercizio. Va notato che se il gruppo $(A, +)$ non è abeliano non è più vero che $\text{End}(A, +)$ è chiusa rispetto all'addizione puntuale; ad esempio $\text{id}_A + \text{id}_A$ non è più un endomorfismo di A . A questo proposito, si veda l'Esercizio 1.B.2.

Esempi, osservazioni, esercizi.

1.B.1. Le operazioni puntuali non sono ovviamente nulla di particolarmente nuovo: quando in analisi, ad esempio, si sommano o moltiplicano tra loro funzioni reali, si stanno utilizzando operazioni puntuali definite dalle operazioni di addizione o di moltiplicazione tra numeri reali.

1.B.2. Sia $(A, +)$ un gruppo, non necessariamente abeliano, e siano α e β suoi endomorfismi. Verificare che l'applicazione somma puntuale $\alpha + \beta$ è un endomorfismo di A se e solo se le immagini in α e in β di α e β si centralizzano (cioè: $a^\alpha + b^\beta = b^\beta + a^\alpha$ per ogni $a, b \in A$). Di conseguenza: $\text{id}_A + \text{id}_A$ è un endomorfismo di A se e solo se A è abeliano.

1.B.3. L'anello degli endomorfismi di un gruppo ciclico infinito (rispettivamente, ciclico di ordine m) è isomorfo all'anello \mathbb{Z} degli interi (rispettivamente, all'anello \mathbb{Z}_m degli interi modulo m). Questo non è difficile da provare: se $(A, +)$ è ciclico infinito, per ogni $n \in \mathbb{Z}$ l'applicazione $\varepsilon_n: a \in A \mapsto na \in A$ è un endomorfismo di A e si può verificare (chi legge è incoraggiato a farlo) che l'applicazione $n \in \mathbb{Z} \mapsto \varepsilon_n \in \text{End}(A, +)$ è un isomorfismo di anelli (unitari); similmente si ragiona nel caso $|A| = m$. Ed analogo è anche il caso del gruppo additivo razionale $(\mathbb{Q}, +)$: l'applicazione che ad ogni numero razionale r associa l'endomorfismo di $(\mathbb{Q}, +)$ definito da $q \mapsto qr$ per ogni $q \in \mathbb{Q}$ è un isomorfismo dal campo dei numeri razionali a $\text{End}(\mathbb{Q}, +)$. Per chi ha familiarità con questa terminologia: l'anello degli endomorfismi di un gruppo localmente ciclico è sempre commutativo.

Nonostante questi esempi, in generale l'anello degli endomorfismi di un gruppo abeliano non è un anello commutativo. Ad esempio, l'anello degli endomorfismi del gruppo di Klein V_4 (il gruppo non ciclico di ordine 4) è isomorfo all'anello delle matrici 2×2 sul campo \mathbb{Z}_2 , che ovviamente non è commutativo.

1.B.4. Alcuni degli esempi forniti al punto precedente sono gruppi abeliani il cui anello degli endomorfismi è un campo. In effetti un classico esercizio consiste nel provare che, se A è un gruppo abeliano, l'anello degli endomorfismi di A è un corpo se e solo se A è ciclico di ordine primo oppure $A \simeq (\mathbb{Q}, +)$; in questi casi $\text{End } A$ è un campo primo, cioè un campo privo di sottocampi propri, ovvero o di ordine primo o isomorfo al campo razionale.

1.2 Moduli e premoduli

La nozione di modulo su un anello è l'ovvia estensione agli anelli unitari di quella di spazio vettoriale su un corpo ed ha un ruolo centrale in diversi ambiti della matematica, a cominciare dall'algebra (commutativa e non). Oltre a questa, definiamo qui una nozione più generale, quella di premodulo, riferita ad anelli non necessariamente unitari.

Sia $(R, +, \cdot)$ un anello commutativo.² Chiamiamo *premodulo* su R , o R -premodulo, una coppia ordinata $((M, \dot{+}), \zeta)$, dove $(M, \dot{+})$ è un gruppo abeliano e ζ è un omomorfismo di anelli da R a $\text{End}(M, \dot{+})$. Se, inoltre, R è unitario e ζ è un omomorfismo di anelli unitari $((M, \dot{+}), \zeta)$ è, per definizione, un *modulo* su R , o un R -modulo.

In questi contesti faremo riferimento a ζ come all'*azione di premodulo*, (o di modulo), di R su M . Spesso si dice semplicemente che M è un (pre)modulo su R ,³ sottintendendo il riferimento a ζ .

Un'azione di (pre)modulo ζ , come appena introdotta, permette di definire un'operazione esterna di R su M , cioè un'applicazione $M \times R \rightarrow M$ in questo modo:

$$\cdot : (a, r) \in M \times R \longmapsto a^{r^\zeta} \in M.$$

Come di consueto con le operazioni, si preferisce usare la notazione infissa per indicare l'immagine di una coppia e scrivere quindi $a \cdot r$ per a^{r^ζ} . L'operazione esterna \cdot verifica queste proprietà:

$$\begin{aligned} \forall a, b \in M \forall r, s \in R \\ (\mathcal{M}_1) : (a \dot{+} b) \cdot r &= a \cdot r \dot{+} b \cdot r \\ (\mathcal{M}_2) : a \cdot (r + s) &= a \cdot r \dot{+} a \cdot s \\ (\mathcal{M}_3) : a \cdot (rs) &= (a \cdot r) \cdot s \end{aligned}$$

e, se R è unitario e ζ è un'azione di modulo,

$$(\mathcal{M}_4) : a \cdot 1_R = a.$$

Infatti, (\mathcal{M}_1) equivale a $(a \dot{+} b)^{r^\zeta} = a^{r^\zeta} \dot{+} b^{r^\zeta}$, quindi il fatto che essa valga per ogni scelta di a e b equivale a dire che r^ζ sia un endomorfismo di $(M, \dot{+})$; (\mathcal{M}_2) equivale a $a^{(r+s)^\zeta} = a^{r^\zeta} \dot{+} a^{s^\zeta} = a^{r^\zeta+s^\zeta}$, quindi il fatto che essa valga per ogni scelta di $a \in M$ equivale a $(r+s)^\zeta = r^\zeta + s^\zeta$, la cui validità per ogni $r, s \in R$ esprime precisamente il fatto che ζ è un omomorfismo additivo. Allo stesso modo (\mathcal{M}_3) esprime il fatto che $(rs)^\zeta = r^\zeta s^\zeta$ per ogni $r, s \in R$, cioè: ζ è un omomorfismo moltiplicativo (dunque, (\mathcal{M}_2) e (\mathcal{M}_3) , considerate insieme, equivalgono alla richiesta che ζ sia un omomorfismo di anelli). Infine (\mathcal{M}_4) equivale a $a^{(1_R)^\zeta} = a$ per ogni $a \in M$, ovvero $(1_R)^\zeta = \text{id}_M$, dunque (\mathcal{M}_4) , in aggiunta a (\mathcal{M}_2) e (\mathcal{M}_3) , equivale all'essere ζ un omomorfismo di anelli *unitari*.

Queste osservazioni mostrano non solo che ogni azione di premodulo ζ determina un'operazione esterna $\cdot = \cdot_\zeta$ che verifica le $(\mathcal{M}_{1,2,3})$ (e anche la (\mathcal{M}_4) se ζ è un'azione di modulo) ma anche che, viceversa, se $\cdot : M \times R \rightarrow M$ è un'operazione esterna che verifica le $(\mathcal{M}_{1,2,3})$, per ogni $r \in R$ l'applicazione $r_\cdot : a \in M \mapsto a \cdot r \in M$ è un endomorfismo di $(M, \dot{+})$ e l'applicazione $\zeta_\cdot : r \in R \mapsto r_\cdot \in \text{End}(M, \dot{+})$ è un omomorfismo di anelli, cioè un'azione di premodulo, che è un'azione di modulo se \cdot verifica anche (\mathcal{M}_4) . È inoltre piuttosto evidente che i passaggi appena

² L'unica ragione per la quale assumiamo l'ipotesi di commutatività solo perché l'argomento di questo corso è limitato alle strutture commutative. Le nozioni di modulo e premodulo che diamo qui si definiscono, senza alcuna modifica, anche per anelli non commutativi.

³ d'ora in avanti useremo spesso espressioni come '(pre)modulo', 'sotto(pre)modulo' o simili per definire concetti o enunciare proprietà che siano riferiti simultaneamente e in modo parallelo a moduli e a premoduli. Ovviamente, scrivendo di un '(pre)modulo M sull'anello commutativo R ' conveniamo anche che se M è inteso come modulo l'anello R sia implicitamente assunto anche unitario.

descritti da un'azione ad un'operazione esterna e viceversa sono l'uno inverso dell'altro (vale a dire: $\zeta \cdot_\bullet = \zeta \cdot \bullet_\zeta = \bullet$ per ogni scelta di ζ e di \bullet). Abbiamo così provato:

Proposizione 1.3. *Siano R un anello commutativo e M un gruppo abeliano. Allora l'applicazione che ad ogni azione di premodulo ζ di R su M associa $\bullet: (a, r) \in M \times R \mapsto a^{r^\zeta} \in M$ è una biezione dall'insieme di tutte le azioni di premodulo di R su M all'insieme delle operazioni esterne $M \times R \rightarrow M$ per le quali sono verificate le condizioni in $(\mathcal{M}_{1,2,3})$.*

Inoltre, se R è anche unitario, la stessa applicazione induce una biezione dall'insieme di tutte le azioni di modulo di R su M all'insieme delle operazioni esterne $M \times R \rightarrow M$ per le quali sono verificate le condizioni in $(\mathcal{M}_{1,2,3,4})$.

Tutto ciò significa che abbiamo a disposizione due modi equivalenti di definire un (pre)modulo su un anello commutativo unitario: specificando l'azione di (pre)modulo, in accordo con la definizione data all'inizio di questa sezione, oppure specificando un'operazione esterna che verifichi le $(\mathcal{M}_{1,2,3})$ (nel caso dei premoduli) o le $(\mathcal{M}_{1,2,3,4})$ (nel caso dei moduli).

Abbiamo usato i simboli $+$ e \bullet per indicare le operazioni interna ed esterna del (pre)modulo M per ragioni di chiarezza espositiva, cioè per evitare di confondere queste operazioni con quelle dell'anello R nell'espressione, ad esempio, delle $(\mathcal{M}_{1,2,3,4})$. Di regola, d'ora in avanti, non faremo più distinzioni notazionali del genere e useremo (con ovvio abuso) $+$ e \cdot per indicare anche le operazioni, interna ed esterna, dei (pre)moduli.

Prendiamo nota di alcune regole di calcolo che valgono in ogni premodulo, quindi in ogni modulo.

Lemma 1.4. *Sia M un premodulo sull'anello commutativo R . Allora, per ogni $a, b \in M$ e $r \in R$ si ha:*

- (i) $a0_R = 0_M r = 0_M$;
- (ii) $-(ar) = (-a)r = a(-r)$;
- (iii) $(a - b)r = ar - br$.

Se R è unitario e M è un R -modulo, $-a = a(-1_R)$ per ogni $a \in M$.

Dimostrazione. La verifica è elementare. Se ζ è l'azione di R su M , allora 0_R^ζ è l'endomorfismo nullo di M e, per ogni $r \in R$, r^ζ , essendo un endomorfismo di M , manda 0_M in 0_M . Questo giustifica (i). In modo simile si può procedere per (ii) e (iii). L'osservazione finale segue da (ii). \square

1.2.1 Alcuni esempi fondamentali

Spazi vettoriali Se R è un campo, le condizioni (\mathcal{M}_{1-4}) rendono evidente che i moduli su R non sono altro che gli spazi vettoriali su R . Quindi, come accennato all'inizio di questa sezione, la nozione di modulo generalizza quella di spazio vettoriale.

Gruppi abeliani D'altra parte, la nozione di modulo generalizza anche quella di gruppo abeliano. Infatti, se $(A, +)$ è un gruppo abeliano, si verifica subito che l'operazione esterna $(a, n) \in A \times \mathbb{Z} \mapsto na \in A$ verifica le (\mathcal{M}_{1-4}) ; qui na è il consueto multiplo di a per l'intero n , come viene definito nei corsi elementari di algebra. Dunque, $(A, +)$ si può riguardare come \mathbb{Z} -modulo. L'azione di questo modulo è l'omomorfismo $n \in \mathbb{Z} \mapsto \varepsilon_n \in \text{End}(A)$, dove $\varepsilon_n: a \in A \mapsto na \in A$. Ora, è molto facile verificare che questo è l'unico omomorfismo di anello unitari da \mathbb{Z} a $\text{End}(A)$;⁴ possiamo dunque concludere che *ogni gruppo abeliano si può riguardare come modulo sull'anello*

⁴ per ogni anello unitario R , esiste uno ed un solo omomorfismo di anelli unitari $\mathbb{Z} \rightarrow R$, quello definito da $n \mapsto n1_R$ per ogni $n \in \mathbb{Z}$; questo è un facile esercizio. In termini categoriali, questo fatto si esprime dicendo che l'anello degli interi è un oggetto iniziale nella categoria degli anelli unitari.

degli interi in uno ed un solo modo. In effetti, in un senso che si può rendere preciso, la teoria dei gruppi abeliani si può identificare con la teoria dei moduli su \mathbb{Z} .

Aggiungiamo anche che, qualunque sia l'anello commutativo R , l'applicazione costante $\zeta_0: R \rightarrow \text{End } A$ che ad ogni $r \in R$ associa l'endomorfismo nullo di A è un omomorfismo di anelli, che struttura così A come R -premodulo. Ad eccezione del caso in cui A sia il gruppo identico, questo non è un R -modulo, perché ζ_0 non è un omomorfismo di anelli unitari se $|A| > 1$. In questo premodulo l'operazione esterna è la costante zero.

R_R Un altro esempio importante: ogni anello commutativo $(R, +, \cdot)$ si può riguardare come premodulo su sé stesso utilizzando la sua moltiplicazione interna \cdot come operazione esterna e l'operazione $+$ di addizione di R anche come operazione interna di addizione del premodulo. Questo premodulo viene spesso indicato come R_R . Dunque, $(R_R, +) = (R, +)$ e l'azione di premodulo che definisce R_R è l'omomorfismo che ad ogni $r \in R$ associa l'endomorfismo $a \mapsto ar$ di $(R, +)$. Se R è, in aggiunta, unitario, R_R è un modulo su R .

1.2.2 Omomorfismi, sotto(pre)moduli

Sia R un anello commutativo e siano A e B premoduli su R . Un omomorfismo (di R -premoduli, o R -omomorfismo, o applicazione R -lineare) da A a B è un'applicazione $\varphi: A \rightarrow B$ che sia un omomorfismo di gruppi e verifichi $(ar)^\varphi = a^\varphi r$ per ogni $a \in A$ ed $r \in R$. Nel caso in cui R sia anche unitario e A e B siano moduli su R , un tale φ si chiama anche, come è ovvio che sia, un omomorfismo di R -moduli. Notiamo che, in entrambi i casi, la condizione richiesta su φ è che esso 'conservi' l'operazione interna ed anche, per ogni $r \in R$, l'operazione unaria di moltiplicazione per r (si veda a questo proposito l'Osservazione 1.C.2). Se $\alpha: R \rightarrow \text{End } A$ e $\beta: R \rightarrow \text{End } B$ sono le azioni che descrivono come R -moduli o R -premoduli A e B , la seconda condizione si può riscrivere anche come: $(\forall a \in A \forall r \in R)(a^{r^\alpha} \varphi = a^\varphi r^\beta)$, ovvero $(\forall r \in R)(r^\alpha \varphi = \varphi r^\beta)$. Dunque, un omomorfismo di gruppi $\varphi: A \rightarrow B$ è un omomorfismo di R -(pre)moduli se e solo se, per ogni $r \in R$ è commutativo il diagramma

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ r^\alpha \downarrow & & \downarrow r^\beta \\ A & \xrightarrow{\varphi} & B. \end{array}$$

I prefissi mono-, epi-, iso-, endo-, auto- riferiti a (omo)morfismi di moduli o premoduli hanno il significato consueto.

Definiti gli omomorfismi, passiamo a definire le sottostrutture. Sia M un R -premodulo. Un *sottopremodulo* (o R -sottopremodulo) di M è un sottogruppo N di M (rispetto, ovviamente, all'operazione interna di M) che sia chiusa rispetto alla moltiplicazione per elementi di R . Se (R è unitario e) M è un R -modulo, i suoi sottopremoduli si chiamano anche *sottomoduli*. Dunque, una parte non vuota N di M ne costituisce un sotto(pre)modulo se e solo se, per ogni $a, b \in N$ e $r \in R$ si ha $a - b \in N$ e $ar \in N$. Per indicare che N è un R -sotto(pre)modulo di M useremo spesso la notazione $N \leq_R M$, o talvolta più semplicemente $N \leq M$, se il riferimento a R può essere omesso senza rischi di ambiguità.⁵ È appena il caso di notare che i sottogruppi banali $\{0_M\}$, usualmente scritto come 0 , e M sono sotto(pre)moduli di M e si chiamano in questo contesto sotto(pre)moduli banali, e che utilizziamo simboli come $< M$ e $<_R M$ per indicare sotto(pre)moduli propri (cioè diversi da M).

⁵ Quanto alla possibile confusione con la nozione di sottogruppo, in genere scriveremo $H \leq_{\mathbb{Z}} M$ per indicare che H è un sottogruppo del gruppo additivo di M . La ragione dietro questa notazione è il fatto che, come già visto, M ha una ed una sola struttura di \mathbb{Z} -modulo e (vedi Esempio 1.C.4) gli \mathbb{Z} -sottomoduli di M sono tutti e soli i suoi sottogruppi.

Nel caso dei moduli (ma non in quello dei premoduli; vedi [Esempio 1.C.3](#)), la verifica della proprietà di essere un sottomodulo può essere resa più diretta da questa semplice osservazione:

Lemma 1.5. *Sia M un modulo su un anello commutativo unitario R e sia $\emptyset \neq N \subseteq M$. Allora $N \leq_R M$ se e solo se, per ogni $a, b \in N$ e $r \in R$ si ha $a + b \in N$ e $ar \in N$.*

Dimostrazione. Se la condizione data è soddisfatta, per ogni $a \in N$ si ha $-a = a(-1_R) \in N$, dunque N è un sottogruppo e quindi anche un sottomodulo di M . \square

Infine, notiamo che, come chi legge non avrà difficoltà a verificare, se R è un anello commutativo e $f: A \rightarrow B$ un omomorfismo di R -(pre)moduli, l'immagine mediante f di ogni sotto(pre)modulo di A è un sotto(pre)modulo di B e l'antiimmagine mediante f di ogni sotto(pre)modulo di B è un sotto(pre)modulo di A .

Osservazioni ed esempi.

1.C.1. Si avverte chi legge che il termine ‘premodulo’ qui introdotto non è affatto di uso comune. Nella letteratura matematica corrente viene quasi sempre usato il termine ‘modulo’ nell’accezione utilizzata in queste note; i pochi autori che introducono quelli che qui abbiamo chiamato premoduli chiamano questi moduli e chiamano invece ‘moduli unitari’ quelli che noi abbiamo chiamato moduli.

Vedremo [più avanti](#) che ogni premodulo su un anello commutativo si può anche riguardare come modulo su un (altro) anello commutativo unitario, quindi in qualche senso la nozione di premodulo si potrebbe ridurre a quella di modulo.

1.C.2. Dal punto di vista dell'algebra universale, le definizioni di sotto(pre)modulo e di omomorfismo di (pre)moduli trovano piena giustificazione nel fatto che, se $\zeta: R \rightarrow \text{End}(M, +)$ è un'azione di (pre)modulo, si riguarda l' R -(pre)modulo M come una struttura algebrica la cui segnatura comprenda i simboli $+$, $-$ e 0_M per le operazioni (binaria, unaria, nullaria) che qualificano M come gruppo e, per ogni $r \in R$, l'endomorfismo r^ζ visto come operazione unaria. Dunque, in accordo con le definizioni generali, i sotto(pre)moduli di M sono costituiti dalle parti non vuote che siano chiuse rispetto a tutte queste operazioni e gli omomorfismi di R -(pre)moduli non sono altro che le applicazioni tra sostegni di R -(pre)moduli che conservino tutte le operazioni elencate.

Il fatto che valga per il [Lemma 1.5](#) dipende da una ridondanza in questa descrizione nel caso dei moduli: l'operazione unaria $(-1_R)^\zeta$ coincide con l'operazione $-$ di selezione dell'opposto.

1.C.3. Come già visto, se R è un anello commutativo e A è un gruppo abeliano, si può riguardare A come R -premodulo con prodotto esterno costante zero: $ar = 0_A$ per ogni $a \in A$ e $r \in R$. In questo premodulo i sottopremoduli sono precisamente i sottogruppi di A .

Questo esempio mostra, tra l'altro, perché l'analogo del [Lemma 1.5](#) non vale per i premoduli. Se A ha un sottomonoide B (quindi B è una parte chiusa rispetto all'operazione binaria di A e $0_A \in B$) che non sia un sottogruppo (ad esempio: $A = (\mathbb{Z}, +)$ e $B = \mathbb{N}$), allora B è chiuso rispetto alla moltiplicazione per elementi di R ed all'operazione in A , ma non è un sottopremodulo.

1.C.4. Se A è un gruppo abeliano, dunque uno \mathbb{Z} -modulo, ogni sottogruppo di A è chiuso rispetto alla moltiplicazione per arbitrari interi, quindi gli \mathbb{Z} -sottomoduli di A sono tutti e soli i suoi sottogruppi. Similmente, è facilissimo verificare che un'applicazione tra gruppi abeliani è un omomorfismo di \mathbb{Z} -moduli se e solo se è un omomorfismo di gruppi.

1.C.5. Allo stesso modo, se R è un campo le nozioni di R -omomorfismo e di R -sottomodulo coincidono con quelle di applicazione R -lineare e di sottospazio vettoriale incontrate nei corsi di geometria.

1.C.6. Se R è un anello commutativo, gli R -sotto(pre)moduli di R_R sono tutti e soli gli ideali di R .

È bene prendere nota del fatto che, per un'applicazione $\varphi: R \rightarrow R$ le proprietà di essere un endomorfismo (di R -premoduli) di R_R , quella di essere un endomorfismo di anelli, o di anelli unitari di R sono diverse tra loro. Perché φ sia un endomorfismo, in ciascuno di questi sensi, è richiesto che φ sia un endomorfismo del gruppo additivo di R , cioè che conservi l'addizione, ma perché φ sia un endomorfismo di R -moduli serve che valga $(rs)^\varphi = r^\varphi s$ per ogni $r, s \in R$; perché φ sia un endomorfismo di anelli questa condizione va rimpiazzata con $(rs)^\varphi = r^\varphi s^\varphi$ per ogni $r, s \in R$, con l'aggiunta di $(1_R)^\varphi = 1_R$ se si vuole che φ sia un endomorfismo di anelli unitari. Ad esempio, per ogni $a \in R$ l'applicazione $\lambda_a: r \in R \mapsto ar \in R$ è un endomorfismo di R_R , ma è un endomorfismo dell'anello R se e solo se $a^2 = a$, ed è un endomorfismo di anelli unitari se e solo se $a = 1_R$. Invece, per ogni primo p , se R è un dominio di integrità unitario di caratteristica p che non sia un campo di ordine p , l'applicazione $r \in R \mapsto r^p \in R$ è un endomorfismo di anelli unitari, ma non è un endomorfismo di R_R . Verificarlo.

1.2.3 Prodotti e somme tra parti; sotto(pre)moduli generati

È ovvio che l'intersezione di un insieme non vuoto di sotto(pre)moduli di un (pre)modulo è ancora un sotto(pre)modulo. Da questo segue che se M è un (pre)modulo su un anello commutativo R e $X \subseteq M$, allora $\bigcap \{N \leq_R M \mid X \subseteq N\}$ è il minimo (rispetto all'inclusione) sotto(pre)modulo di M contenente X , vale a dire il *sotto(pre)modulo di M generato da X* . Per descriverlo in modo più esplicito, introduciamo la nozione di *prodotto tra una parte del (pre)modulo M ed una dell'anello R* .

Siano dunque M un (pre)modulo sull'anello commutativo R , $X \subseteq M$ e $S \subseteq R$. Il prodotto XS è, per definizione, il sottomonoido di M generato dall'insieme dei suoi elementi della forma xs al variare di $x \in X$ e $s \in S$. In modo più esplicito:

$$XS = \left\{ \sum_{i=1}^n x_i s_i \mid n \in \mathbb{N} \wedge \forall i \in \{1, 2, \dots, n\} (x_i \in X \wedge s_i \in S) \right\}.$$

Si noti che tra gli elementi di XS c'è anche 0_M , ottenuto come somma con zero addendi. Gli elementi di XS si possono descrivere come le *combinazioni lineari* di elementi di X a coefficienti in S . Come di consueto, nel caso in cui $X = \{x\}$ sia un singleton può capitare di scrivere xR piuttosto che $\{x\}R$. Si verifica subito che in questo caso il prodotto assume una forma più semplice: $xR = \{xr \mid r \in R\}$.

Lemma 1.6. Sia M un modulo sull'anello commutativo unitario R , e sia $X \subseteq M$. Allora il sottomodulo di M generato da X è XR .

Dimostrazione. È evidente che ogni sottomodulo di M contenente X contiene anche XR . Inoltre $X \subseteq XR$ (per ogni $x \in X$ si ha $x = x1_R \in XR$). Infine, XR è, per sua definizione, chiuso rispetto all'addizione in M ed è, evidentemente, anche chiuso rispetto alla moltiplicazione per elementi di R . Grazie al [Lemma 1.5](#) concludiamo dunque che $XR \leq_R M$. L'enunciato è ora ovvio. \square

Nel caso dei sottopremoduli il corrispondente enunciato è lievemente più complicato; si veda l'[Esercizio 1.D.3](#) o, più avanti, la [Proposizione 1.31](#).

Un caso importante di prodotto tra parti è quello in cui il premodulo a cui si applica la definizione è un anello commutativo R visto come premodulo su sé stesso, vale a dire R_R .

Abbiamo in questo caso una operazione binaria di prodotto tra parti di un anello, che vedremo avere grandissima utilità.

Altra operazione tra parti di un (pre)modulo è quella di addizione. Se n è un intero positivo e X_1, X_2, \dots, X_n sono parti del premodulo M , la loro somma è l'insieme di tutti gli elementi di M che si possano scrivere come somma di n elementi, presi uno in ciascuna delle parti X_i :

$$\sum_{i=1}^n X_i = \left\{ \sum_{i=1}^n x_i \mid \forall i \in \{1, 2, \dots, n\} (x_i \in X_i) \right\}.$$

Nel caso di famiglie infinite la definizione si estende in questo modo: se $(X_i)_{i \in I}$ è una arbitraria famiglia di parti di M , la somma $\sum_{i \in I} X_i$ di questa famiglia è l'insieme delle somme $\sum_{i \in I} x_i$ dove, per ogni $i \in I$, si ha $x_i \in X_i$ e l'insieme $\{i \in I \mid x_i \neq 0_M\}$ è finito (quest'ultima condizione serve a garantire che la somma sia ben definita). Si noti che $\sum_{i \in I} X_i$ è vuota se $\{i \in I \mid 0_M \notin X_i\}$ è infinito.

Lemma 1.7. *Sia $(A_i)_{i \in I}$ una famiglia non vuota di sotto(pre)moduli del (pre)modulo M sull'anello commutativo R . Allora il sotto(pre)modulo di M generato da questa famiglia⁶ è $\sum_{i \in I} A_i$.*

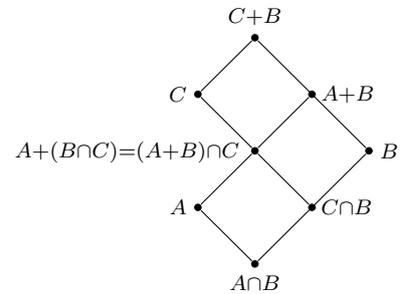
Dimostrazione. Poiché 0_M appartiene a ciascuno degli A_i , è chiaro che $S := \sum_{i \in I} A_i$ contiene $\bigcup \{A_i \mid i \in I\}$. Inoltre, come è evidente, $SR \subseteq S$. Da ciò segue facilmente l'asserto. \square

In particolare, il sotto(pre)modulo generato da due sotto(pre)moduli A e B di un (pre)modulo è la loro somma $A + B$.

Legge di Dedekind Questo semplice risultato si rivela spesso utile. È noto come *legge modulare di Dedekind*; il suo contenuto è illustrato dal diagramma di Hasse sulla destra.

Lemma 1.8. *Siano A, B e C sottopremoduli di uno stesso premodulo. Se $A \subseteq C$, allora $A + (B \cap C) = (A + B) \cap C$.*

Dimostrazione. Avendosi $A, B \leq A + B$, e $A, B \cap C \leq C$, si ha ovviamente $A + (B \cap C) \leq (A + B) \cap C$. Inversamente, sia $c \in (A + B) \cap C$, allora $c = a + b$ per opportuni $a \in A$ e $b \in B$. Poiché $A \subseteq C$, abbiamo anche $a \in C$ e quindi $b = c - a \in C$, dunque $c = a + b \in A + (B \cap C)$. \square



Corollario 1.9. *Siano A, B e C sottopremoduli di uno stesso premodulo e supponiamo $A \subseteq C$. Se $A \cap B = C \cap B$ e $A + B = C + B$, allora $A = C$.*

Dimostrazione. Dalle ipotesi e dal **Lemma 1.8** segue $A = A + (A \cap B) = A + (B \cap C) = (A + B) \cap C = (C + B) \cap C = C$. \square

⁶ cioè: il sotto(pre)modulo generato da $\bigcup \{A_i \mid i \in I\}$.

Esercizi.

1.D.1. Se M è un modulo su un anello commutativo unitario R , allora $MR = M$, perché $M = M1_R \subseteq MR \subseteq M$.

1.D.2. Siano R un anello commutativo, M un R -(pre)modulo, $X, Y \subseteq M$ e $S, T \subseteq R$. Provare:

- i) $(XS)T = X(ST)$
 - ii) $(X + Y)S \subseteq XS + YS$ e $X(S + T) \subseteq XS + ST$;
 - iii) se $0_M \in X \cap Y$, allora $(X + Y)S = XS + YS$; se $0_R \in S \cap T$, allora $X(S + T) = XS + ST$.
- Mostrare con un esempio che in (ii) possono non valere le uguaglianze.

1.D.3. Sia M un premodulo sull'anello commutativo R , e sia $X \subseteq M$. Provare:

- i) XR è un sottopremodulo di M ;
- ii) il sottopremodulo di M generato da X è $XR + \langle X \rangle$, dove $\langle X \rangle$ è il sottogruppo generato da X in $(M, +)$.

Si possono comparare questi enunciati, ed anche il [Lemma 1.6](#), ad una situazione probabilmente già incontrata nella teoria elementare degli anelli: se x è un elemento di un anello commutativo unitario R , l'ideale generato da x (cioè il sottomodulo di R_R generato da x , ovvero da $\{x\}$) è xR ; ma se R non è unitario l'ideale generato da x è $xR + \{nx \mid n \in \mathbb{Z}\}$.

1.D.4. Siano M ed N (pre)moduli di uno stesso anello commutativo R , e siano α e β R -omomorfismi da M a N . Mostrare che se M è generato da una sua parte X e α e β hanno la stessa restrizione a X , allora $\alpha = \beta$. (Suggerimento: $\alpha - \beta: a \in M \rightarrow a^\alpha - a^\beta \in N$ è un R -omomorfismo ed il suo nucleo contiene X . Ovviamente anche altre dimostrazioni sono possibili). Esprimere questo risultato in termini di iniettività di una opportuna 'applicazione restrizione'.

1.D.5. Vale per le altre strutture algebriche, ad esempio per gli anelli (ma anche per gli anelli unitari, per i gruppi non abeliani) un risultato simile a quello dell'esercizio precedente. Dimostrare quanto segue: siano R ed S anelli, e siano α e β omomorfismi di anelli da R a S . Mostrare che se R è generato (come anello) da una sua parte X e α e β hanno la stessa restrizione a X , allora $\alpha = \beta$. La dimostrazione suggerita per l'esercizio precedente va modificata, perché $\alpha - \beta$ non è, in generale, un omomorfismo di anelli. Convienne invece osservare che $\{r \in R \mid r^\alpha = r^\beta\}$ è comunque un sottoanello di R ...

1.2.4 Congruenze e quozienti, teoremi di omomorfismo e di corrispondenza

In accordo con le definizioni generali, una congruenza in un (pre)modulo M su un anello commutativo R è una relazione di equivalenza \sim in M che sia compatibile con le operazioni di M : quella di gruppo e le moltiplicazioni per elementi di R (si veda l'[Osservazione 1.C.2](#)); la richiesta è dunque che \sim sia una congruenza nel gruppo additivo $(M, +)$ di M e, per ogni $a, b \in M$ e $r \in R$, valga $a \sim b \Rightarrow ar \sim br$. Rimarchiamo il fatto che se M è un modulo le congruenze in M come modulo sono precisamente le congruenze in M visto come premodulo e quindi lo stesso vale per i quozienti di M .

Analogamente a quanto accade per i gruppi abeliani, le congruenze nei (pre)moduli sono descritte dai sotto(pre)moduli. Infatti, se \sim è una congruenza nell' R -premodulo M , allora \sim è una congruenza in $(M, +)$ e quindi esiste un sottogruppo H di $(M, +)$ tale che $a \sim b \iff a - b \in H$ per ogni $a, b \in M$ (naturalmente $H = [0_M]_\sim$) e si ha:

Proposizione 1.10. *Con le notazioni appena fissate, \sim è una congruenza nel (pre)modulo M se e solo se $H \leq_R M$.*

Dimostrazione. Sia \sim una congruenza in M . Allora, per ogni $h \in H$ e $r \in R$ abbiamo $h \sim 0_M$ e quindi $hr \sim 0_M r = 0_M$, che vuol dire: $hr \in H$. Dunque $H \leq_R M$. Viceversa, se $H \leq_R M$, per ogni $a, b \in H$ e $r \in R$, abbiamo

$$a \sim b \iff a - b \in H \implies ar - br = (a - b)r \in H \iff ar \sim br,$$

dunque \sim è una congruenza, come richiesto. \square

Sempre con le stesse notazioni, indicheremo come M/H il (pre)modulo quoziente M/\sim . I suoi elementi sono i laterali $a + H = \{a + h \mid h \in H\}$ ($= H + a$), al variare di a in M ; le regole di calcolo in M/H sono: $(a + H) + (b + H) = (a + b) + H$ e $(a + H)r = ar + H$ per ogni $a, b \in M$ e $r \in R$. L'epimorfismo canonico da M a M/H è l'epimorfismo $a \in M \mapsto a + H \in M/H$.

Valgono per i moduli e i premoduli, come per altre strutture algebriche, i teoremi di corrispondenza e di omomorfismo. Le dimostrazioni sono omesse; si ottengono riproducendo quelle già note, ad esempio, per i gruppi (o facendo riferimento a risultati più generali).

Teorema 1.11. *Siano R un anello commutativo e $\varphi: A \rightarrow B$ un omomorfismo di R -(pre)moduli. Allora:*

- (i) $\ker \varphi = \{a \in A \mid a^\varphi = 0_B\} \leq_R A$ e $\text{im } \varphi = \{a^\varphi \mid a \in A\} \leq_R B$;
- (ii) l'applicazione $a + \ker \varphi \in A/\ker \varphi \mapsto a^\varphi \in \text{im } \varphi$ è ben definita ed è un R -isomorfismo.

Teorema 1.12. *Sia M un (pre)modulo sull'anello commutativo R , e sia $N \leq_R M$. Indicati rispettivamente con $[M/N]$ e $\mathcal{L}(M/N)$ l'insieme dei sotto(pre)moduli di M contenenti N e l'insieme dei sotto(pre)moduli del quoziente M/N , l'applicazione $H \in [M/N] \mapsto H/N \in \mathcal{L}(M/N)$ è biettiva.*

Teorema 1.13. *Sia M un (pre)modulo su un anello commutativo R e siano $A, B \leq_R M$. Allora:*

- (i) l'applicazione $a + (A \cap B) \in A/(A \cap B) \mapsto a + B \in (A + B)/B$ è un R -isomorfismo;
- (ii) se $A \leq B$ l'applicazione $x + B \in M/B \mapsto (x + A) + (B/A) \in (M/A)/(B/A)$ è un R -isomorfismo.

1.2.5 Annullatori; moduli fedeli

Sia M un (pre)modulo sull'anello commutativo R e sia $\zeta: R \rightarrow \text{End}(M, +)$ l'azione che lo definisce. Il nucleo $\ker \zeta$ di ζ si chiama *annullatore* di M e si denota anche con $\text{Ann}_R(M)$. Si ha ovviamente

$$\text{Ann}_R(M) = \{r \in R \mid \forall a \in M (ar = 0_M)\},$$

il che suggerisce di estendere la definizione a parti arbitrarie di M : per ogni $X \subseteq M$,

$$\text{Ann}_R(X) = \{r \in R \mid \forall a \in X (ar = 0_M)\}.$$

In realtà anche questa seconda definizione si può ricondurre alla prima. Se infatti X è una parte di M , è facile verificare che l'annullatore di X coincide con l'annullatore del sotto(pre)modulo X^* di M generato da X (si veda l'[Esercizio 1.E.1](#)), cioè col nucleo dell'azione di (pre)modulo di R su X^* . Una conseguenza è che *per ogni $X \subseteq M$, $\text{Ann}_R(X)$ è un ideale di R .*

Come in situazioni analoghe, nel caso in cui $X = \{x\}$ sia un singleton, si scrive spesso $\text{Ann}_R(x)$ per $\text{Ann}_R(X)$.

Un R -(pre)modulo si dice *fedele* se e solo se il suo annullatore è l'ideale nullo $0 = \{0_R\}$ di R , cioè se e solo se l'azione che lo definisce è un monomorfismo di anelli. Sono esempi di moduli fedeli tutti gli spazi vettoriali non nulli e, per ogni anello commutativo unitario R , il modulo R_R .

Va notato, e dovrebbe risultare ovvio, che (pre)moduli isomorfi hanno lo stesso annullatore. Tornerà utile anche questo lemma:

Lemma 1.14. Sia R un anello commutativo e sia $H \triangleleft R$. Sia poi \bar{R} l' R -premodulo quoziente R_R/H . Allora $H \subseteq \text{Ann}_R(\bar{R})$. Se R è unitario e quindi \bar{R} è un R -modulo, si ha $H = \text{Ann}_R(\bar{R})$.

Dimostrazione. Ogni elemento \bar{r} di \bar{R} ha la forma $r + H$ per un opportuno $r \in R$. Per ogni $h \in H$ si ha $rh \in H$ e quindi $\bar{r}h = rh + H = H = 0_{\bar{R}}$. Dunque, $H \subseteq \text{Ann}_R(\bar{R})$. Se R è unitario e $a \in \text{Ann}_R(\bar{R})$, allora $(1_R + H)a = H$, ovvero $a + H = H$ e quindi $a \in H$. Dunque, in questo caso, $\text{Ann}_R(\bar{R}) = H$. \square

È in uso una notazione alternativa per gli annullatori in quozienti. Se R è un anello commutativo, M un R -premodulo, $N \leq_R M$ e $X \subseteq M$, si indica con $(N : X)$, o $(N : X)_R$, l'insieme degli $r \in R$ tali che $Xr \subseteq N$, cioè $\text{Ann}_R(\bar{X})$ dove $\bar{X} = \{x + N \mid x \in X\} \subseteq M/N$ è l'immagine di X mediante l'epimorfismo canonico $M \rightarrow M/N$ (scriveremo anche $X + N/N$ per \bar{X}). Naturalmente $(N : X)_R \triangleleft R$ e $\text{Ann}_R(X) = (0 : X)_R$. Come per altri annullatori, se $x \in M$ si scrive anche $(N : x)$ per $(N : \{x\})$. Le proprietà elencate nel prossimo lemma sono ovvie, la verifica è lasciata per esercizio:

Lemma 1.15. Siano R un anello commutativo ed M un R -(pre)modulo. Allora:

- (i) per ogni $X, Y \subseteq M$, se $X \subseteq Y$ allora $\text{Ann}_R(X) \supseteq \text{Ann}_R(Y)$;
- (ii) per ogni famiglia $(X_i)_{i \in I}$ di parti di M si ha $\text{Ann}_R(\bigcup_{i \in I} X_i) = \bigcap_{i \in I} \text{Ann}_R(X_i)$;
- (iii) per ogni famiglia $(N_i)_{i \in I}$ di sotto(pre)moduli di M ed ogni $X \subseteq M$, si ha $(\bigcap_{i \in I} N_i : X)_R = \bigcap_{i \in I} (N_i : X)_R$.

Esercizi ed esempi.

1.E.1. Provare in dettaglio il fatto che l'annullatore di una qualsiasi parte di un (pre)modulo coincide con l'annullatore del sotto(pre)modulo generato. Può essere utile fare riferimento all'[Esercizio 1.D.3](#).

1.E.2. Sia A un gruppo abeliano, che qui consideriamo come \mathbb{Z} -modulo. Se a è un elemento periodico di A , di periodo n , allora $\text{Ann}_{\mathbb{Z}}(a) = n\mathbb{Z}$; mentre $\text{Ann}_{\mathbb{Z}}(a)$ è l'ideale nullo di \mathbb{Z} se a è aperiodico. Inoltre, per chi conosce la terminologia: se A ha esponente finito n , allora $\text{Ann}_{\mathbb{Z}}(A) = n\mathbb{Z}$, altrimenti A è uno \mathbb{Z} -modulo fedele.

1.E.3. Provare che un anello commutativo unitario R è un campo se e solo se ogni R -modulo non nullo è fedele.

1.2.6 Cambio degli scalari

Sia, ancora una volta, M un (pre)modulo sull'anello commutativo R . Estendendo la terminologia in uso per gli spazi vettoriali, talvolta ci si riferisce ad R come all'anello degli scalari di M . Spesso si può riguardare M anche come (pre)modulo su un anello diverso da R ; è a questa situazione che si riferisce il titolo.

Sia $\zeta : R \rightarrow \text{End}(M, +)$ l'azione di (pre)modulo che definisce M . Se S è un anello commutativo e $\lambda : S \rightarrow R$ è un omomorfismo di anelli, allora $\lambda\zeta : S \rightarrow \text{End}(M, +)$ è un'azione di premodulo, che definisce dunque una struttura di S -premodulo su M . Inoltre, se M è non solo un premodulo ma un modulo (vale a dire: ζ è un omomorfismo di anelli unitari), S è un anello unitario e anche λ un omomorfismo di anelli unitari (ovvero: $(1_S)^\lambda = 1_R$), allora $\lambda\zeta$ è un'azione di modulo che definisce M come S -modulo. Si dice che l' S -(pre)modulo così ottenuto è quello definito dall' R -(pre)modulo M via λ .

In circostanze in cui vengano considerate simultaneamente diverse strutture di (pre)modulo su diversi anelli ma sullo stesso gruppo abeliano $(M, +)$, si usa differenziare i (pre)moduli indicando l'anello degli scalari a pedice.⁷ Ad esempio, nella situazione descritta sopra potremmo scrivere M_R per indicare il (pre)modulo M originario (quello definito da ζ) e M_S per quello definito da $\lambda\zeta$.

In termini espliciti, il prodotto esterno nel modulo M_S qui descritto è, come si verifica facilmente, quello dato da $as = as^\lambda$ per ogni $a \in M$ e $s \in S$, dove il prodotto a secondo membro è calcolato in M_R .

Un caso piuttosto frequente di cambio degli scalari via un omomorfismo λ , come appena discusso, è quello in cui S sia un sottoanello di R e λ sia l'immersione di S in R . In questo caso, per ogni $a \in M$ e $s \in S$, il prodotto as considerato in M_S coincide col prodotto omologo considerato in M_R ; per dirla in modo più sintetico l'operazione esterna $M \times S \rightarrow M$ di M_S è semplicemente la restrizione a $M \times S$ dell'operazione esterna $M \times R \rightarrow M$ di M_R . Naturalmente l'immersione di S in R è un omomorfismo di anelli unitari se e solo se S è un sottoanello unitario di R ; in questo caso certamente M_S sarà un S -modulo se M_R è un R -modulo.

Un altro utilissimo caso di cambio degli scalari si ottiene coinvolgendo l'annullatore del modulo considerato. Assumiamo che H sia un ideale di R contenuto in $\text{Ann}_R(M)$. Allora ζ , per il primo teorema di omomorfismo (per anelli), induce un omomorfismo (iniettivo) di anelli $\zeta': R/\text{Ann}_R(M) \rightarrow \text{End } M$ e questo si può comporre con l'epimorfismo naturale $r + H \in R/H \mapsto r + \text{Ann}_R(M) \in R/\text{Ann}_R(M)$ per ottenere un omomorfismo $\zeta^*: R/H \rightarrow \text{End } M$; questo diagramma è così commutativo (gli omomorfismi non specificati sono epimorfismi canonici):

$$\begin{array}{ccccc}
 & & R & & \\
 & \swarrow & \downarrow & \searrow & \\
 R/H & \xrightarrow{\quad} & R/\text{Ann}_R(M) & \xrightarrow{\zeta'} & \text{End } M \\
 & \searrow & \swarrow & \nearrow & \\
 & & & & \zeta^*
 \end{array}$$

Abbiamo così che M si può riguardare come premodulo su R/H con azione ζ^* . Inoltre, se R è unitario, $(1_{R/H})^{\zeta^*} = (1_R)^\zeta$, dunque ζ^* è un omomorfismo di anelli unitari se (e solo se) ζ lo è. Quindi, se ζ è un'azione di modulo su M , allora ζ^* definisce una struttura di R/H -modulo su M . In entrambi i casi chiameremo ζ^* l'azione indotta da ζ modulo H (o mod H , per evitare confusione).

L'operazione esterna del (pre)modulo $M_{R/H}$ così ottenuto è descritta in modo estremamente semplice da quella del (pre)modulo M_R da cui eravamo partiti: per ogni $r \in R$ e $a \in M$, si ha $a(r + H) = ar$. Una proprietà molto utile (ed altrettanto facile da verificare; si veda l'Esercizio 1.F.1) è questa:

Lemma 1.16. *Nelle notazioni del paragrafo precedente, i sotto(pre)moduli di $M_{R/H}$ sono tutti e soli i sotto(pre)moduli di M_R .*

È chiaro che, continuando con le stesse notazioni, $\text{Ann}_{R/H}(M_{R/H}) = \text{Ann}_R(M_R)/H$. Scegliendo dunque, come è certamente lecito, per H proprio l'ideale $\text{Ann}_R(M)$, il (pre)modulo $M_{R/H}$ ottenuto è un (pre)modulo fedele. Una conclusione è che per ogni (pre)modulo M esiste un (pre)modulo fedele ottenuto da M per cambio degli scalari che ha esattamente gli stessi sotto(pre)moduli di M (si veda anche, a questo proposito l'Osservazione 1.F.2).

⁷ Va da sé che anche questo artificio non risolve le ambiguità se appaiono nel discorso più azioni di (pre)modulo con lo stesso dominio.

Esempi, osservazioni, esercizi.

1.F.1. Supponiamo che ζ e η siano due azioni di (pre)modulo sullo stesso gruppo abeliano M , che definiscano così due strutture di (pre)modulo su di esso, chiamiamole M_ζ e M_η . Assumiamo $\text{im } \zeta = \text{im } \eta$. Allora, se N è una parte di M , si ha che N è un sottomodulo di M_ζ se e solo se è un sottomodulo di M_η ; dimostrarlo.

Detto in termini più informali: che un sottogruppo sia o meno un sotto(pre)modulo dipende esclusivamente dall'immagine dell'azione di (pre)modulo. Come applicazione questo risultato, si verifichi il [Lemma 1.16](#).

1.F.2. Se $\zeta: R \rightarrow \text{End } M$ è un'azione di (pre)modulo, che definisce il modulo M_R , posto $S = \text{im } \zeta$ è evidente che S è un anello commutativo (unitario se ζ è unitario) e l'immersione di S in $\text{End } M$ è un'azione di S -(pre)modulo *fedele* su M . In un certo senso questa costruzione inverte la prima delle costruzioni di cambio degli scalari qui presentate; infatti, come si verifica facilmente, M_R è il (pre)modulo definito dall' S -(pre)modulo M_S via la ridotta di ζ a S (cioè l'applicazione $r \in R \mapsto r^\zeta \in S$). L'esercizio precedente mostra anche che M_R e M_S hanno gli stessi sotto(pre)moduli; questo fornisce un'altra giustificazione di un'affermazione fatta nel testo.

1.F.3. Se $\lambda: S \rightarrow R$ è un omomorfismo di anelli (commutativi) e M_R è un R -(pre)modulo con azione $\zeta: R \rightarrow \text{End } M$, e se M_S è il (pre)modulo definito da M_R via λ , allora ogni sotto(pre)modulo di M_R è un sotto(pre)modulo di M_S , ma in generale non vale il viceversa. Ad esempio, consideriamo in caso in cui $R = \mathbb{Q}$, $M_R = \mathbb{Q}\mathbb{Q}$, $S = \mathbb{Z}$ e $\lambda: \mathbb{Z} \hookrightarrow \mathbb{Q}$ è l'immersione. Allora M_R è uno spazio vettoriale di dimensione 1, quindi un modulo semplice ed ha solo due sottomoduli (quelli banali), invece M_S ha come sottomoduli tutti i sottogruppi di $(\mathbb{Q}, +)$, che sono in numero infinito.

1.F.4. Un esempio importante di cambio degli scalari: siano p un numero primo (positivo) e $(A, +)$ un p -gruppo abeliano elementare (cioè un gruppo abeliano tale che $pa = 0_A$ per ogni $a \in A$). Allora possiamo riguardare A come \mathbb{Z} -modulo e abbiamo $\text{Ann}_{\mathbb{Z}}(A) = p\mathbb{Z}$ se $|A| > 1$; $\text{Ann}_{\mathbb{Z}}(A) = \mathbb{Z}$ se $|A| = 1$. Possiamo allora effettuare un cambio di scalari e riguardare A come modulo sul campo $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, cioè come \mathbb{Z}_p -spazio vettoriale.

1.F.5. Se M_R è un modulo su un anello commutativo unitario R e S è un sottoanello non unitario di R , l' S -premodulo definito da M_R via l'immersione di S in R non è sempre un modulo; ma in certi casi lo è. Vediamo un esempio: se X è un insieme, $R = \mathcal{P}(X)$ è l'anello delle parti di X , $Y \subset X$ e $S = \mathcal{P}(Y)$, allora S è un ideale proprio di R , vale a dire $S <_R R$, quindi S è un R -modulo. Come anello, S è unitario, ma S non è un sottoanello unitario di R . Ora, l' S -premodulo definito da S visto come R -modulo, non è altro che S_S , quindi è un S -modulo.

1.2.7 Premoduli finitamente generati

Una nozione molto importante è quella di (pre)modulo *finitamente generato*, cioè generato da una sua parte finita. Enunciamo qui per il caso dei (pre)moduli un lemma molto elementare che di fatto vale per ogni genere di struttura algebrica.

Lemma 1.17. *Sia M un (pre)modulo su un anello commutativo R , e sia \mathcal{C} una catena non vuota di sotto(pre)moduli di M . Allora*

- (i) $V := \bigcup \mathcal{C}$ è un sotto(pre)modulo di M ;
- (ii) se V è finitamente generato, $V = \max \mathcal{C}$.

Dimostrazione. Per ogni $a \in V$, fissiamo un $C_a \in \mathcal{C}$ tale che $a \in C_a$. Se X è un sottoinsieme finito non vuoto di V , poiché \mathcal{C} è una catena $C(X) := \bigcup \{C_a \mid a \in X\} \in \mathcal{C}$, quindi $C(X) \leq_R M$.

Da ciò segue subito che V è un sotto(pre)modulo di M , infatti $V \neq \emptyset$ e per ogni $a, b \in V$ e $r \in R$ si ha $a - b, ar \in C(\{a, b\}) \subseteq V$. Se poi V è generato da un insieme finito X , da $X \subseteq C(X) \subseteq V$ segue $V = C(X) \in \mathcal{C}$. \square

Come conseguenza del lemma precedente, verifichiamo una delle proprietà più importanti dei premoduli finitamente generati, quella di avere, se non nulli, sottopremoduli massimali. Per definizione, un sotto(pre)modulo massimale di un (pre)modulo M è un elemento massimale nell'insieme dei sotto(pre)moduli propri di M (ordinato per inclusione);⁸ in questo caso scriviamo $H <_R M$. Ad esempio, i sottopremoduli massimali di R_R sono gli ideali massimali di R —la nozione di ideale massimale dovrebbe essere già nota dai corsi elementari di algebra.

Corollario 1.18. *Sia M un (pre)modulo finitamente generato e non nullo su un anello commutativo R . Allora M ha almeno un sotto(pre)modulo massimale.*

Dimostrazione. Sia \mathcal{C} una catena non vuota di sotto(pre)moduli propri, e sia V la sua unione. Abbiamo $V \leq_R M$, per [Lemma 1.17](#). Se fosse $V = M$, allora V sarebbe finitamente generato e quindi, per lo stesso lemma, $M = V$ apparterebbe a \mathcal{C} , una contraddizione. Quindi $V <_R M$. Abbiamo mostrato che l'unione di ogni catena di sotto(pre)moduli propri di M è essa stessa un sotto(pre)modulo proprio. Pertanto l'insieme dei sotto(pre)moduli propri di M , ordinato per inclusione, è induttivo e quindi, per il lemma di Zorn, ha un elemento massimale, cioè un sotto(pre)modulo massimale di M . \square

Corollario 1.19. *Sia M un (pre)modulo finitamente generato su un anello commutativo R , e sia $N <_R M$. Allora M ha almeno un sotto(pre)modulo massimale contenente N .*

Dimostrazione. Per il corollario precedente, M/N ha un sotto(pre)modulo massimale \bar{L} (si sta qui usando il semplice [Esercizio 1.G.1](#)). Segue dal teorema di corrispondenza ([Teorema 1.12](#)) che $\bar{L} = L/N$ per un $L \leq_R M$ tale che $N \subseteq L$ e $L <_R M$. \square

Per questi due corollari è fondamentale l'ipotesi che il (pre)modulo M sia finitamente generato. Ad esempio, il gruppo additivo dei numeri razionali non ha sottogruppi massimali.

Chiudiamo con una curiosa conseguenza del [Lemma 1.17](#), che sarà utile più avanti.

Corollario 1.20. *Sia M un (pre)modulo; allora l'insieme dei sotto(pre)moduli di M non finitamente generati, ordinato per inclusione, è induttivo.*

Dimostrazione. Sia \mathcal{C} una catena non vuota costituita da sotto(pre)moduli non finitamente generati di M e sia $V = \bigcup \mathcal{C}$. Se V fosse finitamente generato si avrebbe $V \in \mathcal{C}$, per il [Lemma 1.17](#) e contro la scelta di \mathcal{C} ; quindi V non è finitamente generato. Ciò prova l'asserto. \square

⁸ nella terminologia a cui si fa cenno nella [sottosezione 2.2.1](#), i sotto(pre)moduli massimali di M sono i coatomi nel reticolo dei sotto(pre)moduli di M .

Esercizi.

1.G.1. Verificare che ogni quoziente di un (pre)modulo finitamente generato è finitamente generato.

1.G.2. In un insieme ordinato (S, \leq) un elemento x si dice compatto se e solo se, scelta comunque una parte X di S tale che $x = \sup X$, esiste un sottoinsieme finito F di X tale che $x = \sup F$. Verificare che nell'insieme dei sottopremoduli di un premodulo, ordinato per inclusione, i compatti sono precisamente i sottopremoduli finitamente generati.

1.G.3. Così come il [Lemma 1.17](#), anche il [Corollario 1.18](#) si estende a tantissimi altri tipi di strutture algebriche (ad esempio: ogni gruppo non identico che sia finitamente generato ha sottogruppi massimali). Nel caso che abbiamo considerato, quello dei (pre)moduli, il [Corollario 1.18](#) è una delle diverse forme di un risultato di grande rilevanza in algebra commutativa, noto come lemma di Nakayama, sul quale torneremo [più avanti](#).

1.G.4. Una caso particolare del [Corollario 1.18](#), almeno per anelli commutativi, è il teorema dell'ideale massimale di Krull, noto dai corsi di Algebra. Infatti se R è un anello commutativo unitario non nullo, il modulo R_R è finitamente generato (è generato da $\{1_R\}$) e quindi ha sottomoduli (ideali) massimali.

Il [Corollario 1.18](#) ed il teorema dell'ideale massimale di Krull dipendono dall'assioma di scelta, esplicitamente usato nella dimostrazione. In effetti è stato dimostrato (nel 1979, da Wilfrid Hodges) che nella teoria degli insiemi di Zermelo-Fraenkel, il teorema di Krull implica l'assioma di scelta; più precisamente, l'assioma di scelta equivale all'affermazione che ogni anello fattoriale abbia ideali massimali.

1.G.5. I due corollari [1.18](#) e [1.19](#) sono ovviamente equivalenti a priori (da [1.19](#) si deduce [1.18](#) ponendo $N = 0$) e sono stati enunciati entrambi solo per chiarezza. Un ulteriore versione dello stesso risultato si ottiene sostituendo, nel [Corollario 1.19](#) l'ipotesi che M sia finitamente generato con l'ipotesi che M sia generato da $N \cup X$ per un sua opportuna parte finita X ; verificarlo.

Come esercizio, si può modificare la dimostrazione del [Corollario 1.18](#) per ottenere direttamente da essa il [Corollario 1.19](#).

1.2.8 Moduli ciclici e premoduli semplici

Per definizione, un (pre)modulo M è *ciclico* se e solo se è generato da un singleton, cioè se e solo se esiste $a \in M$ tale che M sia il sotto(pre)modulo di sé stesso generato da a . Se M è un modulo, questo significa (come segue dal [Lemma 1.6](#) e dalle considerazioni che lo precedono) che $M = aR = \{ar \mid r \in R\}$.

Dunque, gli \mathbb{Z} -moduli ciclici sono niente altro che i gruppi ciclici, se R è un campo gli R -spazi vettoriali ciclici sono quelli di dimensione 0 o 1, per ogni anello commutativo unitario R , il modulo R_R è ciclico (generato da 1_R). È anche chiaro che tutti i quozienti di (pre)moduli ciclici sono a loro volta ciclici.

I moduli ciclici sono molto facili da caratterizzare, in modo strettamente analogo a quanto accade per i gruppi ciclici (si veda anche la [Proposizione 4.20](#)):

Proposizione 1.21. *Sia R un anello commutativo unitario e sia M un R -modulo. Allora M è ciclico se e solo se esiste $H \triangleleft R$ tale che $M \simeq_R R_R/H$. Se questo accade, allora $H = \text{Ann}_R(M)$.*

Dimostrazione. Dalle osservazioni precedenti segue che tutti i quozienti di R_R sono ciclici. Inoltre, come visto nel [Lemma 1.14](#), per ogni $H \triangleleft R$ si ha $H = \text{Ann}_R(R_R/H)$. Basta dunque provare che, se M è ciclico, allora M è isomorfo ad un quoziente di R_R . Sia dunque M ciclico. Sappiamo

che $M = aR$ per un opportuno $a \in M$, e quindi l'applicazione $\varphi: r \in R \mapsto ar \in M$ è suriettiva. È molto semplice verificare che φ è un R -omomorfismo, quindi $M = \text{im } \varphi \simeq R_R / \ker \varphi$. L'enunciato è così provato. \square

Corollario 1.22. *Sia R un anello commutativo unitario. Allora, a meno di isomorfismi, R_R è l'unico R -modulo ciclico fedele.*

La descrizione dei premoduli ciclici non è altrettanto immediata; a questo proposito si veda il [Corollario 1.32](#).

Un (pre)modulo M si dice poi *semplice* (o *irriducibile*) se e solo se non è nullo (cioè è diverso dal suo sotto(pre)modulo nullo 0) e non ha sotto(pre)moduli non banali. È ovvio che ogni (pre)modulo semplice M è ciclico: per ogni $a \in M \setminus 0$, se N è il sotto(pre)modulo di M generato da a si ha $0 < N \leq M$, quindi, essendo M semplice, $M = N$.

Introduciamo una notazione: $H \triangleleft R$ significa che H è un ideale massimale (cioè massimale tra gli ideali propri) dell'anello R , vale a dire: $H < R_R$.

Proposizione 1.23. *Sia R un anello commutativo e sia M un R -(pre)modulo. Allora M è semplice se e solo se vale una delle due:*

- (i) $MR = 0$ e M ha ordine primo;
- (ii) $MR \neq 0$ ed esiste $H \triangleleft R$ tale che $M \simeq_R R_R/H$. Se questo accade, allora $H = \text{Ann}_R(M)$. Se M è un modulo il caso (i) non si può verificare.

Dimostrazione. Sia $H \triangleleft R$; allora i sotto(pre)moduli di R_R/H sono tutti e soli i quozienti I/H al variare di I tra gli ideali di R contenenti H . Dunque, R_R/H è un R -(pre)modulo semplice se e solo se $H \triangleleft R$.

Se vale la (i), allora M non ha sottogruppi non banali, quindi è certamente semplice anche come R -(pre)modulo. Se vale la (ii), allora M è semplice per l'osservazione al paragrafo precedente.

Viceversa, supponiamo M semplice. Sia $N = \{a \in M \mid aR = 0\}$. Si verifica facilmente che $N \leq_R M$, dunque o $N = M$ oppure $N = 0$. Nel primo caso $MR = 0$. Se questo accade, ogni sottogruppo di M è un R -sottopremodulo, quindi il fatto che M sia semplice si traduce nel fatto che M non ha sottogruppi non banali, dunque $|M|$ è primo e vale la (i). Nel secondo caso, esiste $a \in M$ tale che $aR \neq 0$. Poiché $aR \leq_R M$ (vedi [Esercizio 1.D.3](#)) ed M è semplice, si ha dunque $aR = M$. Allora, come nella dimostrazione della [Proposizione 1.21](#), $\varphi: r \in R_R \mapsto ar \in M$ è un R -epimorfismo e quindi $M \simeq_R R_R/H$ dove $H = \ker \varphi$. Per quanto visto all'inizio di questa dimostrazione, $H \triangleleft R$. Abbiamo inoltre $\text{Ann}_R(M) \neq R$ e, per il [Lemma 1.14](#), anche $H \subseteq \text{Ann}_R(M)$. Concludiamo così che vale (ii).

Infine, se M è un modulo, e quindi R è unitario, si ha $MR = M \neq 0$ ([Osservazione 1.D.1](#)), quindi non è verificata la (i). \square

Esercizi.

1.H.1. Descrivere gli R -moduli semplici nel caso in cui R sia un campo e nel caso in cui $R = \mathbb{Z}$. Se R è un anello commutativo unitario, quando è che R_R è semplice?

1.H.2. Dimostrare che se R è un anello a prodotto costante nullo (cioè $RR = 0$) ed M è un R -premodulo semplice, allora $MR = 0$.

1.3 Algebre

Ancora più che per altre strutture qui descritte, esistono in letteratura molte, e molto diverse, versioni della nozione di algebra su un anello. Ci limitiamo qui, rinunciando alla massima generalità, a considerare solo algebre associative e commutative su anelli unitari.

Sia dunque R un anello commutativo unitario. Un'algebra (commutativa associativa; d'ora in avanti questo sarà sottinteso) A su R (o R -algebra) è un anello commutativo $(A, +, \cdot)$ che abbia anche una struttura di R -modulo in modo che, indicando con \cdot l'operazione esterna di questo modulo, per ogni $a, b \in A$ e $r \in R$ si abbia $a(b \cdot r) = (ab) \cdot r$. Ovvvia conseguenza di questa condizione e delle commutatività di A è che, con le stesse quantificazioni, $(a \cdot r)b = (ab) \cdot r$.⁹

L'algebra A si dice unitaria quando A è unitario come anello. Vediamo alcuni esempi.

- Così come ogni gruppo abeliano si può riguardare (equivalentemente) come modulo su \mathbb{Z} , ogni anello commutativo $(R, +, \cdot)$ si può riguardare come \mathbb{Z} -algebra, utilizzando l'unica possibile struttura di \mathbb{Z} -modulo su $(R, +)$.
- Se R è un anello commutativo unitario, R stesso e più in generale ogni quoziente R/H di R è una R -algebra unitaria; la struttura di modulo considerata è qui quella di R_R/H .
- Se R è un sottoanello unitario di un anello commutativo unitario A , è facile verificare che A si struttura come R -algebra unitaria, utilizzando come operazione esterna di modulo la restrizione a $A \times R$ della moltiplicazione interna di A .
- L'anello delle parti di un insieme S è un'algebra sul campo \mathbb{Z}_2 ; l'azione di modulo è, necessariamente, quella che alla classe $[0]_2$ associa l'endomorfismo nullo di $(\mathcal{P}(S), \Delta)$ e alla classe $[1]_2$ associa l'automorfismo identico (dunque, per ogni $X \in \mathcal{P}(S)$, $X[0]_2 = \emptyset$ e $X[1]_2 = X$).
- Ogni modulo M si può riguardare come algebra sul suo anello R degli scalari definendo su M , come operazione interna di moltiplicazione, l'applicazione $M \times M \rightarrow M$ costante 0_M ; dunque $ab = 0_M$ per ogni $a, b \in M$. La verifica del fatto che in questo modo M diventi effettivamente una R -algebra (non unitaria, a meno che $M = 0$) è un semplicissimo esercizio.

In un'algebra unitaria l'operazione esterna (di modulo) è completamente determinata dalla moltiplicazione interna (di anello) e dai prodotti (esterni) dell'unità per gli scalari. Infatti, se A è un'algebra unitaria sull'anello commutativo unitario R , per ogni $a \in A$ e $r \in R$ si ha

$$a \cdot r = (a1_A) \cdot r = a(1_A \cdot r).$$

Questo suggerisce di considerare l'applicazione $\xi: r \in R \mapsto 1_A \cdot r \in A$. Si verifica subito che ξ è un omomorfismo di anelli unitari: per ogni $r, s \in R$ si ha infatti $(r + s)^\xi = 1_A \cdot (r + s) = 1_A \cdot r + 1_A \cdot s = r^\xi + s^\xi$ e

$$r^\xi s^\xi = (1_A \cdot r)(1_A \cdot s) = ((1_A \cdot r)1_A) \cdot s = (1_A \cdot r) \cdot s = 1_A \cdot (rs) = (rs)^\xi;$$

infine $1_R^\xi = 1_A \cdot 1_R = 1_A$. Il semplice calcolo svolto sopra mostra che, per ogni $a \in A$ e $r \in R$, si ha $a \cdot r = a(1_A \cdot r) = ar^\xi$. Chiameremo ξ l'*omomorfismo di struttura* della R -algebra A . Osserviamo che $\ker \xi$ coincide con l'annullatore di A visto come R -modulo.

Viceversa, sia ξ un qualsiasi omomorfismo di anelli (commutativi) unitari $R \rightarrow A$. Possiamo definire un'operazione esterna $\cdot: A \times R \rightarrow A$ ponendo, per ogni $a \in A$ e $r \in R$,

$$a \cdot r = ar^\xi$$

ed è di verifica immediata il fatto che \cdot verifica le condizioni che la rendono operazione esterna di una struttura di R -modulo su A ; inoltre $a(b \cdot r) = abr^\xi = (ab) \cdot r$ per ogni $a, b \in A$ e $r \in R$,

⁹ Il simbolo \cdot viene spesso omissso, lo utilizzeremo esplicitamente solo quando ragioni di chiarezza espositiva consigliano di farlo.

quindi A risulta strutturato in questo modo come R -algebra unitaria. Poiché $1_A \cdot r = 1_A r^\xi = r^\xi$ per ogni $r \in R$, ξ è l'omomorfismo di struttura di quest'algebra.

In sintesi, abbiamo provato questo risultato:

Teorema 1.24. *Siano R e A anelli commutativi unitari, sia \mathcal{E} l'insieme delle operazioni esterne $A \times R \rightarrow A$ che strutturano A come R -algebra (unitaria) e \mathcal{H} l'insieme degli omomorfismi di anelli unitari da R a A . L'applicazione $\mathcal{E} \rightarrow \mathcal{H}$ che ad ogni operazione in \mathcal{E} associa l'omomorfismo di struttura dell'algebra definita da questa operazione, è biettiva.*

Dunque, si può specificare, in modo equivalente a quello suggerito dalla definizione, un'algebra unitaria descrivendo un omomorfismo di anelli unitari. Ad esempio, se R è un anello commutativo unitario e $H \triangleleft R$, la struttura di R -algebra unitaria per R/H vista sopra tra gli esempi più immediati è quella descritta dall'epimorfismo (di anelli unitari) canonico $R \twoheadrightarrow R/H$. Similmente, la struttura di \mathbb{Z} -algebra su R è data dall'unico omomorfismo di anelli unitari $\mathbb{Z} \rightarrow R$ (quello definito da $n \mapsto n1_R$). Se R ha caratteristica c , questo omomorfismo ha nucleo $c\mathbb{Z}$ e induce, via il primo teorema di omomorfismo, un omomorfismo $\mathbb{Z}_c \rightarrow R$ che struttura R come algebra su \mathbb{Z}_c . L'esempio dell'anello delle parti di un insieme S visto come algebra su \mathbb{Z}_2 , è un caso particolare di quest'ultima situazione, dato che, se $S \neq \emptyset$, questo anello ha caratteristica 2.

Vengono definite nel modo ovvio le nozioni di sottoalgebra e di omomorfismo di algebre. Così come un'algebra è un anello che è allo stesso tempo un modulo, una sottoalgebra (o una sottoalgebra unitaria) sarà un sottoanello (o una sottoanello unitario) che è allo stesso tempo un sottomodulo; un omomorfismo di algebre o di algebre unitarie (su un fissato anello) sarà un omomorfismo di anelli, o di anelli unitari, che è allo stesso tempo un omomorfismo di moduli.

Nel caso degli omomorfismi di algebre unitarie la nozione si può rappresentare in termini di diagrammi commutativi. Infatti:

Proposizione 1.25. *Sia R un anello commutativo unitario. Se A e B sono R -algebre unitarie con omomorfismi di struttura $\alpha: R \rightarrow A$ e $\beta: R \rightarrow B$, gli omomorfismi di R -algebre unitarie $A \rightarrow B$ sono tutti e soli gli omomorfismi di anelli unitari $\varphi: A \rightarrow B$ tali che $\alpha\varphi = \beta$.*

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ & \swarrow \alpha & \nearrow \beta \\ & R & \end{array}$$

Dimostrazione. φ è un omomorfismo di algebre unitarie se e solo se è un omomorfismo di anelli unitari ed allo stesso tempo di moduli. Sia φ un omomorfismo di anelli unitari. La condizione richiesta è dunque che, per ogni $a \in A$ e $r \in R$, si abbia $(ar)^\varphi = a^\varphi r$. Ora, $(ar)^\varphi = (ar^\alpha)^\varphi = a^\varphi r^{\alpha\varphi}$ e $a^\varphi r = a^\varphi r^\beta$, quindi la condizione si trasforma in $a^\varphi r^{\alpha\varphi} = a^\varphi r^\beta$ per ogni $a \in A$ e $r \in R$. Questa è certamente verificata se $\alpha\varphi = \beta$. Viceversa, se essa vale, applicandola per $a = 1_A$ otteniamo $\alpha\varphi = \beta$. L'asserto è così provato. \square

In un'algebra unitaria gli ideali sono sottoalgebre, ovviamente non unitarie se proprie; questo non è sempre vero per algebre non unitarie ([Esercizio 1.I.5](#)):

Proposizione 1.26. *Sia A un'algebra unitaria sull'anello commutativo unitario R . Allora ogni ideale di A è una R -sottoalgebra*

Dimostrazione. Sia $a \in H \triangleleft A$. Per ogni $r \in R$ si ha $a \cdot r = a(1_A \cdot r) \in H$. Da ciò segue che H è una R -sottoalgebra di A . \square

Esercizi.

1.I.1. La condizione $\forall a, b \in A (\forall r \in R (a(b \cdot r) = (ab) \cdot r))$ che appare nella definizione di A come R -algebra equivale a richiedere che, per ogni $a \in A$ l'applicazione $b \in A \mapsto ab \in A$ sia un endomorfismo di A visto come R -modulo nonché, in modo ancora equivalente, a richiedere che, per ogni $r \in R$ l'immagine di r nell'azione di modulo, cioè l'applicazione $b \in A \mapsto b \cdot r \in A$, sia un endomorfismo di A_A (cioè di A visto come premodulo su sé stesso).

1.I.2. Supponiamo che due anelli commutativi unitari A e B abbiano in comune un sottoanello unitario R . Allora A e B sono R -algebre unitarie, come visto tra gli esempi iniziali, con le immersioni $R \hookrightarrow A$ e $R \hookrightarrow B$ come omomorfismi di struttura. Come segue subito dalla [Proposizione 1.25](#), gli omomorfismi di R -algebre unitarie da A a B sono precisamente gli omomorfismi anelli da A a B che mandano in sé ogni elemento di R .

1.I.3. Sia K un sottocampo del campo F . Allora F è una K -algebra con l'immersione come omomorfismo di struttura. Chi conosce un po' di teoria di Galois può concludere, dall'osservazione precedente, che il gruppo di Galois dell'estensione F/K non è altro che il gruppo degli automorfismi di F riguardato come K -algebra.

1.I.4. Ragionando come nella dimostrazione della [Proposizione 1.25](#), mostrare quanto segue: se A e B sono algebre unitarie su un anello commutativo unitario R e $\varphi: A \rightarrow B$ è un omomorfismo di R -algebre, allora $(\text{im } \varphi)(1_B - 1_A^\varphi) = 0$. Questa osservazione generalizza il [Lemma 1.1](#).

1.I.5. Costruire un esempio di algebra (necessariamente non unitaria) con un ideale che non ne sia una sottoalgebra. Suggerimento: partire da un opportuno modulo e trasformarlo in un'algebra definendone la moltiplicazione interna come costante zero.

1.3.1 Immersione in un'algebra unitaria: accrescimento

L'importante costruzione che stiamo per effettuare permette di immergere ogni anello (commutativo, per i nostri fini, ma in realtà la stessa costruzione funziona anche per anelli non commutativi) in un anello unitario e più in generale, ogni algebra in un'algebra unitaria sullo stesso anello.

Siano R un anello commutativo unitario ed A una R -algebra, con operazione esterna \cdot . Nel prodotto cartesiano $A_1 := A \times R$ definiamo due operazioni (che, come le operazioni binarie in R e in A indichiamo, al solito, con $+$ e \cdot , omettendo spesso il secondo simbolo), ponendo, per ogni $a, b \in A$ e $r, s \in R$:

$$(a, r) + (b, s) = (a + b, r + s);$$

$$(a, r) \cdot (b, s) = (ab + a \cdot s + b \cdot r, rs).$$

Verifichiamo che A_1 , munito di queste due operazioni, costituisce un anello unitario: è chiaro che $(A_1, +)$ non è altro che la somma diretta esterna dei gruppi additivi di A e di R , quindi è un gruppo abeliano; è inoltre chiaro che \cdot è commutativa. Se $a, b, c \in A$ e $r, s, t \in R$, allora

$$\begin{aligned} ((a, r) \cdot (b, s)) \cdot (c, t) &= ((ab + a \cdot s + b \cdot r)c + (ab + a \cdot s + b \cdot r) \cdot t + c \cdot (rs), rst) \\ &= (abc + ac \cdot s + bc \cdot r + ab \cdot t + a \cdot (st) + b \cdot (rt) + c \cdot (rs), rst) \\ &= (a, r) \cdot ((b, s) \cdot (c, t)), \end{aligned}$$

inoltre

$$\begin{aligned} ((a, r) + (b, s)) \cdot (c, t) &= ((a + b)c + (a + b) \cdot t + c \cdot (r + s), (r + s)t) \\ &= (a, r) \cdot (c, t) + (b, s) \cdot (c, t), \end{aligned}$$

e

$$(a, r) \cdot (0_A, 1_R) = (a0_A + a \cdot 1_R + r \cdot 0_A, r) = (a, r),$$

quindi $(A_1, +, \cdot)$ è un anello commutativo unitario con zero $(0_A, 0_R)$ e unità $(0_A, 1_R)$. Ora, l'applicazione

$$\rho: r \in R \mapsto (0_A, r) \in A_1$$

è chiaramente un omomorfismo di anelli unitari, quindi definisce A_1 come R -algebra (unitaria); l'operazione esterna è così descritta: per ogni $a \in A$ e $r, s \in R$ si ha

$$(a, r)s = (a, r)s^\rho = (a, r) \cdot (0_A, s) = (a \cdot s, rs).$$

È ora di immediata verifica il fatto che

$$\mu: a \in A \mapsto (a, 0_R) \in A_1$$

è un monomorfismo di anelli ma anche di R -moduli, quindi di R -algebre. Inoltre, l'applicazione

$$\varepsilon: (a, r) \in A_1 \mapsto r \in R$$

è un omomorfismo (suriettivo) di R -algebre. Il suo nucleo è $\text{im } \mu = \{(a, 0_R) \mid a \in A\}$, che è così un ideale di A_1 .

Abbiamo così provato la parte principale di:

Teorema 1.27. *Siano R un anello commutativo unitario e A una R -algebra. Esiste allora una R -algebra unitaria A_1 tale che:*

- (i) $A \triangleleft A_1$; in particolare A è una R -sottoalgebra di A_1 ;
- (ii) l'omomorfismo di struttura ρ di A_1 è iniettivo, vale a dire: A_1 è fedele come R -modulo;
- (iii) posto $R_1 = \text{im } \rho$, il gruppo additivo di A_1 è somma diretta del gruppo additivo di A e di quello di R_1 ;
- (iv) A_1/A è isomorfo (come R -algebra) a R .

Dimostrazione. L'enunciato si ottiene dalla discussione precedente, utilizzando μ per identificare ogni elemento a di A con $a^\mu = (a, 0_R) \in A_1$. □

Tornando alla discussione che precede l'enunciato, osserviamo anche l'uguaglianza $\rho\varepsilon = \text{id}_R$, ovvero il diagramma commutativo

$$\begin{array}{ccc} A_1 & \xrightarrow{\varepsilon} & R \\ & \swarrow \rho & \parallel \\ & & R \end{array}$$

che esprime il fatto che ε è un omomorfismo di R -algebre. Notiamo anche l'isomorfismo di R -algebre $r \in R \mapsto r^\rho + A \in A_1/A$, che verrà richiamato nel [Teorema 1.33](#).

Chiameremo l'algebra A_1 appena costruita (o, indifferentemente, la sua copia isomorfa ottenuta effettuando l'identificazione via μ , come nel [Teorema 1.27](#)) l'algebra accresciuta¹⁰ definita da A . Osserviamo che $R_1 = 1_{R_1}R = \{0_A\} \times R$ è isomorfo a R come R -algebra, quindi, una volta effettuata l'identificazione, ogni elemento di A_1 si scrive in unico modo nella forma $a + 1_{R_1}r$, dove $a \in A$ e $r \in R$.

Un importante caso particolare si ha per gli anelli, che, come sappiamo, sono tutte e sole le algebre su \mathbb{Z} ; dunque ogni anello commutativo A è un ideale di un anello commutativo unitario, che chiameremo l'anello accresciuto definito da A .¹¹ Ponendo $R = \mathbb{Z}$ nell'enunciato del [Teorema 1.27](#) si ottiene infatti:

¹⁰ traduzione dell'inglese *augmented*. Chi volesse approfondire può leggere l'[Osservazione 1.J.2](#).

¹¹ lo stesso enunciato vale anche per anelli non commutativi.

Corollario 1.28. *Sia A un anello commutativo, Allora esiste un anello commutativo unitario A_1 tale che $A \triangleleft A_1$ e $A_1/A \simeq \mathbb{Z}$.*

Ripetendo quanto visto nel caso generale, notiamo che ogni elemento dell'anello accresciuto A_1 definito da A si scrive, in unico modo, come $a + n1_{A_1}$ dove $a \in A$ e $n \in \mathbb{Z}$, vale a dire: il gruppo additivo di A_1 è la somma diretta del gruppo additivo di A e di quello del sottoanello minimo $1_{A_1}\mathbb{Z}$ di A_1 che, ricordiamo, è il sottoanello generato dall'unità di A_1 , cioè il più piccolo sottoanello unitario di A_1 . Questo sottoanello è isomorfo a \mathbb{Z} , quindi A_1 ha caratteristica 0.

1.3.2 Riduzione di premoduli a moduli

Quello che stiamo qui per verificare è che ogni premodulo su un anello commutativo R può essere, in modo a molti fini equivalente, riguardato come modulo sull'anello accresciuto definito da R . Questo permette di studiare questioni che riguardano i premoduli riducendole al caso dei moduli.

Proposizione 1.29. *Siano R un anello commutativo, R_1 l'anello accresciuto definito da R e S un anello unitario (non necessariamente commutativo). Allora, detti rispettivamente \mathcal{H} e \mathcal{H}_1 gli insiemi degli omomorfismi di anelli da R a S e di anelli unitari da R_1 a S , l'applicazione $\mathcal{H}_1 \rightarrow \mathcal{H}$ che ad ogni $\alpha \in \mathcal{H}_1$ associa la restrizione di α a R è biettiva.*

Dimostrazione. Basta mostrare che ogni $\varphi \in \mathcal{H}$ ha uno ed un solo prolungamento φ_1 a R_1 che sia un omomorfismo di anelli unitari. Dovendosi avere $r^{\varphi_1} = r^\varphi$ per ogni $r \in R$ e $(1_{R_1})^\varphi = 1_S$, un tale φ_1 deve essere necessariamente l'applicazione:

$$r + n1_{R_1} \in R_1 \mapsto r^\varphi + n1_S \in S.$$

Ora, si verifica senza difficoltà che questa applicazione è un omomorfismo di anelli unitari; in questo modo l'asserto è provato. \square

Applicando questo risultato al caso in cui S sia l'anello degli endomorfismi di un gruppo abeliano M si ha:

Corollario 1.30. *Siano R un anello commutativo e M un gruppo abeliano. Se \mathcal{A} è l'insieme delle azioni di premodulo $R \rightarrow \text{End } M$ e \mathcal{A}_1 è l'insieme delle azioni di modulo $R_1 \rightarrow \text{End } M$, l'applicazione da \mathcal{A}_1 a \mathcal{A} che ad ogni $\zeta \in \mathcal{A}_1$ associa la restrizione di ζ a R è biettiva.*

Abbiamo così che ogni premodulo M su un anello commutativo R si può riguardare come modulo sull'anello accresciuto R_1 definito da R (e viceversa). Si ha, inoltre, con dimostrazione ovvia:

Proposizione 1.31. *Con le notazioni appena stabilite,*

- (i) *una parte di M costituisce un R_1 -sottomodulo se e solo se costituisce un R -sottopremodulo. Dunque, per ogni parte X di M , l' R -sottopremodulo generato da X coincide con XR_1 ;*
- (ii) *se N è un R -premodulo un'applicazione $M \rightarrow N$ è un R -omomorfismo se e solo se è un R_1 -omomorfismo, una volta che N sia visto come R_1 -modulo ai sensi del [Corollario 1.30](#).*

La parte (i) è una riformulazione dell'[Esercizio 1.D.3](#) (ii). Questi risultati giustificano l'affermazione fatta all'inizio della sottosezione: lo studio dei premoduli su un anello commutativo può essere spesso ridotto a quello dei moduli sull'anello accresciuto. A titolo di esempio:

Corollario 1.32. *Sia R un anello commutativo. A meno di isomorfismi i premoduli ciclici sono tutti e soli i quozienti R_1/H , dove R_1 è l'anello accresciuto definito da R (visto come R -modulo) e $H \triangleleft R_1$.*

Dimostrazione. Sia M un R -premodulo ciclico. Allora, per la (i) della [Proposizione 1.31](#), M è ciclico anche come R_1 -modulo, quindi $M \simeq_{R_1} R_1/H$ per un opportuno $H \triangleleft R_1$, come segue dalla [Proposizione 1.21](#), dunque $M \simeq_R R_1/H$ per la [Proposizione 1.31](#) (ii). Anche il viceversa segue dalla [Proposizione 1.31](#) (i). \square

Questo corollario e la [Proposizione 1.21](#) saranno generalizzati nella [Proposizione 4.20](#).

1.3.3 Idealizzazione di un (pre)modulo

Tra i primi esempi di premoduli abbiamo indicato gli ideali di un anello commutativo R : come osservato questi sono precisamente i sotto(pre)moduli di R_R . In questo senso la nozione di (pre)modulo generalizza quella di ideale. Un'applicazione del [Teorema 1.27](#) permette in qualche modo di invertire questa considerazione: ogni (pre)modulo M su un anello commutativo R è un ideale di un anello S che può essere scelto in modo che, a meno di un cambio di scalari, l'azione di modulo di S su M sia identificabile con quella di R .

Teorema 1.33. *Siano R un anello commutativo e M un R -(pre)modulo. Allora esiste un anello commutativo S tale che:*

- (i) $M \triangleleft S$;
- (ii) in S si abbia $M^2 = 0$, vale a dire: $M \subseteq \text{Ann}_S(M)$;
- (iii) $R \simeq S/M$;

Inoltre, visto M come S/M -(pre)modulo per cambio degli scalari utilizzando la (ii), è possibile scegliere l'isomorfismo in (iii) in modo che l'azione di R -(pre)modulo su M definita via questo isomorfismo coincida con quella originale.

Dimostrazione. Consideriamo innanzitutto il caso in cui R è unitario e M è un R -modulo. Come visto in un esempio precedente, M si può riguardare come R -algebra con moltiplicazione interna definita da $ab = 0_M$ per ogni $a, b \in M$. Sia S l' R -algebra accresciuta definita da quest'algebra, allora (a meno di identificazioni) $M \triangleleft S$ e $R \simeq S/M$. Inoltre, la definizione della moltiplicazione interna di M comporta $MM = 0$, ovvero $M \subseteq \text{Ann}_S(M)$. Infine, con le notazioni utilizzate per la dimostrazione del [Teorema 1.27](#), l'isomorfismo $r \in R \rightarrow r^\rho + M \in S/M$ ha la proprietà richiesta dall'ultima parte dell'enunciato.

Passiamo al caso generale. Sia R_1 l'anello accresciuto definito da R e riguardiamo M come R_1 -modulo, nel senso indicato nel [Corollario 1.30](#). Applichiamo la costruzione del caso precedente a questo R_1 -modulo, ottenendo un anello S_1 tale che $M \triangleleft S_1 = M + R_1$. Allora $S := M + R$ è un sottoanello di S_1 che verifica tutte le richieste dell'enunciato. \square

L'anello S (che in effetti è una R -algebra se M è modulo) che appare in questo teorema viene chiamato *idealizzazione* di M e viene spesso indicato col simbolo $M \rtimes R$, preso a prestito dalla teoria dei gruppi.

Conviene riguardare in dettaglio ed in modo esplicito la definizione dell'anello $M \rtimes R$. Per chiarezza, facciamo riferimento alla costruzione iniziale dell'algebra A_1 nella discussione che ha portato al [Teorema 1.27](#) e nelle notazioni usate lì rinunciamo all'identificazione degli elementi di A con le loro immagini mediante μ . Allora, sia nel caso in cui M sia un R -modulo, sia nell'altro caso, $S = M \rtimes R$ ha per sostegno il prodotto cartesiano $M \times R$ e le sue operazioni interne di addizione e moltiplicazione risultano definite da

$$(a, r) + (b, s) = (a + b, r + s) \quad \text{e} \quad (a, r)(b, s) = (a \cdot s + b \cdot r, rs)$$

per ogni $a, b \in M$ e $r, s \in R$, dal momento che $ab = 0_M$. Resta invariato il fatto che $\rho: r \in R \mapsto (0_M, r) \in S$ e $\mu: a \in M \mapsto (a, 0_R) \in S$ sono monomorfismi (di anelli o di R -(pre)moduli). A meno dell'identificazione di M con $\text{im } \mu$ l'isomorfismo in [Teorema 1.33](#) (iii) è descritto da

$r \mapsto r^\rho + \text{im } \mu$. Infine, $\text{im } \mu$ è un S -(pre)modulo in quanto ideale di S ed è annullato da sé stesso, quindi è un $(S/\text{im } \mu)$ -(pre)modulo (considerando l'azione indotta mod $\text{im } \mu$) e un R -(pre)modulo (via l'isomorfismo ora descritto). L'operazione esterna di questo R -(pre)modulo è descritta da $a^\mu r = a^\mu r^\rho = (a, 0_R)(0_M, r) = (a \cdot r)^\mu$ per ogni $a \in M$ e $r \in R$, a conferma dell'ultima frase nell'enunciato del [Teorema 1.33](#).

Esercizi.

1.J.1. Può essere utile fermarsi a riflettere sulla nozione, in genere non formalizzata, di identificazione. Capita spesso, nello studio di una struttura matematica A , di costruire una struttura B che soddisfi alcune proprietà predeterminate ed abbia una sottostruttura A' isomorfa ad A , e concludere da ciò che A è una sottostruttura di una struttura con le proprietà richieste per B , cosa che, in senso stretto, non si è fatto. In questi casi si dice che si 'identifica' A con A' e si procede come se l'isomorfismo tra A e A' fosse l'uguaglianza. È quello che abbiamo fatto nel [Teorema 1.27](#). Perché tutto ciò è lecito?

In generale, se S è il sostegno di un certo tipo di struttura matematica, algebrica o di altro tipo, e $f: S \rightarrow T$ è un'applicazione biettiva, si può usare f per definire su T una struttura isomorfa a quella data su S in modo che f risulti un isomorfismo. Ad esempio, se in S è data un'operazione (oppure una relazione) binaria $*$, si definisce un'operazione (oppure una relazione) binaria \star in T ponendo $a\star b = (a^{f^{-1}} * b^{f^{-1}})^f$ (oppure $a\star b \iff a^{f^{-1}} * b^{f^{-1}}$) per ogni $a, b \in T$; in questo modo f risulta essere un isomorfismo da $(S, *)$ a (T, \star) . Analogamente si procede per operazioni o relazioni di altra arietà. Si usa dire che in questo modo si è usata f per trasferire a T la struttura definita su S .

Tornando alla questione originaria, supponiamo di aver costruito, a partire dalla struttura A una struttura B con una sottostruttura A' ed un isomorfismo $\alpha: A \rightarrow A'$. Se, per semplicità, supponiamo che i sostegni di A e B siano disgiunti, poniamo $B' = A \cup (B \setminus A')$ e definiamo la biezione $f: B \rightarrow B'$ ponendo $a^f = a^{\alpha^{-1}}$ per ogni $a \in A'$ e $b^f = b$ per ogni $b \in B \setminus A'$. Usiamo f per trasferire a B' la struttura definita su B ; si verifica subito che A è una sottostruttura di B' che coincide con la struttura A originale, e ovviamente B' è isomorfo a B . Se, invece i sostegni di A e B non sono disgiunti, basta trasferire preliminarmente la struttura di B su un insieme B_1 disgiunto da A e ripetere la costruzione di B' utilizzando B_1 al posto di B .

Abbiamo così giustificato la liceità delle identificazioni.

1.J.2. Sia R un anello commutativo unitario. Nella terminologia corrente, una R -algebra accresciuta (traduciamo così l'espressione inglese *augmented algebra*) è una coppia ordinata (A, ε) , dove A è una R -algebra unitaria e $\varepsilon: A \rightarrow R$ è un omomorfismo di R -algebre unitarie. Forniamo qui qualche indicazione sul fatto che questa nozione è sostanzialmente equivalente a quella di algebra accresciuta che abbiamo dato nel testo con riferimento alla costruzione che ha portato al [Teorema 1.27](#).

Se A_1 è l'algebra unitaria costruita come nel [Teorema 1.27](#) a partire da un'arbitraria R -algebra A e $\varepsilon: A_1 \rightarrow R$ è definito da $(a, r)^\varepsilon = r$ per ogni $a \in A$ e $r \in R$, allora (A_1, ε) è un'algebra accresciuta. Ovviamente, a meno dell'identificazione degli elementi $a \in A$ con $(a, 0_A) \in A_1$, si ha $A = \ker \varepsilon$.

Viceversa, se (A, ε) è una R -algebra accresciuta, nel senso appena definito qui, si può provare che A è isomorfa, come R -algebra, all'algebra K_1 costruita come nel [Teorema 1.27](#) a partire da $K := \ker \varepsilon$. Infatti, se $\xi: R \rightarrow A$ è l'omomorfismo di struttura, si ha $\xi\varepsilon = \text{id}_R$ per la [Proposizione 1.25](#); da ciò segue che ξ è iniettiva, quindi $R' := \text{im } \xi$ è isomorfo (come R -algebra) a R , ma anche che $A = K + R'$ e $K \cap R' = 0$. Se ne ricava che l'applicazione $(k, r) \in K_1 \mapsto k + r^\xi \in A$ è un isomorfismo di R -algebre.

1.J.3. Siano R un anello commutativo unitario e $\varphi: A \rightarrow B$ un omomorfismo di R -algebre. Allora, se A_1 e B_1 sono le algebre accresciute definite da A e B l'applicazione $\varphi_1: (a, r) \in A_1 \mapsto (a^\varphi, r) \in B_1$ è un omomorfismo di R -algebre unitarie.

Chi conosce questa terminologia può verificare che le assegnazioni $A \mapsto A_1$ e $\varphi \mapsto \varphi_1$ definiscono un funtore dalla categoria delle R -algebre a quella delle R -algebre unitarie.

1.J.4. Sia A l'anello \mathbb{Z}_2 visto come algebra su sé stesso. Descrivere in dettaglio, scrivendo le tavole di Cayley delle due operazioni binarie di anello, l'algebra accresciuta A_1 definita da A .

Confrontare l'anello A_1 con l'idealizzazione $C_2 \rtimes \mathbb{Z}_2$ dove C_2 è un gruppo ciclico di cardinalità 2, visto come \mathbb{Z}_2 -modulo nell'unico modo possibile.

1.J.5. Della nozione di algebra (associativa e commutativa) è possibile dare una versione più generale di quella data qui; esprimendosi informalmente: un anello con una struttura di premodulo, non necessariamente di modulo, compatibile con le operazioni dell'anello.

Sia R un anello commutativo. Conveniamo di chiamare R -prealgebra un anello commutativo A che ha anche una struttura di R -premodulo, con l'aggiunta di A come operazione binaria e tale che, per ogni $a, b \in A$ e $r \in R$, si abbia $(ab) \cdot r = a(b \cdot r)$, dove \cdot indica l'operazione esterna. Verificare che, detto R_1 l'anello accresciuto definito da R e fissato un anello commutativo A , esiste una biezione (indotta da quella definita nel [Corollario 1.30](#), quindi definita dalla restrizione) tra l'insieme delle azioni di R_1 -modulo che strutturano A come R_1 -algebra e quello delle azioni di R -premodulo che strutturano A come R -prealgebra.

Questo significa che, come la nozione di premodulo si può ridurre a quella di modulo, quella di prealgebra qui introdotta si può ridurre a quella di algebra.

2 Divisibilità in monoidi commutativi

Le proprietà di divisibilità di elementi e di ideali hanno grande importanza nello studio degli anelli commutativi. Per questo motivo dedichiamo un capitolo ad una rivisitazione ed approfondimento della teoria elementare della divisibilità e della fattorizzazione nei monoidi commutativi.

2.1 Richiami

Ricordiamo un po' di terminologia, notazioni e risultati elementari, le cui dimostrazioni saranno omesse. Fissiamo un monoide commutativo $(M, \cdot, 1_M)$. Se $a, b \in M$, si dice che a divide b (in M) se e solo se esiste $c \in M$ tale che $b = ac$; in simboli: $a|_M b$ o, più brevemente, $a|b$. Inoltre, a e b sono *associati* in M (e scriviamo $a \sim_M b$) se e solo se $a|_M b$ e $b|_M a$. Per ogni $a \in M$, con $\text{Div}_M(a)$ intendiamo l'insieme $\{x \in M \mid x|a\}$ dei divisori di a in M , mentre l'insieme $\{ax \mid x \in M\}$ dei multipli di a in M è indicato con aM . Con queste notazioni:

Lemma 2.1. *Per ogni $a, b \in M$ sono equivalenti:*

- (i) $a \sim_M b$; (ii) $\text{Div}_M(a) = \text{Div}_M(b)$; (iii) $aM = bM$.

*Inoltre, se a è cancellabile in M , queste condizioni sono equivalenti a $(\exists u \in \mathcal{U}(M))(b = au)$.*¹

La relazione \sim_M è di equivalenza in M , come si verifica direttamente dalla definizione o dalle caratterizzazioni nel lemma precedente. Inoltre essa è compatibile con la moltiplicazione in M (se $a, b, c \in M$ e $a \sim_M b$ allora $ac \sim_M bc$), dando così luogo al monoide quoziente M/\sim_M , che indichiamo con \tilde{M} . Per brevità, scriveremo spesso \tilde{a} per la classe $[a]_{\sim_M}$ degli elementi associati ad un elemento a di M .

Per ogni $a \in M$, tra i divisori di a ci sono i cosiddetti divisori banali: gli elementi invertibili di M e quelli associati ad a . Se $a \notin \mathcal{U}(M)$ e $\text{Div}_M(a) = \mathcal{U}(M) \cup [a]_{\sim_M}$ (vale a dire: i soli divisori di a in M sono quelli banali), allora si dice che a è *irriducibile* in M . Si dice invece che a è *primo* se e solo se $a \notin \mathcal{U}(M)$ e ogni volta che a divide un prodotto in M allora a divide almeno uno dei fattori: $(\forall b, c \in M)(a|bc \Rightarrow (a|b \vee a|c))$.² È facile provare che *ogni elemento primo e cancellabile di M è irriducibile*; il viceversa è in generale falso anche nell'ipotesi che M sia un monoide *cancellativo*, cioè un monoide in cui ogni elemento è cancellabile (si veda l'esempio presentato nell'[Esercizio 2.A.3](#)). È altrettanto facile verificare che ciascuna delle proprietà di essere invertibile, irriducibile, primo è invariante per il passaggio ad associati, nel senso che se $a, b \in M$, allora a verifica la proprietà in questione se e solo se b verifica la stessa proprietà. Meglio ancora: a verifica la proprietà nel monoide M se e solo se \tilde{a} verifica la stessa proprietà in \tilde{M} .

Se M è un monoide commutativo cancellativo, si dice che M è *fattoriale* se e solo se è verificata una delle seguenti tre proprietà, tra loro equivalenti:

F_1): ogni elemento non invertibile di M è prodotto di primi;

¹ $\mathcal{U}(M)$ denota il gruppo degli invertibili di M .

² nella definizione di elemento primo molti autori richiedono anche che l'elemento, in questo caso p , sia cancellabile, vale a dire: tale che l'applicazione $x \in M \mapsto px \in M$ sia iniettiva. La cosa non è molto rilevante, ma notiamo che se, come in queste note, non lo si fa, allora il numero 0 è a tutti gli effetti un primo (non irriducibile!) in (\mathbb{Z}, \cdot) .

F₂): ogni elemento non invertibile di M è prodotto di irriducibili, ed ogni irriducibile è primo;
 F₃): ogni elemento non invertibile di M è prodotto di irriducibili, in modo essenzialmente unico.

Chiariamo il significato dell'ultima espressione. Se un elemento a è espresso come prodotto di elementi di M in due modi: $x_1x_2 \cdots x_r = a = y_1y_2 \cdots y_s$, diciamo che queste due fattorizzazioni sono 'essenzialmente uguali' se e solo se $r = s$ ed esiste una permutazione $\sigma \in \mathbb{S}_r$ tale che $x_i \sim_M y_{i\sigma}$ per ogni $i \in \{1, 2, \dots, r\}$. In altri termini: il numero dei fattori nelle due fattorizzazioni è lo stesso ed è possibile riordinare i fattori y_i in modo che ciascuno degli x_i sia associato in M al corrispondente fattore y_i . Dire che a ha essenzialmente una unica fattorizzazione in irriducibili vuol dire che due qualsiasi fattorizzazioni di a come prodotto di irriducibili devono risultare essenzialmente uguali.

Conseguenza immediata della definizione è che in un monoide fattoriale le proprietà di essere irriducibile e quella di essere primo sono equivalenti.

Esercizi ed Esempi.

2.A.1. Verificare in dettaglio tutte le affermazioni fatte in questa sezione.

2.A.2. Verificare che se $M \simeq (\mathbb{Z}, \cdot, 1)$ allora $\tilde{M} \simeq (\mathbb{N}, \cdot, 1)$.

2.A.3. Sia P il sottomonoido di (\mathbb{N}^+, \cdot) costituito da 1 e dai numeri interi positivi pari. Descrivere gli elementi irriducibili di P , e verificare che in P non esistono elementi primi. Dedurre che P è un monoide commutativo cancellativo in cui ogni elemento non invertibile (cioè diverso da 1) è prodotto di irriducibili, ma non è un monoide fattoriale. Trovare qualche elemento che abbia in P fattorizzazioni in irriducibili che non sono essenzialmente uguali tra loro.

2.A.4. Sia M un monoide commutativo, e sia a un elemento cancellabile di M . Dimostrare:

- i) ogni divisore di a è cancellabile;
- ii) due qualsiasi fattorizzazioni di a come prodotto di primi in M sono essenzialmente uguali.

2.2 Una caratterizzazione dei monoidi fattoriali in termini di ordinamenti

2.2.1 Reticoli

La caratterizzazione a cui allude il titolo di questa sezione è espressa in termini di reticoli; diamo qui qualche rapida informazione su questa importantissima (ed ubiqua, in matematica) nozione, limitandoci allo stretto necessario. Si chiama *reticolo* un insieme ordinato (S, \leq) con la proprietà che, per ogni $a, b \in S$, esistano in (S, \leq) sia l'estremo inferiore $\inf\{a, b\}$ che l'estremo superiore $\sup\{a, b\}$. Più in generale, (S, \leq) è un inf-semireticolo se e solo se per ogni $a, b \in S$, in (S, \leq) esiste $\inf\{a, b\}$; analogamente si definiscono i sup-semireticoli.

Sono esempi di reticoli tutti gli insiemi ordinati, l'insieme delle parti di un qualsiasi insieme, ordinato per inclusione (gli estremi inferiori e superiori sono descritti in questo caso da intersezione ed unione), l'insieme dei sottomoduli di un modulo, ancora ordinato per inclusione (con intersezione e sottomodulo generato a fornire estremi inferiori e superiori—allo stesso modo, in ogni genere di struttura algebrica l'insieme delle sottostrutture costituisce un reticolo). Se (S, \leq) è un reticolo, chiaramente sarà un reticolo anche (S, \geq) , cioè S munito dell'ordinamento duale.

In ogni reticolo (S, \leq) risultano definite due operazioni binarie, indicate abitualmente come \wedge e \vee e chiamate operazioni reticolari, definite ponendo $a \wedge b = \inf\{a, b\}$ e $a \vee b = \sup\{a, b\}$ per ogni $a, b \in S$. Si verifica facilmente che queste due operazioni sono associative e commutative e

verificano le cosiddette leggi di assorbimento: per ogni $a, b \in S$, vale $a \vee (a \wedge b) = a = a \wedge (a \vee b)$. Meno evidente è che vale il viceversa: se in un insieme S sono date due operazioni binarie \wedge e \vee che verificano queste proprietà (che, si noti, sono puramente algebriche), allora è possibile definire in S una relazione d'ordine \leq che rende (S, \leq) un reticolo con \wedge e \vee come operazioni reticolari (la relazione si definisce ponendo, per ogni $a, b \in S$, $a \leq b$ se e solo se $a = a \wedge b$). Questo significa, in sostanza, che si può, in modo equivalente, studiare i reticoli come strutture relazionali (insiemi muniti di, in questo caso, un particolare tipo di relazione d'ordine) o come strutture algebriche. È utile sapere che le due possibili nozioni, quella relazionale e quella algebrica, di isomorfismo tra reticoli coincidono: un'applicazione biettiva tra due reticoli è un isomorfismo tra insiemi ordinati (cioè è crescente ed ha inversa crescente) se e solo se è un isomorfismo tra strutture algebriche (cioè conserva le operazioni reticolari). Faremo anche riferimento ad anti-isomorfismi; un *anti-isomorfismo* da un insieme ordinato S ad un insieme ordinato T è un isomorfismo da S al duale di T , cioè un'applicazione biettiva strettamente decrescente con inversa strettamente decrescente (se S e T sono reticoli gli anti-isomorfismi da S a T si interpretano, in termini algebrici, come isomorfismi da (S, \wedge, \vee) a (T, \vee, \wedge)). Esiste una nozione, algebrica, di *sottoreticolo*: è il reticolo costituito da una parte non vuota che sia chiusa rispetto alle operazioni reticolari. Si faccia però attenzione: un sottoinsieme di un reticolo S può essere esso stesso un reticolo rispetto all'ordinamento indotto pur non essendo un sottoreticolo di S ; in altri termini, per i reticoli, le nozioni algebrica e relazionale di sottostruttura non coincidono. Ad esempio, ordinati entrambi per inclusione, sia l'insieme delle parti che l'insieme dei sottomoduli di un modulo sono reticoli, ma in generale il secondo non è un sottoreticolo del primo perché non è chiuso per l'operazione reticolare di estremo superiore del primo, cioè per l'unione.³

Un reticolo può avere o non avere minimo e/o massimo (se li ha si dice che è limitato). In un reticolo (o più in generale, in un insieme ordinato) con minimo si dicono *atomi* gli elementi che siano minimali tra quelli diversi dal minimo (ad esempio, i singleton nell'insieme delle parti di un insieme), dualmente, in un insieme ordinato con massimo i *coatomi* sono gli elementi massimali tra quelli diversi dal massimo (ad esempio, nel reticolo dei sottogruppi di un gruppo i coatomi sono i sottogruppi massimali, in quello degli ideali di un anello commutativo i coatomi sono gli ideali massimali).

2.2.2 Il preordinamento divisibilità

Un *preordinamento* in un insieme S è una relazione binaria in S che sia riflessiva e transitiva. Se σ è un preordinamento in S , si può definire in S una relazione binaria ρ ponendo, per ogni $a, b \in S$, $a \rho b$ se e solo se $a \sigma b$ e $b \sigma a$. È facile verificare che ρ è una relazione di equivalenza (che si dice associata a σ) e che σ induce una relazione d'ordine (largo) σ^* nel quoziente S/ρ definita ponendo, per ogni $a, b \in S$, $[a]_\rho \sigma^* [b]_\rho$ se e solo se $a \sigma b$.

Un esempio di questa costruzione l'abbiamo già per le mani: la relazione di divisibilità in un (arbitrario) monoide commutativo M è un preordinamento e la relazione di equivalenza associata a questa è, evidentemente, la relazione \sim_M 'essere elementi associati' in M . La relazione d'ordine indotta nel quoziente $M/\sim_M = \tilde{M}$ dalla divisibilità in M non è altro che la relazione di divisibilità in \tilde{M} , che è così un ordinamento, in accordo col fatto che \tilde{M} ha un unico elemento invertibile, il suo elemento neutro $\tilde{1}_M$ (a questo proposito può essere utile esaminare l'Osservazione 2.B.2).

Siano $a, b \in M$. Un elemento $d \in M$ divide a (in M) se e solo se \tilde{d} divide \tilde{a} in \tilde{M} . Da ciò e dall'analoga osservazione per b al posto di a segue facilmente che d è un massimo comun divisore (MCD) tra a e b in M se e solo se \tilde{d} è un MCD tra \tilde{a} e \tilde{b} in \tilde{M} . Poiché la divisibilità è una

³ anzi, è un semplice esercizio verificare che l'unione di due sotto(pre)moduli di un (pre)modulo è un sotto(pre)modulo se e solo se i due sotto(pre)moduli sono confrontabili per inclusione.

relazione d'ordine in \tilde{M} quest'ultima affermazione equivale a dire che \tilde{d} è l'estremo inferiore di $\{\tilde{a}, \tilde{b}\}$ nell'insieme ordinato $(\tilde{M}, |)$. Ciò suggerisce di usare la notazione consueta in teoria dei reticoli e scrivere $\tilde{d} = \tilde{a} \wedge \tilde{b}$ per indicare che d è un MCD tra a e b . In modo del tutto analogo, per ogni $m \in M$ abbiamo che m è un minimo comune multiplo (mcm) tra a e b se e solo se \tilde{m} è un mcm tra \tilde{a} e \tilde{b} , ovvero $\tilde{m} = \tilde{a} \vee \tilde{b}$ è l'estremo superiore di $\{\tilde{a}, \tilde{b}\}$ in $(\tilde{M}, |)$.

Un richiamo sembra opportuno: l'insieme dei MCD tra due elementi è, in generale, una classe di elementi associati, quindi se d è un MCD tra a e b allora \tilde{d} è l'insieme di tutti i MCD tra a e b in M . Nel passaggio a \tilde{M} si guadagna in definizione: le classi di elementi associati sono singleton, quindi, sempre nel caso in cui d sia un MCD tra a e b , \tilde{d} sarà l'unico MCD tra \tilde{a} e \tilde{b} in \tilde{M} . Analogo discorso vale per i mcm.

Ci occupiamo ora del problema dell'esistenza o meno di un MCD o di un mcm per due elementi di un monoide commutativo M . Come ben noto l'esistenza di questi non è generalmente garantita neanche nel caso in cui M sia cancellativo, ma lo è nel caso dei monoidi fattoriali. Infatti, se M è fattoriale e $a, b \in M$, esistono $n \in \mathbb{N}$, elementi irriducibili p_1, p_2, \dots, p_n di M a due a due non associati tra loro ed interi $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n \in \mathbb{N}$ tali che $a \sim_M \prod_1^n p_i^{\alpha_i}$ e $b \sim_M \prod_1^n p_i^{\beta_i}$. In questo caso, posto $\delta_i = \min\{\alpha_i, \beta_i\}$ e $\mu_i = \max\{\alpha_i, \beta_i\}$ per ogni $i \in \{1, 2, \dots, n\}$, si ha che $\prod_1^n p_i^{\delta_i}$ e $\prod_1^n p_i^{\mu_i}$ sono rispettivamente un MCD ed un mcm tra a e b . Questo ovviamente prova che se M è un monoide fattoriale allora \tilde{M} , ordinato per divisibilità, è un reticolo. Dimosteremo ora che questa proprietà è non lontana dal caratterizzare i monoidi fattoriali.

Introduciamo una notazione che utilizzeremo nelle prossime dimostrazioni. Se a e b sono elementi di un monoide commutativo M in cui a sia cancellabile e $a|b$, allora esiste un unico $c \in M$ tale che $b = ac$. In queste condizioni (ma solo in queste) indicheremo tale c con $\left(\frac{b}{a}\right)$. Dunque, se a è cancellabile, $b = a\left(\frac{b}{a}\right)$ equivale a $a|b$.

Assumendo che M sia cancellativo, l'ipotesi che \tilde{M} sia un reticolo implica che ogni irriducibile in M è primo. Il primo passo per la dimostrazione è questo lemma:

Lemma 2.2. *Siano a, b, c elementi di un monoide commutativo cancellativo M . Sia d un MCD tra a e b in M . Supponiamo che anche ac e bc abbiano un MCD e in M . Allora $e \sim_M dc$.*

Dimostrazione. Ovviamente dc è un divisore comune ad ac e bc , quindi $dc|e$. Da $e = dc\left(\frac{e}{dc}\right)|ac$, cancellando c , segue $d\left(\frac{e}{dc}\right)|a$. Allo stesso modo si ottiene $d\left(\frac{e}{dc}\right)|b$. Di conseguenza $d\left(\frac{e}{dc}\right)$ divide il MCD d tra a e b ; quindi $\left(\frac{e}{dc}\right)$ è invertibile ed $e \sim_M cd$. \square

Il precedente enunciato sembra del tutto ovvio (lo è ad esempio, nell'ipotesi che M sia fattoriale), e potrebbe sorgere il dubbio che l'ipotesi che esista un MCD tra ac e bc sia superflua. Non è così, l'esistenza di un MCD tra a e b non garantisce quella di un MCD tra ac e bc ; un esempio è dato nell'[Esercizio 2.B.5](#).

Lemma 2.3. *Sia M un monoide cancellativo e supponiamo che \tilde{M} , ordinato per divisibilità sia un reticolo. Allora, in M , ogni irriducibile è primo.*

Dimostrazione. Assunta l'ipotesi, sia p un irriducibile in M . Allora $p \notin \mathcal{U}(M)$. Per ogni $a, b \in M$, se $p|ab$ e $p \nmid a$ abbiamo ovviamente $\tilde{1}_M = \tilde{a} \wedge \tilde{p}$, dunque $\tilde{b} = \tilde{a}\tilde{b} \wedge \tilde{p}b$, per il [Lemma 2.2](#). Ma p divide sia ab che pb , quindi $p|b$. È così provato che p è primo. \square

Lemma 2.4. *Sia M un monoide cancellativo e supponiamo che \tilde{M} , ordinato per divisibilità verifichi la condizione minimale. Allora, in M , ogni elemento non invertibile è prodotto di irriducibili.*

Dimostrazione. Sia S l'insieme degli elementi in $M \setminus \mathcal{U}(M)$ che non siano prodotto di irriducibili in M . Supposta la tesi falsa, $S \neq \emptyset$ e quindi $\tilde{S} = \{\tilde{a} \mid a \in S\} \neq \emptyset$. Esiste allora $a \in M$ tale che \tilde{a}

sia minimale (rispetto a $|$) in \tilde{S} . Ovviamente a non è irriducibile, quindi esistono $b, c \in M \setminus \mathcal{U}(M)$ tali che $a = bc$, quindi b e c sono divisori propri di a , sicché $\tilde{a} \neq \tilde{b}|\tilde{a}$ e $\tilde{a} \neq \tilde{c}|\tilde{a}$. La minimalità di \tilde{a} garantisce che sia b che c sono prodotti di irriducibili in M , quindi lo stesso vale per a . Questa è una contraddizione. \square

Mettendo assieme i risultati ottenuti negli ultimi due lemmi arriviamo al risultato principale di questa sezione.

Teorema 2.5. *Sia M un monoide commutativo cancellativo. Allora M è fattoriale se e solo se \tilde{M} , ordinato per divisibilità, è un reticolo a condizione minimale.*

Dimostrazione. Se \tilde{M} è un reticolo a condizione minimale, allora i due lemmi precedenti mostrano che ogni elemento non invertibile di M è prodotto di irriducibili e tutti gli irriducibili di M sono primi; dunque M è fattoriale. Viceversa, supponiamo che M sia fattoriale. Abbiamo già osservato che in questo caso ogni coppia di elementi di M ha MCD, quindi $(\tilde{M}, |)$ è un reticolo. Possiamo definire un'applicazione $\tau: \tilde{M} \rightarrow \mathbb{N}$, associando a ciascun $\tilde{a} \in \tilde{M}$ il numero dei fattori in una decomposizione di a in prodotto di irriducibili (poiché M è fattoriale questo numero è univocamente definito e non dipende dalla scelta del rappresentante a in \tilde{a}); si osservi che $\tilde{1}_M^\tau = 0$. Ora, se $\tilde{a}, \tilde{b} \in \tilde{M}$ e $\tilde{a}|\tilde{b}$, allora $\tilde{b}^\tau \leq \tilde{a}^\tau$ e $\tilde{b}^\tau < \tilde{a}^\tau$ se $\tilde{a} \neq \tilde{b}$. Se ne deduce che se S è un sottoinsieme non vuoto di \tilde{M} e $n = \min S^\tau$, ogni $\tilde{a} \in S$ tale che $\tilde{a}^\tau = n$ è un elemento minimale in S . Questo mostra che $(\tilde{M}, |)$ verifica la condizione minimale. A questo punto la dimostrazione è completa. \square

Corollario 2.6. *Sia M un monoide commutativo cancellativo. Allora M è fattoriale se e solo se \tilde{M} è fattoriale.*

Dimostrazione. Posto $M_1 = \tilde{M}$, abbiamo ovviamente $\tilde{M}_1 \simeq \tilde{M}$; altrettanto ovvio è che \tilde{M} è cancellativo. Dunque, per il [Teorema 2.5](#), \tilde{M} è fattoriale se e solo se \tilde{M} , ordinato per divisibilità, è un reticolo a condizione minimale, ma, per lo stesso teorema, questo equivale all'essere M fattoriale. \square

Osserviamo esplicitamente che se M è fattoriale, i suoi elementi irriducibili sono gli a tali che \tilde{a} sia un *atomo* nel reticolo \tilde{M} .

Si noti che nella dimostrazione della sufficienza della condizione nel [Teorema 2.5](#) abbiamo usato l'esistenza di MCD tra coppie di elementi di M , ma non sono apparsi nella discussione minimi comuni multipli, quindi, apparentemente, abbiamo provato un risultato più forte di quello enunciato: M è fattoriale se e solo se \tilde{M} , ordinato per divisibilità, è un inf-semireticolo a condizione minimale. In realtà, l'esistenza di MCD e l'esistenza di mcm in un monoide commutativo non sono affatto condizioni indipendenti tra loro, come stiamo per verificare; ne seguirà che questo secondo enunciato non differisce sostanzialmente dal primo.

Proposizione 2.7. *Sia M un monoide cancellativo.*

- (i) *Per ogni $a, b \in M$, se esiste un mcm m tra a e b , allora esiste un MCD d tra a e b , e si ha $ab \sim_M dm$.*
- (ii) *Se per ogni $a, b \in M$ esiste un MCD tra a e b , allora per ogni $a, b \in M$ esiste un mcm tra a e b .*

Dimostrazione. Siano $a, b \in M$, ed esista $m \in M$ tale che $\tilde{m} = \tilde{a} \vee \tilde{b}$. Poiché m divide ab , possiamo porre $d = \left(\frac{ab}{m}\right)$, dunque $md = ab$. Da quest'ultima uguaglianza seguono $b = \left(\frac{m}{a}\right)d$ e $a = \left(\frac{m}{b}\right)d$, dunque d divide sia a che b . Sia e un arbitrario divisore comune ad a e b . Posto $n := a\left(\frac{b}{e}\right)$ abbiamo $ne = ab = b\left(\frac{a}{e}\right)e$, quindi, per la cancellabilità in M , $n = b\left(\frac{a}{e}\right)$. Dunque n è

un multiplo comune ad a e b , quindi $m|n$. Da $ne = ab = md$ segue $\binom{n}{m}e = d$, quindi $e|d$. È così provato che d è un MCD tra a e b ; la dimostrazione di (i) è completa.

Proviamo ora (ii). Nell'ipotesi di (ii), siano $a, b \in M$ e $\tilde{d} = \tilde{a} \wedge \tilde{b}$. Abbiamo $a \binom{b}{\tilde{d}} = b \binom{a}{\tilde{d}}$, perché moltiplicando per d ciascuno dei due membri di questa uguaglianza si ottiene ab . Chiamando questo elemento m , abbiamo così $ab = md$. Chiaramente $a|m$ e $b|m$; proveremo che $\tilde{m} = \tilde{a} \vee \tilde{b}$. Sia n un multiplo comune ad a e b . Per ipotesi, n ed m hanno in M un MCD, chiamiamolo n_1 . Ovviamente, a e b dividono n_1 , che a sua volta divide m . Allora $n_1 \binom{m}{n_1} d = ab = n_1 \binom{a}{n_1} b$, da cui $\binom{m}{n_1} d = \binom{a}{n_1} b$. Quindi $e := \binom{m}{n_1} d|b$; allo stesso modo $e|a$ e quindi, poiché $\tilde{d} = \tilde{a} \wedge \tilde{b}$, abbiamo $e|d$. Pertanto $e \sim_M d$ e così $\binom{e}{n_1} = \binom{e}{\tilde{d}}$ è invertibile. Di conseguenza $m \sim_M n_1$ e quindi $m|n$. Concludiamo che $\tilde{m} = \tilde{a} \vee \tilde{b}$; la dimostrazione è ora completa. \square

Può sorprendere la mancanza di simmetria tra le due parti dell'enunciato della [Proposizione 2.7](#): l'esistenza di un mcm per una coppia di elementi di M comporta l'esistenza del corrispondente MCD; per ottenere l'implicazione inversa abbiamo richiesto che *tutte* le coppie di elementi di M abbiano un mcm. L'esempio costruito nell'[Esercizio 2.B.4](#) mostra che questa asimmetria è inevitabile: è possibile che, in un monoide commutativo cancellativo, due elementi abbiano un MCD ma non un mcm.

Abbiamo comunque dimostrato che le condizioni di esistenza di MCD e mcm, considerate globalmente, sono equivalenti. Abbiamo così:

Corollario 2.8. *Se M è un monoide commutativo cancellativo, sono equivalenti le proprietà:*

- (i) M , ordinato per divisibilità, è un reticolo.
- (ii) Per ogni $a, b \in M$, esiste un MCD tra a e b in M (vale a dire: \tilde{M} è un inf-semireticolo).
- (iii) Per ogni $a, b \in M$, esiste un mcm tra a e b in M (vale a dire: \tilde{M} è un sup-semireticolo).

Esercizi, Esempi, Osservazioni.

2.B.1. Verificare in dettaglio tutte le affermazioni fatte e non dimostrate in questa sezione.

2.B.2. Se M è un monoide commutativo, la relazione di divisibilità non è, in generale, d'ordine; lo è se e solo se \sim_M è l'uguaglianza. In questo caso, l'unità è l'unico elemento invertibile di M . Se M è cancellativo questa condizione si inverte: la divisibilità in M è una relazione d'ordine se e solo se $\mathcal{U}(M) = \{1_M\}$. Nel caso generale questa equivalenza non vale; chi è interessato può verificarlo con l'esempio fornito al prossimo esercizio.

2.B.3. Si definisca sull'insieme $S = (\mathbb{N} \times \{0, 1\}) \cup (\{0\} \times \mathbb{N})$ un'operazione binaria $*$ ponendo, per ogni $u, v, s, t \in \mathbb{N}$, $(u, v) * (s, t) = (u + s, r)$, dove r è $v + t$ se $u = s = 0$, il resto di $v + t$ modulo 2 altrimenti. Si verifichi che $(S, *, (0, 0))$ è un monoide commutativo e che in S esiste un solo elemento invertibile (quello neutro), ma gli elementi $a = (1, 0)$ e $b = (1, 1)$ sono associati. In questo monoide, dunque, la relazione di divisibilità non è d'ordine.

2.B.4. In questo esercizio viene costruito un monoide commutativo cancellativo M , generato da elementi a, b, c, d con la proprietà che a e c siano coprimi, ed abbiano quindi un MCD, ma non abbiano un mcm.

Sia F il gruppo abeliano libero sulla base $\{a_0, b_0, c_0, d_0\}$. Siano poi H is sottogruppo di F generato da $a_0 b_0 c_0^{-1} d_0^{-1}$ e $P = \{a_0^\alpha b_0^\beta c_0^\gamma d_0^\delta \mid \alpha, \beta, \gamma, \delta \in \mathbb{N}\}$ (P è un monoide commutativo libero sulla base $\{a_0, b_0, c_0, d_0\}$). È chiaro che $M := PH/H$ è un monoide commutativo cancellativo (perché immerso nel gruppo F/H) generato da $a := a_0 H$, $b := b_0 H$, $c := c_0 H$, $d := d_0 H$, in cui vale l'uguaglianza $ab = cd$. Si provi che ciascuno di a, b, c, d è irriducibile, quindi 1_M è un MCD tra a e c , ma non esistono mcm tra a e c .

Suggerimento: si può osservare che se, per $i \in \{1, 2\}$, poniamo $x_i = a^{\alpha_i} b^{\beta_i} c^{\gamma_i} d^{\delta_i}$, dove gli esponenti sono interi arbitrari, abbiamo $x_1 = x_2$ se e solo se $\alpha_1 - \alpha_2 = \beta_1 - \beta_2 = \gamma_2 - \gamma_1 =$

$\delta_2 - \delta_1$. Da ciò si può dedurre che un elemento $x = a^\alpha b^\beta c^\gamma d^\delta$ di F/H è in M se e solo se esiste $\lambda \in \mathbb{Z}$ tale che $\alpha + \lambda, \beta + \lambda, \gamma - \lambda$ and $\delta - \lambda$ siano tutti non negativi, ovvero: $\min\{\alpha, \beta\} \geq \max\{-\gamma, -\delta\}$. Visto ciò, diventa facile stabilire se due assegnati elementi di M si dividano o meno (e che 1_M è l'unico elemento invertibile di M), ed arrivare alle conclusioni desiderate.

2.B.5. In questo esercizio viene costruito un monoide commutativo cancellativo M , con elementi a, b, c , in cui esiste un MCD tra a e b ma non esiste un MCD tra ac e bc . La costruzione è simile a quella in [Esercizio 2.B.4](#), ma un po' più elaborata.

Sia F il gruppo abeliano libero di rango 7, sulla base $\{x_1, x_2, \dots, x_7\}$. Siano poi H il sottogruppo di F generato da $x_1 x_3 x_4 x_5^{-1} x_6^{-1}$ e $x_2 x_3 x_4 x_5^{-1} x_7^{-1}$. Sia poi $P = \{\prod_{i=1}^7 x_i^{\alpha_i} \mid (\forall i \in \{1, 2, \dots, 7\})(\alpha_i \in \mathbb{N})\}$, il monoide (commutativo libero) generato in F da x_1, \dots, x_7 , e sia $M = PH/H$. Allora M è un monoide commutativo cancellativo. Ponendo $a = x_1 x_4 H$, $b = x_2 x_4 H$, $c = x_3 H$, si verifichi che $d := x_4 H$ è un MCD in M tra a e b , ma ac e bc non hanno un MCD in M .

Suggerimento: si osservi che F/H è abeliano libero di rango 5: ogni elemento di F/H può essere rappresentato (unicamente) come xH , dove $x = \prod_{i=1}^5 x_i^{\alpha_i}$ per opportuni interi $\alpha_1, \dots, \alpha_5$. Si verifichi poi che questo l'elemento è in M se e solo se $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \geq 0$ e $\alpha_1 + \alpha_2, \alpha_3, \alpha_4 \geq -\alpha_5$. A questo punto è facile verificare che l'unità H di M e d sono gli unici divisori comuni ad a e b . Inoltre $x_5 H$ divide ac e bc ma non cd , quindi cd non è un MCD tra ac e bc .

2.3 Parti sature e saturazioni

Una parte X di un semigrupp commutativo (M, \cdot) si dice *satura* se e solo se, per ogni $x \in X$, ogni divisore (in M) di x appartiene a X . È chiaro che ogni intersezione di parti sature di M è ancora satura. Per ogni $S \subseteq M$, la parte satura generata da S è l'intersezione delle parti sature di M contenenti S , quindi la più piccola parte satura di M contenente S . Questa è facile da descrivere:

Lemma 2.9. *Siano (M, \cdot) un semigrupp commutativo e $S \subseteq M$. Allora la parte satura T generata da S in M è $S \cup \bigcup\{\text{Div}_M(s) \mid s \in S\}$, che coincide con $\bigcup\{\text{Div}_M(s) \mid s \in S\}$ se M è un monoide. Se S è una parte chiusa rispetto a \cdot , anche T è chiusa; se inoltre M è un monoide T ne è un sottomonoid.*

La semplice dimostrazione viene lasciata per esercizio. Se M è un monoide, è chiaro che ogni sua parte satura non vuota contiene $\mathcal{U}(M)$.

Chiameremo *saturazione* di una parte S di un semigrupp M la parte satura generata dalla parte chiusa generata da S in M (quindi la parte “chiusa e satura” generata da S). Indicheremo la saturazione di S in M come \hat{S} (almeno quando si può sottintendere un riferimento a M); per quanto detto sopra \hat{S} consiste dei divisori di prodotti di elementi di S , e se M è un monoide e $S \neq \emptyset$, allora \hat{S} ne è un sottomonoid.

Lemma 2.10. *In ogni monoide commutativo M , il sottoinsieme S costituito dagli elementi invertibili e dagli elementi che siano prodotti di primi cancellabili⁴ in M è un sottomonoid saturo.*

Dimostrazione. Che S sia un sottomonoid di M è chiaro, bisogna solo verificare che è saturo. Ovviamente i divisori degli elementi invertibili sono invertibili, quindi appartengono ad S ; va

⁴ a scanso di equivoci: ogni primo cancellabile è in S : è un prodotto con un solo fattore.

dimostrato che sono in S tutti i divisori in M di ogni elemento della forma $p_1 p_2 \cdots p_n$, dove $n \in \mathbb{N}^+$ e ciascuno dei p_i è un primo cancellabile di M . Possiamo farlo ragionando per induzione su n , essendo l'asserto ovviamente vero se $n = 1$. Per semplicità, poniamo $s = p_1 p_2 \cdots p_{n-1}$ e $p = p_n$; per ipotesi induttiva (o direttamente, se $n = 1$) $\text{Div}_M(s) \subseteq S$. Sia $a \in \text{Div}_M(sp)$, dunque esiste $b \in M$ tale che $ab = sp$. Dal momento che p è primo e divide ab , o $p|_M a$ oppure $p|_M b$. Nel primo caso, esiste $a_1 \in M$ tale che $a = pa_1$, ma allora, poiché p è cancellabile, $s = a_1 b$ e $a_1|s$, quindi $a_1 \in S$ e così $a = pa_1 \in S$. Nel secondo caso, altrettanto chiaramente, $a|s$, quindi, ancora, $a \in S$. L'asserto è così dimostrato. \square

Esercizi.

2.C.1. Sia $(R, +, \cdot)$ un anello commutativo ed H un suo sottogruppo additivo. Allora $H \triangleleft R$ se e solo se $R \setminus H$ è satura in (R, \cdot) .

2.C.2. Sia R un anello commutativo. Qual è la parte satura di (R, \cdot) generata da $\{0_R\}$?

2.C.3. Sia $S = \{a, b, c, d\}$ un insieme di cardinalità 4. Nel monoide $(\mathcal{P}(S) \setminus \mathcal{P}_1(S), \cup)$, la parte $\{\emptyset, \{a, b\}, \{c, d\}\}$ è satura, ma il sottomonoido (ovvero la parte chiusa) che essa genera non lo è (notazione: $\mathcal{P}_1(S) = \{\{x\} \mid x \in S\}$).

2.C.4. Verificare che l'insieme degli elementi cancellabili in un semigrupp commutativo ne è una parte chiusa satura e lo stesso vale per l'insieme degli invertibili in un monoide commutativo.

3 Ideali

La teoria degli anelli commutativi è, in larga misura, la teoria dei loro ideali. In questo capitolo raccogliamo alcune osservazioni generali sugli ideali di un anello commutativo e sulle operazioni definite per essi, concentrando l'attenzione sugli ideali primi e su quelli massimali, che spesso svolgono un ruolo particolarmente significativo.

3.1 Operazioni tra parti e ideali in un anello

Ricordiamo dalla [sottosezione 1.2.3](#) che nell'insieme delle parti di un anello commutativo R sono definite due operazioni binarie di addizione e moltiplicazione: se $H, K \subseteq R$,

$$H + K = \{h + k \mid h \in H \wedge k \in K\}$$

è l'insieme di tutte le somme tra un elemento di H ed uno di K , mentre HK è il sottomonoido di $(R, +)$ generato da $\{hk \mid h \in H \wedge k \in K\}$, dunque

$$HK = \left\{ \sum_{i=1}^n h_i k_i \mid n \in \mathbb{N} \wedge \forall i \in \{1, 2, \dots, n\} (h_i \in H \wedge k_i \in K) \right\}.$$

Le operazioni di addizione e moltiplicazione di $\mathcal{P}(R)$ sono associative (questo è del tutto ovvio nel caso dell'addizione, richiede un attimo di riflessione in più per la moltiplicazione; si veda l'[Esercizio 1.D.2](#) nella [sottosezione 1.2.3](#)). Rispetto all'addizione l'ideale nullo $0 = \{0_R\}$ è elemento neutro, quindi $(\mathcal{P}(R), +, 0)$ è un monoide.

Un ideale di R , come già detto, è semplicemente un sottopremodulo del premodulo R_R , quindi un sottogruppo H di $(R, +)$ tale che $HR \subseteq H$. Indicheremo con $\mathcal{I}(R)$ l'insieme degli ideali di R . Questo insieme è chiuso sia rispetto all'addizione che rispetto alla moltiplicazione. Infatti, sempre da [1.2.3](#), sappiamo che H e K sono ideali di R , allora $H + K$ è ancora un ideale di R , precisamente l'ideale generato da H e K , e abbiamo poi:

Lemma 3.1. *Siano R un anello commutativo, $H, K \triangleleft R$ e $X \subseteq R$. Allora:*

- (i) XH è un ideale di R contenuto in H ;
- (ii) $X(H + K) = XH + XK$;
- (iii) $\mathcal{I}(R)$ è chiuso rispetto alla moltiplicazione tra parti di R . Se R è unitario, $(\mathcal{I}(R), \cdot)$ è un monoide di elemento neutro R .

Dimostrazione. La (i) segue da $(XH)R = X(HR) \subseteq XH$. Per la (ii): gli elementi di $X(H + K)$ sono somme di prodotti della forma $x(h + k)$ al variare di $x \in X$, $h \in H$ e $k \in K$. Ma $x(h + k) = xh + xk \in XH + XK$; dunque $X(H + K) \subseteq XH + XK$. D'altra parte, essendo $H, K \subseteq H + K$, certamente $XH, XK \subseteq X(H + K)$, quindi da $X(H + K) \triangleleft R$ segue $XH + XK \subseteq X(H + K)$. È così verificata la (ii). La (iii) segue immediatamente da (i) e dall'[Osservazione 1.D.1](#). \square

Caso particolare della (i) del lemma precedente è che il prodotto HK tra due ideali H e K è sempre contenuto nella loro intersezione: $HK \subseteq H \cap K$. Una condizione sufficiente perché qui valga l'uguaglianza è data da uno dei prossimi risultati.

Due ideali H e K di un anello R si dicono *comassimali* se e solo se $R = H + K$.

Lemma 3.2. Siano R un anello commutativo unitario, e $H, K, I \triangleleft R$. Se H e K sono comassimali con I , allora anche HK è comassimale con I .

Dimostrazione. Da $R = H + I = K + I$ e dalla (ii) di Lemma 3.1 segue $R = RR = (H + I)(K + I) = HK + (H + K + I)I \subseteq HK + I$, quindi $R = HK + I$. \square

Lemma 3.3. Siano R un anello commutativo unitario, $n \in \mathbb{N}^+$ e H_1, H_2, \dots, H_n ideali di R a due a due comassimali. Allora $H_1H_2 \cdots H_n = H_1 \cap H_2 \cap \cdots \cap H_n$.

Dimostrazione. Non c'è nulla da provare se $n = 1$. Per il caso $n = 2$: da $R = H_1 + H_2$ deduciamo $H_1 \cap H_2 = (H_1 \cap H_2)(H_1 + H_2) = (H_1 \cap H_2)H_1 + (H_1 \cap H_2)H_2 \subseteq H_2H_1 + H_1H_2 = H_1H_2$, quindi $H_1 \cap H_2 = H_1H_2$. Per gli altri casi basta procedere per induzione: assunto l'asserto vero per $n - 1$ ideali, quindi $I := H_1H_2 \cdots H_{n-1} = H_1 \cap H_2 \cap \cdots \cap H_{n-1}$, siccome I è comassimale con H_n come segue dal Lemma 3.2, si ha $H_1H_2 \cdots H_n = IH_n = I \cap H_n = H_1 \cap H_2 \cap \cdots \cap H_n$. \square

Dunque, il prodotto tra due ideali comassimali in un anello commutativo unitario coincide con la loro intersezione. In altri casi questa uguaglianza può non valere, alcuni sono illustrati nell'Esempio 3.A.1.

Se X è una parte dell'anello commutativo R , l'ideale generato da X in R è descritto dal Lemma 1.6 nel caso in cui R sia unitario, dall'Esercizio 1.D.3 (o dalla Proposizione 1.31 (i)) nel caso generale. Questo ideale viene spesso indicato con $\langle X \rangle$; si ha dunque $\langle X \rangle = XR + \langle X \rangle$, e $\langle X \rangle = XR$ se R è unitario o se, comunque, $X \subseteq XR$. Usuali varianti di questa notazione sono scritte come (a, b, c, \dots) per $(\{a, b, c, \dots\})$ o $(a \mid \dots)$ per $(\{a \mid \dots\})$.

Quando R è un unitario è particolarmente semplice esprimere un prodotto tra ideali in termini dei rispettivi generatori: in questo caso si ha infatti $\langle X \rangle \langle Y \rangle = \{xy \mid x \in X \wedge y \in Y\}R$, come si verifica immediatamente. Ad esempio, se a, b, c sono elementi dell'anello commutativo unitario R , $H = (a)$ e $K = (b, c)$, allora $H^2 = (a^2)$, $HK = (ab, ac)$ e $K^2 = (b^2, c^2, bc)$.

Anche questa semplice osservazione è spesso utile:

Lemma 3.4. Sia R un anello commutativo e sia $a \in R$. Allora $R = aR$ se e solo se R è unitario e $a \in \mathcal{U}(R)$.

Dimostrazione. Sia $R = aR$. Allora $a \in aR$, dunque esiste $e \in R$ tale che $a = ae$. Inoltre, per ogni $r \in R$ esiste $s \in R$ tale che $r = as$, quindi $er = (ae)s = as = r$. Dunque, e è l'unità in R , quindi R è unitario. Essendo $e = 1_R \in aR$, segue anche che a è invertibile. Così è provata una implicazione; l'altra è ovvia. \square

Un'altra operazione tra ideali dell'anello commutativo R è quella di divisione, caso particolare dell'annullatore nei quozienti che abbiamo già definito per premoduli: se $H \triangleleft R$ e $X \subseteq R$ (non necessariamente $X \triangleleft R$), $(H : X)_R = \text{Ann}_R(X + H/H) = \{r \in R \mid Xr \subseteq H\} \triangleleft R$. Alla lista di proprietà sostanzialmente ovvie sugli annullatori che si chiede a chi legge di verificare aggiungiamo (con la consueta sostituzione nella notazione di un singleton col suo elemento):

Lemma 3.5. Siano R un anello commutativo, $H \triangleleft R$ e $X \subseteq R$. Allora $H \subseteq (H : X)_R$. Inoltre, per ogni $a, b \in R$:

- (i) $(H : a)_R \subseteq (H : ab)_R$;
- (ii) $H \cap aR = a(H : a)_R$.

Esempi, osservazioni , esercizi.

3.A.1. Nei lemmi 3.2 e 3.3 è essenziale l'ipotesi che l'anello ambiente sia unitario. Se, ad esempio, R è un anello non nullo con prodotto costante nullo, R è comassimale con qualsiasi suo ideale proprio ma $RR = 0$ non lo è, e, pur essendo R comassimale con sé stesso, $0 = RR \neq R \cap R = R$.

Anche nel caso degli anelli unitari è facile trovare esempi di coppie di ideali per le quali prodotto ed intersezione non coincidano. Ad esempio, in \mathbb{Z} si ha $2\mathbb{Z} \cdot 2\mathbb{Z} = 4\mathbb{Z} \neq 2\mathbb{Z} \cap 2\mathbb{Z}$.

Naturalmente è anche possibile costruire esempi di ideali, distinti o meno, H e K tali che $HK = H \cap K$ pur non essendo H e K comassimali. Un modo molto facile è questo: se R è un anello commutativo unitario e S è un suo sottoanello che sia unitario come anello ma non come sottoanello di R , basta scegliere come H e K due ideali di R contenuti in S tali che $S = H + K$. Una possibile scelta è data da: $R = \mathcal{P}(X)$ per un qualche insieme X , e $S = \mathcal{P}(Y)$, $H = \mathcal{P}(A)$ e $K = \mathcal{P}(B)$, dove $A \cup B = Y \subset X$.

3.A.2. Non è difficile interpretare le operazioni tra ideali nel caso dell'anello degli interi (si tratta in ultima analisi del teorema di Bézout). Quando è che due ideali $a\mathbb{Z}$ e $b\mathbb{Z}$ di \mathbb{Z} sono comassimali? In termini di aritmetica elementare, cosa dicono i lemmi 3.2 e 3.3 se applicati all'anello degli interi?

3.2 Ideali primi e massimali

Centrale nella teoria degli anelli commutativi è la nozione di ideale primo. In diversi casi che incontreremo le proprietà degli ideali primi di un anello commutativo unitario R determinano le proprietà di tutti gli ideali di R ed in definitiva quelle di R .

3.2.1 Primi

La definizione è senz'altro già nota: in un anello commutativo R un ideale P è *primo* se e solo se R/P è un dominio di integrità, cioè se e solo se $P \neq R$ e, per ogni $r, s \in R$, se $rs \in P$ allora almeno uno tra r e s è in P , vale a dire: $R \setminus P$ è una parte chiusa e non vuota di R rispetto alla moltiplicazione—si ricorda che, almeno in queste note, l'anello nullo non è considerato dominio di integrità. L'insieme degli ideali primi di R si chiama *spettro* (o spettro primo) di R e si indica con $\text{Spec}(R)$. Vediamo altre caratterizzazioni elementari degli ideali primi:

Lemma 3.6. *Siano R un anello commutativo e P un ideale proprio di R . Allora sono equivalenti:*

- (i) P è primo in R ;
- (ii) per ogni $r \in R \setminus P$ si ha $(P : r)_R = P$;
- (iii) scelti comunque $I, J \triangleleft R$, se $IJ \subseteq P$ allora $I \subseteq P$ o $J \subseteq P$;
- (iv) scelti comunque I e J tra gli ideali di R contenenti P , se $IJ \subseteq P$ allora $I = P$ o $J = P$.

Dimostrazione. Siano $r \in R$ e $K_r = (P : r)_R$. Allora $P \subseteq K_r$ e K_r/P è l'insieme degli elementi k di R/P tali che $(r + P)k = 0_{R/P}$. Dunque, $K_r \neq P$ se e solo se $r + P$ è un divisore dello zero in R/P . Pertanto la (ii) significa precisamente che R/P non ha divisori dello zero non nulli, cioè che P è un ideale primo. Dunque (ii) equivale a (i).

Valga (ii), e siano $I, J \triangleleft R$ tali che $IJ \subseteq P$ e $I \not\subseteq P$. Scelto $r \in I \setminus P$, abbiamo allora $J \subseteq (P : r)_R = P$. Questo mostra che (ii) implica (iii). Che (iii) implichi (iv) è ovvio.

Infine, se P non è primo esistono $r, s \in R \setminus P$ tali che $rs \in P$. Allora, detti I e J , nell'ordine, gli ideali di R generati da $P \cup \{r\}$ e $P \cup \{s\}$, si ha $IJ \subseteq P$ (ad esempio perché $I = P + rR + \{nr \mid n \in \mathbb{Z}\}$ e J ha una descrizione analoga), $P \subset I$ e $P \subset J$, quindi non vale la (iv). È così provato che (iv) implica (i). \square

Dunque, se un ideale primo è il prodotto di (un numero finito di) ideali che lo contengono, allora è uno di essi. Una proprietà in un senso (molto lasco) duale è nota come *prime-avoidance*: se un sottoanello di un anello commutativo non è incluso in nessuno degli ideali in un certo insieme finito di ideali primi, allora non è incluso (cioè ‘evita’) la loro unione:

Lemma 3.7 (Il ‘prime-avoidance lemma’). *Sia \mathcal{P} un insieme finito di ideali primi in un anello commutativo R . Allora ogni sottoanello A di R che sia contenuto in $\bigcup \mathcal{P}$ è contenuto in almeno un elemento di \mathcal{P} .*

Dimostrazione. Ragionando per assurdo, supponiamo che R , A e \mathcal{P} forniscano un controesempio in cui $|\mathcal{P}|$ ha il minimo valore possibile. Chiaramente $|\mathcal{P}| > 1$ e, per minimalità, scelto comunque $P \in \mathcal{P}$ e posto $\hat{\mathcal{P}}_P = \mathcal{P} \setminus \{P\}$, si ha $A \not\subseteq \bigcup \hat{\mathcal{P}}_P$. Per ogni $P \in \mathcal{P}$ possiamo allora scegliere $a_P \in A \setminus \bigcup \hat{\mathcal{P}}_P$. Vediamo che a_P appartiene a P , dal momento che non appartiene a nessun altro elemento di \mathcal{P} . Poniamo anche, sempre per ogni $P \in \mathcal{P}$, $b_P = \prod_{Q \in \hat{\mathcal{P}}_P} a_Q$; si ha $b_P \in A \cap Q$ per ogni $Q \in \hat{\mathcal{P}}_P$, ma $b_P \notin P$, perché P è primo e, per ogni $Q \in \hat{\mathcal{P}}_P$, $a_Q \notin P$. Sia ora $a = \sum_{P \in \mathcal{P}} b_P$. Ovviamente $a \in A$, quindi esiste $Q \in \mathcal{P}$ tale che $a \in Q$. Ma $b_P \in Q$ per ogni $P \in \hat{\mathcal{P}}_Q$ e $b_Q \notin Q$, questa è dunque una contraddizione. \square

Come chi legge già sa,¹ un ideale H di un anello commutativo R si dice *massimale* se è massimale nell’insieme degli ideali propri di R , ordinato per inclusione. È anche ben noto, dai corsi elementari di algebra, che se R è unitario, questo equivale a richiedere che R/H sia un campo. Una caratterizzazione degli ideali massimali che comprenda anche il caso non unitario è data da:

Lemma 3.8. *Sia H un ideale di un anello commutativo R . Sono allora equivalenti:*

- (i) $H \triangleleft R$;
- (ii) l’ R -premodulo R_R/H è semplice;
- (iii) si verifica una delle due:
 - a) R/H è un campo; oppure
 - b) $R^2 \subseteq H$ e $|R/H|$ è un numero primo.

Inoltre, se è verificata (iii.a) H è primo, se è verificata (iii.b) non lo è. Se R è unitario (iii.b) non si può verificare.

Dimostrazione. Che (i) e (ii) siano equivalenti e che (iii) implichi (ii) è ovvio. Supponiamo R_R/H semplice. Per la [Proposizione 1.23](#), o R_R/H è annullato da R (ovvero: $R^2 \subseteq H$) ed ha quindi ordine primo, oppure $H = \text{Ann}_R(R_R/H)$. In questo secondo caso, per ogni $a \in R \setminus H$ si ha $aR \not\subseteq H$, quindi $R = H + aR$, ovvero $R/H = (a+H)(R/H)$. Il [Lemma 3.4](#) mostra allora che R/H è un campo. È così provato che (iii) equivale a (i) e (ii). L’ultima annotazione è ovvia. \square

Dunque, *gli ideali massimali di un anello commutativo unitario sono tutti primi*, ma lo stesso non vale per anelli non unitari. Ad esempio, se R è un anello di cardinalità un numero primo e con moltiplicazione costante nulla, allora il suo ideale nullo è del tipo descritto in (iii.b), quindi è massimale ma non primo.

L’esempio degli ideali massimali in anelli commutativi unitari si generalizza in un lemma che fornisce un utilissimo metodo generale per la costruzione di ideali primi.

Lemma 3.9. *Sia R un anello commutativo; siano S una parte chiusa di (R, \cdot) e $H \triangleleft R$ tali che $S \cap H = \emptyset \neq S$. Allora l’insieme $\mathcal{S} = \{I \triangleleft R \mid I \supseteq H \wedge I \cap S = \emptyset\}$, ordinato per inclusione, è induttivo; ogni suo elemento massimale è un ideale primo di R .*

¹ la nozione, del resto, è stata già usata in queste note.

Dimostrazione. È chiaro che l'unione di una arbitraria catena non vuota di elementi di \mathcal{S} è in \mathcal{S} (certamente è un ideale, per il [Lemma 1.17](#)), quindi \mathcal{S} è induttivo. Sia P un suo elemento massimale. Dal momento che $P \cap S = \emptyset$, $P \subset R$. Se P non è primo esistono $I, J \triangleleft R$ tali che $IJ \subseteq P \subset I, J$. La massimalità di P in \mathcal{S} implica $I, J \notin \mathcal{S}$, dunque $I \cap S \neq \emptyset \neq J \cap S$. Siano $i \in I \cap S$ e $j \in J \cap S$. Allora $ij \in S$ ma, d'altra parte, $ij \in IJ \subseteq P$. Dunque $ij \in P \cap S$, contraddicendo così la scelta di P . Si conclude in questo modo che P è un ideale primo. \square

Ad esempio, se R è unitario, $S = \{1_R\}$ e $H = 0$, l'insieme \mathcal{S} descritto nell'enunciato è l'insieme degli ideali propri di R , quindi il lemma fornisce di nuovo l'informazione che R ha ideali massimali (il già menzionato teorema di Krull) e questi sono tutti primi.

Un'altra applicazione del [Lemma 3.9](#) è la seguente descrizione delle parti chiuse e sature di un anello in termini di ideali primi:

Lemma 3.10. *Sia R un anello commutativo e sia S una sua parte. Allora S è una parte chiusa e satura di (R, \cdot) se e solo se $R \setminus S$ è unione di ideali primi di R .*

Dimostrazione. Per ogni $P \in \text{Spec}(R)$, sappiamo che $R \setminus P$ è una parte chiusa di (R, \cdot) , ed è anche satura per l'[Esercizio 2.C.1](#). Sia $\emptyset \neq \mathcal{S} \subseteq \text{Spec}(R)$. Poiché ogni intersezione di parti chiuse e sature ha le stesse proprietà, $R \setminus \bigcup \mathcal{S} = \bigcap_{P \in \mathcal{S}} (R \setminus P)$ è una parte chiusa e satura di (R, \cdot) . Viceversa, sia S una parte chiusa e satura di (R, \cdot) . Per ogni $a \in R \setminus S$ si ha $aR \cap S = \emptyset$, dal momento che se esistesse $s \in aR \cap S$ allora a sarebbe un divisore di $s \in S$ e quindi appartenerrebbe ad S perché S è saturo. Possiamo allora utilizzare il [Lemma 3.9](#) per ottenere un ideale primo P_a disgiunto da S (quindi contenuto in $R \setminus S$) e contenente aR . Abbiamo $P_a \subset R$; scelto $r \in R \setminus P_a$ da $ar \in aR \subseteq P_a$ e $r \notin P_a$ deduciamo $a \in P_a$. A questo punto è chiaro che $R \setminus S = \bigcup \{P_a \mid a \in R \setminus S\}$. La dimostrazione è così completata. \square

Una caratterizzazione degli anelli fattoriali Si ricorda che gli anelli fattoriali sono, per definizione, i domini di integrità unitari R tali che $(R \setminus 0, \cdot)$ sia un monoide fattoriale. Una conseguenza del [Lemma 3.10](#) (e del [Lemma 2.10](#)) è la seguente caratterizzazione:

Lemma 3.11. *Sia R un dominio di integrità unitario. Allora R è un anello fattoriale se e solo se ogni suo ideale primo non nullo contiene un elemento primo non nullo.*

Dimostrazione. Supponiamo R fattoriale, e siano $0 \neq P \in \text{Spec}(R)$ e $0_R \neq a \in P$. Allora $a = p_1 p_2 \cdots p_r$ per opportuni $n \in \mathbb{N}^+$ ed elementi primi p_1, p_2, \dots, p_n di R . Poiché P è primo, da $p_1 p_2 \cdots p_n \in P$ segue che almeno uno dei p_i è contenuto in P . Questo prova che la condizione è necessaria.

Viceversa, assumiamo che ogni ideale primo non nullo di R contenga un primo non nullo. Per il [Lemma 2.10](#), gli elementi di R che siano invertibili oppure prodotti di primi non nulli costituiscono un sottomonoido saturo S di (R, \cdot) , dunque, come segue dal [Lemma 3.10](#), $R \setminus S$ è unione di ideali primi. Ma, per ipotesi, $S \cap P \neq \emptyset$ per ogni ideale primo non nullo di R ; di conseguenza $R \setminus S = \emptyset$. Questo significa che ogni elemento non nullo e non invertibile di R è prodotto di primi, vale a dire: R è fattoriale. \square

Corollario 3.12. *Sia P un elemento minimale (per inclusione) tra gli ideali primi non nulli di un anello fattoriale. Allora P è principale.*

Dimostrazione. Per il lemma precedente, P contiene un elemento primo non nullo p . Allora $0 \neq pR \in \text{Spec}(R)$ e quindi $pR = P$ per la minimalità di P . \square

Facciamo infine un'acceso alla *dimensione di Krull* di un anello commutativo unitario. Se R è un tale anello, si dice che R ha per dimensione di Krull un intero n (o, semplicemente, ha

dimensione n) se n è la massima lunghezza possibile per una catena di ideali primi di R , cioè, per essere più espliciti, se $n + 1$ è il massimo delle cardinalità degli insiemi di ideali primi di R che siano totalmente ordinati per inclusione.² Ad esempio, i campi hanno dimensione di Krull 0, l'anello degli interi ha dimensione 1, perché le catene di lunghezza massima di ideali primi in \mathbb{Z} sono quelle costituite dall'ideale nullo e da un ideale della forma $p\mathbb{Z}$, dove p è un numero primo.

Esercizi.

3.B.1. Per ogni intero n , l'insieme dei numeri interi coprimi con n è un sottomonoido saturo di (\mathbb{Z}, \cdot) . Interpretare questo fatto alla luce del [Lemma 3.10](#).

3.B.2. Siano R un anello commutativo, $H \triangleleft R$ e $P \in \text{Spec}(H)$. Verificare che $P^* = (P : H)_R \in \text{Spec}(R)$ e $P = R \cap P^*$.

3.B.3. Due risultati in teoria dei gruppi (il primo dei quali del tutto elementare, il secondo un poco meno) mostrano che un gruppo non può essere unione di due suoi sottogruppi propri e che se è unione di un numero finito di sottogruppi almeno uno di questi deve avere indice finito. Usare questi due fatti per estendere il [Lemma 3.7](#) in questi modi (in entrambi i casi \mathcal{P} è un insieme finito di ideali di R):

- vale la stessa conclusione del [Lemma 3.7](#) se l'ipotesi $\mathcal{P} \subseteq \text{Spec}(R)$ è sostituita dall'ipotesi che al massimo due ideali in \mathcal{P} non siano primi;
- vale la stessa conclusione del [Lemma 3.7](#) se l'ipotesi $\mathcal{P} \subseteq \text{Spec}(R)$ è sostituita dalle ipotesi che R sia unitario, $A \triangleleft R$ e valga una delle due: (a) R/M è infinito per ogni $M \triangleleft R$; (b) R contiene un campo infinito come sottoanello unitario.

Il primo enunciato si trova (all'incirca: lì gli anelli sono unitari) in Sharp, Theorem 3.61. A proposito del secondo si osservi che un anello unitario ha la proprietà che tutti i suoi ideali massimali abbiano indice infinito se ha un sottoanello unitario con questa proprietà. Dunque, la condizione in (a) è conseguenza di (b).

A questo proposito, partendo dal gruppo V_4 di Klein (il gruppo non ciclico di ordine 4), che è l'unione dei suoi tre sottogruppi non banali, mostrare che esiste un anello commutativo R che ha un campo infinito come sottoanello ed un ideale massimale che è unione di un numero finito di ideali propriamente contenuti in esso.

3.B.4. Dimostrare che l'intersezione di una catena di ideali primi in un anello commutativo è sempre un ideale primo.

Conseguenza di questo fatto è, ad esempio, che se R è un anello commutativo unitario e H è un suo ideale proprio, esiste sempre un ideale che sia minimale tra quelli primi contenenti H .

3.3 Nilradicale e radicale di Jacobson di un anello commutativo

3.3.1 Il nilradicale di un anello; varietà e radicale di un ideale

Un elemento a di un anello commutativo R si dice *nilpotente* se e solo se esiste $n \in \mathbb{N}^+$ tale che $a^n = 0_R$. Chiaramente 0_R è nilpotente e, se R non è l'anello nullo, ogni elemento nilpotente è un divisore dello zero, quindi in un dominio di integrità lo zero è l'unico elemento nilpotente. È possibile dimostrare per via diretta che gli elementi nilpotenti di un anello commutativo ne costituiscono un ideale (vedi [Esercizio 3.C.2](#)), ma lo si può fare in modo più efficiente (ed elegante) provando che questo insieme è precisamente l'intersezione degli ideali primi dell'anello

² tradizionalmente si chiama lunghezza di una catena finita il numero dei suoi elementi meno uno.

(con la consueta convenzione che questa intersezione sia l'intero anello se questo è privo di ideali primi).

Se R è un anello commutativo, si chiama *nilradicale* di R l'ideale

$$\text{NilRad}(R) := \bigcap (\{R\} \cup \text{Spec}(R)),$$

dunque $\text{NilRad}(R) = R$ se R non ha ideali primi, $\text{NilRad}(R) = \bigcap \text{Spec}(R)$ altrimenti.

Proposizione 3.13. *Se R è un anello commutativo, $\text{NilRad}(R)$ è l'insieme degli elementi nilpotenti di R .*

Dimostrazione. Sia a un elemento nilpotente di R e sia $P \in \text{Spec}(R)$. Esiste $n \in \mathbb{N}^+$ tale che $a^n = 0 \in P$; poiché P è primo questo implica $a \in P$. Dunque, ogni elemento nilpotente di R è in $\text{NilRad}(R)$.

Sia ora a un elemento non nilpotente di R . L'insieme $S = \{a^n \mid n \in \mathbb{N}^+\}$ delle potenze di a ad esponente positivo è ovviamente chiuso rispetto alla moltiplicazione; per la scelta di a si ha $0_R \notin S$. Possiamo dunque applicare il [Lemma 3.9](#) ad S e all'ideale nullo di R per ottenere un ideale primo P disgiunto da S (difatti, massimale tra gli ideali disgiunti da S). Dal momento che $a \in S$, abbiamo $a \notin P$; abbiamo così provato che $a \notin \bigcap \text{Spec}(R) = \text{NilRad}(R)$. La dimostrazione è completa. \square

Se poi H è un ideale dell'anello commutativo R , si chiama *varietà* di H , e si indica con $\text{Var } H$ o $\text{Var}_R(H)$, l'insieme degli ideali primi di R contenenti H . Se $H \subseteq I \triangleleft R$, allora I/H è primo se e solo se I è primo, dal momento che $(R/H)/(I/H) \simeq R/I$, quindi $\{P/H \mid P \in \text{Var } H\} = \text{Spec}(R/H)$. La [Proposizione 3.13](#) mostra dunque che l'intersezione tra (R) e gli ideali nella varietà di H è l'insieme degli $r \in R$ tali che $r + H$ sia un elemento nilpotente di R/H ; questo insieme è un ideale di R che si chiama *radicale* di H in R , indicato in genere con uno dei simboli \sqrt{H} , $\sqrt{(H)}$, $\sqrt[R]{H}$, $\text{Rad}_R H$. Dunque, il radicale di H in R è

$$\sqrt{H} = \bigcap (\{R\} \cup \text{Var}_R(H)) = \{r \in R \mid \exists n \in \mathbb{N} (r^n \in H)\};$$

vale a dire: $\sqrt{H}/H = \text{NilRad}(R/H)$. Ovviamente $\sqrt{0} = \text{NilRad } R$, e $\sqrt{P} = P$ per ogni ideale primo P .

Lemma 3.14. *Siano R un anello commutativo e $H, K \triangleleft R$. Allora:*

- (i) $H \subseteq K \Rightarrow \sqrt{H} \subseteq \sqrt{K}$;
- (ii) $\sqrt{H} \cap \sqrt{K} = \sqrt{HK} = \sqrt{H} \cap \sqrt{K}$;
- (iii) Se R è unitario, $\sqrt{H} = R \iff H = R$;

Dimostrazione. La (i) e la (iii) sono ovvie. Per provare la (ii), si osservi che da $HK \subseteq H \cap K$ segue $\sqrt{HK} \subseteq \sqrt{H \cap K} \subseteq \sqrt{H} \cap \sqrt{K}$, usando due volte la (i). Se poi $r \in \sqrt{H} \cap \sqrt{K}$, esistono $n, m \in \mathbb{N}$ tali che $r^n \in H$ e $r^m \in K$, quindi $r^{n+m} \in HK$ e $r \in \sqrt{HK}$; così anche la (ii) è dimostrata. \square

In generale, se H è un ideale di un anello commutativo R , non è detto che H contenga una potenza del suo radicale in R . Questo però accade in un importante caso particolare: quando \sqrt{H} è finitamente generato (o, più in generale, quando \sqrt{H}/H è finitamente generato). Estendendo agli ideali la terminologia utilizzata per gli elementi di un anello, si dice che un ideale I è *nilpotente* se e solo se $I^n = 0$ per un opportuno $n \in \mathbb{N}$.

Lemma 3.15. *Siano R un anello commutativo e $I \triangleleft R$. Se I è finitamente generato ed ogni suo elemento è nilpotente, allora I è nilpotente.*

Dimostrazione. Sia F un insieme finito di generatori di I . Per ogni $a \in F$ esiste $\lambda_a \in \mathbb{N}^+$ tale che $a^{\lambda_a} \in H$. Ogni elemento r di I è una combinazione lineare di elementi di F a coefficienti nell'anello accresciuto definito da R ; per ogni $n \in \mathbb{N}^+$, allora, r^n è una combinazione lineare di elementi della forma $\prod_{a \in F_0} a^{\mu_a}$, dove $F_0 \subseteq F$ e gli esponenti μ_a sono numeri interi positivi tali che $\sum_{a \in F} \mu_a = n$. Se n è scelto in modo che $n > \sum_{a \in F_0} (\lambda_a - 1)$, allora la condizione sugli interi μ_a assicura che $\mu_a \geq \lambda_a$, e quindi $a^{\mu_a} \in H$, per almeno un $a \in F$, dunque r^n . Ciò prova che, per ogni tale n , $I^n \subseteq H$. \square

Corollario 3.16. *Siano R un anello commutativo, H e J ideali di R tali che $H \subseteq J \subseteq \sqrt{H}$ e J/H è finitamente generato. Allora esiste $n \in \mathbb{N}^+$ tale che $J^n \subseteq H$.*

Dimostrazione. L'ideale $I := J/H$ di R/H è finitamente generato e costituito da elementi nilpotenti. Per il lemma precedente esiste allora $n \in \mathbb{N}^+$ tale che $I^n = 0$, ovvero $J^n \subseteq H$. \square

3.3.2 Il radicale di Jacobson

Il radicale di Jacobson³ di un anello commutativo R si indica con $\text{Jac}(R)$ ed è l'intersezione di tutti gli ideali massimali di R se R ha almeno un ideale massimale, R nel caso contrario. Dunque

$$\text{Jac}(R) = \bigcap \{H \mid H = R \vee H \triangleleft R\}.$$

Questo ideale ha una grande importanza nella teoria generale degli anelli commutativi (e lo stesso si può dire per il caso non commutativo); una ragione è quella indicata nell'Osservazione 3.C.12.

Nel caso in cui R sia unitario, $\text{Jac}(R)$ ha una descrizione piuttosto semplice. Per formularla, iniziamo a fare un'osservazione sull'unione degli ideali massimali. Come è ben noto, in un anello commutativo unitario R un elemento a è invertibile se e solo se aR (che è l'ideale generato da a) coincide con R . Dunque, a non è invertibile se e solo se a appartiene ad un ideale proprio di R . Ma, per il Corollario 1.19, in questo secondo caso a appartiene ad un ideale massimale di R . In definitiva, per ciascun $a \in R$ si verifica una ed una sola delle due: o a è invertibile, oppure $a \in M$ per qualche $M \triangleleft R$. Abbiamo così:

Lemma 3.17. *Sia R un anello commutativo unitario. Allora $\mathcal{U}(R) = R \setminus \bigcup \{M \mid M \triangleleft R\}$.*

Lemma 3.18. *Siano R un anello commutativo unitario, $a \in R$ e $M \triangleleft R$. Allora $a \in M$ se e solo se, per ogni $r \in R$ si ha $1_R - ar \notin M$.*

Dimostrazione. Se $a \in M$ e $r \in R$, allora $ar \in M$. Dal momento che $1_R \notin M$, allora $1_R - ar \notin M$. Sia invece $a \notin M$. Allora l'ideale generato da $M \cup \{a\}$, ovvero $M + aR$, coincide con R . Dunque $1_R = m + ar$ per opportuni $m \in M$ e $r \in R$ quindi $1_R - ar = m \in M$; ciò prova l'asserto. \square

Proposizione 3.19. *Sia R un anello commutativo unitario. Allora*

$$\text{Jac}(R) = \{a \in R \mid 1_R + aR \subseteq \mathcal{U}(R)\}.$$

Dimostrazione. Sia $a \in R$. Ovviamente $a \in \text{Jac}(R)$ se e solo se per ogni $M \triangleleft R$ si ha $a \in M$, cioè, per il Lemma 3.18, $(1_R + aR) \cap M = \emptyset$. Utilizzando anche il Lemma 3.17 otteniamo così che $a \in \text{Jac}(R)$ se e solo $1_R + aR \subseteq R \setminus \bigcup \{M \mid M \triangleleft R\} = \mathcal{U}(R)$. \square

Corollario 3.20. *Sia R un anello commutativo unitario. Allora per ogni $a \in \text{Jac}(R)$ si ha $|aR| \leq |\mathcal{U}(R)|$. In particolare:*

- (i) se $\mathcal{U}(R) = \{1_R\}$, allora $\text{Jac}(R) = 0$;
- (ii) se $\text{Jac}(R)$ contiene un elemento cancellabile in R , allora $|\mathcal{U}(R)| = |R|$;

³ che prende il nome da Nathan Jacobson (1910–1999).

(iii) se R è un dominio di integrità e $\text{Jac}(R) \neq 0$, allora $|\mathcal{U}(R)| = |R|$.

Dimostrazione. La prima parte dell'enunciato segue subito dalla [Proposizione 3.19](#), dal momento che $1+aR$ è equipotente ad aR . Se $0_R \neq a \in \text{Jac}(R)$, allora $|aR| > 1$ e, se a è cancellabile, $|aR| = |R|$. Da ciò e da quanto appena visto seguono (i) e (ii), da (ii) segue poi immediatamente (iii). \square

Una seconda caratterizzazione del radicale di Jacobson ha anche un corrispettivo debole per anelli non unitari; si vedano per questo l'[Esercizio 3.C.11](#) e anche l'[Osservazione 3.C.12](#):

Proposizione 3.21. *Sia R un anello commutativo unitario. Allora $\text{Jac}(R)$ è l'insieme di tutti gli $r \in R$ tali che $Mr = 0$ per ogni R -modulo semplice M .*

Dimostrazione. La [Proposizione 1.23](#) mostra che gli annullatori degli R -moduli semplici sono tutti e soli gli ideali massimali di R . Da ciò segue immediatamente l'asserto. \square

Nel caso degli anelli unitari, la comparazione tra il nilradicale ed il radicale di Jacobson fornisce:

Proposizione 3.22. *Sia R un anello commutativo unitario. Allora $\text{NilRad}(R) \subseteq \text{Jac}(R)$. Inoltre, per ogni $a, u \in R$, se a è nilpotente e u è invertibile, $a + u$ è invertibile.*

Dimostrazione. L'inclusione $\text{NilRad}(R) \subseteq \text{Jac}(R)$ è immediata dalle definizioni, dal momento che gli ideali massimali di R sono tutti primi. Se a e u sono come all'enunciato, $a \in \text{NilRad}(R) \subseteq \text{Jac}(R)$ ([Proposizione 3.13](#)), mentre $u \notin V := \bigcup \{M \mid M \triangleleft R\}$; di conseguenza, per ogni $M \triangleleft R$, si ha $a + u \notin M$. Allora $a + u \notin V$ e quindi $a + u \in \mathcal{U}(R)$ per il [Lemma 3.17](#). \square

Anelli locali Chiamiamo *anello locale* un anello commutativo unitario che abbia esattamente un ideale massimale, cioè tale che il suo radicale di Jacobson sia un ideale massimale⁴. Dal [Lemma 3.17](#) si ricava immediatamente:

Corollario 3.23. *Sia R un anello commutativo unitario. Allora R è locale se e solo se $R \setminus \mathcal{U}(R)$ è un ideale di R . Se ciò accade, questo è l'ideale massimale di R .*

Sono ovviamente anelli locali i campi (sono quelli con 0 come ideale massimale). Un altro esempio interessante è, per ogni numero primo p , quello del sottoanello

$$\mathbb{Q}_{p'} = \{a/b \mid a \in \mathbb{Z} \wedge b \in \mathbb{Z} \setminus p\mathbb{Z}\}$$

del campo razionale, costituito da quei numeri razionali che, rappresentati come frazione ridotta, hanno denominatore non divisibile per p . È facile vedere che questo insieme forma effettivamente un sottoanello (per giunta unitario) di \mathbb{Q} i cui elementi non invertibili sono i multipli di p , quindi l'ideale massimale di $\mathbb{Q}_{p'}$ è $p\mathbb{Q}_{p'}$. Questo esempio ritornerà a più riprese in queste note, venendo tra l'altro discusso in maggior dettaglio [in uno dei prossimi capitoli](#) nel contesto di una procedura per costruire in modo sistematico anelli locali.

⁴ alcuni autori, tra i quali Sharp, richiedono in aggiunta che l'anello sia noetheriano e chiamano semilocali gli anelli che abbiamo chiamato locali.

Esempi, osservazioni, esercizi.

3.C.1. Per ogni intero positivo n , descrivere il nilradicale ed il radicale di Jacobson di \mathbb{Z}_n . Per quale motivo coincidono?

3.C.2. Sia R un anello commutativo. Provare per via diretta (senza usare la [Proposizione 3.13](#)) che l'insieme degli elementi nilpotenti di R costituisce un ideale (l'unica cosa non del tutto ovvia da provare è che la somma di due elementi nilpotenti è sempre nilpotente)

Similmente, se R è unitario, a è un elemento nilpotente di R e $u \in \mathcal{U}(R)$, provare che $a + u$ è invertibile, descrivendone l'inverso e senza usare la [Proposizione 3.22](#).

3.C.3. Verificare che se R , e S sono anelli commutativi, $H \triangleleft R$ e $\alpha: R \rightarrow S$ è un omomorfismo, in S si ha $(\sqrt{H})^{\overline{\alpha}} \subseteq \sqrt{H^{\overline{\alpha}}}$. In particolare, $(\sqrt{H} + I)/I \subseteq \sqrt{(H + I)/I}$ per ogni $I \triangleleft R$. L'uguaglianza non vale, in generale (si consideri ad esempio il caso $R = \mathbb{Z}$, $H = 0$ e $I = 4\mathbb{Z}$), ma vale se $I \subseteq H$.

3.C.4. In relazione al [Lemma 3.14](#), provare che, se H e K sono ideali di uno stesso anello commutativo R , si ha $\sqrt{H + K} = \sqrt{(\sqrt{H} + \sqrt{K})}$, ma non necessariamente $\sqrt{H + K} = \sqrt{H} + \sqrt{K}$ né $\sqrt{HK} = \sqrt{H}\sqrt{K}$. (Suggerimento per la seconda parte: per l'affermazione su $\sqrt{H + K}$ si considerino un campo F , il suo anello di polinomi $F[x, y, z]$ (gli anelli di polinomi verranno discussi [più avanti](#) in queste note) e il quoziente $R = F[x, y, z]/(x + y - z^2)$; per l'affermazione che riguarda il radicale di un prodotto si cerchi un anello commutativo il cui nilradicale N verifichi $N^2 = 0 \neq N$.)

3.C.5. Siano R un anello commutativo e P un suo ideale primo. Verificare che per ogni $n \in \mathbb{N}^+$ si ha $P = \sqrt{P^n}$.

3.C.6. L'applicazione che ad ogni ideale di un anello commutativo R associa il suo radicale è un operatore di chiusura nel reticolo degli ideali di R , nel senso che è crescente, estensiva ($H \subseteq \sqrt{H}$ per ogni $H \triangleleft R$) e idempotente ($\sqrt{(\sqrt{H})} = \sqrt{H}$ per ogni $H \triangleleft R$).

3.C.7. Verificare in dettaglio quanto asserito a proposito dell'anello locale \mathbb{Q}_p dei razionali a denominatore coprimo col primo p . Generalizzando una delle sue proprietà, verificare che se R è un anello fattoriale che non sia un campo ed in cui tutti gli elementi irriducibili sono associati tra loro, allora R è locale e il suo ideale massimale è pR , dove p è un elemento irriducibile di R .

3.C.8. In un anello commutativo unitario si può avere $\text{NilRad}(R) \subset \text{Jac}(R)$. ad esempio, questo accade se R è un dominio di integrità locale che non sia un campo, come l'anello \mathbb{Q}_p presentato in questa sezione. Per un tale R sia ha infatti $\text{NilRad}(R) = 0$, mentre $\text{Jac}(R)$ è l'ideale massimale di R , che non è l'ideale nullo perché R non è un campo.

Se R è un anello con prodotto costante nullo, $R = \text{NilRad}(R)$. Se R è finito e non nullo, certamente R ha ideali massimali (i sottogruppi massimali di $(R, +)$) e quindi $\text{Jac}(R) \subset \text{NilRad}(R)$.

3.C.9. Sia R un anello commutativo unitario e supponiamo $R = N + S$, dove N è un ideale di R contenuto in $\text{NilRad}(R)$ e S è un sottoanello unitario di R . Allora $\text{Jac} R = N + \text{Jac}(S)$; dimostrarlo.

3.C.10. Il [Corollario 3.20](#) può essere in certi casi usato per dimostrare che un anello commutativo unitario ha radicale di Jacobson nullo. Esempi di anelli per i quali l'ipotesi in (i) (l'unico elemento invertibile è l'unità) è verificata sono l'anello delle parti di un qualsiasi insieme e, come seguirà dalla [Proposizione 5.10](#), gli anelli di polinomi su di esso. I domini di integrità con un numero finito di elementi invertibili hanno anch'essi radicale di Jacobson nullo: quelli finiti perché sono campi, quelli infiniti (come \mathbb{Z} o gli anelli di polinomi su \mathbb{Z}) per via della (iii) in [Corollario 3.20](#).

3.C.11. Estendere la [Proposizione 3.21](#) provando quanto segue. Siano R un anello commutativo e \mathcal{M} l'insieme dei suoi ideali massimali primi, dunque $\mathcal{M} = \{H \mid R^2 \not\subseteq H \triangleleft R\}$ e $J = \bigcap(\{R\} \cup \mathcal{M})$. Allora J è l'insieme degli elementi di R che annullano ogni R -premodulo

semplice.

Notare che questo vale anche se R è unitario, nel qual caso $J = \text{Jac}(R)$.

Aggiungiamo che alcuni autori propongono una definizione di premodulo semplice diversa dalla definizione standard qui adottata, richiedendo che i premoduli per essere semplici non debbano essere annullati dall'intero anello degli scalari. Per chi assume questa definizione, anche nel caso in cui R non sia unitario l'insieme degli elementi di R che annullano ogni R -premodulo semplice è $\text{Jac}(R)$.

3.C.12. Gli R -(pre)moduli semplici, o più in generale *semisemplici* (cioè generati da (pre)moduli semplici) hanno una grande importanza nella teoria generale degli R -(pre)moduli. Segue dall'esercizio precedente che il radicale di Jacobson di un anello commutativo R annulla tutti gli R -(pre)moduli semisemplici. Questo mostra che la teoria degli R -(pre)moduli semisemplici si riduce a quella dei (pre)moduli semisemplici su $R/\text{Jac}(R)$.

3.3.3 Versioni del Lemma di Nakayama

Al radicale di Jacobson di un anello commutativo è associato questo risultato, noto come lemma di Nakayama, che è una versione debole del [Corollario 1.18](#):

Lemma 3.24 (Lemma di Nakayama). *Siano R un anello commutativo, $J = \text{Jac}(R)$ e M un R -(pre)modulo finitamente generato. Allora $MJ = M$ se e solo se $M = 0$.*

Dimostrazione. Se $M = 0$, ovviamente $MJ = M$. Se invece $M \neq 0$, allora M ha un sotto(pre)modulo massimale N . Ovviamente M/N è semplice, quindi annullato da J , per la [Proposizione 1.23](#) (si veda anche l'[Osservazione 3.C.12](#)). Questo significa che $MJ \subseteq N$, quindi $MJ \neq M$. \square

Corollario 3.25. *Siano R un anello commutativo, $J = \text{Jac}(R)$, M un R -(pre)modulo finitamente generato e $N \leq_R M$. Se $M = N + MJ$, allora $N = M$.*

Dimostrazione. Basta applicare il [Lemma 3.24](#) al (pre)modulo M/N . \square

Una versione più forte del lemma di Nakayama, spesso associata ai nomi di Nakayama, Azumaya e Krull e talvolta chiamato quindi 'lemma NAK' (ma spesso anch'esso lemma di Nakayama) è data dal [Lemma 3.27](#). Per dimostrarla, iniziamo con semplice lemma:

Lemma 3.26. *Siano M un premodulo sull'anello commutativo R , $a \in M$ e $H, K \triangleleft R$. Allora $aH \subseteq aK$ se e solo se $H \subseteq K + \text{Ann}_R(a)$.*

Dimostrazione. Se $H \subseteq K + \text{Ann}_R(a)$, è ovvio che $aH \subseteq a(K + \text{Ann}_R(a)) = aK$. Viceversa, se $aH \subseteq aK$, per ogni $h \in H$ esiste $k \in K$ tale che $ah = ak$, quindi $a(h - k) = 0_M$, dunque $h - k \in \text{Ann}_R(a)$ e $h = k + (h - k) \in K + \text{Ann}_R(a)$. \square

Lemma 3.27 (NAK). *Sia M un premodulo finitamente generato sull'anello commutativo R . Sia $H \triangleleft R$. Sono allora equivalenti:*

- (i) $MH = M$;
- (ii) esiste $h \in H$ tale che $ah = a$ per ogni $a \in M$.

Inoltre, (i) implica:

- (iii) $R = H + \text{Ann}_R(M)$.

e, se R è unitario e M è un R -modulo, (iii) implica (i)

Dimostrazione. È ovvio che (i) segue da (ii) e, se M è un R -modulo e quindi $MR = M$, anche da (iii). Vanno dimostrate le implicazioni (i) \Rightarrow (iii) e (i) \Rightarrow (ii). Iniziamo a farlo nel caso in cui R sia unitario e M sia un R -modulo. Supponiamo $MH = M$; vogliamo provare che vale la (iii). Sia X un insieme finito di generatori di M e ragioniamo per induzione su $|X|$. La (iii) è banalmente vera se $X = \emptyset$; possiamo allora assumere $|X| > 0$ e che l'implicazione (i) \Rightarrow (iii) valga se M è sostituito da un modulo generato da un insieme di cardinalità minore di $|X|$. Fissiamo $a \in X$, e sia \bar{M} il modulo quoziente M/aR . Poniamo anche $I = \text{Ann}_R(\bar{M})$ e $J = \text{Ann}_R(a)$. Si ha $MI \subseteq aR$ e $aRJ = aJ = 0$, quindi $MIJ = 0$, ovvero $IJ \subseteq \text{Ann}_R(M)$. Dovrebbe essere chiaro che $\bar{M}H = \bar{M}$ e che \bar{M} è generato da $\{x + aR \mid x \in X \setminus \{a\}\}$, che ha cardinalità minore di $|X|$, quindi, per l'assunzione fatta, $R = H + I$. Da $MI \subseteq aR$ otteniamo anche $MIH \subseteq aRH$, ovvero $MI \subseteq aH$ (ricordiamo: $MH = M$), quindi $aI \subseteq aH$. Dal [Lemma 3.26](#) segue $I \subseteq H + J$, quindi $R = H + I$ comporta $R = H + J$. A questo punto possiamo applicare il [Lemma 3.2](#) per concludere che H è comassimale con IJ , ma, come avevamo visto, $IJ \subseteq \text{Ann}_R(M)$, dunque $R = H + IJ = H + \text{Ann}_R(M)$ e vale la (iii). Ora, sempre nell'ipotesi che M sia un R -modulo, la (iii) implica $1_R \in H + \text{Ann}_R(M)$, quindi esistono $h \in H$ e $k \in \text{Ann}_R(M)$ tali che $h + k = 1_R$, dunque per ogni $a \in M$ si ha $ah = a(1_R - k) = a - ak = a$ e vale la (ii).

Passiamo ora al caso generale rimuovendo l'ipotesi che M sia un modulo e assumendo semplicemente che M sia un premodulo finitamente generato per il quale valga (i). Sia R_1 l'anello accresciuto definito da R e riguardiamo M come R_1 -modulo in accordo con il [Corollario 1.30](#). Anche come R_1 -modulo M è finitamente generato. Dal momento che H è un ideale anche di R_1 , per il caso precedente da $MH = M$ deduciamo che continua a valere (ii) e che $R_1 = H + \text{Ann}_{R_1}(M)$. Da quest'ultima, utilizzando la legge dei Dedekind ([Lemma 1.8](#)), otteniamo $R = R_1 \cap R = H + (\text{Ann}_{R_1}(M) \cap R) = H + \text{Ann}_R(M)$, ovvero la (iii). A questo punto la dimostrazione è completa. \square

Corollario 3.28. *Sia M un premodulo fedele finitamente generato sull'anello commutativo R . Sia H un ideale proprio di R . Allora $MH \neq M$.*

Esempi, osservazioni, esercizi.

3.D.1. Si mostri con un esempio che, nella situazione del [Lemma 3.27](#), se M non è un modulo su R , è possibile che, per ogni ideale H di R , valga la (iii) ma non la (i).

3.D.2. La dimostrazione del lemma di Nakayama ([Lemma 3.24](#)) che abbiamo fornito prova, in effetti, questo: se M è un (pre)modulo finitamente generato e non nullo su un anello commutativo R , allora esiste $H \triangleleft R$ tale che $H = R$ o $H \triangleleft R$ tale che $MH \neq M$.

3.D.3. Le dimostrazioni qui fornite per i lemmi [3.24](#) e [3.27](#) sono tra loro indipendenti, ma in realtà è piuttosto facile (quasi immediato nel caso dei moduli) provare il primo come conseguenza del secondo. Quindi, in senso stretto, non sarebbe stato necessario fornire la dimostrazione del [Lemma 3.24](#). Lo si è fatto comunque perché la dimostrazione supplementare è molto semplice ed illustra un'idea utile anche in altre situazioni.

3.D.4. Nelle varie versioni del lemma di Nakayama, incluso il [Corollario 1.18](#), l'ipotesi che il (pre)modulo coinvolto sia finitamente generato è essenziale. Ad esempio, se M è il gruppo additivo dei razionali, visto come \mathbb{Z} -modulo, allora M è fedele e non ha sottomoduli massimali, come è facile verificare, e per ogni ideale non nullo H di \mathbb{Z} si ha $MH = M$.

3.D.5. Chi ha studiato un po' di teoria dei gruppi oltre il contenuto dei corsi del primo anno potrebbe aver incontrato la nozione di sottogruppo di Frattini, l'intersezione tra i sottogruppi massimali di un gruppo, che è in qualche senso l'analogo grupitale del radicale di Jacobson (ma il sottogruppo di Frattini è storicamente di molto precedente). Chi ha anche qualche familiarità con l'argomento di Frattini potrebbe aver riconosciuto nel [Lemma 3.26](#) una semplice variante di questa idea.

3.D.6. Enunciati e dimostrazioni del lemma NAK e di quello che lo precede possono essere almeno in parte riformulate in termini di azioni e di omomorfismi. Ad esempio, il [Lemma 3.26](#) esprime di fatto una proprietà elementare dell'omomorfismo di gruppi $r \in R \mapsto ar \in R$, mentre la (ii) del [Lemma 3.27](#) si potrebbe enunciare in termini dell'azione di premodulo $\zeta: R \rightarrow \text{End}_Z(M)$: esiste $h \in H$ tale che $h^\zeta = \text{id}_M$.

3.D.7. Come nel caso del [Corollario 1.18](#), anche per i lemmi [3.24](#) e [3.27](#) ed i loro corollari l'ipotesi che M sia finitamente generato non può essere rimossa. Ad esempio, ponendo $R = \mathbb{Z}$, e scegliendo come M il gruppo additivo dei razionali (o, in alternativa, qualsiasi gruppo abeliano divisibile non identico), si ha che M è fedele e $MH = H$ per ogni ideale non nullo H di R .

3.4 Divisibilità e ideali in anelli unitari

Sia R un anello commutativo unitario non nullo; indichiamo con $\mathfrak{I}_P(R)$ l'insieme degli ideali principali di R , ordinato per inclusione. Consideriamo l'applicazione $\varphi: a \in R \mapsto aR \in \mathfrak{I}_P(R)$. Chiaramente φ è suriettiva. Inoltre, se a e b sono in R , si ha $aR = bR$ se e solo se $a \sim_R b$, cioè se e solo se a e b sono associati nel monoide moltiplicativo di R . In altri termini, il nucleo di equivalenza di φ è la relazione \sim_R , dunque φ induce un'applicazione biettiva

$$\tilde{\varphi}: \tilde{a} \in \tilde{R} \mapsto aR \in \mathfrak{I}_P(R),$$

dove abbiamo posto (come faremo d'ora in poi) $\tilde{R} = R/\sim_R$, quoziente del monoide moltiplicativo di R . È anche chiaro che sia $\tilde{\varphi}$ che la sua inversa sono (strettamente) decrescenti, vale a dire: φ è un anti-isomorfismo da \tilde{R} (insieme ordinato per divisibilità) a $\mathfrak{I}_P(R)$, ordinato per inclusione.

Questo anti-isomorfismo permette di stabilire una connessione tra proprietà di ideali (principali) in anelli commutativi unitari e proprietà relative alla divisibilità nei corrispondenti monoidi moltiplicativi. Ad esempio, con le notazioni fissate nel paragrafo precedente, un elemento $a \in R$ è irriducibile (si intende: in (R, \cdot)) se e solo se \tilde{a} è minimale tra gli elementi diversi da $\tilde{1}$ in \tilde{R} , quindi se e solo se $(\tilde{a})^{\tilde{\varphi}}$, ovvero aR , è massimale tra gli ideali principali diversi da $(\tilde{1})^{\tilde{\varphi}} = R$. Dunque, per ogni $a \in R$,

$$a \text{ è irriducibile in } R \iff aR \text{ è massimale tra gli ideali principali propri di } R$$

A titolo di comparazione, è di verifica più o meno immediata che

$$a \text{ è primo in } R \iff aR \text{ è un ideale primo di } R.$$

Un'applicazione piuttosto elegante dell'anti-isomorfismo φ e di quanto visto nella [sezione 2.2](#) permette di ricavare immediatamente alcuni risultati elementari sugli anelli principali, vediamo come.

Se R è un dominio di integrità unitario, $R^* = R \setminus 0$ è un sottomonoido moltiplicativo di R ed è cancellativo, e \tilde{R}^* risulta anti-isomorfo, come insieme ordinato, all'insieme $\mathfrak{I}_P^*(R)$ degli ideali principali non nulli di R . Se R è anche principale, $\mathfrak{I}_P^*(R)$ è l'insieme degli ideali non nulli di R , che è un sottoreticolo di $\mathfrak{I}(R)$ (perché l'intersezione tra due ideali non nulli è certamente non nulla). Un risultato elementare che incontreremo più avanti ([Proposizione 6.8](#)) mostra che R è noetheriano, cioè che $\mathfrak{I}(R)$ verifica la condizione massimale, quindi $\mathfrak{I}_P^*(R)$ è un reticolo a condizione massimale; di conseguenza \tilde{R}^* (anti-isomorfo a $\mathfrak{I}_P^*(R)$) è un reticolo a condizione minimale. Per il [Teorema 2.5](#), allora R^* è un monoide fattoriale; il che, ricordiamo, significa che R è un anello fattoriale. Dunque, otteniamo una rapida dimostrazione del fatto che *ogni anello principale è fattoriale*. Inoltre, dal fatto che per elementi non nulli di R le proprietà di essere

primo e di essere irriducibile sono equivalenti, osservazioni fatte [poco sopra](#) garantiscono che gli ideali primi non nulli in un anello principale sono necessariamente massimali (vale a dire: *gli anelli principali hanno dimensione di Krull al più 1*).

Anche il teorema di Bézout e le sue varianti possono essere ottenuti in modo simile. Siano a e b elementi di un anello commutativo unitario R . Poiché gli anti-isomorfismi tra insiemi ordinati mandano eventuali estremi inferiori in estremi superiori (e viceversa), per ogni $d \in R$ si ha $\tilde{d} = \tilde{a} \wedge \tilde{b}$ se e solo se dR è estremo superiore di aR e bR in $\mathfrak{I}_P(R)$, vale a dire: il minimo (rispetto all'inclusione) tra gli ideali principali di R contenenti aR e bR , cioè contenenti $aR + bR$. Dualmente, un $m \in R$ sarà un mcm tra a e b se e solo se mR è il massimo ideale principale contenuto in $aR \cap bR$. In particolare, per ogni $a, b \in R$:

se $aR + bR$ è principale, allora i suoi generatori sono tutti e soli i MCD tra a e b in R ; (B)

se $aR \cap bR$ è principale, allora i suoi generatori sono tutti e soli i mcm tra a e b in R . (\hat{B})

Il primo enunciato, (B) è una delle tante versioni del *Teorema di Bézout*. Questo ed il suo duale (\hat{B}) si possono senz'altro applicare nel caso in cui R sia un anello principale, perché in questo caso l'ipotesi sull'ideale $aR + bR$ o $aR \cap bR$ è banalmente verificata. Per quanto riguarda (B) , lo stesso vale nel caso in cui ogni ideale finitamente generato di R sia principale. I domini di integrità unitari con questa proprietà si chiamano *anelli di Bézout* e verranno brevemente discussi nella [sezione 10.2](#).

4 Costruzioni per moduli e per anelli

In questo capitolo descriveremo delle costruzioni standard, alcune delle quali dovrebbero essere sostanzialmente già note a chi legge

4.1 Prodotti e somme dirette di moduli

Prodotti diretti Siano R un anello commutativo e $(M_i)_{i \in I}$ una famiglia di R -(pre)moduli. Si definiscono un'operazione binaria interna $+$ nel prodotto cartesiano $C = \text{Cr}_{i \in I} M_i$ ed un'operazione esterna $C \times R \rightarrow C$ ponendo, per ogni $a = (a_i)_{i \in I}, b = (b_i)_{i \in I} \in C$ e $r \in R$,

$$a + b = (a_i + b_i)_{i \in I} \quad \text{e} \quad ar = (a_i r)_{i \in I}$$

(come al solito, abbiamo usato lo stesso simbolo $+$ tutte le operazioni binarie interne che appaiono e lo stesso simbolo, peraltro omesso, per quelle esterne. Queste operazioni su C sono, come si dice, definite componente per componente). È del tutto ovvio che in questo modo risulta definita su C una struttura di R -(pre)modulo che si chiama il *prodotto diretto* (esterno) della famiglia $(M_i)_{i \in I}$ e si indica come $\prod_{i \in I} M_i$.

Con il prodotto diretto sono poi definite due famiglie di omomorfismi $(\pi_i)_{i \in I}$ e $(\mu_i)_{i \in I}$. Per ogni $i \in I$,

$$\pi_i: (a_j)_{j \in I} \in \prod_{j \in I} M_j \mapsto a_i \in M_i$$

è l'applicazione (nota come proiezione i -esima) che ad ogni elemento del prodotto cartesiano associa la sua i -esima componente (in M_i); evidentemente π è un epimorfismo di R -(pre)moduli. L'applicazione $\mu_i: M_i \rightarrow \prod_{j \in I} M_j$ (chiamata talvolta monomorfismo canonico) associa ad ogni $x \in M_i$ la famiglia che ha x come componente i -esima e, per ogni $j \in I \setminus \{i\}$, 0_{M_j} come componente j -esima; μ_i è un monomorfismo di R -(pre)moduli. Per ogni $i \in I$ si ha, come si vede facilmente, $\mu_i \pi_i = \text{id}_{M_i}$. Se poniamo $M_i^* = \text{im } \mu_i$ e $\hat{M}_i^* = \ker \pi_i$, abbiamo, utilizzando il primo teorema di omomorfismo, $M_i^* \simeq M_i \simeq (\prod_{i \in I} M_i) / \hat{M}_i^*$. Naturalmente \hat{M}_i^* è il sotto(pre)modulo di $\prod_{i \in I} M_i$ costituito dalle famiglie con componente i -esima nulla, mentre M_i^* è costituito dalle famiglie con componente j -esima nulla per ogni $j \in I \setminus \{i\}$, vale a dire $M_i^* = \bigcap \{\hat{M}_j^* \mid i \neq j \in I\}$.

Somme dirette Proseguendo con le stesse notazioni, per ogni $a = (a_i)_{i \in I} \in \prod_{i \in I} M_i$, il *supporto* di a è l'insieme $\text{supp}(a) = \{i \in I \mid a_i \neq 0_{M_i}\}$. Ovviamente $\text{supp}(a + b) \subseteq \text{supp}(a) \cup \text{supp}(b)$ e $\text{supp}(ar) \subseteq \text{supp}(a)$ per ogni $a, b \in C$ e $r \in R$, ne segue che l'insieme D costituito dalle famiglie in C di supporto finito forma un R -sotto(pre)modulo di C , noto come la *somma diretta esterna* $\prod_{i \in I} M_i$ della famiglia $(M_i)_{i \in I}$. Nel caso in cui I sia finito, ovviamente $\prod_{i \in I} M_i = \prod_{i \in I} M_i$.

Evidentemente $M_j^* \leq \prod_{i \in I} M_i$ per ogni $j \in I$. D'altra parte, per ogni $a = (a_i)_{i \in I} \in \prod_{i \in I} M_i$ si ha $a = \sum_{i \in I} a_i^{\mu_i}$, dove la somma a secondo membro ha senso perché, anche nel caso in cui I sia infinito, gli addendi non nulli sono comunque in numero finito. Di conseguenza $\prod_{i \in I} M_i = \sum_{i \in I} M_i^*$. Si usa chiamare monomorfismi canonici anche le ridotte a $\prod_{i \in I} M_i$ dei monomorfismi canonici $\mu_i: M_i \rightarrow \prod_{i \in I} M_i$, cioè i monomorfismi $a \in M_i \mapsto a^{\mu_i} \in \prod_{i \in I} M_i$.

Osserviamo anche che, per ogni $i \in I$, la restrizione di π_i a $\prod_{i \in I} M_i$ è suriettiva, quindi in aggiunta a quanto visto sopra, $M_i \simeq (\prod_{i \in I} M_i) / (\hat{M}_i^* \cap \prod_{i \in I} M_i)$.

Somme dirette interne Supponiamo ora che $(M_i)_{i \in I}$ sia una famiglia di sotto(pre)moduli di un R -(pre)modulo M . Si dice che M è *somma diretta interna* della famiglia $(M_i)_{i \in I}$, e si scrive in questo caso $M = \bigoplus_{i \in I} M_i$, se e solo se:

- $M = \sum_{i \in I} M_i$, e
- per ogni $i \in I$ si ha $M_i \cap \sum_{i \neq j \in I} M_j = 0$.

Notiamo che richiedere queste due condizioni equivale a richiedere che il gruppo additivo di M sia somma diretta dei gruppi additivi degli M_i . L'informazione aggiuntiva che qui appare in premessa è che gli M_i non sono solo sottogruppi, ma R -sotto(pre)moduli di M .

Le somme dirette esterne sono esempi di somme dirette interne. Infatti, da quanto visto sopra segue facilmente che, per un'arbitraria famiglia $(A_i)_{i \in I}$ di (pre)moduli, si ha

$$\prod_{i \in I} A_i = \bigoplus_{i \in I} A_i^*,$$

dove, con notazione analoga a quelle usate in precedenza, le A_i^* sono le immagini dei monomorfismi canonici. Vale, in sostanza, anche il viceversa, la qual cosa ci permette di considerare interscambiabili le nozioni di somma diretta interna e di somma diretta esterna:

Proposizione 4.1. *Siano R un anello commutativo e $(M_i)_{i \in I}$ una famiglia di sotto(pre)moduli di un R -(pre)modulo M . Sono allora equivalenti:*

- (i) $M = \bigoplus_{i \in I} M_i$;
- (ii) $M = \sum_{i \in I} M_i$ e, scelti comunque una parte finita J di I e, per ogni $i \in J$, un elemento $a_i \in M_i$ in modo che $\sum_{i \in J} a_i = 0_M$, allora $a_i = 0_M$ per ogni $i \in J$;
- (iii) l'applicazione $\varphi: (a_i)_{i \in I} \in \prod_{i \in I} M_i \mapsto \sum_{i \in I} a_i \in M$ è un R -isomorfismo.

Dimostrazione. Supponiamo $M = \bigoplus_{i \in I} M_i$. Allora, per definizione, $M = \sum_{i \in I} M_i$; se J e gli elementi a_i , al variare di i in J sono scelti come in (ii), per ogni tale i si ha $a_i = -\sum_{i \neq j \in I} a_j \in M_i \cap \sum_{i \neq j \in I} M_j = 0$, quindi $a_i = 0_M$, dunque vale la (ii). Supponiamo ora che valga (ii). È evidente che φ , come definita in (iii), è un R -omomorfismo, il fatto che valga $M = \sum_{i \in I} M_i$ garantisce che φ è suriettiva, l'altra condizione in (ii) fornisce $\ker \varphi = 0$. Dunque, φ è un isomorfismo e vale (iii). Infine, assumiamo (iii). Chiamando, come sopra, per ogni $i \in I$, M_i^* l'immagine dell' i -esimo omomorfismo canonico, sappiamo che $\prod_{i \in I} M_i = \bigoplus_{i \in I} M_i^*$, ed è anche evidente che, per ogni $i \in I$, M_i è l'immagine di M_i^* mediante l'isomorfismo φ , da ciò segue facilmente $M = \bigoplus_{i \in I} M_i$. \square

Un'ultima, si immagina non sorprendente, annotazione: come in situazioni analoghe, i simboli \prod e \bigoplus vengono talvolta (soprattutto in relazione a famiglie finite) sostituiti dai corrispondenti simboli \times e \oplus in notazione infissa; ad esempio $M_1 \times M_2$ per $\prod_{i \in \{1,2\}} M_i$ e $M_1 \oplus M_2 \oplus M_3$ per $\bigoplus_{i \in \{1,2,3\}} M_i$, che si scrive anche $\bigoplus_{i=1}^3 M_i$. La stessa avvertenza si applica a situazioni analoghe che incontreremo per altre nozioni di prodotto o somma diretta.

Esercizi.

4.A.1. Siano R un anello commutativo, $(M_i)_{i \in I}$ una famiglia di R -(pre)moduli, J una partizione di I . Verificare che $\prod_{i \in I} M_i \simeq \prod_{J \in \mathcal{J}} \prod_{i \in J} M_i$ e $\prod_{i \in I} M_i \simeq \prod_{J \in \mathcal{J}} \prod_{i \in J} M_i$.

4.A.2. Siano R e $(M_i)_{i \in I}$ come nell'esercizio precedente, e sia, per ogni $i \in I$ $N_i \leq_R M_i$. Verificare che $(\prod_{i \in I} M_i) / (\prod_{i \in I} N_i) \simeq \prod_{i \in I} M_i / N_i$ e $(\prod_{i \in I} M_i) / (\prod_{i \in I} N_i) \simeq \prod_{i \in I} M_i / N_i$.

4.A.3. Prodotti e somme dirette della stessa famiglia di moduli possono essere molto diversi tra loro. Ad esempio, considerati i gruppi ciclici $(\mathbb{Z}_n, +)$ come moduli su \mathbb{Z} , $\prod_{n \in \mathbb{N}} \mathbb{Z}_n$ è un gruppo numerabile periodico, $\prod_{n \in \mathbb{N}} \mathbb{Z}_n$ non è né numerabile né periodico.

4.2 Prodotti e somme dirette di anelli e algebre

Le definizioni di prodotti diretti e somme dirette per anelli sono simili a quelle date per (pre)moduli. Il prodotto diretto $\prod_{i \in I} R_i$ di una famiglia $(R_i)_{i \in I}$ di anelli ha per sostegno il prodotto cartesiano della famiglia e operazioni binarie definite ‘componente per componente’. Che quello così ottenuto sia un anello è molto facile da verificare, così come il fatto che $\prod_{i \in I} R_i$ è commutativo se e solo se ciascuno degli R_i è commutativo, unitario se e solo se ciascuno degli R_i è unitario; chiaramente lo zero di questo anello è la famiglia $(0_{R_i})_{i \in I}$ e, qualora esista, l’unità è $(1_{R_i})_{i \in I}$. Se $\prod_{i \in I} R_i$ è unitario si ha anche $\mathcal{U}(\prod_{i \in I} R_i) = \prod_{i \in I} \mathcal{U}(R_i)$, dove il prodotto a secondo membro è un prodotto diretto di gruppi abeliani (con la terminologia della teoria dei moduli; con quella della teoria dei gruppi è un prodotto cartesiano).

Anche le proiezioni $\pi_i: \prod_{j \in I} R_j \rightarrow R_i$ e i monomorfismi canonici $\mu_i: R_i \rightarrow \prod_{j \in I} R_j$ sono definiti esattamente come nel caso dei (pre)moduli, e verificano le stesse proprietà che in quel caso. In aggiunta, rispetto al caso dei (pre)moduli, si ha che, per ogni $i \in I$, l’immagine R_i^* di μ_i è un ideale di $\prod_{j \in I} R_j$; lo si riconosce osservando che R_i^* coincide con $\bigcap_{i \neq j \in I} \ker \pi_j$, o, in alternativa, che per ogni $r \in R_i$ e $s = (s_j)_{j \in I} \in \prod_{j \in I} R_j$ si ha $r^{\mu_i} s = (rs_i)^{\mu_i}$, essendo nulle tutte le componenti di r^{μ_i} tranne al più la i -esima.

Per motivi che saranno chiari più avanti, per la somma diretta esterna di anelli (il sottoanello del prodotto diretto costituito dalle famiglie a supporto finito; come è facile vedere si tratta di un ideale, la somma degli ideali $R_i^* = \text{im } \mu_i$ al variare di $i \in I$) non viene utilizzato il simbolo \coprod . Anche se ciascuno degli anelli R_i è unitario, a meno che non sia finito l’insieme degli $i \in I$ tali che R_i non sia nullo, la somma diretta esterna di $(R_i)_{i \in I}$ non è un anello unitario. Lo si verifica direttamente, o anche attraverso una proprietà dei suoi ideali propri. Abbiamo infatti.

Proposizione 4.2. *Siano $(R_i)_{i \in I}$ una famiglia di anelli commutativi e S la sua somma diretta esterna, e supponiamo che l’insieme degli $i \in I$ tali che R_i non sia nullo sia infinito. Allora S è unione insiemistica di suoi ideali propri e quindi non è unitario.*

Dimostrazione. Come sopra, per ogni $i \in I$, indichiamo con R_i^* l’immagine dell’ i -esimo monomorfismo canonico da R_i a $\prod_{i \in I} R_i$. Sappiamo che R_i^* è un ideale di $\prod_{i \in I} R_i$ contenuto in S , dunque $R_i^* \triangleleft S$. Ogni $s \in S$ appartiene a $\sum_{i \in \text{supp}(s)} R_i^*$, che è un ideale di S ; siccome $\text{supp}(s)$ è finito, l’ipotesi comporta che questo ideale è proprio. È così giustificata la prima parte dell’enunciato. Dal momento che, se esiste, 1_S non può appartenere ad un ideale proprio di S , se ne ricava che S non è unitario. \square

Infine, riprendendo le notazioni iniziali, se supponiamo che gli R_i non siano solo anelli ma algebre su un prefissato anello commutativo unitario R , allora $\text{Cr}_{i \in I} R_i$ è anche munito dell’operazione esterna che lo rende R -modulo prodotto diretto di $(R_i)_{i \in I}$, nel senso definito in precedenza, ed è di immediata verifica il fatto che questa rende $\prod_{i \in I} R_i$ una R -algebra. Inoltre la somma diretta degli anelli R_i ne è una sottoalgebra; otteniamo così la nozione di prodotto diretto e di somma diretta di R -algebre.

Anelli di funzioni Un caso particolare di prodotto diretto di anelli si ha quando la famiglia di anelli su cui il prodotto è costruito è costante.

Siano R un anello e I un insieme. Il prodotto cartesiano $\text{Cr}_{i \in I} R$ della famiglia $(R)_{i \in I}$ non è altro che l’insieme R^I delle applicazioni da I a R . Il corrispondente anello prodotto diretto, $\prod_{i \in I} R$, viene chiamato l’anello delle funzioni da I a R ed è commutativo, o unitario, se e solo se R ha la stessa proprietà. Si verifica facilmente che le operazioni di addizione e moltiplicazione in questo anello sono le operazioni puntuali definite dalle omologhe operazioni di R , che avevamo definito nella [sottosezione 1.1.1](#).

Somme dirette interne di anelli Siano R un anello commutativo e $(H_i)_{i \in I}$ una famiglia di ideali di R . In termini di premoduli, questa situazione si può equivalentemente esprimere dicendo che $(H_i)_{i \in I}$ è una famiglia di sottopremoduli dell' R -premodulo R_R . Se $R_R = \bigoplus_{i \in I} H_i$ (e solo in questo caso), diciamo anche che R (come anello) è somma diretta (interna) della famiglia $(H_i)_{i \in I}$, e scriviamo anche $R = \bigoplus_{i \in I} H_i$. Osserviamo che questo equivale anche all'essere $(R, +) = \bigoplus_{i \in I} (H_i, +)$ (cioè: che il gruppo additivo di R sia somma diretta dei gruppi additivi degli H_i) a condizione, non lo dimentichiamo, che gli H_i siano tutti ideali di R .

Una proprietà ovvia ma essenziale delle somme dirette interne $\bigoplus_{i \in I} H_i$ di anelli è la cosiddetta ortogonalità dei sommandi diretti: per ogni $i, j \in I$ e $i \neq j$, si ha $H_i \cap H_j = 0$ e quindi $H_i H_j = 0$, in conseguenza del [Lemma 3.1](#) (i).

Come accade per i (pre)moduli, si possono in qualche senso identificare le nozioni di somma diretta interna ed esterna di anelli commutativi. Infatti, poiché l'analogo enunciato vale per i premoduli, se $(R_i)_{i \in I}$ è una famiglia di anelli commutativi, indicando, per ogni $i \in I$, con H_i l'immagine dell' i -esimo monomorfismo canonico da R_i a $\prod_{j \in I} R_j$, abbiamo che la somma diretta esterna di $(R_i)_{i \in I}$ è la somma diretta interna di $(H_i)_{i \in I}$ (abbiamo già visto che ciascuno degli H_i è un ideale di questa somma). Inoltre, la [Proposizione 4.1](#), tradotta nel linguaggio degli anelli, diventa:

Proposizione 4.3. *Siano R un anello commutativo e S la somma diretta esterna di una famiglia $(H_i)_{i \in I}$ di ideali di R . Allora $R = \bigoplus_{i \in I} H_i$ se e solo se l'applicazione*

$$\varphi: (a_i)_{i \in I} \in S \longmapsto \sum_{i \in I} a_i \in R$$

è un isomorfismo di anelli.

Dimostrazione. Come osservato, abbiamo $R = \bigoplus_{i \in I} H_i$ se e solo se $(R, +) = \bigoplus_{i \in I} (H_i, +)$, e questo, in accordo con la [Proposizione 4.1](#) applicata al caso degli \mathbb{Z} -moduli, equivale a dire che φ sia un isomorfismo di gruppi additivi. Bisogna dunque verificare che φ è un isomorfismo di gruppi additivi se e solo se è un isomorfismo di anelli. Siano $a = (a_i)_{i \in I}, b = (b_i)_{i \in I} \in S$. Se $i, j \in I$ e $i \neq j$, abbiamo $a_i b_j = 0$, dal momento che $H_i H_j = 0$, come visto sopra. Pertanto $a^\varphi b^\varphi = (\sum_{i \in I} a_i)(\sum_{i \in I} b_i) = \sum_{i \in I} a_i b_i = (ab)^\varphi$. Concludiamo che φ conserva la moltiplicazione; l'asserto è ora chiaro. \square

Se un anello commutativo R è somma diretta interna di suoi ideali: $R = \bigoplus_{i \in I} H_i$, allora, visti come anelli, gli ideali H_i sono sottoanelli di R ma sono anche isomorfi a quozienti di R , avendosi, per ogni $i \in I$, $H_i \simeq R / (\sum_{i \neq j \in I} H_j)$. Quindi, se R è unitario, gli ideali H_i sono necessariamente anelli unitari (ma non, salvo che in casi banali, sottoanelli unitari). L'ovvio epimorfismo $R \rightarrow H_i$ che abbiamo implicitamente utilizzato è spesso chiamato proiezione di R su H_i ed è strettamente imparentato con le proiezioni definite a proposito dei prodotti diretti: se identifichiamo R con la somma diretta esterna degli ideali H_i utilizzando l'isomorfismo φ della [Proposizione 4.3](#), la proiezione di R su H_i è semplicemente la restrizione a R della proiezione $\pi_i: \prod_{j \in I} R_j \rightarrow R_i$. Come è facile verificare, se H_i è unitario, la proiezione di R su H_i è l'applicazione che ad ogni $r \in R$ associa $r1_{H_i} \in H_i$.

Gli ideali di una somma diretta di anelli commutativi unitari sono facili da descrivere in termini degli ideali dei sommandi diretti:

Proposizione 4.4. *Sia $R = \bigoplus_{i \in I} H_i$ un anello commutativo, somma diretta di una famiglia $(H_i)_{i \in I}$ di suoi ideali che siano tutti unitari. Allora:*

- (i) *gli ideali di R sono tutte e sole le somme dirette $\bigoplus_{i \in I} K_i$ dove $K_i \triangleleft H_i$ per ogni $i \in I$;*
- (ii) *gli ideali massimali di R sono tutti soli quelli della forma $M_i \oplus (\bigoplus_{i \neq j \in I} H_j)$ dove $M_i \triangleleft H_i$, al variare di i in I ;*

(iii) gli ideali primi di R sono tutti soli quelli della forma $P_i \oplus (\bigoplus_{i \neq j \in I} H_j)$ dove $P_i \in \text{Spec}(H_i)$, al variare di i in I .

Dimostrazione. Dal momento che $H_i H_j = 0$ per ogni scelta di i e j distinti in I , è facile riconoscere che le somme dirette menzionate in (i) sono tutte ideali di R . Viceversa, sia $H \triangleleft R$. Per ogni $i \in I$ sia $K_i = H1_{H_i}$, l'immagine di H mediante la proiezione $p_i: r \in R \mapsto r1_{H_i} \in H_i$ di R sul suo sommando diretto H_i ; chiaramente $K_i \subseteq H_i$. Siccome $h = \sum_{i \in I} h^{p_i}$ per ogni $h \in H$ (si noti che la somma è ben definita perché è finito il numero degli addendi non nulli), $H \subseteq \sum_i K_i$. D'altra parte $\sum_{i \in I} K_i \subseteq H$; si ottiene così la (i).

La (ii) segue facilmente da (i). Anche la (iii) ne è una conseguenza: se $P = \bigoplus_{i \in I} K_i \triangleleft R$ (e $K_i \triangleleft H_i$ per ogni i), allora (si veda l'Esercizio 4.A.2) $R/P \simeq \bigoplus_{i \in I} H_i/K_i$. Ora, per la proprietà di ortogonalità dei sommandi di una somma diretta, R/P è un dominio di integrità se e solo se esattamente uno dei quozienti H_i/K_i non è nullo, e quello non nullo è un dominio di integrità. Dunque, P è primo se e solo se esiste un $i \in I$ tale che K_i sia primo in H_i e $K_j = H_j$ per ogni $j \in I \setminus \{i\}$; questo è il contenuto di (iii). \square

Dalle (ii) e (iii) di [Proposizione 4.4](#) segue direttamente che il radicale di Jacobson ed il nilradicale di una somma diretta di anelli unitari sono le somme dirette dei corrispondenti radicali dei sommandi. Lo stesso si può dimostrare anche per anelli non unitari:

Proposizione 4.5. Sia $R = \bigoplus_{i \in I} H_i$ un anello commutativo, somma diretta di una famiglia $(H_i)_{i \in I}$ di suoi ideali. Allora:

- (i) $\text{Jac}(R) = \bigoplus_{i \in I} \text{Jac}(H_i)$;
- (ii) $\text{NilRad}(R) = \bigoplus_{i \in I} \text{NilRad}(H_i)$.

Dimostrazione. La (ii) è molto semplice da provare: per ogni $r \in R$, indicando per ogni $i \in I$ con p_i la proiezione di R su H_i , si vede molto facilmente che r è nilpotente se e solo se r^{p_i} è nilpotente per ogni $i \in I$ (il fatto che $r^{p_i} \neq 0_R$ solo per un numero finito di scelte di i è qui essenziale). Da ciò la (ii) segue immediatamente.

Per provare la (i), osserviamo che, per ogni $i \in I$ ed ogni $K_i \triangleleft H_i$ la somma $K_i \oplus (\bigoplus_{i \neq j \in I} H_j)$ è un ideale massimale di R . L'intersezione tra tutti questi ideali massimali di R (assumendo l'intersezione uguale a R se l'insieme intersecato è vuoto) è $\bigoplus_{i \in I} \text{Jac}(H_i)$; questa somma contiene dunque $\text{Jac}(R)$. Viceversa, se $M \triangleleft R$ e $i \in I$, allora o $H_i \subseteq M$ oppure $R = H_i + M$. In questo secondo caso $\bar{H} := H_i/(M \cap H_i) \simeq_R R/M$ per il secondo teorema di omomorfismo, quindi \bar{H} è un R -premodulo semplice. Posto $K = \bigoplus_{i \neq j \in I} H_j$, si ha $R = H_i + K$, e $\bar{H}K = 0$. Da ciò segue che ogni H_i -sottopremodulo di \bar{H} è anche un R -premodulo, quindi \bar{H} è semplice anche come H_i -premodulo, sicché $M \cap H_i \triangleleft H_i$ e $\text{Jac}(H_i) \subseteq M \cap H_i \subseteq M$. Abbiamo mostrato che, in ciascuno dei due casi, $\text{Jac}(H_i) \subseteq M$. Pertanto $\bigoplus_{i \in I} \text{Jac}(H_i) \subseteq \text{Jac}(R)$; ora la dimostrazione è completa. \square

Esercizi.

4.B.1. Sia I uno spazio topologico. Verificare che nell'anello delle funzioni da I a \mathbb{R} l'insieme C delle funzioni continue costituisce un sottoanello unitario. Provare inoltre che:

- i) $\mathcal{U}(C) = \{f \in C \mid (\forall a \in I)(a^f \neq 0)\}$;
- ii) se I è compatto, gli ideali massimali di C sono tutti e soli gli insiemi $M_i = \{f \in C \mid i^f = 0\}$ al variare di i in I . (Suggerimento: per ogni $f \in C$, sia Z_f l'antiimmagine di $\{0\}$ mediante f ; osservare che se F è una parte finita di un ideale proprio H di C allora $\bigcap \{Z_f \mid f \in F\} \neq \emptyset$ e dedurne, utilizzando la compattezza di I , che $\bigcap \{Z_f \mid f \in H\} \neq \emptyset$.)

4.B.2. L'anello delle parti di un insieme può essere riguardato come anello di funzioni. Infatti, per ogni insieme S , l'applicazione da $(\mathcal{P}(S), \Delta, \cap)$ all'anello delle funzioni da S a \mathbb{Z}_2 che ad ogni parte di S associa la sua funzione caratteristica è un isomorfismo. Verificarlo.

4.B.3. Questo esempio si riferisce alla definizione di somma diretta interna per anelli ed ha lo scopo di illustrare la rilevanza del fatto che i sottoanelli sommandi diretti siano ideali.

Sia $R = H \oplus K$ un anello commutativo, somma diretta interna di due ideali H e K tra loro isomorfi tramite un isomorfismo (di anelli) $\alpha: H \rightarrow K$. Allora $D = \{hh^\alpha \mid h \in H\}$ è un sottoanello (anche unitario, se R è unitario) di R isomorfo, come anello, ad H e certamente $(R, +) = (H, +) \oplus (D, +)$ è una somma diretta di gruppi abeliani. (Può essere utile visualizzare la situazione in termini di somme dirette esterne, identificando R con $H \times H$ e, utilizzando i monomorfismi canonici, H con il suo ideale $H \times 0$ e K con $0 \times H$; in questo modo D diventa la diagonale $\{(h, h) \mid h \in H\}$ di H). È chiaro che, escluso il caso particolare in cui H sia un anello a prodotto costante nullo (cioè $H^2 = 0$), D non è un ideale di R , infatti $H \supseteq HD = H^2 \not\subseteq D$, quindi R non è, come anello, somma diretta interna di H e D , benché lo sia come gruppo abeliano e, come anello, $D \simeq K \simeq R/H$. In termini delle operazioni sugli elementi, in cosa la decomposizione $R = H + D$ differisce dalla decomposizione $R = H \oplus K$? Nel fatto che mentre, rispetto alla seconda decomposizione, il prodotto tra elementi di R si ottiene 'addendo per addendo' ('componente per componente' se ci riferiamo alla rappresentazione di R come somma diretta esterna), cioè $(h_1 + k_1)(h_2 + k_2) = h_1h_2 + k_1k_2$ per ogni $h_1, h_2 \in H$ e $k_1, k_2 \in K$, l'analoga descrizione non si applica alla decomposizione $R = H + D$. Infatti, ogni elemento di R si scrive in unico modo nella forma $h + d$ per opportuni $h \in H$ e $d \in D$, ma se $h_1, h_2 \in H$ e $d_1, d_2 \in D$ si ha $(h_1 + d_1)(h_2 + d_2) = h^* + d_1d_2$ dove ovviamente $d_1d_2 \in D$, ma $h^* = h_1h_2 + h_1d_2 + h_2d_1$ è un elemento di H in generale diverso da h_1h_2 : si ha $d_1 = uu^\alpha$ e $d_2 = vv^\alpha$ per opportuni $u, v \in H$ e $h^* = h_1h_2 + h_1v + h_2u$.

4.B.4. Proseguendo con le considerazioni sulle somme dirette di anelli, notiamo che se $R = H \oplus K$, dove $H, K \triangleleft R$, allora $K \subseteq \text{Ann}_R(H)$ e, per la legge di Dedekind ([Lemma 1.8](#)), $\text{Ann}_R(H) = \text{Ann}_H(H) + K$. Dunque, se H è tale che $\text{Ann}_H(H) = 0$ (ad esempio, se H è unitario oppure è un dominio di integrità), allora $K = \text{Ann}_R(H)$ è univocamente determinato da H : non esistono altri ideali $I \triangleleft R$ tali che $R = H \oplus I$.

4.B.5. Sia $R = \prod_{i \in I} R_i$ il prodotto di una famiglia di anelli commutativi unitari. Dopo aver verificato che, come detto nel testo, $\mathcal{U}(R) = \prod_{i \in I} \mathcal{U}(R_i)$, dedurre $\text{Jac}(R) = \prod_{i \in I} \text{Jac}(R_i)$.

4.B.6. In contrasto con l'esercizio precedente, nelle stesse notazioni, si ha (ovviamente) $\text{NilRad}(R) \subseteq \prod_{i \in I} \text{NilRad}(R_i)$, ma non sempre vale l'uguaglianza. Ad esempio, in $\prod_{i \in \mathbb{N}^+} \mathbb{Z}_{2^i}$ l'elemento $([2]_{2^i})_{i \in \mathbb{N}^+}$ non è nilpotente, pur appartenendo a $\prod_{i \in \mathbb{N}^+} \text{NilRad}(\mathbb{Z}_{2^i})$.

4.B.7. L'analogo della [Proposizione 4.4](#) non vale se gli H_i non sono assunti unitari, né vale per prodotti diretti di anelli, anche unitari. Ad esempio, il gruppo V_4 di Klein si può descrivere come somma diretta di due gruppi di ordine 2: $\langle a \rangle \oplus \langle b \rangle$. Una volta munito del prodotto costante nullo, V_4 costituisce un anello (non unitario) commutativo in cui $\langle a \rangle$ e $\langle b \rangle$ sono ideali (abbiamo quindi una somma diretta di anelli), ma il sottogruppo generato da $a + b$ è un ideale, per giunta massimale, che non è della forma indicata in (i) della [Proposizione 4.4](#).

Sia ora $R = \prod_{i \in I} R_i$ il prodotto di una famiglia di anelli commutativi unitari, e chiamiamo fattorizzati gli ideali di R della forma $\prod_{i \in I} K_i$, dove ciascuno dei K_i è un ideale di R_i . Tra gli ideali fattorizzati, quelli che sono massimali come ideali di R sono quelli ottenuti scegliendo $K_i \triangleleft R_i$ per un $i \in I$ e $K_j = R_j$ per ogni altro $j \in I$. Mostriamo che possono esistere in un tale R ideali massimali non fattorizzati.

Se S è un insieme infinito, come visto in un esercizio precedente, l'anello $\mathcal{P}(S)$ è isomorfo all'anello di funzioni \mathbb{Z}_2^S , ovvero (verificarlo!) a $R := \prod_{x \in S} \mathcal{P}(\{x\})$. Dal momento che, per ogni $x \in S$, l'unico ideale proprio di $\mathcal{P}(\{x\})$ è quello nullo, cioè $\{\emptyset\}$, in questo prodotto gli

ideali massimali fattorizzati sono quelli della forma $M_x = \{\emptyset\} \times \prod_{x \neq y \in S} \mathcal{P}(\{y\})$ al variare di x in S . Ora, nell'ovvio isomorfismo tra $\mathcal{P}(S)$ e R , ciascun M_x corrisponde all'ideale massimale $\mathcal{P}(S \setminus \{x\})$ di $\mathcal{P}(S)$. Si può verificare che non tutti gli ideali massimali di $\mathcal{P}(S)$ sono di questo tipo, dunque non tutti gli ideali massimali di R sono fattorizzati. Un modo semplice per arrivarci è questo: l'insieme delle parti finite di S costituisce un ideale proprio F di $\mathcal{P}(S)$; per il teorema di Krull dell'ideale massimale $F \subseteq M$ per qualche $M \triangleleft \mathcal{P}(S)$. Ma, chiaramente, per ogni $x \in S$ si ha $F \not\subseteq \mathcal{P}(S \setminus \{x\})$, quindi M è un ideale massimale che corrisponde ad un ideale non fattorizzato di R .

Chi ha incontrato la nozione di ultrafiltro potrebbe interpretare il discorso appena fatto in questo modo: gli ideali massimali di $\mathcal{P}(S)$ hanno come complementi in $\mathcal{P}(S)$ gli ultrafiltri di S ; tra questi gli ultrafiltri principali sono quelli della forma $\mathcal{P}(S) \setminus \mathcal{P}(S \setminus \{x\})$ al variare di $x \in S$, ma, assumendo l'assioma di scelta, esistono in $\mathcal{P}(S)$ anche ultrafiltri non principali, e da ciò segue la conclusione.

4.2.1 Idempotenti e decomposizioni dirette in anelli

In una struttura algebrica in cui sia definita un'operazione binaria $*$ un elemento e si dice *idempotente* (rispetto a $*$) se e solo se $e * e = e$. In un anello R il termine idempotente è sempre riferito all'operazione di moltiplicazione, quindi un idempotente di R è per definizione un elemento e che coincida col proprio quadrato. Ovviamente, se e è idempotente si ha $e = e^n$ per ogni $n \in \mathbb{N}^+$. Sono idempotenti 0_R e, se R è unitario, 1_R ; questi sono detti gli *idempotenti banali* di R . Assumendo R commutativo, si dice poi che due idempotenti e, e' di R sono *ortogonali* tra loro se e solo se $ee' = 0_R$. Ad esempio: nell'anello \mathbb{Z}_{10} gli elementi $[5]_{10}$ e $[6]_{10}$ sono idempotenti tra loro ortogonali.

Lemma 4.6. *Sia e un elemento idempotente in un anello commutativo unitario R . Allora $1_R - e$ è un idempotente ortogonale a e . Inoltre, o $e = 1_R$ oppure e è un divisore dello zero in R .*

Dimostrazione. Si ha $(1_R - e)^2 = 1_R - 2e + e^2 = 1_R - 2e + e = 1_R - e$, quindi $1_R - e$ è idempotente. Inoltre $e(1_R - e) = e - e^2 = 0_R$, quindi e e $1_R - e$ sono ortogonali. L'ultima affermazione è un'ovvia conseguenza: se $e \neq 1_R$ allora $1_R - e \neq 0_R$, quindi e è un divisore dello zero. \square

È evidente che l'assegnazione $e \mapsto 1_R - e$ definisce una permutazione involutoria (cioè di periodo due, a meno che R sia nullo) nell'insieme degli elementi idempotenti di R .

È facile costruire idempotenti, anche tra loro ortogonali, in prodotti diretti. Sia infatti $R = \prod_{i \in I} R_i$, dove, per ogni i , R_i è un anello commutativo unitario. Ogni elemento $(r_i)_{i \in I} \in R$ tale che per ogni $i \in I$ si abbia $r_i \in \{0_{R_i}, 1_{R_i}\}$ è evidentemente idempotente. Sempre per ogni $i \in I$ poniamo $e_i = 1_{R_i}^{\mu_i}$, dove μ_i è il monomorfismo canonico $R_i \rightarrow R$; dunque e_i ha i -esima componente 1_{R_i} ed ogni altra componente nulla. Gli elementi e_i , al variare di $i \in I$, si chiamano *idempotenti canonici* del prodotto R e sono tra loro, a due a due, ortogonali.

Nel caso in cui I sia finito, possiamo sommare tra loro gli idempotenti canonici di R ottenendo, evidentemente, $\sum_{i \in I} e_i = 1_R$; si usa dire che quella data dagli e_i è una decomposizione dell'unità di R in (somma di) idempotenti ortogonali.

Come stiamo per vedere, viceversa, ad ogni tale decomposizione corrisponde una decomposizione in somma diretta. Infatti, già nella situazione del Lemma 4.6 si può dimostrare che R è somma diretta degli ideali eR e $(1_R - e)R$; più in generale abbiamo:

Lemma 4.7. *Siano R un anello commutativo unitario, $n \in \mathbb{N}$ e e_1, e_2, \dots, e_n elementi idempotenti di R a due a due ortogonali tali che $\sum_{i=1}^n e_i = 1_R$. Allora, per ogni $i \in I_n = \{1, 2, \dots, n\}$, l'ideale $e_i R$ è, come anello, unitario con unità e_i e $R = \bigoplus_{i \in I_n} e_i R$.*

Dimostrazione. Per ogni $i \in I_n$ poniamo $H_i = e_i R$. Sia $h \in H_i$, allora $h = e_i r$ per un opportuno $r \in R$, quindi $e_i h = e_i^2 r = h$, dunque $e_i = 1_{H_i}$, come richiesto.

Per ogni $r \in R$ si ha $r = r 1_R = r \sum_{i=1}^n e_i = \sum_{i=1}^n r e_i \in \sum_{i=1}^n H_i$. Dunque $R = \sum_{i=1}^n H_i$. Siano poi $r_1, r_2, \dots, r_n \in R$ tali che $\sum_{i=1}^n e_i r_i = 0_R$. Per ogni $j \in I_n$ abbiamo $0_R = e_j \sum_{i=1}^n e_i r_i = \sum_{i=1}^n e_j e_i r_i = e_j r_j$ per via dell'ortogonalità e del fatto che $e_j = 1_{H_j}$. Pertanto $R = \bigoplus_{i \in I_n} H_i$ ed il lemma è dimostrato. \square

Sia R un anello commutativo unitario. Chiamiamo \mathcal{J} l'insieme degli insiemi finiti E di elementi idempotenti di R a due a due ortogonali tali che $1_R = \sum_{e \in E} e$ (informalmente: l'insieme delle decomposizioni dell'unità di R in somma di idempotenti ortogonali) e \mathcal{S} l'insieme degli insiemi finiti \mathcal{I} di ideali di R tali che $R = \bigoplus_{H \in \mathcal{I}} H$ (informalmente: l'insieme delle decomposizioni di R in somma diretta finita).

Teorema 4.8. *Nelle notazioni appena fissate, l'applicazione da \mathcal{J} a \mathcal{S} che ad ogni $E \in \mathcal{J}$ associa $\{eR \mid e \in E\} \in \mathcal{S}$ è biettiva.*

Dimostrazione. Il Lemma 4.7 mostra che l'applicazione è ben definita. Ricordando che i sommandi che appaiono in una decomposizione diretta di un anello unitario sono certamente unitari, definiamo l'inversa di questa applicazione associando a ciascun $\mathcal{I} \in \mathcal{S}$ l'insieme $\{1_H \mid H \in \mathcal{I}\}$; è facile verificare che questo insieme è un elemento di \mathcal{J} : nell'isomorfismo tra $\prod_{H \in \mathcal{I}} H$ e R stabilito nella Proposizione 4.3 i suoi elementi corrispondono agli idempotenti canonici del prodotto. Dalle costruzioni effettuate risulta anche agevole la verifica del fatto che, come detto, le due applicazioni sono l'una inversa dell'altra. \square

Corollario 4.9. *Sia R un anello commutativo unitario. Allora R è indecomponibile in somma diretta (cioè: non è somma diretta di suoi ideali non banali) se e solo se non ha idempotenti non banali.*

Esercizi.

4.C.1. Verificare che se in un anello commutativo unitario R gli elementi e_1, e_2, \dots, e_n sono tali che $1_R = \sum_{i=1}^n e_i$ e $e_i e_j = 0_R$ per ogni scelta di i e j tra loro distinti, allora necessariamente tutti gli e_i sono idempotenti.

In Lemma 4.7, l'ipotesi che gli elementi e_i siano idempotenti è quindi sovrabbondante.

4.C.2. Uno studente, Dario Esposito, che ha partecipato al corso qualche anno fa, ha proposto un'elegante applicazione del Teorema 4.8: per ogni $n \in \mathbb{N}$ si ha $5^{2^n} + 6^{5^n} \equiv_{10^{n+1}} 1$, vale a dire: scritto in base 10, il numero $5^{2^n} + 6^{5^n}$ termina con n zeri seguiti da un 1. Provare a dimostrarlo dopo aver verificato che:

- i) per ogni $n \in \mathbb{N}$, $5^{2^n} \equiv_{2^{n+1}} 1$ e $6^{5^n} \equiv_{5^{n+1}} 1$, quindi $[5^{2^n}]_{10^{n+1}}$ e $[6^{5^n}]_{10^{n+1}}$ sono elementi idempotenti nell'anello $\mathbb{Z}_{10^{n+1}}$. Questo si può dimostrare per induzione su n , ma anche, in alternativa, utilizzando il teorema di Fermat-Eulero e qualche informazione sulla struttura del gruppo degli automorfismi di un gruppo ciclico di ordine potenza di primo (oppure, il che è lo stesso, sulla struttura del gruppo degli invertibili degli anelli quoziente di \mathbb{Z} .)
- ii) per ogni $n \in \mathbb{N}$, il gruppo ciclico $(\mathbb{Z}_{10^{n+1}}, +)$ ha (al massimo) una decomposizione non banale in somma diretta interna; questo segue dal fatto che 10^{n+1} ha esattamente due divisori primi.

4.C.3. Siano R un anello commutativo e $H \triangleleft R$. Provare che se si verifica una delle seguenti:

- i) come R -(pre)modulo, H è finitamente generato e $H^2 = H$;
- ii) come anello, H è unitario,

allora $R = H \oplus K$ per un opportuno $K \triangleleft R$.

4.2.2 Immersioni in prodotti diretti di quozienti

Se una famiglia $(N_i)_{i \in I}$ di sotto(pre)moduli di un (pre)modulo M ha intersezione nulla, allora il prodotto diretto dei (pre)moduli M/N_i ha un sotto(pre)modulo isomorfo a M . Questo è un caso particolare del seguente lemma:

Lemma 4.10. *Siano M un (pre)modulo e $(N_i)_{i \in I}$ una famiglia di suoi sotto(pre)moduli. Allora l'applicazione $\theta: a \in M \mapsto (a + N_i)_{i \in I} \in \prod_{i \in I} (M/N_i)$ è un omomorfismo di (pre)moduli. Il suo nucleo è $\bigcap_{i \in I} N_i$.*

Dimostrazione. Che θ sia un omomorfismo è ovvio (e segue anche dalla [Proposizione 4.26](#), non ancora dimostrata). Sia $a \in M$. Per ogni $i \in I$, la i -esima componente di a^θ è $a + N_i$, che è $0_{M/N_i}$ se e solo se $a \in N_i$. Dunque, $\ker \theta = \bigcap_{i \in I} N_i$. \square

Il risultato analogo, per anelli e algebre, è più interessante, anche nelle sue applicazioni immediate all'anello degli interi.

Lemma 4.11. *Siano R un anello commutativo e $(H_i)_{i \in I}$ una famiglia di ideali di R . Allora l'applicazione $\theta: r \in R \mapsto (r + H_i)_{i \in I} \in \prod_{i \in I} (R/H_i)$ è un omomorfismo di anelli di nucleo $\ker \theta = \bigcap_{i \in I} H_i$.*

Inoltre, se R è unitario, θ è un omomorfismo di R -algebre unitarie e si ha:

- (i) *se θ è suriettivo, per ogni $J \subset I$ tale che $J \neq \emptyset$, $\bigcap_{i \in J} H_i$ e $\bigcap_{i \in I \setminus J} H_i$ sono comassimali e, in particolare, gli ideali H_i , al variare di $i \in I$, sono a due a due comassimali;*
- (ii) *se I è finito, θ è suriettivo se e solo se gli ideali H_i , al variare di $i \in I$, sono a due a due comassimali.*

Dimostrazione. La prima parte dell'enunciato è ovvia. Assumendo R unitario, basta provare (i) e (ii). Poniamo $P := \prod_{i \in I} (R/H_i)$.

Per ogni $S \subseteq I$, indichiamo con e_S l'elemento (idempotente) di P la cui i -esima componente sia $1_R + H_i$ se $i \in S$ e H_i se $i \notin S$. Questa notazione ci aiuta nella dimostrazione di (i): se θ è suriettivo e $\emptyset \neq J \subset I$, allora esistono $x, y \in R$ tali che $x^\theta = e_{I \setminus J}$ e $y^\theta = e_J$. Posto $X = \bigcap_{i \in J} H_i$ e $Y = \bigcap_{i \in I \setminus J} H_i$, abbiamo chiaramente $x \in X$ e $y \in Y$, e $(x + y)^\theta = e_J + e_{I \setminus J} = 1_P$. Dunque, $1_R \in x + y + \ker \theta$. Ma $\ker \theta \subseteq Y$; da ciò segue $1_R \in X + Y$, quindi X e Y sono comassimali, come richiesto dall'enunciato. Fissati poi $i, j \in I$ tali che $i \neq j$, scegliendo $\{j\}$ come J , con le notazioni appena usate si ottiene $X = H_j$ e $Y \subseteq H_i$, quindi $R = H_j + H_i$, vale a dire: H_i e H_j sono comassimali; in questo modo è provata la (i).

Per provare la (ii), supponiamo ora che I sia finito e $R = H_i + H_j$ per ogni $i, j \in I$ tali che $i \neq j$. Per ogni $i \in I$, segue dai lemmi [3.2](#) e [3.3](#) che H_i è comassimale con $K_i = \bigcap_{i \neq j \in I} H_j$, dunque $1_R = h_i + k_i$ per opportuni $h_i \in H_i$ e $k_i \in K_i$. Ma allora $k_i + H_i = 1_R + H_i$ e $k_i + H_j = H_j$ se $i \neq j \in I$, quindi $k_i^\theta = e_{\{i\}}$, nelle notazioni del paragrafo precedente, vale a dire: k_i^θ è l' i -esimo idempotente canonico di P . Pertanto $E := \{e_{\{i\}} \mid i \in I\} \subseteq \text{im } \theta$. Ma $P = ER$, di conseguenza $\text{im } \theta = P$ e θ è suriettiva. È così provata una delle due implicazioni richieste; l'altra era già contenuta in (i). La dimostrazione è completa. \square

Due applicazioni aritmetiche

Teorema 4.12 (Il teorema cinese dei resti). *Siano n un numero intero positivo e a_1, a_2, \dots, a_n interi positivi a due a due coprimi. Allora $\mathbb{Z}_{a_1 a_2 \dots a_n} \simeq \prod_{i=1}^n \mathbb{Z}_{a_i}$. Un isomorfismo è descritto dall'applicazione $[t]_{a_1 a_2 \dots a_n} \in \mathbb{Z}_{a_1 a_2 \dots a_n} \mapsto ([t]_{a_i})_{i \in I} \in \prod_{i=1}^n \mathbb{Z}_{a_i}$.*

Dimostrazione. Basta applicare il [Lemma 4.11](#) all'anello \mathbb{Z} ed alla famiglia $(a_i\mathbb{Z})_{i \in I}$ di suoi ideali, dove $I = \{1, 2, \dots, n\}$. Posto $P = \prod_{i=1}^n \mathbb{Z}_{a_i}$, il lemma fornisce l'omomorfismo di anelli unitari

$$\theta: t \in \mathbb{Z} \mapsto ([t]_{a_i})_{i \in I} \in P,$$

con nucleo $K := \bigcap_{i \in I} a_i\mathbb{Z}$. Il fatto che gli interi a_i siano a due a due coprimi mostra, per il teorema di Bézout, che gli ideali $a_i\mathbb{Z}$ sono a due a due comassimali, quindi $K = (a_1\mathbb{Z})(a_2\mathbb{Z}) \cdots (a_n\mathbb{Z}) = (a_1 a_2 \cdots a_n)\mathbb{Z}$ per il [Lemma 3.3](#) e, per il [Lemma 4.11](#), θ è suriettiva. Di conseguenza, per il primo teorema di isomorfismo, $\mathbb{Z}_{a_1 a_2 \cdots a_n} = \mathbb{Z}/K \simeq P$. \square

La *funzione di Eulero* $\varphi: \mathbb{N}^+ \rightarrow \mathbb{N}^+$ è definita associando ad ogni $n \in \mathbb{N}^+$ l'intero positivo $\varphi(n) = |\mathcal{U}(\mathbb{Z}_n)|$, che è uguale al numero degli interi compresi tra 1 ed n che siano coprimi con n . La funzione di Eulero non è un omomorfismo né rispetto all'addizione né rispetto alla moltiplicazione, ma è quella che in teoria dei numeri viene chiamata una funzione moltiplicativa, intendendo con questo che vale questo risultato:

Corollario 4.13. *Se a e b sono due interi positivi coprimi, $\varphi(ab) = \varphi(a)\varphi(b)$.*

Dimostrazione. Abbiamo $\varphi(ab) = |\mathcal{U}(\mathbb{Z}_{ab})|$. Per il [Teorema 4.12](#), $\mathbb{Z}_{ab} \simeq \mathbb{Z}_a \times \mathbb{Z}_b$ e quindi, per l'[Esercizio 4.B.5](#), $\mathcal{U}(\mathbb{Z}_{ab}) \simeq \mathcal{U}(\mathbb{Z}_a) \times \mathcal{U}(\mathbb{Z}_b)$; da ciò segue subito l'asserto. \square

Si verifica anche che, viceversa, se a e b sono interi positivi *non* coprimi tra loro, allora $\varphi(ab) \neq \varphi(a)\varphi(b)$; questo è il contenuto dell'[Esercizio 4.D.2](#).

Esercizi.

4.D.1. Non si conoscono algoritmi che permettano di calcolare in modo efficiente il valore $\varphi(a)$ assunto della funzione di Eulero per un arbitrario intero positivo a , ma è facile calcolare questo valore se di a si conosce la fattorizzazione in potenze di primi. Infatti è facile verificare che, se p è un numero primo positivo e $n \in \mathbb{N}^+$, si ha $\varphi(p^n) = (p-1)p^{n-1}$. Da questa osservazione e dal [Corollario 4.13](#) segue che, se $a = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$ dove $k \in \mathbb{N}$, p_1, p_2, \dots, p_k sono primi positivi a due a due distinti e $\lambda_1, \lambda_2, \dots, \lambda_k \in \mathbb{N}^+$, allora $\varphi(a) = \prod_{i=1}^k (p_i - 1)p_i^{\lambda_i - 1}$.

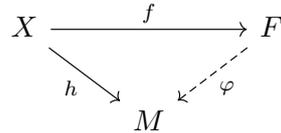
4.D.2. Usare l'osservazione precedente per dimostrare questa inversione del [Corollario 4.13](#): se a e b sono interi positivi tali che $\varphi(ab) = \varphi(a)\varphi(b)$, allora a e b sono coprimi tra loro.

4.3 Costruzioni universali: oggetti liberi, prodotti e coprodotti

Introduciamo qui alcuni esempi di costruzioni che sono di grande importanza in tanti settori della matematica. Una descrizione precisa richiede il linguaggio della teoria delle categorie; ci limitiamo qui a dire che un oggetto A (una struttura algebrica, nel nostro caso) ha una proprietà universale rispetto ad un certo tipo di diagrammi quando, ogni volta che siano dati diagrammi del tipo indicato esiste uno ed un solo omomorfismo di dominio o codominio A che, aggiunto ai diagrammi, li renda commutativi. La descrizione è piuttosto nebulosa, ma gli esempi che seguono dovrebbero chiarire l'idea. Uno degli aspetti che rende estremamente utile questa nozione è il fatto che si può dimostrare, piuttosto facilmente, che due oggetti che verifichino una data proprietà universale sono necessariamente isomorfi tra loro. Di conseguenza è possibile utilizzare proprietà universali per definire, a meno di isomorfismi, oggetti che in molti casi svolgono un ruolo di grande importanza nella teoria.

4.3.1 Moduli e premoduli liberi

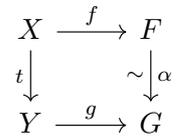
Siano R un anello commutativo, F un R -(pre)modulo e $f: X \rightarrow F$ un'applicazione da un insieme X al sostegno di F . Si dice che F è un R -(pre)modulo libero su X con applicazione universale f , o che (f, F) descrive un R -(pre)modulo libero, se e solo se per ogni R -(pre)modulo M ed ogni applicazione h da X al sostegno di M esiste uno ed un solo omomorfismo $\varphi: F \rightarrow M$ di R -(pre)moduli tale che $f\varphi = h$.



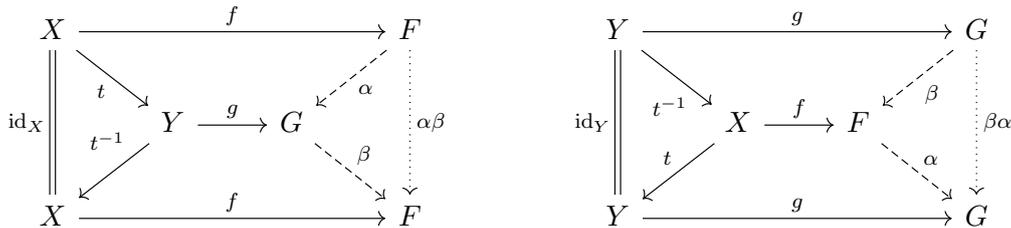
In queste condizioni, si dice anche che X è una base di F .

Prima di porci il problema dell'esistenza di (pre)moduli liberi, osserviamo la loro proprietà di unicità a meno di isomorfismi.

Proposizione 4.14. *Siano R un anello commutativo, X e Y insiemi equipotenti, con una biezione $t: X \rightarrow Y$. Supponiamo che F e G siano R -(pre)moduli liberi su X e Y rispettivamente, con applicazioni universali $f: X \rightarrow F$ e $g: Y \rightarrow G$. Allora esiste uno ed un solo R -omomorfismo $\alpha: F \rightarrow G$ tale che $tg = f\alpha$, e questo è un isomorfismo.*



Dimostrazione. La dimostrazione consiste nell'usare ripetutamente la proprietà universale che definisce i (pre)moduli liberi; la si può seguire con l'aiuto di questi diagrammi:



Poiché (f, F) descrive un (pre)modulo libero, esiste uno ed un solo R -omomorfismo α tale che $tg = f\alpha$, cioè tale che il 'trapezio' superiore nel diagramma a sinistra sia commutativo. Similmente, poiché (g, G) descrive un (pre)modulo libero, esiste uno ed un solo R -omomorfismo β tale che $t^{-1}f = g\beta$. L'intero diagramma a sinistra è dunque commutativo e si ha $f\alpha\beta = tg\beta = tt^{-1}f = f$. Ora, per definizione di (pre)modulo libero, deve esistere un solo R -omomorfismo θ tale che $f\theta = f$; dal momento che sia $\alpha\beta$ che id_F hanno questa proprietà, $\alpha\beta = \text{id}_F$. Passiamo al secondo diagramma; avendosi $tg = f\alpha$ e $t^{-1}f = g\beta$ anch'esso è commutativo, quindi ragionando come fatto per $\alpha\beta$, da $g\beta\alpha = g$ traiamo $\beta\alpha = \text{id}_G$. Abbiamo così verificato che β è l'inversa di α , dunque α è biettiva e la dimostrazione è conclusa. \square

Questo risultato mostra che la struttura di un (pre)modulo libero su un insieme X dipende, in ultima analisi, solo da $|X|$ (che viene chiamato *rango* del (pre)modulo libero): premoduli liberi su insiemi equipotenti sono isomorfi—vale anche il viceversa: si veda l'[Esercizio 4.E.3](#). Invertendo il risultato in un'altra direzione, è molto facile osservare che un (pre)modulo libero su un insieme X è libero su ogni insieme equipotente a X , e che ogni (pre)modulo che sia isomorfo ad esso ha la stessa proprietà:

Proposizione 4.15. *Siano R un anello commutativo e $t: X \rightarrow Y$ un'applicazione biettiva tra due insiemi X e Y . Supponiamo che F sia un (pre)modulo libero su X con applicazione universale $f: X \rightarrow F$ e che $\alpha: F \rightarrow G$ sia un isomorfismo di R -(pre)moduli. Allora G è un (pre)modulo libero su Y con applicazione universale $t^{-1}f\alpha$.*

Dimostrazione. Sia $h: Y \rightarrow M$ un'applicazione da Y al sostegno di un R -(pre)modulo M . Poiché (f, F) descrive un (pre)modulo libero, esiste uno ed un solo R -omomorfismo φ tale che $th = f\varphi$; da ciò segue che $\psi := \alpha^{-1}\varphi$ è l'unico R -omomorfismo tale che $(t^{-1}f\alpha)\psi = h$. Questo prova l'asserto. \square

Occupiamoci ora dell'esistenza o meno di (pre)moduli liberi. Iniziamo dal caso dei moduli, che è quello che ci interessa maggiormente. Sia dunque R un anello commutativo unitario. Fissato un insieme I consideriamo la somma diretta esterna, indicata in I , di copie di R considerato come modulo su sé stesso: $F = \coprod_{i \in I} R_R$; notiamo che F è un modulo nullo se $I = \emptyset$. Per ogni $i \in I$, sia e_i l'elemento di F che ha 1_R come i -esima coordinata e 0_R come j -esima coordinata per ogni $j \in I \setminus \{i\}$.¹

Proposizione 4.16. *Con le notazioni appena fissate, F è un R -modulo libero su I , con applicazione universale $f: i \in I \mapsto e_i \in F$.*

Di conseguenza, per ogni insieme I esiste un R -modulo libero su I ; inoltre ogni R -modulo libero ha come applicazione universale un'applicazione iniettiva.

Dimostrazione. Sia $h: I \rightarrow M$ un'applicazione da I al sostegno di un R -modulo M . Dobbiamo dimostrare che esiste uno ed un solo R -omomorfismo $\varphi: F \rightarrow M$ tale che $h = f\varphi$. Se φ verifica queste condizioni, allora per ogni $i \in I$ si ha $e_i^\varphi = i^{f\varphi} = i^h$. Di conseguenza, per ogni $(a_i)_{i \in I} \in F$, si ha $((a_i)_{i \in I})^\varphi = (\sum_{i \in I} e_i a_i)^\varphi = \sum_{i \in I} e_i^\varphi a_i = \sum_{i \in I} i^h a_i$. Dunque, l'unica applicazione $F \rightarrow M$ che può soddisfare le condizioni richieste per φ è l'applicazione $(a_i)_{i \in I} \in F \mapsto \sum_{i \in I} i^h a_i \in M$ (che, come al solito, è ben definita perché ogni elemento di F ha solo un numero finito di componenti non nulle). Chiamiamo allora φ questa applicazione. È evidente che vale $h = f\varphi$; resta solo da dimostrare che φ è un R -omomorfismo. Per ogni $a = (a_i)_{i \in I}, b = (b_i)_{i \in I} \in F$ e $r \in R$ si ha $a^\varphi + b^\varphi = \sum_{i \in I} i^h a_i + \sum_{i \in I} i^h b_i = \sum_{i \in I} i^h (a_i + b_i) = (a + b)^\varphi$ e $(ar)^\varphi = \sum_{i \in I} i^h (a_i r) = (\sum_{i \in I} i^h a_i) r = a^\varphi r$, quindi φ è effettivamente un R -omomorfismo. A questo punto abbiamo provato che, come richiesto, (f, F) descrive un R -modulo libero. Notiamo che f è un'applicazione iniettiva.

Abbiamo così verificato che ogni insieme è base di un R -modulo libero. Infine, per giustificare l'ultima affermazione, consideriamo un'arbitraria applicazione g da un insieme I al sostegno di un R -modulo G tale che (g, G) descriva un R -modulo libero. Allora, utilizzando le notazioni del paragrafo precedente, la [Proposizione 4.14](#) fornisce un isomorfismo $\alpha: F \rightarrow G$ tale che $g = f\alpha$; essendo f iniettiva anche g sarà iniettiva. \square

Abbiamo così, utilizzando anche [Proposizione 4.14](#), che se R è un anello commutativo unitario, gli R -moduli liberi sono le somme dirette (interne) di moduli isomorfi a R_R . Per chiarezza: se $I = \emptyset$ la somma diretta $\coprod_{i \in I} R$ è un modulo nullo (verificarlo direttamente dalle definizioni), quindi gli R -moduli liberi sull'insieme vuoto sono gli R -moduli nulli.

La proposizione precedente descrive anche i premoduli liberi, grazie a questo lemma che permette di tradurre ogni questione su premoduli liberi in una questione su moduli liberi.

Lemma 4.17. *Siano R un anello commutativo, X un insieme, F un R -premodulo e $f: X \rightarrow F$ un'applicazione. Sia poi R_1 l'anello accresciuto definito da R . Allora (f, F) descrive un R -premodulo libero se e solo se, riguardato F come R_1 -modulo, (f, F) descrive un R_1 -modulo libero.*

Dimostrazione. L'asserto segue dal fatto (stabilito nella [Proposizione 1.31](#)) che, per ogni R -premodulo G , un'applicazione $\varphi: F \rightarrow G$ è un omomorfismo di R -premoduli se e solo se, riguardanti F e G come R_1 -moduli, è un omomorfismo di R_1 -moduli. \square

¹ potremmo descrivere e_i come $(\delta_{ij})_{j \in I}$, intendendo con δ_{ij} una versione del simbolo di Kroneker nell'anello R . Nella terminologia dei prodotti diretti di anelli, e_i corrisponde ad un idempotente canonico.

Corollario 4.18. Sia R un anello commutativo e sia R_1 l'anello accresciuto definito da R . Per ogni insieme X esistono R -premoduli liberi di base X . Questi sono le somme dirette interne di $|X|$ premoduli isomorfi a R_1 , riguardato come R -premodulo.

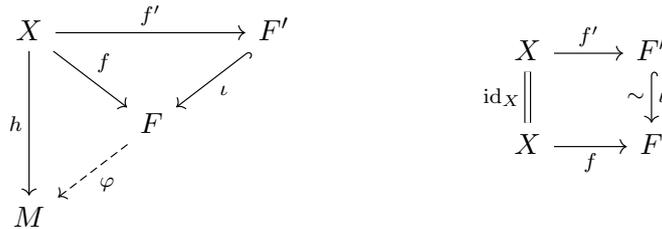
Abbiamo così che ogni (pre)modulo libero non nullo è fedele.

Un'altra utile osservazione è che ogni (pre)modulo libero è libero su un suo sottinsieme, con l'applicazione immersione come applicazione universale. Infatti, se (f, F) descrive un (pre)modulo libero, allora la [Proposizione 4.15](#) mostra che F è libero anche su $\text{im } f$ con applicazione universale $\text{im } f \hookrightarrow F$, dal momento che f è, per la [Proposizione 4.16](#) (e il [Lemma 4.17](#)), iniettiva. Nel discutere di (pre)moduli liberi è dunque lecito (e lo si fa spesso) assumere implicitamente che la base sia una parte del (pre)modulo e che l'applicazione universale sia la corrispondente immersione. In questo caso la base è un particolare insieme di generatori del (pre)modulo. Infatti:

Proposizione 4.19. Supponiamo che (f, F) descriva un (pre)modulo libero. Allora F è generato da $\text{im } f$.

Dimostrazione. Questo è chiaro dalle descrizioni esplicite date per i (pre)moduli liberi, ma può essere più interessante quest'altra dimostrazione 'a priori' che ne prescinde.

Siano X il dominio di f e F' il sotto(pre)modulo di F generato da $\text{im } f$; siano poi ι l'immersione $F' \hookrightarrow F$ e $f': X \rightarrow F'$ la ridotta di f a F' , dunque $f = f'\iota$. Verifichiamo che (f', F') descrive un modulo libero. Scelti comunque un (pre)modulo M (sullo stesso anello di scalari di F) ed un'applicazione $h: X \rightarrow M$, esiste un unico omomorfismo $\varphi: F \rightarrow M$ tale che $h = f\varphi$.



Allora $h = f'(\iota\varphi)$. Inoltre $\iota\varphi$ è l'unico omomorfismo che composto con f' dia h : se infatti ψ è un omomorfismo $F' \rightarrow M$ e $f'\psi = h$, ovvero $f'\psi = f'(\iota\varphi)$, allora le restrizioni di ψ e $\iota\varphi$ a $\text{im } f'$ coincidono, ma allora $\psi = \iota\varphi$ per l'[Esercizio 1.D.4](#). Concludiamo che effettivamente F' è libero con applicazione universale f' . Ci troviamo allora, per la [Proposizione 4.14](#), nella situazione descritta nel diagramma commutativo di destra e concludiamo che ι è un isomorfismo, cioè: $F' = F$. \square

Forse, ciò che più di ogni altra proprietà rende evidente l'importanza dei (pre)moduli liberi è il fatto che, a meno di isomorfismi, tutti i (pre)moduli sono quozienti di (pre)moduli liberi:

Proposizione 4.20. Siano R un anello commutativo unitario e M un R -(pre)modulo. Allora esiste un R -(pre)modulo libero F tale che $M \simeq_R F/N$ per un opportuno $N \leq_R F$. Se M è generato da un suo sottinsieme X , si può scegliere F libero su X .

Dimostrazione. Sia M generato da X e sia F un R -(pre)modulo libero su X con applicazione universale f . Sia h l'immersione di X in M . Esiste allora un R -omomorfismo $\varphi: F \rightarrow M$ tale che $h = f\varphi$. Si ha dunque $X = \text{im } h \subseteq \text{im } \varphi$. Poiché X genera M , allora, $\text{im } \varphi = M$. Di conseguenza $M \simeq F/\ker \varphi$. \square

Ritroviamo, come caso particolare di quest'ultima proposizione la [Proposizione 1.21](#) ed il [Corollario 1.32](#), che, dal punto di vista assunto in questa sezione, descrivono i (pre)moduli liberi di rango uno e mostrano che i (pre)moduli ciclici sono isomorfi a loro quozienti.

Esercizi.

4.E.1. Se R è un campo, ogni R -modulo (ovvero R -spazio vettoriale) è somma diretta di sottospazi di dimensione 1, ciascuno dei quali è isomorfo a R_R . Dunque la [Proposizione 4.16](#) mostra che ogni spazio vettoriale è un modulo libero. Inoltre l'applicazione universale f che appare nell'enunciato della [Proposizione 4.16](#) ha per immagine quella che, nel caso in cui R sia un campo, è la ben nota base canonica di uno spazio vettoriale numerico. Questo (tenendo sempre presente la [Proposizione 4.15](#)) mostra che le basi degli spazi vettoriali, come definite in algebra lineare, sono effettivamente basi di moduli liberi (con l'immersione come applicazione universale), nel senso che abbiamo qui definito.

Per un arbitrario anello commutativo unitario R , sia F un R -modulo libero e X una sua base contenuta in esso (con $X \hookrightarrow F$ applicazione universale). X ha in comune con le basi degli spazi vettoriali la proprietà di essere un insieme minimale di generatori di F (questo dovrebbe essere chiaro) ma non necessariamente vale il viceversa. Ad esempio, $\mathbb{Z}_{\mathbb{Z}}$ è un \mathbb{Z} -modulo libero in cui $\{2, 3\}$ è un insieme minimale di generatori, ma $\mathbb{Z}_{\mathbb{Z}}$ non è libero su un insieme di cardinalità due, quindi $\{2, 3\}$ non ne è una base,

4.E.2. A complemento dell'osservazione precedente verificare che un anello commutativo unitario R è un campo se e solo se ogni R -modulo è libero.

4.E.3. Invertendo un'osservazione provata nel testo, verificare che se R è un anello commutativo unitario non nullo, X e Y sono due insiemi e F_X e F_Y sono R -moduli liberi rispettivamente su X e Y , se $F_X \simeq_R F_Y$ allora $|X| = |Y|$. Si può procedere secondo le indicazioni che seguono, utilizzando il fatto che il risultato vale per gli spazi vettoriali. Sia $M \triangleleft R$ e siano $V_X = F_X M/M$ e $V_Y = F_Y M/M$; questi, per cambio di scalari, si possono riguardare come due (R/M) -spazi vettoriali. Basta allora provare che V_X e V_Y sono (R/M) -liberi su X e Y e che sono isomorfi tra loro se $F_X \simeq_R F_Y$.

Una volta dimostrato questo, usando il [Lemma 4.17](#) è facile estendere lo stesso risultato anche al caso dei premoduli: premoduli liberi isomorfi (sullo stesso anello commutativo) hanno necessariamente basi equipotenti.

4.E.4. Per prevenire un possibile dubbio: se R è un anello commutativo unitario non nullo, R_R è un R -modulo, quindi anche un R -premodulo, ma mentre è libero come R -modulo non è libero come R -premodulo. Quest'ultima affermazione può essere dedotta, ad esempio, dal fatto che, detto S l'anello accresciuto definito da R , se R_R fosse libero come R -premodulo lo sarebbe anche come S -modulo, ma R_R , riguardato come S -modulo non è fedele, dal momento che, in S , l'ideale R è annullato da $1_R - 1_S$. Per trarre la stessa conclusione in modo diretto, supponiamo per assurdo che R_R sia un R -premodulo libero su un insieme X . Allora certamente $X \neq \emptyset$. Ora, S (lo stesso di prima) ha un'ovvia struttura di R -premodulo (ma non di R -modulo!) in cui l'operazione esterna $S \times R \rightarrow S$ è la restrizione della moltiplicazione interna di S , ed esiste un'applicazione $h: X \rightarrow S$ la cui immagine non è contenuta in R . L'assunzione che R_R sia libero su X come R -premodulo implica che debba esistere un omomorfismo di R -premoduli $\varphi: R_R \rightarrow S$ la cui immagine contenga $\text{im } f$. Però, per ogni R -omomorfismo $\varphi: R_R \rightarrow S$ ed ogni $r \in R$, si ha $r^\varphi = (r1_R)^\varphi = r^\varphi 1_R \in R$, essendo $R \triangleleft S$, quindi $\text{im } \varphi \subseteq R$ e dunque $\text{im } f \not\subseteq \text{im } \varphi$. Questa contraddizione completa la dimostrazione.

4.E.5. La definizione di oggetto libero si dà in ogni categoria, ad esempio per ogni tipo di struttura algebrica; la definizione di ottiene da quella fornita per il caso dei (pre)moduli, sostituendo l'espressione R -(pre)modulo con quella che indica il tipo di struttura (monoide, gruppo, etc.) pertinente. Gli analoghi dei principali risultati generali qui provati continuano a valere, con la stessa dimostrazione: questo vale per le proposizioni [4.14](#), [4.15](#) e, nel caso in cui oggetti liberi esistano per ogni insieme, [4.20](#). Quest'ultima condizione è soddisfatta, ad esempio, per le categorie dei semigrupperi, dei monoidi, dei gruppi, degli anelli, delle algebre su un fissato anello commutativo unitario, ma non per quella dei campi, come suggerito dal

prossimo esercizio.

4.E.6. Sia $X = \{x\}$ un singleton. Mostrare che non esistono campi liberi su X . Suggerimento: se F fosse un campo libero su X , scelto un campo K di caratteristica diversa da quella di F dovrebbe esistere un omomorfismo di campi da F a K , ma questo non è possibile (qui per omomorfismo di campi si intende un omomorfismo di anelli unitari tra due campi).

Mostrare anche che non esistono oggetti liberi su X nella categoria dei gruppi abeliani finiti.

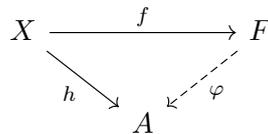
4.E.7. Non per ogni categoria di strutture algebriche le applicazioni universali che descrivono oggetti liberi sono necessariamente iniettive. Ad esempio, consideriamo la categoria dei gruppi identici. Dal fatto che per ogni insieme X ed ogni gruppo identico E esiste esattamente un'applicazione da X a E segue che ogni gruppo identico è un 'gruppo identico libero' su qualsiasi insieme; abbiamo così abbondanza di applicazioni universali non iniettive.

4.E.8. Fornire una dimostrazione alternativa della [Proposizione 4.19](#) che utilizzi solo un diagramma in cui appaiono, con le notazioni lì usate, X , F ed $M = F/F'$. Questa dimostrazione è più semplice di quella fornita nel testo, ma ha lo svantaggio di non essere, a differenza di quella, immediatamente riproducibile per altri tipi di strutture (non, ad esempio, per anelli liberi o per gruppi liberi).

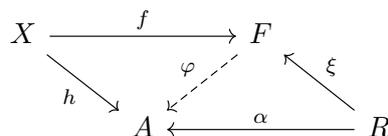
4.E.9. Le [Proposizioni 4.19](#) e [4.20](#) mostrano bene in che senso, fissato un anello commutativo R , gli R -(pre)moduli liberi sono quelli di tipo 'più generale possibile'. Infatti, se F è un R -(pre)modulo libero su una base X , vediamo che F è generato da un insieme di $|X|$ elementi e ogni R -(pre)modulo che sia generato da $|X|$ elementi è isomorfo ad un quoziente di F .

4.3.2 Algebre unitarie libere: anelli di polinomi

Fissato un anello commutativo unitario R , passiamo ora a considerare gli oggetti liberi nella categoria delle R -algebre unitarie (come sempre in queste note 'algebra' sta per 'algebra commutativa associativa'). Riproducendo la definizione data per (pre)moduli, se X è un insieme diciamo che F è una R -algebra unitaria libera con applicazione universale f se e solo se F è una R -algebra unitaria, f è un'applicazione da X al sostegno di F e, per ogni R -algebra unitaria A ed ogni applicazione h da X al sostegno di A esiste uno ed un solo omomorfismo di R -algebre unitarie $\varphi: F \rightarrow A$ tale che $h = f\varphi$.



Ricordando il [Teorema 1.24](#) e la [Proposizione 1.25](#), chiamando ξ l'omomorfismo di struttura di F possiamo riformulare la stessa proprietà in questo modo: scelti comunque un anello commutativo unitario A , un omomorfismo di anelli unitari $\alpha: R \rightarrow A$ ed un'applicazione h da X al sostegno di A , esiste uno ed un solo omomorfismo di anelli unitari $\varphi: F \rightarrow A$ che renda commutativo il diagramma:



Valgono per le algebre unitarie libere proprietà analoghe a quelle provate per i (pre)moduli liberi; dalle [proposizioni 4.14](#), [4.15](#) e [4.20](#), sostituendo l'espressione 'algebra unitaria' a

‘(pre)modulo’ e duplicando le dimostrazioni si ottengono i corrispondenti risultati per le algebre unitarie libere su un anello commutativo unitario. Ad esempio, otteniamo l’unicità a meno di isomorfismi: se F e G sono algebre unitarie libere su un prefissato anello commutativo unitario R , con applicazioni universali $f: X \rightarrow F$ e $g: Y \rightarrow G$, dove X e Y sono insiemi legati tra loro dalla biezione $t: X \rightarrow Y$, allora esiste uno ed un solo isomorfismo di R -algebre unitarie $\alpha: F \rightarrow G$ tale che $f\alpha = tg$.

Anche la questione dell’esistenza di oggetti liberi ha per le algebre unitarie la stessa risposta positiva che ha per i (pre)moduli: per ogni anello commutativo unitario R ed ogni insieme X esiste un’algebra unitaria libera su X , e l’applicazione universale che la descrive è iniettiva. L’oggetto libero che si ottiene in questo caso è già familiare a chi legge: è infatti, a meno di isomorfismi, un anello di polinomi.

Descriviamo, rapidamente ed in modo schematico, una costruzione delle algebre unitarie libere. Fissato l’insieme X , sia $M(X)$ il monoide costituito dalle applicazioni $X \rightarrow \mathbb{N}$ a supporto finito, cioè tali che sia finito l’insieme degli elementi di X con immagine diversa da 0, munito dell’operazione di addizione puntuale. Convieni usare la notazione moltiplicativa per $M(X)$ e identificare ogni $x \in X$ con l’applicazione $X \rightarrow \mathbb{N}$ che manda x in 1 ed ogni altro elemento di X in 0. In questo modo gli elementi di $M(X)$ vengono tutti rappresentati nella forma $\prod_{x \in X_0} x^{\lambda_x}$ per una opportuna parte finita X_0 di X , dove ciascuno degli esponenti λ_x è un numero naturale: tale elemento è l’applicazione che manda ogni $x \in X_0$ in λ_x e ciascun elemento di $X \setminus X_0$ in 0 (si può provare, farlo per esercizio, che questo è il monoide commutativo libero su X , con applicazione universale suggerita dall’identificazione fatta). Per quanto banale sia, osserviamo che se a e b sono elementi di $M(X)$ e X_0 è una parte finita di X contenente i supporti di a e di b , si possono rappresentare a e b come $\prod_{x \in X_0} x^{\alpha_x}$ e $\prod_{x \in X_0} x^{\beta_x}$ e la definizione di $M(X)$ fornisce, non sorprendentemente, $ab = \prod_{x \in X_0} x^{\alpha_x + \beta_x}$. Sia ora F l’ R -modulo libero su $M(X)$, cioè la somma diretta esterna $\prod_{a \in M(X)} R_R$; come nella costruzione effettuata nella sottosezione 4.3.1 ad ogni $a \in M(X)$ associamo l’elemento e_a di F che ha 1_R come coordinata corrispondente ad a ed ogni altra coordinata 0_R . Muniamo F della moltiplicazione definita da $fg = \sum_{a,b \in M(X)} e_{ab} f_a g_b$ per ogni $f = \sum_{a \in M(X)} e_a f_a$ e $g = \sum_{a \in M(X)} e_a g_a$ in F (come al solito, f_a ed g_a sono diversi da zero solo per un numero finito di scelte di a). Si verifica senza particolari difficoltà che in questo modo F risulta strutturato come R -algebra unitaria, che risulta inoltre libera con applicazione universale $e: x \in X \mapsto e_x \in F$ (ricordiamo che ogni elemento di X è stato identificato con un elemento di $M(X)$): per ogni R -algebra unitaria A ed ogni applicazione $h: X \rightarrow A$ l’unico omomorfismo $\varphi: F \rightarrow A$ di R -algebre unitarie tale che $e\varphi = h$ è quello definito da $e_a^\varphi = \prod_{x \in X_0} (x^h)^{\alpha_x}$ per ogni $a = \prod_{x \in X_0} x^{\alpha_x} \in M(X)$ e $f^\varphi = \sum_{a \in M(X)} e_a^\varphi f_a$ per ogni $f = \sum_{a \in M(X)} e_a f_a \in F$.

La costruzione mostra che, come accade per i (pre)moduli, le algebre unitarie libere hanno applicazioni universali iniettive e sono generate (come algebre unitarie) dall’immagine di una loro applicazione universale. Notiamo anche che, essendo F libero e non nullo, quindi fedele come R -modulo, l’omomorfismo di struttura $r \in R \mapsto 1_F r \in F$ è iniettivo, dunque R è isomorfo al sottoanello unitario $1_F R$ di F .

Utilizzando l’analogo della [Proposizione 4.15](#) per algebre unitarie (e le considerazioni svolte nell’[Osservazione 1.J.1](#)), ne possiamo trarre questa conseguenza: scelti comunque un anello commutativo unitario R ed un insieme X disgiunto da R , esiste una R -algebra unitaria libera F su X che contenga X come sottoinsieme ed R come sottoanello unitario, ed abbia le immersioni $X \hookrightarrow F$ e $R \hookrightarrow F$ come applicazione universale ed omomorfismo di struttura. Si chiama *anello di polinomi a coefficienti in R nell’insieme di indeterminate X^2* un’algebra con queste proprietà; una tale algebra viene denotata con il simbolo $R[X]$,³ o anche con simboli come $R[x, y, \dots, z]$

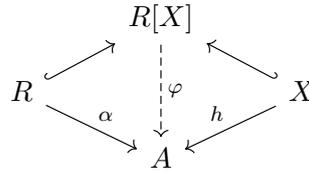
² si usano ovviamente anche forme abbreviate di questa espressione, come ‘anello di polinomi in R su X ’.

³ questo simbolo porta con sé un certo livello di ambiguità, dal momento che lo stesso simbolo viene usato anche

se x, y, \dots, z sono gli elementi (distinti) di X .⁴ Ovviamente, fissati R ed X , esistono più anelli di polinomi in R su X , ma questi sono tutti isomorfi tra loro, quindi ci si prende usualmente la libertà di non distinguere tra essi. Come di abitudine, si chiamano polinomi gli elementi di un anello di polinomi.

Ovviamente, a meno di isomorfismi, gli anelli di polinomi su R non sono altro che le R -algebre unitarie libere; se S è un anello isomorfo a R e Y un insieme equipotente a X , poi, l'analogo della [Proposizione 4.14](#) fornisce $S[Y] \simeq R[X]$.

Rendendo esplicita la condizione sintetizzata nel diagramma commutativo della pagina precedente, notiamo che l'anello di polinomi $R[X]$ verifica (ed è, a meno di isomorfismi, caratterizzato da) questa proprietà universale: per ogni anello commutativo unitario A , ogni omomorfismo $\alpha: R \rightarrow A$ di anelli unitari ed ogni applicazione $h: X \rightarrow A$, esiste uno ed un solo omomorfismo di anelli unitari $\varphi: R[X] \rightarrow A$ che prolunghi simultaneamente α e h .

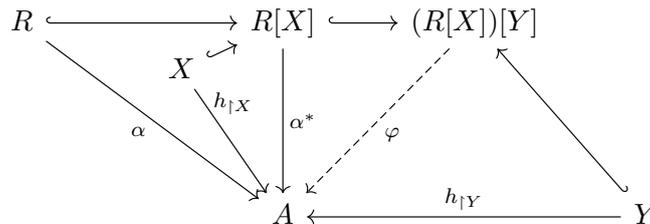


Queste due osservazioni sono spesso utili:

Lemma 4.21. *Siano R un anello commutativo unitario, $R[X]$ un anello di polinomi su R e $(R[X])[Y]$ un anello di polinomi su $R[X]$. Allora $(R[X])[Y]$ è isomorfo all'anello di polinomi $R[X \cup Y]$.*

Dimostrazione. Si tratta di provare che $(R[X])[Y]$ è una R -algebra unitaria libera su $X \cup Y$ (l'omomorfismo di struttura sottinteso è l'immersione). A questo scopo, sia A una R -algebra unitaria con omomorfismo di struttura α , e sia $h: X \cup Y \rightarrow A$ un'applicazione. Ciò che va provato è che esiste uno ed un solo omomorfismo di anelli unitari $\varphi: (R[X])[Y]$ che abbia h e α come restrizioni a $X \cup Y$ e R .

Essendo $R[X]$ libero su X , esiste uno ed un solo omomorfismo di anelli unitari $\alpha^*: R[X] \rightarrow A$ le cui restrizioni a X ed a R siano $h|_X$ (la restrizione di h a X) e α .



Ora, poiché $(R[X])[Y]$ è libero, come $R[X]$ -algebra unitaria, su Y , esiste uno ed un solo omomorfismo di anelli unitari $\varphi: (R[X])[Y] \rightarrow A$ le cui restrizioni a Y e $R[X]$ sono $h|_Y$ e α^* . Dunque, il diagramma qui sopra è commutativo; ne segue che le restrizioni di φ a $X \cup Y$ e R sono h e α , come richiesto.

D'altra parte, se $\psi: (R[X])[Y] \rightarrow A$ è un omomorfismo di anelli unitari tale che $\psi|_{X \cup Y} = h$ e $\psi|_R = \alpha$, allora le restrizioni di $\psi|_{R[X]}$ a X e R sono $h|_X$ e α , quindi, per l'unicità di α^* , si ha $\psi|_{R[X]} = \alpha^*$; da questa segue, sempre per unicità, $\psi = \varphi$. Con questo la dimostrazione è completa. \square

per indicare l'anello (o l'algebra) generato da $R \cup X$ anche in contesti in cui l'algebra risultante non sia libera; faremo in modo che il discorso chiarisca sempre a cosa ci riferiamo.

⁴ anche il simbolo $R[x]$ presenta un problema di ambiguità: si riferisce ad un anello di polinomi sull'insieme x di indeterminate o sull'insieme $\{x\}$ (cioè su una sola indeterminata)? Stabiliamo una convenzione: quando usiamo una lettera minuscola ci riferiamo al secondo caso.

Tenendo presente che gli anelli di polinomi sono in realtà definiti a meno di isomorfismi, il [Lemma 4.21](#) mostra che, nelle notazioni date, $R[X]$ si può identificare col sottoanello generato da $R \cup X$ (ovvero la R -sottoalgebra unitaria generata da X) in $R[X \cup Y]$ e quindi $R[X \cup Y]$ con $(R[X])[Y]$, cosa che d'ora in poi faremo, a cominciare da prossimo lemma.

Lemma 4.22. *Nelle notazioni del lemma precedente, $\nu: f \in R[X] \rightarrow f + (Y) \in R[X \cup Y]/(Y)$ è un isomorfismo di R -algebre unitarie.*

Dimostrazione. È chiaro che ν è un omomorfismo suriettivo di R -algebre unitarie, perché ogni polinomio in $R[X \cup Y]$ è congruo modulo (Y) ad un polinomio in $R[X]$. Consideriamo l'applicazione $h: X \cup Y \rightarrow R[X]$ definita ponendo $x^h = x$ e $y^h = 0_R$ per ogni $x \in X$ e $y \in Y$.

$$\begin{array}{ccccc}
 X \cup Y & \hookrightarrow & R[X \cup Y] & \longleftarrow & R[X] \\
 & \searrow h & \tau \downarrow & \swarrow & \downarrow \nu \\
 & & R[X] & \xleftarrow{\theta} & R[X \cup Y]/(Y)
 \end{array}$$

Utilizzando la proprietà universale, vediamo che h si estende ad un (unico) omomorfismo di anelli $\tau: R[X \cup Y] \rightarrow R[X]$ che manda in sé ogni elemento di $R[X]$ e tale che $Y \subseteq \ker \tau$, cioè $(Y) \subseteq \ker \tau$. Per il primo teorema di omomorfismo, τ induce l'omomorfismo $\theta: f + (Y) \in R[X \cup Y]/(Y) \mapsto f^\tau \in R[X]$. Per ogni $x \in X$ abbiamo $x^{\nu\theta} = x^\tau = x^h = x$; da ciò segue $\nu\theta = \text{id}_{R[X]}$. Essendo ν suriettiva se ne ricava che ν è biettiva, quindi un isomorfismo. \square

Come già accennato, vale l'analogo della [Proposizione 4.20](#), il che significa che se $R[X]$ è un anello di polinomi sull'anello commutativo unitario R , ogni R -algebra unitaria che sia generata da al più $|X|$ suoi elementi è isomorfa ad un quoziente di $R[X]$. Come caso particolare, abbiamo:

Corollario 4.23. *Sia R un sottoanello unitario di un anello commutativo unitario S , e sia Y una parte di S tale che, come anello, S sia generato da $R \cup Y$. Allora S è isomorfo ad un quoziente di un anello di polinomi $R[X]$ su un insieme di indeterminate X equipotente a Y .*

Più precisamente, in questa situazione, l'immersione $R \hookrightarrow S$ si prolunga ad un omomorfismo suriettivo $\varepsilon: R[X] \rightarrow S$.

Dimostrazione. S è una R -algebra unitaria via immersione $R \hookrightarrow S$; dire che, come anello (o come anello unitario), S è generato da $R \cup Y$ equivale a dire che S , come R -algebra unitaria, è generato da Y . L'asserto segue dunque immediatamente dalla proprietà universale per gli anelli di polinomi. \square

Questo corollario fornisce il metodo di uso più frequente per realizzare ampliamenti di anelli commutativi unitari (si dice che l'anello commutativo unitario S è un ampliamento di R se, come nella situazione del [Corollario 4.23](#), R è un sottoanello unitario di S). Un esempio è stato certamente già incontrato nei corsi elementari di algebra: un'ampliamento algebrico semplice di un campo F (dunque: un campo di cui F sia un sottocampo e che sia generato come anello da F e da un elemento F -algebra, da un singleton) è stato costruito come quoziente dell'anello di polinomi ad una indeterminata su F . Il [Corollario 4.23](#) mostra che, essenzialmente, questa era l'unica maniera di procedere.

Esercizi e osservazioni.

4.F.1. Verificare i dettagli della costruzione delle algebre unitarie libere, ed il fatto che questa costruzione soddisfi la proprietà universale richiesta dalla definizione. Con riferimento alle notazioni usate nel testo, esplicitare le unità di $M(X)$ e di F .

4.F.2. Dati un anello commutativo unitario R ed un insieme X , si può costruire una R -algebra libera su X in modo analogo a quanto fatto per costruire una R -algebra unitaria libera su X , sostituendo il monoide commutativo libero $M(X)$ su X con il semigrupp commutativo libero $M^+(X) = M(X) \setminus \{1_M\}$ su X .

Se $X \cap R = \emptyset$, l'ideale generato da X nell'anello di polinomi $R[X]$ è una R -algebra libera su X .

4.F.3. Dal momento che gli anelli commutativi si possono riguardare equivalentemente come \mathbb{Z} -algebre, la teoria esposta per le algebre ha quella per gli anelli commutativi come caso particolare. In particolare gli anelli di polinomi su \mathbb{Z} forniscono gli oggetti liberi nella categoria degli anelli commutativi unitari.

4.F.4. Se R è un anello commutativo unitario, cosa è $R[\emptyset]$?

4.F.5. Come accennato già subito dopo il [Corollario 4.23](#), gli anelli di polinomi forniscono lo strumento adatto a costruire anelli commutativi unitari con elementi che verifichino proprietà preassegnate. Ad esempio, supponiamo di voler costruire, nelle maniera più economica possibile, un anello commutativo unitario di caratteristica 0 che abbia un elemento non nullo a quadrato nullo, cioè un anello commutativo unitario R che abbia un sottoanello unitario isomorfo a \mathbb{Z} ed un elemento a tale che $a \neq 0_R = a$. Se un tale R esiste, anche il suo sottoanello generato da $\{1_R, a\}$ ha le stesse proprietà, quindi possiamo anche limitarci a cercare di costruire R tra gli anelli che siano, come anelli unitari, generati dall'elemento a richiesto. Per il [Corollario 4.23](#), un tale anello dovrà essere isomorfo ad un quoziente dell'anello di polinomi $\mathbb{Z}[x]$ ad una indeterminata; sapere questo rende la ricerca molto più semplice. Meglio ancora: per lo stesso corollario, se esiste un R con le proprietà richieste, esiste un (unico) omomorfismo suriettivo $\varepsilon: \mathbb{Z}[x] \rightarrow R$ di anelli unitari che manda x in a ; dunque $R \simeq \mathbb{Z}[x] / \ker \varepsilon$, inoltre a deve corrispondere nell'isomorfismo al laterale individuato da x . Ora, avendo noi richiesto $a^2 = 0$, si deve avere $x^2 \in \ker \varepsilon$; da ciò segue che R deve essere isomorfo ad un quoziente di $\bar{\mathbb{Z}} := \mathbb{Z}[x] / (x^2)$. A questo punto la nostra ricerca è finita: si vede subito che $\bar{\mathbb{Z}}$ verifica le proprietà richieste per R : il suo elemento $\bar{x} = x + (x^2)$ non è nullo, perché $x \notin (x^2)$, ma ha quadrato nullo.

Dovrebbe essere piuttosto evidente l'analogia con la costruzione fatta nei corsi elementari di algebra dell'estensione di un campo ottenuta aggiungendo una radice di un polinomio irriducibile di grado maggiore di uno.

4.F.6. Costruire un anello commutativo unitario che abbia una copia del campo razionale come sottoanello unitario ed elementi non nulli a, b, c tali che $ab = ac$ e $b \neq c$.

4.3.3 Prodotti e coprodotti

Anche le costruzioni, già presentate, delle somme dirette e dei prodotti diretti di (pre)moduli hanno una interpretazione categoriale come oggetti universali, vediamo come.

Prodotti Sia R un anello commutativo, e siano dati un R -(pre)modulo P , una famiglia $(M_i)_{i \in I}$ di R -(pre)moduli e, per ogni $i \in I$, un R -omomorfismo $\pi_i: P \rightarrow M_i$. Si dice che P è *prodotto* della famiglia $(M_i)_{i \in I}$ con famiglia di proiezioni $(\pi_i)_{i \in I}$, o che $(P, (\pi_i)_{i \in I})$ è un prodotto di $(M_i)_{i \in I}$ se e solo se, scelti comunque un R -(pre)modulo A e, per ogni $i \in I$, un R -omomorfismo $\alpha_i: A \rightarrow M_i$, esiste uno ed un solo R -omomorfismo $\varphi: A \rightarrow P$ tale che, per ogni $i \in I$, si abbia $\alpha_i = \varphi \pi_i$.

4 Costruzioni per moduli e per anelli

È bene soffermarsi su un punto: la richiesta è che esista e sia unico l' R -omomorfismo φ che renda commutativo, *simultaneamente* ciascuno dei diagrammi

$$\begin{array}{ccc} P & \xrightarrow{\pi_i} & M_i \\ & \swarrow \varphi & \nearrow \alpha_i \\ & A & \end{array}$$

al variare di $i \in I$. La nozione di prodotto si può dare (anzi, si dà) in ogni categoria. Sostituendo l'espressione ' R -(pre)modulo' con 'anello', 'anello commutativo', 'anello commutativo unitario', 'gruppo' etc, e R -omomorfismo con 'omomorfismo di anelli', di anelli unitari, di gruppi etc, nella definizione appena data si ottengono le definizioni di prodotto nelle corrispondenti categorie.

Quella di prodotto è una costruzione universale, e come per tutte le costruzioni universali vale per i prodotti un teorema di unicità a meno di isomorfismi analogo alla [Proposizione 4.14](#); lo enunciamo e dimostriamo nel caso dei (pre)moduli.

Proposizione 4.24. *Sia R un anello commutativo, siano $(M_i)_{i \in I}$ e $(N_j)_{j \in J}$ famiglie di R -(pre)moduli; supponiamo che $*$: $I \rightarrow J$ sia una biezione e, per ogni $i \in I$, $\tau_i: M_i \rightarrow N_{i^*}$ un R -isomorfismo. Siano P un prodotto di $(M_i)_{i \in I}$ con famiglia di proiezioni $(\pi_i)_{i \in I}$ e Q un prodotto di $(N_j)_{j \in J}$ con famiglia di proiezioni $(\theta_j)_{j \in J}$. Allora esiste uno ed un solo R -isomorfismo $\alpha: P \rightarrow Q$ tale che per ogni $i \in I$ si abbia $\pi_i \tau_i = \alpha \theta_{i^*}$.*

$$\begin{array}{ccc} P & \xrightarrow{\pi_i} & M_i \\ \alpha \downarrow & & \downarrow \tau_i \\ Q & \xrightarrow{\theta_{i^*}} & N_{i^*} \end{array}$$

Dimostrazione. Per ogni $i \in I$, sia $\alpha_i = \pi_i \tau_i: P \rightarrow N_{i^*}$. Per ogni $j \in J$, indichiamo con $*j$ l'immagine di j mediante l'inversa di $*$, quindi α_{*j} è un R -omomorfismo $P \rightarrow N_{*j}$. Per la proprietà che definisce i prodotti, esiste uno ed un solo R -omomorfismo $\alpha: P \rightarrow Q$ tale che $\alpha_{*j} = \alpha \theta_j$ per ogni $j \in J$, vale a dire: $\alpha_i = \alpha \theta_{i^*}$ per ogni $i \in I$. Simmetricamente, ma in modo più diretto, per ogni $i \in I$ poniamo $\beta_i = \theta_{i^*} \tau_i^{-1}: Q \rightarrow M_i$, e ricaviamo che esiste uno ed un solo R -omomorfismo $\beta: Q \rightarrow P$ tale che $\beta_i = \beta \pi_i$ per ogni $i \in I$.

$$\begin{array}{ccccc} P & \xrightarrow{\alpha} & Q & \xrightarrow{\beta} & P \\ \pi_i \downarrow & \searrow \alpha_i & \downarrow \theta_{i^*} & \searrow \beta_i & \downarrow \pi_i \\ M_i & \xrightarrow{\tau_i} & N_{i^*} & \xrightarrow{\tau_i^{-1}} & M_i \end{array}$$

Come si legge da questo diagramma commutativo, per ogni $i \in I$, si ha $\alpha \beta \pi_i = \alpha \beta_i = \alpha \theta_{i^*} \tau_i^{-1} = \alpha_i \tau_i^{-1} = \pi_i \tau_i \tau_i^{-1} = \pi_i$. Dalla definizione di prodotto segue che esiste esattamente un R -omomorfismo $\varphi: P \rightarrow P$ tale che $\varphi \pi_i = \pi_i$ per ogni $i \in I$. Poiché sia $\alpha \beta$ che id_P soddisfano questa condizione per φ , si ha $\alpha \beta = \text{id}_P$. Scambiano i ruoli di P e Q e delle corrispondenti proiezioni, si prova allo stesso modo $\beta \alpha = \text{id}_Q$. Pertanto α è un R -isomorfismo. La dimostrazione è completa. \square

Quasi sempre si incontra questo risultato nella forma semplificata in cui i prodotti sono riferiti ad un'unica famiglia: se R è un anello commutativo unitario, $(M_i)_{i \in M}$ una famiglia di R -(pre)moduli e $(P, (\pi_i)_{i \in I})$ e $(Q, (\theta_i)_{i \in I})$ due suoi prodotti, allora esiste uno ed un solo R -isomorfismo $\alpha: P \rightarrow Q$ tale che $\pi_i = \alpha \theta_i$ per ogni $i \in I$. In effetti questo enunciato è equivalente alla [Proposizione 4.24](#) se si tiene in conto del seguente analogo della [Proposizione 4.15](#), la cui dimostrazione si lascia per esercizio:

Proposizione 4.25. *Siano R un anello commutativo unitario e $(P, (\pi_i)_{i \in I})$ un prodotto di una famiglia $(M_i)_{i \in I}$ di R -(pre)moduli. Se $\sigma: P_1 \rightarrow P$ un isomorfismo di R -(pre)moduli, $s: J \rightarrow I$ un'applicazione biettiva, $(N_j)_{j \in J}$ una famiglia di R -(pre)moduli e, per ogni $j \in J$, $\sigma_j: M_{j^s} \rightarrow N_j$ è un R -isomorfismo, allora $(P_1, (\sigma \pi_{j^s} \sigma_j)_{j \in J})$ è un prodotto di $(N_j)_{j \in J}$.*

A meno di isomorfismi i prodotti di famiglie di (pre)moduli sono i prodotti diretti, con le proiezioni canoniche come proiezioni:

Proposizione 4.26. *Sia $(M_i)_{i \in I}$ una famiglia di (pre)moduli sull'anello commutativo R . Allora il prodotto diretto $\prod_{i \in I} M_i$ è un prodotto di $(M_i)_{i \in I}$ con le proiezioni canoniche come proiezioni.*

Dimostrazione. Verifichiamo che le richieste della definizione di prodotto siano soddisfatte da $P := \prod_{i \in I} M_i$ e dalle proiezioni canoniche $\pi_i: (a_j)_{j \in J} \in P \mapsto a_i \in M_i$.

Siano A un R -(pre)modulo e, per ogni $i \in I$, un R -omomorfismo $\alpha_i: A \rightarrow M_i$. Allora, come dovrebbe risultare chiaro, esiste un'unica applicazione $\varphi: A \rightarrow P$ tale che $\varphi\pi_i = \alpha_i$ per ogni $i \in I$, precisamente $\varphi: a \in A \mapsto (a^{\alpha_i})_{i \in I} \in P$. Inoltre, come si verifica immediatamente, φ è un R -omomorfismo. Ciò mostra che $(P, (\pi_i)_{i \in I})$ è un prodotto di $(M_i)_{i \in I}$, come richiesto. \square

Similmente, e si lascia la dimostrazione come esercizio, sia nel caso degli anelli commutativi che in quello degli anelli commutativi unitari, e quindi delle algebre su un fissato anello commutativo unitario, i prodotti (nel senso categoriale) sono, a meno di isomorfismi, i prodotti diretti con le proiezioni canoniche. Ulteriore conseguenza è che in tutti i casi considerati ((pre)moduli, anelli commutativi, anelli commutativi unitari, algebre) le proiezioni ottenute per i prodotti sono omomorfismi suriettivi.

Coprodotti La nozione di coprodotto è duale di quella di prodotto, il che, come sempre per concetti categoriali, significa che si ottiene dalla seconda 'invertendo il verso' dei morfismi.

Nel caso dei (pre)moduli la definizione è questa: fissato un anello commutativo R , siano dati un R -(pre)modulo C , una famiglia $(M_i)_{i \in I}$ di R -(pre)moduli e, per ogni $i \in I$, un R -omomorfismo $\mu_i: M_i \rightarrow C$. Si dice che C è *coprodotto* della famiglia $(M_i)_{i \in I}$ con famiglia di iniezioni $(\mu_i)_{i \in I}$, o che $(C, (\mu_i)_{i \in I})$ è un coprodotto di $(M_i)_{i \in I}$ se e solo se, scelti comunque un R -(pre)modulo A e, per ogni $i \in I$, un R -omomorfismo $\alpha_i: M_i \rightarrow A$, esiste uno ed un solo R -omomorfismo $\varphi: C \rightarrow A$ tale che, per ogni $i \in I$, si abbia $\alpha_i\varphi = \mu_i$.

$$\begin{array}{ccc} M_i & \xrightarrow{\mu_i} & C \\ & \searrow \alpha_i & \swarrow \varphi \\ & & A \end{array}$$

Valgono per i coprodotti, con dimostrazioni simili, proposizioni analoghe a quelle enunciate per i prodotti di (pre)moduli:

Proposizione 4.27. *Sia R un anello commutativo, siano $(M_i)_{i \in I}$ e $(N_j)_{j \in J}$ famiglie di R -(pre)moduli; supponiamo che $*$: $I \rightarrow J$ sia una biezione e, per ogni $i \in I$, $\tau_i: M_i \rightarrow N_{i^*}$ un R -isomorfismo. Siano C un coprodotto di $(M_i)_{i \in I}$ con famiglia di iniezioni $(\mu_i)_{i \in I}$ e D un coprodotto di $(N_j)_{j \in J}$ con famiglia di proiezioni $(\nu_j)_{j \in J}$. Allora esiste uno ed un solo R -isomorfismo $\alpha: C \rightarrow D$ tale che per ogni $i \in I$ si abbia $\mu_i\alpha = \tau_i\nu_{i^*}$.*

$$\begin{array}{ccc} M_i & \xrightarrow{\mu_i} & C \\ \tau_i \downarrow & & \downarrow \nu_{i^*} \\ N_{i^*} & \xrightarrow{\nu_{i^*}} & D \end{array}$$

Proposizione 4.28. *Siano R un anello commutativo unitario e $(C, (\mu_i)_{i \in I})$ un coprodotto di una famiglia $(M_i)_{i \in I}$ di R -(pre)moduli. Se $\sigma: C \rightarrow C_1$ un isomorfismo di R -(pre)moduli, $s: J \rightarrow I$ è un'applicazione biettiva, $(N_j)_{j \in J}$ una famiglia di R -(pre)moduli e, per ogni $j \in J$, $\sigma_j: N_j \rightarrow M_{j^s}$ è un R -isomorfismo, allora $(C_1, (\sigma_j\nu_{j^s})_{j \in J}\sigma)$ è un coprodotto di $(N_j)_{j \in J}$.*

I coprodotti dei (pre)moduli sono, essenzialmente, le somme dirette:

Proposizione 4.29. *Sia $(M_i)_{i \in I}$ una famiglia di (pre)moduli sull'anello commutativo R . Allora la somma diretta $\coprod_{i \in I} M_i$ è un coprodotto di $(M_i)_{i \in I}$ con i monomorfismi canonici come iniezioni.*

Dimostrazione. Sia $C := \coprod_{i \in I} M_i$ e, per ogni $i \in I$, $\mu_i: M_i \rightarrow C$ l' i -esimo monomorfismo canonico. Per verificare che $(C, (\mu_i)_{i \in I})$ sia un coprodotto di $(M_i)_{i \in I}$ consideriamo un arbitrario R -(pre)modulo A e, per ogni $i \in I$, un R -omomorfismo $\alpha_i: M_i \rightarrow A$. Supponiamo che φ sia un R -omomorfismo $C \rightarrow A$ tale che $\mu_i \varphi = \alpha_i$ per ogni $i \in I$. Sia $a = (a_i)_{i \in I} \in C$; dal momento che $a = \sum_{i \in I} a_i^{\mu_i}$, si deve avere $a \varphi = \sum_{i \in I} a_i^{\alpha_i}$. D'altra parte l'applicazione $(a_i)_{i \in I} \in C \mapsto \sum_{i \in I} a_i^{\alpha_i}$ è, come si verifica direttamente, un omomorfismo di R -(pre)moduli tale che $\mu_i \varphi = \alpha_i$ per ogni $i \in I$; dunque l'unico con questa proprietà. L'asserto è così provato. \square

A differenza di quanto accade nel caso dei prodotti, i coprodotti di anelli commutativi, anelli commutativi unitari, algebre su un fissato anello commutativo unitario, che pure esistono, non sono descritti allo stesso modo che nel caso dei (pre)moduli: non dalle somme dirette, ma dai prodotti tensoriali, che qui non discuteremo.

Esercizi.

4.G.1. A titolo di comparazione, nella categoria dei gruppi il prodotto (nel senso categoriale) è descritto dalla costruzione del prodotto cartesiano, analogamente a quanto accade per moduli e anelli; il coprodotto non è dato dall'analogo della somma diretta di moduli (che nella terminologia usuale della teoria dei gruppi si chiama prodotto diretto, fare attenzione al diverso uso di questa espressione per diverse categorie di strutture algebriche) ma da un'altra costruzione, quella del prodotto libero.

4.G.2. I simboli \prod e \coprod sono utilizzati in teoria delle categorie per denotare prodotti e coprodotti. Quanto qui discusso spiega perché abbiamo usato il simbolo \coprod per le somme dirette di (pre)moduli ma non di anelli.

5 Proprietà di anelli di polinomi e di serie formali di potenze

Terminologia e prime proprietà degli anelli di polinomi su un insieme arbitrario di indeterminate ricalcano abbastanza da vicino quelle già note nel caso dei polinomi ad una indeterminata. Fissato un anello di polinomi $(R[X], +, \cdot)$ sull'anello commutativo unitario R , per ogni $Y \subseteq X$ indichiamo con $\text{Mon } Y$ il sottomonoido generato da Y in $(R[X], \cdot)$ e ricordiamo anche che $R[Y]$ è, salvo indicazione contraria, tacitamente identificato con il sottoanello generato da $R \cup Y$ in $R[X]$. Gli elementi di $\text{Mon } X$ hanno la forma $\ell = \prod_{x \in X} x^{\lambda_x}$ dove ciascuno degli λ_x è un numero naturale e solo un numero finito di essi è positivo; inoltre sappiamo dalla costruzione delle algebre unitarie libere che ogni tale ℓ è univocamente determinato dalla famiglia $(\lambda_x)_{x \in X}$. I polinomi in $R[X]$, a loro volta, hanno la forma $f = \sum_{\ell \in \text{Mon } X} a_\ell \ell$, dove $a_\ell \in R$ per ogni $\ell \in \text{Mon } X$ e $\{\ell \in \text{Mon } X \mid a_\ell \neq 0_R\}$ è finito; inoltre f è univocamente determinato dalla famiglia $(a_\ell)_{\ell \in \text{Mon } X}$. Questa famiglia è la cosiddetta *famiglia dei coefficienti di f* ; in maggior dettaglio, per ogni $\ell \in \text{Mon } X$, l'elemento a_ℓ è il coefficiente di f relativo a ℓ . Il coefficiente di f relativo a $1_{\text{Mon } X} = 1_R$ prende il nome, tradizionale quanto brutto, di *termine noto*. Esso è l'immagine di f nell'omomorfismo (suriiettivo) di R -algebre unitarie $\varepsilon_0: R[X] \rightarrow R$ che manda ogni elemento di X in 0_R . Evidentemente $\ker \varepsilon_0 = (X)$, quindi $R[X]/(X) \simeq R$; questo è un caso particolare del [Lemma 4.22](#).

Di una indeterminata $x \in X$ si dice che appare nel polinomio $f \in R[X]$ se e solo se esiste un ℓ in $\text{Mon } X$ che sia multiplo di x e tale che il coefficiente di f relativo a ℓ non sia 0_R . In modo equivalente, dire che x appare in f significa dire, nel contesto dato, che $f \notin R[X \setminus \{x\}]$. Evidentemente, per ogni $f \in R[X]$, l'insieme delle indeterminate che appaiono in f è finito.

Indicheremo con νf il grado del polinomio ad una indeterminata f ; ad altre nozioni di grado, per anelli di polinomi a più indeterminate, si fa cenno nell'[Osservazione 5.A.1](#).

5.1 Due risultati elementari

Iniziamo con l'estensione al caso generale di un risultato noto dai corsi elementari di algebra per polinomi ad una indeterminata. In effetti questo risultato segue anche da quanto sarà provato, per via indipendente, nella [sezione 5.3](#), ma l'importanza di questo risultato suggerisce di fornirne comunque una dimostrazione diretta e più semplice.

Proposizione 5.1. *Sia $R[X]$ un anello di polinomi sull'anello commutativo unitario R . Allora:*

- (i) $R[X]$ è un dominio di integrità se e solo se R lo è;
- (ii) se R è un dominio di integrità, $\mathcal{U}(R[X]) = \mathcal{U}(R)$.

Dimostrazione. Questo risultato è ben noto nel caso $|X| = 1$ e quindi, ragionando per induzione sul numero delle indeterminate ed utilizzando il [Lemma 4.21](#), che comporta $R[X] \simeq (R[X \setminus \{x\}])[x]$ per ogni $x \in X$, è facile provarlo, più in generale, nel caso in cui X sia finito. Nel caso generale, è ovvio che R è un dominio di integrità se $R[X]$ lo è. Supponiamo invece che R sia un dominio di integrità, e sia $f \in R[X]$. Se f è un divisore dello zero oppure è invertibile, esiste $g \in R[X] \setminus 0$ tale che fg sia 0_R oppure 1_R . In entrambi i casi esiste un sottoinsieme finito X_0 di X tale che $f, g \in R[X_0]$, e quindi f è un divisore dello zero oppure un elemento

invertibile in $R[X_0]$. Poiché, come detto, il risultato vale per anelli di polinomi su un numero finito di indeterminate, e quindi per $R[X_0]$, $f = 0_R$ nel primo caso, $f, g \in \mathcal{U}(R)$ nel secondo. Con questo il lemma è provato.¹ \square

Lemma 5.2. *Siano R un anello commutativo unitario e $R[X]$ un anello di polinomi a coefficienti in R . Allora ogni elemento primo di R è primo anche in $R[X]$.*

Dimostrazione. Sia p un elemento primo in R . Allora $\bar{R} := R/pR$ è un dominio di integrità e quindi, per la [Proposizione 5.1](#), anche l'anello di polinomi $\bar{R}[X]$ è un dominio di integrità.² Per la proprietà universale degli anelli di polinomi, l'epimorfismo canonico $\nu: R \twoheadrightarrow \bar{R}$ si estende ad un omomorfismo $\varepsilon: R[X] \rightarrow \bar{R}[X]$ che manda in sé ogni elemento di X . È chiaro che anche ε è suriettivo, quindi $\bar{R}[X] \simeq R[X]/\ker \varepsilon$; dunque $\ker \varepsilon$ è un ideale primo di $R[X]$. Gli elementi di $\ker \varepsilon$ sono i polinomi i cui coefficienti sono multipli (in R) di p , quindi $\ker \varepsilon = pR[X]$. Abbiamo così provato che $pR[X]$ è un ideale primo, dunque p è un elemento primo in $R[X]$. \square

Esercizi.

5.A.1. Sia $R[X]$ un anello di polinomi sull'anello commutativo unitario R e sia $f \in R[X]$. Esiste più di un modo per estendere a f la nozione di grado di un polinomio ad una indeterminata. Uno è questo: per ogni $x \in X$ si chiama grado di f rispetto a x il grado di f riguardato come polinomio a coefficienti in $R[X \setminus \{x\}]$ nell'indeterminata x , utilizzando dunque l'isomorfismo tra $R[X]$ e $(R[X \setminus \{x\}])[x]$. Altrettanto utile è la nozione di grado totale. Ogni $\ell = \prod_{x \in X} x^{\lambda_x} \in \text{Mon } X$ ha per grado totale il numero naturale $\sum_{x \in X} \lambda_x$ (ben definito, come al solito, perché solo un numero finito di addendi è non nullo). Se $f = \sum_{\ell \in \text{Mon } X} a_\ell \ell \neq 0_R$, quindi $L := \{\ell \in \text{Mon } X \mid a_\ell \neq 0_R\}$ è un insieme finito non vuoto e quindi è lecito definire il grado totale di f come il massimo tra i gradi totali degli elementi di L . Se $f = 0_R$ si usa definire ogni grado di f come $-\infty$.

5.A.2. Con riferimento a quanto nell'osservazione precedente, si dimostri che se R è un dominio di integrità unitario, in ogni anello di polinomi su X vale la regola di addizione dei gradi (il grado di un prodotto fg è la somma tra il grado di f e quello di g) per ciascuna delle nozioni di grado definite. (Il caso del grado totale richiede un po' di attenzione in più; può essere utile fissare un ordinamento totale in X ed usarle questo per ordinare lessicograficamente gli elementi di $\text{Mon } X$.)

Utilizzare poi la regola di addizione dei gradi totali per fornire una dimostrazione alternativa della [Proposizione 5.1](#).

5.2 Fattorialità di anelli di polinomi

Il principale scopo di questa sezione è quello di provare che gli anelli di polinomi a coefficienti in un anello fattoriale sono essi stessi anelli fattoriali.

Conviene fissare delle notazioni. In questa sezione R indica (sempre) un anello fattoriale e $K = Q(R)$ un suo fissato campo dei quozienti (contenente R come sottoanello unitario). $K[x]$ ed il suo sottoanello unitario $R[x]$ sono anelli di polinomi nell'indeterminata x .

¹ una dimostrazione alternativa è contenuta nell'[Esercizio 5.A.2](#).

² qui, ad essere precisi, c'è un problema: non è detto, a priori, che X sia disgiunto da \bar{R} , quindi $\bar{R}[X]$ potrebbe non essere ben definito come anello di polinomi. Uno dei (tanti) modi semplici per rimediare consiste nel sostituire X con un insieme X' ad esso equipotente che sia disgiunto da $R \cup \bar{R}$, dimostrare il lemma per $R[X']$ e poi sfruttare l'isomorfismo $R[X] \simeq R[X']$ per trarre la stessa conclusione per $R[X]$.

Indicando con $|_{R[x]}$ e $|_{K[x]}$ le relazioni di divisibilità in $R[x]$ e $K[x]$, nell'ordine, definiamo la relazione binaria \sim_R in $K[x]$ ponendo, per ogni $f, g \in K[x]$, $f \sim_R g$ se e solo se $g = uf$ per un opportuno $u \in \mathcal{U}(R)$. Chiaramente \sim_R è una relazione di equivalenza che è più forte delle relazione 'essere elementi associati' in $K[x]$ ed estende la relazione 'essere elementi associati' in $R[x]$. Ricordando dalla [Proposizione 5.1](#) che $\mathcal{U}(R) = \mathcal{U}(R[x])$ e $K[x]$ è un dominio di integrità, osserviamo poi che, per ogni $f, g \in K[x]$, si ha $f \sim_R g$ se e solo se esistono $u, v \in R[x]$ tali che $g = uf$ e $f = vg$.

Per ogni $f \in R[x]$ si chiama *contenuto* di f (in R) ogni massimo comun divisore in R dell'insieme dei coefficienti di f . Come si riconosce facilmente, un qualsiasi elemento di R divide f in $R[x]$ se e solo se divide, in R , ogni coefficiente di f ; di conseguenza, dire che c è un contenuto di f equivale a dire che c è un divisore di f in $R[x]$ che è (in $R[x]$, o equivalentemente in R) multiplo di ogni elemento di R che divida f in $R[x]$. Evidentemente l'insieme dei contenuti di f è una classe di equivalenza modulo \sim_R .

Un polinomio in $R[x]$ si dice *primitivo* se e solo se ha 1_R come contenuto, cioè se e solo se non è divisibile per alcun elemento non invertibile di R .

Un'osservazione semplice ma di grande rilevanza è espressa dal seguente lemma. Esso, o in alternativa il [Lemma 5.2](#) del quale è immediata conseguenza, è noto come Lemma di Gauss, etichetta che del resto viene talvolta attribuita anche ad altri tra i risultati presentati in questa sezione.

Lemma 5.3. *Ogni prodotto tra polinomi primitivi in $R[x]$ è primitivo.*

Dimostrazione. Siano f e g due polinomi primitivi in $R[x]$. Se fg non è primitivo esiste un primo p in R che lo divide (in $R[x]$). Ma, essendo p primo in $R[x]$, questo comporta che p divida uno tra f e g , cosa esclusa dal fatto che f e g sono primitivi. \square

Se $0_R \neq f \in R[x]$ e c è un contenuto di f , allora $f = c\hat{f}$ per un opportuno \hat{f} in $R[x]$ che risulta evidentemente primitivo (se $u \in R$ e $u |_{R[x]} \hat{f}$ allora $cu |_{R[x]} f$, quindi $cu |_{R[x]} f$ e $u \in \mathcal{U}(R)$). Questa osservazione si estende a polinomi in $K[x]$:

Lemma 5.4. *Sia $0_R \neq f \in K[x]$. Allora esistono $k \in K$ e $\hat{f} \in R[x]$ tali che $f = k\hat{f}$ e \hat{f} è primitivo. Inoltre questa decomposizione di f è unica modulo \sim_R , nel senso che, scelti comunque $k' \in K$ e $f' \in R[x]$ tali che $f = k'f'$ e f' sia primitivo, allora $k' \sim_R k$ e $f' \sim_R \hat{f}$.*

Dimostrazione. Esiste certamente $a \in R \setminus 0$ tale che $g := af \in R[x]$. Come appena visto, $g = c\hat{g}$ dove c è un contenuto di g e \hat{g} è primitivo. Ponendo $k = ca^{-1}$ e $\hat{f} = \hat{g}$ otteniamo la decomposizione $f = k\hat{f}$ richiesta dall'enunciato. Siano poi $k' \in K$ e f' primitivo in $K[x]$ tali che $f = k'f'$. Ponendo, come certamente lecito, $k' = st^{-1}$ per opportuni $s, t \in R \setminus 0$, abbiamo $h := ct\hat{f} = saf'$. Ora $ct |_{R[x]} h$, quindi, se d è un contenuto di h , $d = cte$ per un opportuno $e \in R$. Ma allora, da $h = ct\hat{f}$ e $d |_{R[x]} h$ segue $e |_{R[x]} \hat{f}$, quindi $e \in \mathcal{U}(R)$, perché \hat{f} è primitivo. Pertanto ct è un contenuto di h . Ragionando allo stesso modo si verifica che anche sa è un contenuto di h . Di conseguenza $ct \sim_R sa$ ed esiste $u \in \mathcal{U}(R)$ tale che $sa = ctu$; se ne ricava $k' = ku$, quindi $k' \sim_R k$, e dunque anche $f' = u^{-1}\hat{f}$, quindi $f' \sim_R \hat{f}$. \square

Questo risultato suggerisce di estendere la definizione di contenuto di un polinomio in $R[x]$ a polinomi in $K[x]$ in questo modo: l'unico contenuto del polinomio nullo è 0_R ; se $0_R \neq f \in K[x]$ si chiama contenuto di f ogni elemento $k \in K$ tale che $f = k\hat{f}$ per un opportuno polinomio primitivo $\hat{f} \in R[x]$. Come segue dal [Lemma 5.4](#), i contenuti di f costituiscono una classe di equivalenza modulo \sim_R , il che mostra che per i polinomi in $R[x]$ questa nuova definizione di contenuto è equivalente alla precedente.

Se f è un polinomio primitivo in $R[x]$ e $k \in K$, allora k è un contenuto di kf . Dal [Lemma 5.4](#) si può quindi ricavare questa utile osservazione:

Corollario 5.5. *Siano f un polinomio primitivo in $R[x]$ e $k \in K$. Allora $kf \in R[x]$ se e solo se $k \in R$.*

Il passaggio chiave nella dimostrazione presentata in questa sezione è questo ulteriore corollario:

Corollario 5.6. *Sia f un polinomio primitivo in $R[x]$ e sia $g \in R[x]$. Se $f \mid_{K[x]} g$, allora $f \mid_{R[x]} g$.*

Dimostrazione. Supponiamo $f \mid_{K[x]} g$, dunque $g = fq$ per qualche $q \in K[x]$. Abbiamo $q = k\hat{q}$, dove \hat{q} è un polinomio primitivo in $R[x]$ e $k \in K$. Poiché anche f è primitivo, il [Lemma 5.3](#) mostra che $f\hat{q}$ è primitivo. Ma $g = k(f\hat{q}) \in R[x]$, quindi dal [Corollario 5.5](#) segue $k \in R$ e quindi $q = k\hat{q} \in R[x]$. Pertanto $f \mid_{R[x]} g$. \square

Proposizione 5.7. *Sia $f \in R[x]$. Allora f è irriducibile in $R[x]$ se e solo se o è un elemento primo di R oppure è primitivo ed è irriducibile in $K[x]$. Inoltre, se ciò accade, f è primo in $R[x]$.*

Dimostrazione. Se $f \in R$, l'asserto segue dal [Lemma 5.2](#); possiamo allora assumere $f \notin R$. Supponiamo f irriducibile in $R[x]$. Allora f è sicuramente primitivo (altrimenti il suo contenuto ne sarebbe un divisore non banale in $R[x]$), dobbiamo provare che è irriducibile in $K[x]$. Avendo grado positivo, f non è invertibile in $K[x]$. Sia g un divisore di f in $K[x]$. Abbiamo $g = k\hat{g}$ dove $k \in K$ e \hat{g} è un polinomio primitivo; chiaramente \hat{g} è un associato di g in $K[x]$ e quindi $\hat{g} \mid_{K[x]} f$. Ma allora $\hat{g} \mid_{R[x]} f$ per il [Corollario 5.6](#). Poiché f è irriducibile in $R[x]$ ne segue che \hat{g} è un divisore banale di f in $R[x]$ e, di conseguenza, g è un divisore banale di f in $K[x]$. È così provato che f è irriducibile in $K[x]$.

Viceversa, supponiamo che f sia primitivo e irriducibile in $K[x]$. Per completare la dimostrazione basta mostrare che f è primo in $R[x]$. Ovviamente $f \notin \mathcal{U}(R) = \mathcal{U}(R[x])$. Siano $g, h \in R[x]$ tali che $f \mid_{R[x]} gh$. Dal momento che $K[x]$ è fattoriale, f è primo in $K[x]$, quindi f divide uno tra g e h in $K[x]$ e quindi anche in $R[x]$ per il [Corollario 5.6](#). Pertanto f è primo in $R[x]$; a questo punto la dimostrazione è completa. \square

Teorema 5.8. *Ogni anello di polinomi a coefficienti in un anello fattoriale è fattoriale.*

Dimostrazione. Iniziamo col dimostrare che $R[x]$ è fattoriale. Sappiamo che $R[x]$ è un dominio di integrità unitario, resta da provare che ogni suo elemento non invertibile f è prodotto di primi. In $K[x]$ possiamo rappresentare un tale f nella forma $f = cf_1f_2 \cdots f_n$, dove $c \in R$, $n \in \mathbb{N}$ e, per ogni $i \in \{1, 2, \dots, n\}$, f_i è un polinomio irriducibile in $K[x]$, che possiamo scrivere come $f_i = k_i\hat{f}_i$ per opportuni $k_i \in K$ e \hat{f}_i primitivo in $R[x]$ (si noti: non è escluso il caso $n = 0$). Essendo \hat{f}_i associato a f_i e quindi irriducibile in $K[x]$, esso è primo in $R[x]$ per la [Proposizione 5.7](#). Posto $k = ck_1k_2 \cdots k_n$, abbiamo $f = k\hat{f}_1\hat{f}_2 \cdots \hat{f}_n$; dal [Lemma 5.3](#) ed il [Corollario 5.5](#) deduciamo $k \in R$. Allora k è o invertibile in R (cioè in $R[x]$) o, per il [Lemma 5.2](#), prodotto di primi di $R[x]$. Abbiamo così provato che f è un prodotto di primi in $R[x]$, come desiderato, quindi $R[x]$ è un anello fattoriale.

Argomentando per induzione, ed utilizzando il fatto che, per ogni insieme X disgiunto da R ed ogni $x \in X$ l'anello di polinomi $R[X]$ è isomorfo a $(R[X \setminus \{x\}])[x]$ ([Lemma 4.21](#)), verifichiamo rapidamente che ogni anello di polinomi su un insieme finito di indeterminate è fattoriale.

Sia infine $R[X]$ un anello di polinomi su un insieme arbitrario di indeterminate X . Allora $R[X]$ è un dominio di integrità. Sia f un suo elemento non invertibile. Esiste un sottoinsieme finito X_0 di X tale che $f \in R[X_0]$. Per quanto sopra, f è un prodotto di primi in $R[X_0]$. Ma, per il [Lemma 5.2](#) e per l'isomorfismo $R[X] \simeq (R[X_0])[X \setminus X_0]$, ogni elemento primo di $R[X_0]$ è primo anche in $R[X]$, quindi f è prodotto di primi in $R[X]$. Possiamo così concludere che $R[X]$ è un anello fattoriale. \square

Limitandoci al caso dei polinomi ad una indeterminata, possiamo esaminare in maggior dettaglio le fattorizzazioni in prodotto di irriducibili (ovvero primi) dei polinomi in $R[x]$. Quello che emerge dalla dimostrazione del [Teorema 5.8](#) è che se f è un polinomio non invertibile in $R[x]$, una sua fattorizzazione in prodotto di irriducibili avrà la forma $p_1 p_2 \cdots p_r f_1 f_2 \cdots f_s$, dove $r, s \in \mathbb{N}$, gli elementi p_i sono primi di R e f_1, f_2, \dots, f_s sono polinomi primitivi irriducibili in $K[x]$. Evidentemente, $c = p_1 p_2 \cdots p_r$ è un contenuto di f , e $(c f_1) f_2 \cdots f_s$ una fattorizzazione di f in prodotto di irriducibili in $K[x]$, se f ha grado positivo (ovvero $s > 0$). Dunque, nelle fattorizzazioni di f in prodotto di irriducibili in $R[x]$ ed in $K[x]$, i fattori irriducibili di grado positivo sono gli stessi a meno di associati. A questo proposito si veda l'[Esercizio 5.B.1](#): polinomi primitivi di $R[x]$ che siano associati in $K[x]$ sono necessariamente equivalenti modulo \sim_R .

Un'altra osservazione dello stesso genere è contenuta nell'[Esercizio 5.B.2](#): ogni fattorizzazione in $K[x]$ di un elemento di $R[X]$ dà luogo ad una fattorizzazione in $R[x]$ con fattori associati agli originali.

I risultati di questa sezione trovano immediata applicazione al caso dei polinomi sugli interi, quando cioè $R = \mathbb{Z}$ e $K = \mathbb{Q}$, o anche al caso dei polinomi su un campo. Abbiamo ad esempio, che ogni anello di polinomi su \mathbb{Z} o su un campo è fattoriale (ma, ad eccezione del caso dei polinomi ad una indeterminata su un campo, questi anelli non sono principali, vedi [Esercizio 5.B.6](#)).

Chiudiamo la sezione con un lemma che ha un'importante applicazione in teoria dei numeri:

Lemma 5.9. *Siano $f \in K[x]$ e $g \in R[x]$ polinomi monici. Se $f \mid_{K[x]} g$, allora $f \in R[x]$.*

Dimostrazione. Poniamo $f = k\hat{f}$, dove k è un contenuto di f e \hat{f} è primitivo. Allora $\hat{f} \in R[x]$ e $\hat{f} \mid_{K[x]} g$, quindi $\hat{f} \mid_{R[x]} g$ per il [Corollario 5.6](#). Di conseguenza, essendo g monico, il coefficiente direttore di \hat{f} è invertibile in R . Ma, poiché anche $f = k\hat{f}$ è monico, questo coefficiente direttore è k^{-1} , quindi $k \in R$ e così $f \in R[x]$. \square

Esercizi ed osservazioni.

5.B.1. Siano f e g due polinomi primitivi in $R[x]$. Allora $f \sim_R g$ se e solo se f e g sono associati in $K[x]$.

5.B.2. Sia $f = gh$, dove $f \in R[x]$ e $g, h \in K[x]$. Allora $f = g_1 h_1$ per opportuni $g_1, h_1 \in R[x]$ che siano associati (in $K[x]$) rispettivamente a g e ad h .

5.B.3. Provare questa estensione del [Corollario 5.5](#) (equivalente al corollario che lo segue): se f è un polinomio primitivo in $R[x]$ e $q \in K[x]$, allora $f q \in R[x]$ se e solo se $q \in R[x]$.

5.B.4. Mostrare che nei corollari [5.5](#) e [5.6](#) l'ipotesi che f sia primitivo è essenziale; anzi: le proprietà espresse da questi corollari sono equivalenti all'essere f primitivo.

5.B.5. Fattorizzare in prodotto di irriducibili in $\mathbb{Z}[x]$ il polinomio $(4x^3 + 4)(3x^5 - 6x^3 + 18x - 9)$.

5.B.6. Provare che se R è un anello commutativo unitario ma non un campo, allora $R[x]$ non è principale. Suggerimento: supposto $R[x]$ principale, certamente R è un dominio di integrità. Sia a un elemento non invertibile di R e sia f un massimo comun divisore tra a e x , quindi $\nu f \leq 1$. Sapendo che $f = ag + xh$ per opportuni $g, h \in R[x]$ è facile verificare che f è associato a uno tra a e x ed ottenere così una contraddizione.

Questo stesso ragionamento dimostra un risultato migliore: se R non è un campo $R[x]$ non è un anello di Bézout.

5.B.7. Come si vede senza difficoltà, il lemma di Gauss si può estendere al caso di polinomi in $R[X]$, per un arbitrario insieme di indeterminate X . C'è da fare attenzione alla corretta generalizzazione della nozione di polinomio primitivo: un polinomio primitivo di $R[X]$ rispetto a R è un polinomio che non abbia come divisore alcun elemento non invertibile di R , quindi quelli che abbiamo chiamato polinomi primitivi di $R[x]$ sono i polinomi di $R[x]$

primitivi rispetto a R . Va osservato che se $f \in R[X]$ ed f è primitivo rispetto a R e $Y \subseteq X$ non è in generale vero che f sia primitivo rispetto a $R[Y]$. Questo è lampante nel caso $Y = X$; come ulteriore esempio, se $X = \{x, y\}$ e $x \neq y$, allora $xy + y$ è un polinomio di $R[X]$ primitivo rispetto a R ma non rispetto a $R[y]$.

5.3 Invertibili, nilpotenti, divisori dello zero

Descriviamo in questa sezione, per quanto possibile, i polinomi che hanno le proprietà indicate nel titolo e, di conseguenza, traiamo informazioni sul radicale di Jacobson ed il nilradicale di un anello di polinomi.

Proposizione 5.10. *Sia $R[X]$ un anello di polinomi a coefficienti nell'anello commutativo unitario R sull'insieme di indeterminate X e sia $f \in R[X]$. Allora:*

- (i) f è invertibile in $R[X]$ se e solo se il suo termine noto è invertibile in R ed ogni suo altro coefficiente³ è nilpotente.
- (ii) Per ciascun $x \in X$ sono equivalenti:
 - a) f è nilpotente;
 - b) $1_R + xf$ è invertibile;
 - c) ogni coefficiente di f è nilpotente.

Dimostrazione. Alcune implicazioni sono ovvie: in (i), se f ha termine noto invertibile e gli altri coefficienti tutti nilpotenti, allora f è somma di un elemento invertibile ed uno nilpotente, quindi è invertibile per la [Proposizione 3.22](#); in (ii), per la stessa ragione a) implica b) e, chiaramente, c) implica a). Sono solo da provare la necessità della condizione in (i) e l'implicazione (ii.b) \Rightarrow (ii.c).

Iniziamo dalla verifica di (i) nel caso $|X| = 1$ (se $X = \emptyset$ non c'è nulla da provare); poniamo dunque $X = \{x\}$. Ragionando per assurdo, supponiamo che f sia un controesempio di grado minimo, cioè un polinomio di grado minimo per la proprietà di essere invertibile ma non della forma descritta in (i). Sia $g = f^{-1}$. Posto $n = \nu f$ ed $m = \nu g$, sia $f = \sum_{i=0}^n a_i x^i$ e $g = \sum_{i=0}^m b_i x^i$. Il coefficiente di fg relativo a $x^0 = 1_R$ è $a_0 b_0$, quindi da $fg = 1_R$ segue $a_0 \in \mathcal{U}(R)$ e $b_0 = a_0^{-1}$. Allora certamente $n > 0$. Ci proponiamo di dimostrare che si ha

$$a_n^{i+1} b_{m-i} = 0_R \text{ per ogni intero } i \text{ compreso tra } 0 \text{ e } m. \quad (*)$$

Ragionando per ricorsione assumiamo che l'uguaglianza valga per ogni naturale minore di un assegnato naturale $i \leq m$ e proviamola per i . Il coefficiente di $1_R = fg$ relativo a x^{n+m-i} è $\sum_{j=0}^i a_{n-j} b_{m+j-i}$ (ponendo $a_\ell = 0_R$ se $\ell < 0$), che è 0_R perché $n+m-i \geq n > 0$. Dal momento che, per ipotesi ricorsiva, a_n^i annulla b_ℓ per ogni intero $\ell > m-i$, ne deduciamo $a_n^{i+1} b_{m-i} = 0_R$, che è quanto si voleva. La (*) è così provata. Per $i = m$ si ottiene $a_n^{m+1} b_0 = 0_R$ che, essendo b_0 invertibile, fornisce $a_n^{m+1} = 0_R$. Abbiamo così verificato che il coefficiente direttore a_n di f è nilpotente. Ora, per la [Proposizione 3.22](#), $f_1 := f - a_n x^n \in \mathcal{U}(R[x])$. Ma $\nu f_1 < n$, quindi, per la minimalità di n i coefficienti di f_1 , escluso il termine noto, sono tutti nilpotenti; ma questo vuol dire che anche f ha la stessa proprietà, e ricaviamo così una contraddizione. Dunque, la (i) è provata nel caso $|X| = 1$.

Usando quanto appena provato è facile dimostrare (ii). Bisogna solo verificare che (ii.b) implica (ii.c). Ragioniamo per induzione su $t := |X_0 \cup \{x\}|$, dove X_0 l'insieme delle indeterminate che appaiono in f . Assumiamo $1_R + xf \in \mathcal{U}(R[X])$. Se $t = 1$, cioè se $f \in R[x]$, allora la (i), già provata in questo caso, mostra che tutti i coefficienti di f sono nilpotenti, perché

³ quest'espressione, sintetica ma leggermente ambigua, va letta come: ciascuno dei coefficienti che sia relativo ad un elemento di $\text{Mon } X$ (nelle notazioni all'apertura del capitolo) diverso da 1_R .

appaiono anche tra i coefficienti di $1_R + xf$ in posizione diversa da quella del termine noto. Sia $t > 1$ e sia $x \neq y \in X_0$. Allora possiamo scrivere $f = \sum_{i=0}^r f_i y^i$ per opportuni $r \in \mathbb{N}$ e $f_0, f_1, \dots, f_r \in R[X_0 \setminus \{y\}]$. Sempre per il caso già dimostrato di (i), applicato per $R[X_0 \setminus \{y\}]$ al posto di R e y al posto di x , dal fatto che $1_R + xf$ è invertibile deduciamo che $1_R + xf_0$ è invertibile e ciascuno degli xf_i al variare di i tra 1 e r è nilpotente, e quindi, anche in questo caso, $1_R + xf_i \in \mathcal{U}(R[X_0 \setminus \{y\}])$. A questo punto l'ipotesi di induzione mostra che tutti i coefficienti di ciascuno dei polinomi f_i , e quindi tutti i coefficienti di f , sono nilpotenti. Con questo (ii) è completamente dimostrata.

Completiamo ora la dimostrazione di (i), ragionando ancora per induzione sulla cardinalità dell'insieme X_0 delle indeterminate che appaiono in f ; possiamo assumere $|X_0| > 1$. Scelto, come sopra, $y \in X_0$ e posto ancora $f = \sum_{i=0}^r f_i y^i$ dove $r \in \mathbb{N}$ e $f_0, f_1, \dots, f_r \in R[X_0 \setminus \{y\}]$, dal caso $|X| = 1$ deduciamo che f_0 è invertibile, e quindi per ipotesi di induzione ha termine noto invertibile e gli altri coefficienti nilpotenti mentre, per ogni $i > 0$, f_i è nilpotente e quindi, per (ii), ha tutti i coefficienti nilpotenti. Dal momento che il termine noto di f è il termine noto di f_0 , l'asserto è provato. \square

Dalla equivalenza in (ii) e dalla [Proposizione 3.19](#) segue immediatamente:

Corollario 5.11. *Con le stesse notazioni, se $X \neq \emptyset$, si ha $\text{Jac}(R[X]) = \text{NilRad}(R[X])$ e quindi, se R è un dominio di integrità, $\text{Jac}(R[X]) = 0$.*

La descrizione dei polinomi divisori dello zero non è altrettanto esplicita. Si dimostra che *se un polinomio f è un divisore dello zero, esso è annullato da un polinomio costante non nullo*; più in generale:

Proposizione 5.12. *Sia $R[X]$ un anello di polinomi a coefficienti nell'anello commutativo unitario R sull'insieme di indeterminate X e sia $S \subseteq R[X]$. Se $\text{Ann}_{R[X]}(S) \neq 0$, allora $\text{Ann}_R(S) \neq 0$.*

Dimostrazione. Poiché in ciascun polinomio che annulla S appare solo un numero finito di indeterminate, esiste una parte finita Y della cardinalità minima possibile per la condizione $A := \text{Ann}_{R[Y]}(S) \neq 0$. Ciò che dobbiamo provare è che Y è l'insieme vuoto. Supposto $Y \neq \emptyset$, fissiamo $x \in Y$. Tra gli elementi non nulli di A se ne scelga uno, f , che abbia il minimo grado possibile, n , rispetto a x (cioè come polinomio nell'indeterminata x a coefficienti in $R[Y \setminus \{x\}]$). La scelta di Y implica $n > 0$. Allora $f = \sum_{i=0}^n f_i x^i$, dove, per ogni i , $f_i \in R[Y \setminus \{x\}]$ e $f_n \neq 0$. Osserviamo che ogni $h \in \text{Ann}_{R[Y \setminus \{x\}]}(f_n)$ annulla f , infatti $hf \in A$ ed il grado di hf rispetto a x è minore di n , quindi, per la scelta di f , $hf = 0_R$.

Sia $0_R \neq s \in S$. Scriviamo s come polinomio a coefficienti in $R[Y]$ nell'insieme di indeterminate $X \setminus Y$: $s = \sum_{i \in I} s_i \sigma_i$ per un opportuno insieme finito $I = I_s \neq \emptyset$, dove, per ogni $i, j \in I$, $0_R \neq s_i \in R[Y]$, $\sigma_i \in \text{Mon}(X \setminus Y)$ e $\sigma_i \neq \sigma_j$ se $i \neq j$. Da $sf = 0_R$ segue $s_i f = 0_R$ per ogni $i \in I$. Per ciascun tale i , scritto $s_i = \sum_{j=0}^{m_i} h_{ij} x^j$ come polinomio nell'indeterminata x (quindi $h_{ij} \in R[Y \setminus \{x\}]$) per ogni i e j) si ha allora $h_{i,m_i} f_n = 0_R$ e quindi, per un'osservazione fatta sopra, $h_{i,m_i} f = 0_R$. Allora anche $s_i - h_{i,m_i} x^{m_i}$ annulla f , quindi $h_{i,m_i-1} f_n = 0_R$ e di conseguenza $h_{i,m_i-1} f = 0_R$. Iterando il ragionamento arriviamo a concludere che f e f_n annullano ciascuno dei coefficienti h_{ij} di s_i . Ciò vale per ogni scelta di $s \in S$ e di $i \in I_s$. Ora, l'ideale generato da tutti gli elementi h_{ij} ottenuti come appena descritto al variare di $s \in S$ contiene evidentemente S , quindi $f_n \in A$. La minimalità di n comporta allora $n = 0$, vale a dire: $f \in R[Y \setminus \{x\}]$, ma questo contraddice la scelta di Y . È così provato che Y è l'insieme vuoto, e con ciò l'asserto. \square

Esercizi.

5.C.1. Trovare, nell'anello di polinomi $\mathbb{Z}_4[x]$, polinomi invertibili di grado arbitrariamente alto.

5.4 Serie formali di potenze

Sia R un anello commutativo unitario. L'insieme $R^{\mathbb{N}}$ delle successioni di elementi di R indicate in \mathbb{N} si può dotare di due operazioni binarie, l'addizione puntuale e la moltiplicazione di convoluzione, definite da: per ogni $a = (a_n)_{n \in \mathbb{N}}$ e $b = (b_n)_{n \in \mathbb{N}}$, $a + b = (a_n + b_n)_{n \in \mathbb{N}}$ e $ab = (c_n)_{n \in \mathbb{N}}$ dove, per ogni $n \in \mathbb{N}$, $c_n = \sum_{i=0}^n a_i b_{n-i}$. Si verifica (chi legge è invitato a farlo) che con queste operazioni $R^{\mathbb{N}}$ risulta strutturato come anello commutativo unitario, che l'applicazione μ che a ogni $a \in R$ associa la successione che manda 0 in a ed ogni intero positivo in 0_R è un monomorfismo di anelli unitari (dunque, 0_R^μ e 1_R^μ sono lo zero e l'unità di questo anello). Inoltre, indicata con x la successione che associa 1_R a 1 e 0 ad ogni altro numero naturale, si verifica che il sottoanello generato da $\text{im } \mu \cup \{x\}$ è costituito dalle successioni definitivamente nulle (cioè definitivamente costanti 0_R) ed è, a meno dell'identificazione di R con $\text{im } \mu$ via μ , un anello di polinomi su R nell'indeterminata x . Quest'anello costruito su $R^{\mathbb{N}}$ si chiama *anello delle serie formali di potenze* su R e si indica abitualmente con $R[[x]]$; per quanto detto, a meno di identificazioni che d'ora in avanti assumiamo, $R[[x]]$ ha l'anello di polinomi $R[x]$ come sottoanello unitario. Come è ragionevole fare, si usa chiamare *serie formali di potenze* (o semplicemente serie di potenze, o serie formali, o serie) i suoi elementi, che vengono rappresentati con il corrispondente formalismo, indicando ogni $(a_n)_{n \in \mathbb{N}} \in R[[x]]$ come $\sum_{n \in \mathbb{N}} a_n x^n$. Questa notazione è compatibile con quella abituale per i polinomi, a meno di convenire (come si fa) di scrivere le successioni definitivamente nulle (cioè i polinomi) come somma di un numero finito di termini, omettendo termini nulli.

Estendendo la terminologia relativa ai polinomi, per ogni $a = \sum_{n \in \mathbb{N}} a_n x^n \in R[[x]]$ chiamiamo coefficienti di a gli elementi a_n e, tra questi, chiamiamo a_0 il termine noto di a . Evidentemente l'applicazione che ad ogni elemento di $R[[x]]$ associa il suo termine noto, con codominio R , è un omomorfismo suriettivo di anelli unitari; il suo nucleo è l'ideale generato da x . Di conseguenza:

Lemma 5.13. *Sia R un anello commutativo unitario. Allora $R[[x]]/(x) \simeq R$.*

Proposizione 5.14. *Sia R un anello commutativo unitario. Allora:*

- (i) $R[[x]]$ è un dominio di integrità se e solo se R lo è;
- (ii) $\mathcal{U}(R[[x]])$ è costituito dalle serie di potenze con termine noto invertibile in R ;
- (iii) $\text{Jac}(R[[x]])$ è costituito dalle serie di potenze con termine noto in $\text{Jac}(R)$.

Dimostrazione. Sia R un dominio di integrità e siano f e g elementi non nulli in $R[[x]]$. Esistono $n, m \in \mathbb{N}$, $f_1, g_1 \in R[[x]]$ ed elementi non nulli $a, b \in R$ tali che $f = x^n(a + x f_1)$ e $g = x^m(b + x g_1)$. Allora fg ha $ab \neq 0_R$ come coefficiente relativo a x^{n+m} , quindi $fg \neq 0_R$. Questo dimostra l'implicazione non ovvia in (i).

Occupiamoci di (ii) e di (iii). Sia $a = \sum_{n \in \mathbb{N}} a_n x^n \in R[[x]]$.⁴ Ovviamente $a \in \mathcal{U}(R[[x]])$ se e solo se esiste $b = \sum_{n \in \mathbb{N}} b_n x^n \in R[[x]]$ tale che $ab = 1_R$, cioè $a_0 b_0 = 1_R$ e, per ogni $n \in \mathbb{N}^+$,

$$\sum_{i=0}^n a_i b_{n-i} = 0_R. \quad (E_n)$$

⁴ conveniamo che, salvo diversa indicazione, scrivendo una serie formale in questo modo sottintendiamo che gli a_n siano i suoi coefficienti, cioè che per ogni $n \in \mathbb{N}$ sia $a_n \in R$.

La prima equazione ci dice che se $a \in \mathcal{U}(R[[x]])$, allora $a_0 \in \mathcal{U}(R)$. Viceversa, supponiamo a_0 invertibile in R . Sia $b_0 = a_0^{-1}$. Per ogni $n \in \mathbb{N}^+$ possiamo riscrivere (E_n) come $b_n = -b_0 \sum_{i=0}^{n-1} a_i b_{n-i}$; possiamo quindi usare queste equazioni per definire ricorsivamente una successione $(b_n)_{n \in \mathbb{N}}$ di elementi di R in modo che tutte le (E_n) siano soddisfatte. Fatto questo, otteniamo che $\sum_{n \in \mathbb{N}} b_n x^n$ è inverso di a in $R[[x]]$, dunque $a \in \mathcal{U}(R[[x]])$. È così provata la (ii). Proviamo infine la (iii). Dalla [Proposizione 3.19](#) e da quanto appena dimostrato sappiamo che $a \in \text{Jac}(R[[x]])$ se e solo se, per ogni $f \in R[[x]]$ il termine noto di $1_R + af$ è invertibile in R . Questo, evidentemente, equivale a richiedere $1 + a_0 r \in \mathcal{U}(R)$ per ogni $r \in R$, vale a dire: $a_0 \in \text{Jac}(R)$. \square

Corollario 5.15. *Sia R un anello commutativo unitario locale. Allora $R[[x]]$ è un anello locale.*

Dimostrazione. Sia $M = \text{Jac}(R)$ l'ideale massimale di R . Allora, $M_1 := M + xR[[x]] \triangleleft R[[x]]$ ed ogni elemento di $R[[x]] \setminus M_1$ è invertibile per la [Proposizione 5.14](#), quindi il [Corollario 3.23](#) porta a concludere che M_1 è l'unico ideale massimale di $R[[x]]$. \square

In particolare, se R è un campo, $R[[x]]$ è un anello locale.

Rispetto al caso degli anelli di polinomi, le informazioni note su elementi nilpotenti e divisori dello zero in anelli di serie formali di potenze sono molto più frammentarie. Ad esempio, solo per alcune classi di anelli commutativi unitari sono pienamente descritti gli elementi nilpotenti (alcune informazioni sono tra gli esercizi che seguono) e, in contrasto con la [Proposizione 5.12](#), esistono serie di potenze che sono divisori dello zero ma hanno alcuni coefficienti invertibili. È stato comunque dimostrato (Fields, 1971) che per serie di potenze su anelli commutativi noetheriani valgono risultati analoghi a quelli che abbiamo visto valere per i polinomi: se R è un anello commutativo unitario noetheriano e $a \in R[[x]]$, allora a è nilpotente se e solo se ogni suo coefficiente è nilpotente; inoltre a è un divisore dello zero in $R[[x]]$ se e solo se a è annullato da un elemento non nullo di R .

Esercizi.

5.D.1. La dimostrazione della prima parte della [Proposizione 5.14](#) illustra il fatto che spesso, lavorando su serie formali di potenze, si può utilizzare il primo coefficiente non nullo di una serie non nulla in modo analogo a come, ragionando su polinomi ad una indeterminata, si utilizza il coefficiente direttore.

5.D.2. Determinare, in $\mathbb{Z}[[x]]$, l'inverso del polinomio $1 + x^2$.

5.D.3. Verificare che per ogni anello commutativo unitario R si ha $R[[x]]/\text{Jac}(R[[x]]) \simeq R/R[[x]]$. Quest'affermazione generalizza il [Corollario 5.15](#).

5.D.4. Verificare che, se K è un campo, ogni elemento di $K[[x]]$ si scrive, in modo unico come $x^n u$ per opportuni $n \in \mathbb{N}$ e $u \in \mathcal{U}(K[[x]])$. Segue immediatamente da ciò che $K[[x]]$ è un anello fattoriale con una sola classe di associazione di elementi irriducibili. Dedurre che $K[[x]]$ è euclideo.

5.D.5. La notazione e la terminologia usata per le serie formali di potenze potrebbe far pensare ad una nozione di convergenza e quindi ad una topologia che stia dietro la loro definizione. In effetti è possibile assumere questo punto di vista. Sia infatti R un anello commutativo unitario, e siano $a, b \in R[[x]]$. Si definisce (non è difficile verificarlo) una metrica su $R[[x]]$ ponendo la distanza tra due serie formali a e b uguale a 0 se $a = b$ ed a 2^{-n} se $a \neq b$ e n è il massimo numero naturale tale che x^n divida $a - b$. Nello spazio metrico così definito, ciascun $a = \sum_{n \in \mathbb{N}} a_n x^n$ risulta essere il limite della successione dei polinomi $(\sum_{i=0}^n a_i x^i)_{n \in \mathbb{N}}$, che potremo chiamare "somme parziali" di a , e $R[[x]]$ è il completamento del suo sottospazio $R[x]$.

5 Proprietà di anelli di polinomi e di serie formali di potenze

Si può anche adottare questo punto di vista per definire $R[[x]]$ (dopo aver introdotto una nozione di anello topologico): introdurre nell'anello $R[x]$ la metrica descritta sopra poi usare questa per definire $R[[x]]$ come completamento (come spazio metrico) dell'anello $R[x]$ prolungando a quest'ultimo le operazioni di $R[x]$.

5.D.6. Sia R un anello commutativo unitario. Provare che se a è un elemento nipotente di $R[[x]]$, tutti i coefficienti di a sono elementi nilpotenti di R .

Una possibile dimostrazione parte dal fatto che il termine noto di a è certamente nilpotente e procede per induzione per dimostrare lo stesso per tutti gli altri coefficienti, utilizzando il fatto che x è cancellabile in $R[[x]]$.

5.D.7. Si può mostrare che risultato dell'esercizio precedente non si inverte, procedendo ad esempio come segue.

Sia $(i_n)_{n \in \mathbb{N}}$ una successione di numeri naturali tale che $i_{n+1} > ni_n$ per ogni $n \in \mathbb{N}$. Supponiamo che R sia un anello commutativo unitario e che, in R , esista per ogni $n \in \mathbb{N}$ un elemento nilpotente a_n tale che $a_n^n \neq 0_R$. Verificare che la serie formale $\sum_{n \in \mathbb{N}} a_n x^{i_n} \in R[[x]]$, pur avendo tutti i coefficienti nilpotenti, non è nilpotente. Costruire poi in modo esplicito un anello ed una successione di suoi elementi con le proprietà appena descritte.

5.D.8. È possibile costruire esempi più significativi di quello all'esercizio precedente, determinando, su un anello commutativo unitario R , una serie formale di potenze non nilpotente $\sum_{n \in \mathbb{N}} a_n x^n$ tale che $a_n^2 = 0_R$ per ogni $n \in \mathbb{N}$.

Sia infatti $R[X]$ un anello di polinomi a coefficienti in un anello commutativo unitario A di caratteristica 0 su un insieme numerabile X di indeterminate, scritto come $X = \{x_i \mid i \in \mathbb{N}\}$ dove, per ogni $i, j \in \mathbb{N}$, $i \neq j \Rightarrow x_i \neq x_j$. Sia $A = R[X]/H$, dove $H = (x_i^2 \mid i \in \mathbb{N}) \triangleleft R[X]$; poniamo anche $a_i = x_i + H$ per ogni $i \in \mathbb{N}$. Allora la serie $f = \sum_{i \in \mathbb{N}} a_i x^i \in A[[x]]$ ha tutti i coefficienti a quadrato nullo ($a_i^2 = 0_A$ per ogni $i \in \mathbb{N}$), ma non è nilpotente. Per riconoscerlo, si verifichi che, per ogni $k \in \mathbb{N}^+$, il coefficiente $\binom{k}{2}$ -esimo di f^k è $k!a_0a_1 \cdots a_{k-1} \neq 0_A$.

6 Condizioni di catena per moduli e anelli

Nella teoria dei moduli e degli anelli hanno grande importanza due condizioni finitarie definite dall'imposizione di condizioni di catena (vedi [sezione 13.1](#)) all'insieme dei sotto(pre)moduli di un (pre)modulo o degli ideali di un anello.

6.1 Definizioni e prime proprietà

Per ogni (pre)modulo M su un anello commutativo unitario R , indichiamo con $\mathcal{L}_R(M)$ l'insieme degli R -sotto(pre)moduli di M ordinato per inclusione. Si dice che M è *artiniano* se e solo se \mathcal{L}_R verifica la condizione minimale; M è invece *noetheriano* se e solo se \mathcal{L}_R verifica la condizione massimale. Questi nomi ricordano due matematici che hanno dato un enorme impulso allo sviluppo dell'algebra nella prima metà del '900: [Emil Artin](#) (1898–1962) ed [Emmy Noether](#) (1882–1935). Qualche volta useremo espressioni come R -artiniano e R -noetheriano per evidenziare il ruolo dell'anello degli scalari R , cioè come abbreviazioni di 'artiniano/noetheriano come R -(pre)modulo'. Ad esempio, rispetto alle consuete operazioni, \mathbb{Q} , riguardato come spazio vettoriale sul campo \mathbb{Q} è un modulo artiniano, ma il gruppo abeliano $(\mathbb{Q}, +)$, cioè \mathbb{Q} , riguardato come modulo su \mathbb{Z} , non lo è; possiamo dire allora che \mathbb{Q} è \mathbb{Q} -artiniano ma non \mathbb{Z} -artiniano.

Dovrebbe risultare chiaro che tutti i (pre)moduli finiti sono sia artiniani che noetheriani; in questo senso sia la proprietà di essere artiniano che quella di essere noetheriano sono, come si dice, condizioni finitarie. Altrettanto chiaramente, ogni (pre)modulo che sia isomorfo ad un (pre)modulo artiniano o noetheriano ha la stessa proprietà.

Un anello commutativo R è, invece, artiniano (risp. noetheriano) se e solo se l' R -(pre)modulo R_R ha la corrispondente proprietà, cioè se e solo se l'insieme $\mathfrak{I}(R)$ degli ideali di R , ordinato ancora per inclusione, verifica la condizione minimale (risp. massimale).

Nel caso dei (pre)moduli le condizioni di essere artiniano o noetheriano sono chiuse per il passaggio a sotto(pre)moduli, quozienti ed estensioni,¹ come vediamo nel prossimo lemma. Il significato preciso della parola 'estensione' verrà chiarito [più avanti](#); diciamo per ora, in modo un po' informale, che un (pre)modulo M è estensione di un (pre)modulo A mediante un (pre)modulo B se ha un sotto(pre)modulo N isomorfo ad A tale che M/N sia isomorfo a B .

Lemma 6.1. *Sia M un (pre)modulo sull'anello commutativo R , e sia $N \leq M$. Allora M è artiniano (risp. noetheriano), se e solo se sia N che M/N sono artiniani (risp. noetheriani).*

Dimostrazione. $\mathcal{L}_R(N)$ è un sottoinsieme di $\mathcal{L}_R(M)$; per il teorema di corrispondenza ([Teorema 1.12](#)) $\mathcal{L}_R(M/N)$ è isomorfo, come insieme ordinato, al sottoinsieme $\{H \leq_R M \mid N \subseteq H\}$ di $\mathcal{L}_R(M)$. Dunque sia N che M/N sono artiniani (risp. noetheriani) se lo è M .

Viceversa, supponiamo che N e M/N siano artiniani. Sia $(H_n)_{n \in \mathbb{N}}$ una successione decrescente di sotto(pre)moduli di M . Allora $(N \cap H_n)_{n \in \mathbb{N}}$ è una successione decrescente di sotto(pre)moduli di N e $(H_n + N/N)_{n \in \mathbb{N}}$ è una successione decrescente di sotto(pre)moduli di M/N ; quindi queste

¹ se \mathcal{P} è un proprietà relativa a (pre)moduli, si dice che \mathcal{P} è chiusa per sotto(pre)moduli (o che si eredita a sotto(pre)moduli) se tutti i sotto(pre)moduli di moduli che verificano \mathcal{P} verificano anch'essi \mathcal{P} ; si dice che \mathcal{P} è chiusa per (o si eredita a) quozienti se tutti i quozienti di moduli che verificano \mathcal{P} verificano anch'essi \mathcal{P} ; si dice poi che \mathcal{P} è chiusa per estensioni se ogni (pre)modulo M che abbia un sotto(pre)modulo N tale che N e M/N verifichino entrambi \mathcal{P} verifica anch'esso \mathcal{P} .

due ultime successioni sono definitivamente costanti ed esiste così $n \in \mathbb{N}$ tale che, per ogni $t \in \mathbb{N}$, si abbia $N \cap H_{n+t} = N \cap H_n$ e $H_{n+t} + N = H_n + N$, e quindi $H_{n+t} = H_n$ per il [Corollario 1.9](#) e perché $H_{n+t} \subseteq H_n$. Dunque, $(H_n)_{n \in \mathbb{N}}$ è definitivamente costante. Abbiamo così provato che M è artiniano.

La dimostrazione per il caso dei moduli noetheriani è analoga. \square

Corollario 6.2. *Siano B e C sotto(pre)moduli di un (pre)modulo A . Se A/B e A/C sono entrambi artiniani (risp. noetheriani), allora $A/(B \cap C)$ è artiniano (risp. noetheriano).*

Dimostrazione. Il secondo teorema di isomorfismo fornisce $B/(B \cap C) \simeq (B + C)/C$ e vediamo quindi, usando anche il terzo teorema di isomorfismo, che $A/(B \cap C)$ è una estensione di $(B + C)/C$, che è un sotto(pre)modulo di A/C , mediante A/B . L'asserto segue allora dal lemma precedente. \square

Corollario 6.3. *Un (pre)modulo che sia la somma di un numero finito di suoi sotto(pre)moduli artiniani (risp. noetheriani) è esso stesso artiniano (risp. noetheriano).*

Dimostrazione. Basta ovviamente provare l'enunciato nel caso di un (pre)modulo che sia la somma di due sotto(pre)moduli. Poniamo $M = A + B$, dove A e B sono entrambi artiniani o entrambi noetheriani. Dal secondo teorema di omomorfismo si ha $M/A \simeq B/(A \cap B)$, quindi M è estensione di A mediante il quoziente $B/(A \cap B)$ di B e l'asserto segue ora direttamente dal [Lemma 6.1](#). \square

I (pre)moduli finiti sono ovviamente artiniani e noetheriani. Questi (pre)moduli hanno una semplice caratterizzazione. Una *serie finita* di sotto(pre)moduli di un (pre)modulo M è una sequenza finita $(N_i)_{i \in \{0, 1, \dots, n\}}$ di sotto(pre)moduli di M tale che $N_0 = 0 \subseteq N_1 \subseteq N_2 \subseteq \dots \subseteq N_n = M$. I (pre)moduli N_{i+1}/N_i si chiamano *fattori* della serie.

Proposizione 6.4. *Sia M un (pre)modulo su un anello commutativo R . Allora M è artiniano e noetheriano se e solo se ha una serie finita i cui fattori sono (pre)moduli semplici.*

Dimostrazione. I (pre)moduli semplici sono chiaramente sia artiniani che noetheriani, quindi se M ha una serie finita a fattori semplici, allora il [Lemma 6.1](#) mostra che M è sia artiniano che noetheriano. Viceversa, supponiamo M artiniano e noetheriano. Poiché M è artiniano, per ogni $N < M$ esiste un sotto(pre)modulo N' di M che sia minimale rispetto alla proprietà di contenere propriamente N . Dovrebbe essere chiaro che se N' ha questa proprietà il (pre)modulo N'/N è semplice. Si definisce ricorsivamente una successione crescente $(N_i)_{i \in \mathbb{N}}$ di sotto(pre)moduli di M ponendo $N_0 = 0$ e, per ogni $i \in \mathbb{N}$, ponendo $N_{i+1} = M$ se $N_i = M$ e, su $N_i < M$, scegliendo come N_{i+1} un sotto(pre)modulo di M che sia minimale rispetto alla proprietà di contenere propriamente N_i (sicché N_{i+1}/N_i è semplice). Dal momento che M è noetheriano, esiste un $n \in \mathbb{N}$ tale che $N_n = N_{n+1}$; la definizione della successione mostra che, di conseguenza, $N_n = M$. La serie $(N_i)_{i \in \{0, 1, \dots, n\}}$ ha la proprietà richiesta dall'enunciato. \square

Benché l'artinianità e la noetherianità di un anello commutativo R sono definite in termini dell'analoga proprietà per il (pre)modulo R_R , non è vero che valgano per gli anelli le stesse proprietà di chiusura che per i (pre)moduli artiniani e noetheriani. Ad esempio, ogni campo, avendo esattamente due ideali, è, come anello, sia artiniano che noetheriano, ma i suoi sottoanelli, anche unitari, possono non avere queste proprietà, come accade per \mathbb{Z} , che è un sottoanello unitario non artiniano del campo \mathbb{Q} , o, se R è un dominio di integrità non noetheriano,² per R stesso, che è un sottoanello unitario non noetheriano del suo campo dei quozienti. Si possono anche ottenere (vedi [Esempio 6.A.6](#)) esempi in cui un anello commutativo unitario R artiniano

² per un esempio esplicito si vedano ad esempio l'[Esempio 6.A.5](#) e la [Proposizione 5.1](#).

e noetheriano ha un ideale H che non ha, come anello, nessuna delle due proprietà, pur dovendo essere, per il [Lemma 6.1](#), artiniano e noetheriano come R -modulo.

Si osservi in generale che, per un ideale H di un anello commutativo R , la proprietà di essere artiniano o noetheriano come anello (vale a dire: H -artiniano o H -noetheriano, come modulo) è più forte che quella di essere artiniano o noetheriano come R -(pre)modulo.

Vale comunque, con dimostrazione ovvia utilizzando il [Lemma 6.1](#), il [Corollario 6.2](#) e l'[Esercizio 6.A.1](#):

Lemma 6.5. *Siano R un anello commutativo unitario e $H, K \triangleleft R$. Allora:*

- (i) *se R è artiniano (risp. noetheriano), anche R/H è artiniano (risp. noetheriano);*
- (ii) *se R/H , come anello, e H , come R -modulo, sono artiniani (risp. noetheriani), allora R è artiniano (risp. noetheriano);*
- (iii) *se $R = H + B$, dove B è un sottoanello di R , e sia B , come anello, che H , come R -modulo, sono artiniani (risp. noetheriani), allora R è artiniano (risp. noetheriano);*
- (iv) *se R/H e R/K sono artiniani (risp. noetheriani) anche $R/(H \cap K)$ è artiniano (risp. noetheriano).*

Abbiamo visto che, in alcuni casi, cambiare l'anello degli scalari di un (pre)modulo M da un anello commutativo R ad un anello commutativo S non altera l'insieme dei sotto(pre)moduli di M . In tali casi, ovviamente, M è R -artiniano (risp. R -noetheriano) se e solo se è S -artiniano (risp. S -noetheriano). Ad esempio, ricaviamo dal [Lemma 1.16](#) e dalla [Proposizione 1.31](#):

Lemma 6.6. *Siano R un anello commutativo e M un R -(pre)modulo.*

- (i) *Se $\text{Ann}_R(M) \supseteq H \triangleleft R$ e $M_{R/H}$ è M riguardato come (R/H) -(pre)modulo via azione mod H , allora M è artiniano (risp. noetheriano) se e solo se lo è $M_{R/H}$.*
- (ii) *Se R_1 è l'anello accresciuto definito da R , e M_{R_1} è M riguardato come modulo su R_1 , allora M_{R_1} è artiniano (risp. noetheriano) se e solo se lo è M .*

È poi conseguenza immediata di [Lemma 6.5\(ii\)](#) che l'anello accresciuto definito da un anello noetheriano è anch'esso noetheriano mentre, poiché \mathbb{Z} non è artiniano, l'anello accresciuto definito da un anello non è mai artiniano.

Alcuni esempi Come già osservato, i (pre)moduli (e quindi gli anelli commutativi) finiti sono sempre sia artiniano che noetheriani. Il viceversa non vale, abbiamo infatti osservato che i campi sono anelli artiniani e noetheriani.

- Generalizzando questa osservazione, se K è un campo e V è un K -modulo, cioè un K -spazio vettoriale, sono equivalenti per V le proprietà di essere artiniano, noetheriano, di dimensione finita. Infatti, se $\dim_K(V)$ è finita, V è somma diretta di un numero finito di copie di K_K , quindi è artiniano e noetheriano per il [Corollario 6.3](#). Se invece $\dim_K(V)$ è infinita, allora V è somma dirette di infinite copie di K_K , ed allora V non è né artiniano né noetheriano, come spiegato dalla prossima osservazione.
- Sia M un (pre)modulo somma diretta di una famiglia infinita di (pre)moduli non nulli. Allora M non è né artiniano né noetheriano. Infatti, posto $M = \bigoplus_{i \in I} M_i$, dove I è infinito e $M_i \neq 0$ per ogni $i \in I$, se $(i_n)_{n \in \mathbb{N}}$ è una successione iniettiva a valori in I , e, per ogni $n \in \mathbb{N}$ si pone $A_n = \sum_{n \leq j \in \mathbb{N}} M_{i_j}$ e $B_n = \sum_{n > j \in \mathbb{N}} M_{i_j}$, allora $(A_n)_{n \in \mathbb{N}}$ e $(B_n)_{n \in \mathbb{N}}$ sono, rispettivamente, una successione strettamente crescente ed una successione strettamente decrescente di sotto(pre)moduli di M .

Di conseguenza, tenendo conto del [Lemma 6.1](#), lo stesso vale per prodotti diretti di infiniti (pre)moduli non nulli, ed anche per anelli commutativi che siano somma o prodotto diretto di infiniti anelli non nulli.

- \mathbb{Z} , visto come gruppo (cioè come \mathbb{Z} -modulo), o anche come anello è noetheriano ma, come già detto, non artiniiano. Infatti gli ideali dell'anello \mathbb{Z} sono tutti e soli i suoi sottogruppi additivi, e questi, escluso quello nullo, hanno indice finito in \mathbb{Z} . Se $(H_n)_{n \in \mathbb{N}}$ è una successione crescente di ideali di \mathbb{Z} , $H_n = 0$ per ogni $n \in \mathbb{N}$ oppure esiste un $n \in \mathbb{Z}$ tale che $H_n \neq 0$, nel qual caso \mathbb{Z}/H_n è finito e quindi $\{H_m \mid n \leq m \in \mathbb{N}\}$ è finito; in entrambi i casi la successione $(H_n)_{n \in \mathbb{N}}$ è definitivamente costante. Quindi \mathbb{Z} è noetheriano (come gruppo e come anello). Invece, per ogni numero primo positivo p , la successione di ideali $(p^n \mathbb{Z})_{n \in \mathbb{N}}$ è strettamente decrescente; quindi \mathbb{Z} non è artiniiano.
- Fissato un numero primo positivo p , sia P un p -gruppo di Prüfer (cioè un gruppo isomorfo al gruppo \mathbb{Q}_p/\mathbb{Z} , dove $\mathbb{Q}_p = \{mp^n \mid m \in \mathbb{N} \wedge n \in \mathbb{Z}\}$). È noto che ogni sottogruppo proprio di P è finito (ed è un p -gruppo ciclico). Da ciò segue che, riguardato come \mathbb{Z} -modulo, P è artiniiano: basta ragionare in modo duale rispetto a quanto fatto per \mathbb{Z} . D'altra parte P è infinito ed è l'unione insiemistica dei suoi sottogruppi propri, quindi non ha sottogruppi massimali (dunque: l'insieme dei sottogruppi propri di P non ha elementi massimali). Di conseguenza P , come \mathbb{Z} -modulo non è artiniiano. Se muniamo P della moltiplicazione costante 0_P rendiamo P un anello commutativo artiniiano ma non noetheriano. Notiamo che P non è unitario; dimostreremo in un capitolo successivo (nel [Teorema 8.6](#)) che gli anelli (commutativi) unitari artiniani sono tutti noetheriani.

Generalizzando quanto osservato sopra a proposito degli spazi vettoriali verificiamo ora che se un modulo è annullato da un prodotto tra un numero finito di ideali, per esso sono equivalenti le proprietà di essere artiniiano o noetheriano.

Lemma 6.7. *Sia M un modulo sull'anello commutativo unitario R e supponiamo che esistano $n \in \mathbb{N}^+$ e ideali massimali H_1, H_2, \dots, H_n di R tali che $H_1 H_2 \cdots H_n \subseteq \text{Ann}_R(M)$. Allora M è artiniiano se e solo se è noetheriano.*

Dimostrazione. Poniamo $M_0 = M$ e, per ogni $i \in \{1, 2, \dots, n\}$, $M_i = M H_1 H_2 \cdots H_i$. Abbiamo così una catena finita di sottomoduli:

$$0 = M_n \subseteq M_{n-1} \subseteq M_{n-2} \subseteq \cdots \subseteq M_1 \subseteq M_0 = M.$$

Applicando ripetutamente il [Lemma 6.1](#) vediamo che M è artiniiano (risp. noetheriano) se e solo se lo è ciascuno dei quozienti $F_i := M_{i-1}/M_i$ al variare di $i \in \{1, 2, \dots, n\}$. Inoltre, per ogni i abbiamo $M_i = M_{i-1} H_i$, dunque $H_i \subseteq \text{Ann}_R(F_i)$. Possiamo così riguardare F_i anche come R/H_i -modulo. Per il [Lemma 6.6](#), F_i è R/H_i -artiniiano (risp. R/H_i -noetheriano) se e solo se è R -artiniiano (risp. R -noetheriano). Ma R/H_i è un campo, quindi, per le osservazioni fatte sopra a proposito degli spazi vettoriali, F_i è R/H_i -artiniiano se e solo se è R/H_i -noetheriano. In definitiva, otteniamo che ciascuno degli F_i è R -artiniiano se e solo se è R -noetheriano. Avevamo però anche detto che M verifica una delle due condizioni di catena che consideriamo se e solo se ciascuno dei moduli F_i la verifica; concludiamo, come richiesto, che M è artiniiano se e solo se è noetheriano. \square

Esercizi.

6.A.1. Se R è un anello commutativo e $H \triangleleft R$, allora R/H è artiniiano (risp. noetheriano) come anello se e solo se lo è come R -premodulo.

6.A.2. Le dimostrazione del [Corollario 6.3](#) mostra che ogni proprietà di (pre)moduli che sia invariante per isomorfismi e sia chiusa per quozienti ed estensioni è, nel senso ovvio, chiusa per somme finite.

6.A.3. Si verifichi che per (pre)moduli su un fissato anello commutativo R la proprietà di essere finitamente generato è chiusa per estensioni (la chiusura per quozienti è stata già osservata nell'Esercizio 1.G.1), ma non, in generale, per sotto(pre)moduli (come seguirà dalla Proposizione 6.8, questo accade se e solo se R è noetheriano).

6.A.4. Siano R un anello commutativo e M un R -(pre)modulo. Dimostrare che se M ha un sotto(pre)modulo proprio $M_1 \simeq_R M$, allora M non è artiniano. (Suggerimento: essendo $M_1 \simeq M$, anche M_1 avrà un sotto(pre)modulo proprio isomorfo a se stesso ...). Dimostrare per questa via che $\mathbb{Z}_{\mathbb{Z}}$ non è artiniano.

Dualmente, dimostrare che se M ha un sotto(pre)modulo $M_1 \triangleleft 0$ tale che $M \simeq_R M/M_1$, allora M non è noetheriano.

Le negazioni delle proprietà qui usate come ipotesi hanno un nome: un (pre)modulo si dice hopfiano se e solo se non ha quozienti propri (cioè quozienti modulo un sotto(pre)modulo non nullo) isomorfi a se stesso; cohopfiano se non ha sotto(pre)moduli propri isomorfi a se stesso. L'esercizio potrebbe quindi essere riformulato così: i (pre)moduli noetheriani sono hopfiani, quelli artiniani sono cohopfiani.

Enunciare e verificare le analoghe proprietà per gli anelli.

6.A.5. Sia $R[X]$ un anello di polinomi su un insieme infinito X di indeterminate, a coefficienti su un arbitrario anello commutativo unitario $R \neq 0$. Allora $R[X]$ non è noetheriano. Lo si può vedere come conseguenza dell'esercizio precedente; infatti sappiamo dal Lemma 4.22 che, scelto comunque $x \in X$, $R[X]/(x) \simeq R[X \setminus \{x\}]$, ma, essendo $|X \setminus \{x\}| = |X|$, $\simeq R[X \setminus \{x\}] \simeq R[X]$, quindi $R[X]$ non è hopfiano come anello.

6.A.6. Siano K un campo e $R = K[x]/(x^2)$, dove $K[x]$ è un anello di polinomi ad una indeterminata, x , su K . Allora R è artiniano e noetheriano; il suo ideale $H = (x)/(x^2)$, come anello ha questa struttura: il suo gruppo additivo è isomorfo a quello di K , la sua moltiplicazione è costante nulla. Se, ad esempio, $K = \mathbb{Q}$ (basta in effetti che K sia infinito) allora H , come anello, non è né artiniano né noetheriano.

6.A.7. Non si può costruire un esempio come quello precedente in cui H , come anello sia unitario. Infatti, se R è un anello commutativo noetheriano e H è un suo ideale che, come anello, è unitario, allora H è un sommando diretto di R , per l'Esercizio 4.C.3, quindi è un anello noetheriano.

6.2 Caratterizzazioni di moduli e anelli noetheriani

Sappiamo dal Lemma 1.17 e dal Corollario 1.18 del rapporto tra la proprietà di essere, per un (pre)modulo, finitamente generato da una parte e il comportamento di catene di sotto(pre)moduli e l'esistenza di sotto(pre)moduli massimali dall'altra. Questo rapporto si manifesta in modo evidente in una notissima caratterizzazione elementare della noetherianità:

Proposizione 6.8. Per un (pre)modulo M sono equivalenti le affermazioni:

- (i) M è noetheriano;
- (ii) l'insieme dei sotto(pre)moduli finitamente generati di M , ordinato per inclusione, verifica la condizione massimale;
- (iii) ogni sotto(pre)modulo di M è finitamente generato.

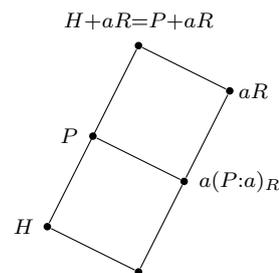
Dimostrazione. Ovviamente (i) implica (ii). Supponiamo che valga (ii) e sia $N \leq_R M$. Se N non è finitamente generato, possiamo definire ricorsivamente una successione strettamente crescente di sotto(pre)moduli finitamente generati di N in questo modo: poniamo $A_0 = 0$ e, supposto definito, per un qualche $n \in \mathbb{N}$, il sotto(pre)modulo finitamente generato A_n di N , dal

momento che N non è finitamente generato si ha $A_n \subset N$, quindi possiamo scegliere $a \in N \setminus A_n$ e definire A_{n+1} come il sotto(pre)modulo generato da $A_n \cup \{a\}$, che è ancora un sotto(pre)modulo finitamente generato A_n di N e contiene propriamente A_n . L'esistenza della successione così costruita falsifica la (ii); concludiamo che N deve essere finitamente generato. Dunque (ii) implica (iii). Infine, se vale (iii), il [Lemma 1.17](#) mostra immediatamente che ogni catena non vuota di sotto(pre)moduli di M ha massimo, quindi M è noetheriano. \square

La [Proposizione 6.8](#) fornisce immediatamente anche una caratterizzazione degli anello commutativo noetheriani: *un anello commutativo è noetheriano se e solo se ogni suo ideale è finitamente generato*, inoltre è sufficiente per questo richiedere la condizione massimale sugli ideali finitamente generati. Nel caso degli anelli commutativi unitari basta che siano finitamente generati gli ideali primi perché lo siano anche tutti gli altri. È un primo caso in cui vediamo quanto fortemente la struttura di un anello commutativo unitario sia influenzata dai suoi ideali primi. La dimostrazione consiste essenzialmente in questo lemma:

Lemma 6.9. *Sia R un anello commutativo unitario non noetheriano. Allora l'insieme degli ideali non finitamente generati di R ha elementi massimali, e questi sono tutti ideali primi.*

Dimostrazione. L'insieme degli ideali non finitamente generati di R non è vuoto, per la [Proposizione 6.8](#), ed è induttivo per il [Corollario 1.20](#), quindi ha elementi massimali. Sia P uno di essi. Per ogni $a \in R \setminus P$, l'ideale $P + aR$ è finitamente generato. Da ciò segue $P + aR = H + aR$ per un qualche ideale finitamente generato H di R contenuto in P . Infatti, esistono $n \in \mathbb{N}$ ed elementi $h_1, h_2, \dots, h_n \in P$ e $r_1, r_2, \dots, r_n \in R$ tali che $P + aR$ sia generato da $\{h_1 + ar_1, h_2 + ar_2, \dots, h_n + ar_n\}$; posto $H = \sum_{i=1}^n h_i R$ si ha ovviamente $P + aR \subseteq H + aR \subseteq P + aR$, quindi H ha le proprietà richieste. Ora, per la legge di Dedekind ([Lemma 1.8](#)) e per il [Lemma 3.5](#), $P = H + (aR \cap P) = H + a(P : a)_R$. Supponiamo $P \neq (P : a)_R$, quindi $P \subset (P : a)_R$, allora $(P : a)_R$ è finitamente generato per la massimalità di P . Ma $a(P : a)_R$ è l'immagine di $(P : a)_R$ mediante l'omomorfismo (di R -moduli) $r \in R \mapsto ar \in R$, quindi è isomorfo ad un quoziente di $(P : a)_R$ ed è così finitamente generato. Ne segue che $P = H + a(P : a)_R$ è finitamente generato, una contraddizione. Dunque $(P : a)_R = P$. Concludiamo, grazie al [Lemma 3.6](#), che P è primo. \square



Proposizione 6.10. *Sia R un anello commutativo unitario. Allora R è noetheriano se e solo se ogni suo ideale primo è finitamente generato.*

Dimostrazione. Il lemma precedente mostra che se R non è noetheriano R ha un ideale primo non finitamente generato. \square

Come molti dei risultati che mostrano l'influenza degli ideali primi per la struttura di un anello commutativo, anche quest'ultima proposizione richiede l'ipotesi che l'anello sia unitario. Infatti, se $(A, +)$ è un qualsiasi gruppo abeliano non finitamente generato, munito A della moltiplicazione costante nulla A si struttura come anello commutativo privo di ideali primi, ma l'insieme dei suoi ideali, che coincide con l'insieme $\mathcal{L}_{\mathbb{Z}}(A)$ dei sottogruppi di A non è a condizione massimale (perché?).

È facile trovare esempi di (pre)moduli finitamente generati non noetheriani, ad esempio il modulo ciclico R_R se R è un anello commutativo unitario non noetheriano; ma per (pre)moduli su anelli noetheriano queste condizioni sono equivalenti.

Proposizione 6.11. *Sia M un (pre)modulo su un anello commutativo noetheriano R . Allora M è noetheriano se e solo se è finitamente generato.*

Dimostrazione. Se M è noetheriano allora M è finitamente generato, per la [Proposizione 6.8](#). Viceversa, assumiamo che M sia finitamente generato. Supponiamo che M sia un R -modulo. Allora M è isomorfo ad un quoziente di un R -modulo libero finitamente generato F , per la [Proposizione 4.20](#), ed F è somma diretta di un numero finito di copie di R_R , quindi è noetheriano per il [Corollario 6.3](#). Ne segue che anche M è noetheriano. Se invece M non è un modulo su R , comunque M è un modulo finitamente generato sull'anello accresciuto R_1 definito da R , che è noetheriano per il [Lemma 6.5\(ii\)](#), quindi, per il caso precedente, M è noetheriano come R_1 -modulo e dunque come R -premodulo per il [Lemma 6.6](#). \square

6.3 Il teorema della base di Hilbert

Teorema 6.12 (Il teorema della base; D. Hilbert). *Sia R un anello commutativo unitario noetheriano. Allora ogni anello di polinomi a coefficienti in R su un insieme finito di indeterminate è noetheriano.*

Dimostrazione. Basta provare l'asserto per un anello $R[x]$ di polinomi ad una indeterminata; il risultato segue poi da un semplice ragionamento per induzione sul numero di indeterminate. Sia dunque $H \triangleleft R[x]$; intendiamo dimostrare che H è finitamente generato.

Sia C l'insieme dei coefficienti direttori dei polinomi in H (ivi incluso 0_R , come coefficiente direttore di sé stesso). Verifichiamo che C è un ideale di R : per ogni $c, d \in C$ e $r \in R$, esistono in H elementi h_c e h_d che abbiano, rispettivamente, c e d come coefficienti direttori; allora o $c-d = 0_R$ oppure $c-d$ è il coefficiente direttore di $h_c - h_d \in H$, in entrambi i casi $c-d \in C$; allo stesso modo o $cr = 0_R$ oppure cr è il coefficiente direttore di $h_cr \in H$, quindi $cr \in C$. Dunque, $C \triangleleft R$. Allora C è R -finitamente generato; possiamo porre $C = FR$ per un insieme finito F . Per ogni $c \in F$ sia h_c un elemento di H di cui c è il coefficiente direttore; poniamo $\lambda_c = \nu h_c$ e $\lambda = \max_{c \in F} \lambda_c$; siano poi $S = \{h_c \mid c \in C\}$ e $H_0 = SR[x]$, dunque $H_0 \subseteq H$. Proveremo: $H \subseteq A := H_0 + \{x^i \mid \lambda > i \in \mathbb{N}\}R$. A questo scopo, ragionando per assurdo, supponiamo che f sia un elemento di grado minimo n in $H \setminus A$; ovviamente $n \geq \lambda$. Il coefficiente direttore a di f appartiene a C , quindi $a = \sum_{c \in F} cr_c$ per opportuni elementi $r_c \in R$. Sia $h = \sum_{c \in F} x^{n-\lambda_c} h_cr_c$. Allora h è un elemento di H_0 con coefficiente relativo a x^n uguale a quello, a , di f . Dunque $f - h \in H \setminus A$ e $\nu(f - h) < n$, in contraddizione con la scelta di f .

Si ha dunque $H_0 \subseteq H \subseteq A$. Ora, A/H_0 è un R -modulo finitamente generato, quindi un R -modulo noetheriano per la [Proposizione 6.11](#), sicché il suo R -sottomodulo H/H_0 è finitamente generato. Ma questo implica, banalmente, che H/H_0 è finitamente generato come $R[x]$ -modulo. Essendo anche H_0 finitamente generato, se ne deduce che H è $R[x]$ -finitamente generato.³ Grazie alla [Proposizione 6.8](#) la dimostrazione è ora completa. \square

Corollario 6.13. *Siano R un anello commutativo unitario e A una R -algebra unitaria finitamente generata. Allora A , come anello, è noetheriano.*

Dimostrazione. Per la proprietà universale degli anelli di polinomi, A è, come R -algebra e quindi come anello, isomorfo ad un quoziente di un anello di polinomi in R su un insieme finito di indeterminate, quindi è noetheriano. \square

L'ipotesi che A sia unitaria è qui essenziale (si veda l'[Esempio 6.B.1](#)).

Anche per gli anelli di serie formali di potenze vale l'analogo del teorema della base:

Teorema 6.14. *Sia R un anello commutativo unitario noetheriano. Allora anche l'anello $R[[x]]$ è noetheriano.*

³ Questo segue dall'[Esercizio 6.A.3](#), oppure, in alternativa, dal fatto che $H = H_0 + (A \cap H)$ e $A \cap H$ è finitamente generato come R -modulo.

Dimostrazione. Come mostra la [Proposizione 6.10](#), basterà provare che ogni ideale primo H di $R[[x]]$ è finitamente generato. Fissato $H \in \text{Spec}(R[[x]])$, supponiamo innanzitutto $x \in H$. Dal momento che $R[[x]]/xR[[x]] \simeq R$ è noetheriano ([Lemma 5.13](#)), il suo ideale $H/xR[[x]]$ è finitamente generato e quindi anche H è finitamente generato (se $H/xR[[x]]$ è generato da elementi $h_1 + xR[[x]]$, $h_2 + xR[[x]]$, \dots , $h_n + xR[[x]]$, allora $H = (h_1, h_2, \dots, h_n, x)$). Possiamo dunque assumere $x \notin H$.

Come per un passaggio analogo nella dimostrazione del [Teorema 6.12](#), che concerne coefficienti direttori, si riconosce facilmente che l'insieme C dei termini noti degli elementi di H costituisce un ideale di R . Esiste dunque un sottoinsieme finito F di R tale che $C = FR$. Per ogni $c \in C$ si fissi un $g_c \in H$ di cui c sia il termine noto. Proveremo che H è generato da $\{g_c \mid c \in F\}$. A questo scopo, sia $h \in H$. Indichiamo con $\varepsilon: R[[x]] \rightarrow R$ l'omomorfismo di anelli unitari che ad ogni serie associa il suo termine noto. Allora $h^\varepsilon \in C$, quindi $h^\varepsilon = \sum_{c \in F} cr_{c,0}$ per opportuni elementi $r_{c,0}$ di R . Evidentemente, se $s_0 = \sum_{c \in F} g_cr_{c,0}$ si ha $h^\varepsilon = s_0^\varepsilon$, quindi $h - s_0 \in \ker \varepsilon = xR[[x]]$ (detto diversamente, h ed s_0 hanno lo stesso termine noto, quindi $h - s_0$ è multiplo di x). Esiste allora $h_1 \in R[[x]]$ tale che $h = s_0 + xh_1$. Ora, chiaramente $s_0 \in H$, quindi $xh_1 = h - s_0 \in H$; poiché H è primo e $x \notin H$ ne segue $h_1 \in H$. Possiamo allora ripetere il procedimento per h_1 , mostrando così che esistono elementi $r_{c,1}$ di R , uno per ogni $c \in F$, ed $h_2 \in H$ tali che, ponendo $s_1 = \sum_{c \in F} g_cr_{c,1}$, si abbia $h_1 = s_1 + xh_2$, e quindi $h = s_0 + xs_1 + x^2h_2$. Procedendo in maniera analoga definiamo ricorsivamente $|F|$ successioni $(r_{c,n})_{n \in \mathbb{N}}$ di elementi di R , una per ciascun $c \in C$, ed una successione $(h_n)_{n \in \mathbb{N}^+}$ di elementi di $R[[x]]$ con la proprietà che, ponendo $s_i = \sum_{c \in F} g_cr_{c,i}$ per ogni $i \in \mathbb{N}$, si abbia, per ogni $n \in \mathbb{N}$, $h = x^{n+1}h_{n+1} + \sum_{i=0}^n x^i s_i$, vale a dire:

$$h = \sum_{c \in F} \left(g_c \sum_{i=0}^n r_{c,i} x^i \right) + x^{n+1} h_{n+1}.$$

Per ogni $c \in F$ poniamo $r_c = \sum_{i \in \mathbb{N}} r_{c,i} x^i$. Quanto appena visto mostra che, per ogni $n \in \mathbb{N}$, la differenza $h - \sum_{c \in F} g_cr_c$ è divisibile per x^{n+1} ; da ciò segue che questa differenza è 0_R , quindi $h = \sum_{c \in F} g_cr_c$ appartiene a $(g_c \mid c \in F)$. Pertanto $H = (g_c \mid c \in F)$ è finitamente generato, come si voleva dimostrare. \square

Esercizi, osservazioni, esempi.

6.B.1. Sia $A = \bigoplus_{i \in \mathbb{N}} \langle a_i \rangle$ un gruppo abeliano libero di base $\{a_i \mid i \in \mathbb{N}\}$, dove $a_i \neq a_j$ se $i \neq j$. Si strutturi A come modulo sull'anello di polinomi ad una indeterminata $\mathbb{Z}[x]$ tramite l'omomorfismo di anelli unitari $\mathbb{Z}[x] \rightarrow \text{End}(A, +)$ che ad x associa l'endomorfismo di A definito da $a_i \mapsto a_{i+1}$ per ogni $i \in \mathbb{N}$. Munito poi A del prodotto costante nullo, A diventa una $\mathbb{Z}[x]$ -algebra non unitaria. Verificare che, come $\mathbb{Z}[x]$ -algebra, A è generata da un elemento, ma, benché $\mathbb{Z}[x]$ sia noetheriano, A non è un anello noetheriano.

6.B.2. Tra questi anelli, quali sono noetheriani? E quali sono artiniani? $\mathbb{Z}_8[x]$; $\mathbb{Q}[x]/(x^{10})$; il sottoanello del campo complesso $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ (questo è l'anello degli interi di Gauss); $\mathbb{Z}[X]/(x^2 \mid x \in X)$ per un insieme infinito X indeterminate; $(\mathcal{P}(\mathbb{N}), \Delta, \cap)$.

6.B.3. Sia K un campo e sia $K[X]$ l'anello dei polinomi su un insieme infinito di indeterminate. Individuare un ideale di $K[X]$ che sia massimale tra quelli non finitamente generati. Ripetere l'esercizio dopo aver sostituito \mathbb{Z} a K .

6.B.4. Il teorema della base di Hilbert ha una importante applicazione geometrica. In sostanza: ogni sistema di equazioni polinomiali su un campo, in cui sia coinvolto solo un numero finito di indeterminate, ha lo stesso insieme di soluzioni di un sistema con un numero finito di equazioni.

Più esplicitamente: fissati un campo K , un intero positivo n ed un anello di polinomi $R = K[x_1, x_2, \dots, x_n]$ ad n indeterminate su K , ogni parte S di R definisce, nello spazio vettoriale

6 Condizioni di catena per moduli e anelli

numerico K^n , l'insieme $V(S) = \{(a_1, a_2, \dots, a_n) \in K^n \mid \forall (f \in S)(f(a_1, a_2, \dots, a_n) = 0_K)\}$ delle soluzioni comuni a tutte le equazioni $f = 0_K$ al variare di f in S ; questo insieme è la cosiddetta varietà algebrica (o insieme algebrico; alcuni autori riservano l'espressione varietà algebrica ad insiemi che verificano un'ulteriore proprietà di irriducibilità) definito da S in K^n . È facile rendersi conto del fatto che $V(S) = V(H)$ se $H = SR$ è l'ideale generato da S in $R[X]$. Ora, per il teorema della base, H è finitamente generato; se F è un suo insieme finito di generatori si ha $V(S) = V(F)$, e questo giustifica la frase con cui abbiamo aperto questa osservazione. Un insieme F di polinomi tale che $V(S) = V(F)$ veniva (e certi contesti viene ancora) chiamato 'base' di $V(H)$ (o di H) e questo spiega il nome che ha ricevuto il teorema: ogni ideale di R , ovvero ogni varietà algebrica in K^n , ha una base finita.

A questo proposito, menzioniamo un altro teorema dovuto a David Hilbert che ha grande importanza in geometria algebrica, il teorema degli zeri (o *Nullstellensatz*): con le notazioni qui introdotte, nel caso in cui il campo K sia algebricamente chiuso, l'insieme degli $f \in R$ tali che ogni elemento di $V(S)$ sia soluzione dell'equazione $f = 0_K$ è il radicale di H in R .

7 Decomposizione primaria

La nozione di ideale primario è una ampia ed utile generalizzazione di quella di ideale primo. Esiste una classica teoria della decomposizione primaria di ideali, cioè della maniera in cui un ideale di un anello commutativo unitario può essere rappresentato come intersezione di un numero finito di ideali primari, che ha particolare rilevanza per lo studio degli anelli noetheriani.

7.1 Ideali primari

Sia R un anello commutativo. Un ideale H di R si dice *primario* (in R) se e solo se $H \neq R$ e, nell'anello quoziente R/H , ogni divisore dello zero è un elemento nilpotente. Come sappiamo, dire che un elemento $a + H$ di R/H è nilpotente equivale a dire che $a \in \sqrt{H}$. Dire invece che $a + H$ è un divisore dello zero in R/H equivale a dire che esiste $b \in R \setminus H$ tale che $ab \in H$, ovvero $b \in (H : a)_R$ o, ancora, $a \in (H : b)_R$. Tenendo conto che in ogni caso si ha $H \subseteq (H : a)_R$, abbiamo così:

Lemma 7.1. *Siano R un anello commutativo e $H \triangleleft R$. Per ogni $a \in R$ sono equivalenti:*

- (i) $a + H$ è un divisore dello zero in R/H ;
- (ii) $(H : a)_R \neq H$;
- (iii) $a \in \bigcup \{(H : b)_R \mid b \in R \setminus H\}$.

Definizioni alternative sono suggerite da questo semplice lemma:

Lemma 7.2. *Siano R un anello commutativo e H un suo ideale proprio. Sono allora equivalenti:*

- (i) H è primario in R ;
- (ii) per ogni $r \in R \setminus \sqrt{H}$, $(H : r)_R = H$;
- (iii) per ogni $r \in R \setminus H$, $(H : r)_R \subseteq \sqrt{H}$;
- (iv) per ogni $r, s \in R$ tali che $rs \in H$, o $r \in H$ oppure $s \in \sqrt{H}$.

Dimostrazione. L'equivalenza tra (i) e (ii) e quella tra (i) e (iii) seguono subito dalle equivalenze tra le corrispondenti affermazioni in [Lemma 7.1](#). La (iv) è una riformulazione di (iii): essa afferma che se $r, s \in R$ e $s \in (H : r)_R$, allora $r \in H$ o $s \in \sqrt{H}$. \square

È evidente che tutti gli ideali primi sono primari. Il viceversa non vale; ad esempio è facile verificare (segue immediatamente dal [Lemma 7.5](#)) che per ogni primo p e ogni numero intero positivo n , l'ideale $p^n\mathbb{Z}$ è primario in \mathbb{Z} , ma non primo se $n > 1$. Più in generale, si ha infatti:

Lemma 7.3. *In un anello commutativo R sia p un elemento cancellabile tale che pR sia un ideale primo. Allora, per ogni $n \in \mathbb{N}^+$, p^nR è un ideale primario in R .*

Dimostrazione. Certamente $p^nR = (pR)^n \subseteq pR \subset R$, e $pR = \sqrt{p^nR}$ per l'[Esercizio 3.C.5](#). Supponiamo n minimo possibile per la proprietà che p^nR non sia primario. Allora $n > 1$ ed esistono $a, b \in R$ tali che $ab \in p^nR$, $a \notin p^nR$ e $b \notin pR$. Dal momento che pR è primo, $a \in pR$; esiste dunque $c \in R$ tale $a = pc$. Da $p^n \mid ab = pcb$ e dalla cancellabilità di p deduciamo $p^{n-1} \mid cb$, ovvero $cb \in p^{n-1}R$. Per la minimalità di n , $p^{n-1}R$ è primario e quindi da $b \notin pR = \sqrt{p^{n-1}R}$ segue $c \in p^{n-1}R$. Questo comporta $a = pc \in p^nR$, una contraddizione. \square

Abbiamo però:

Lemma 7.4. Se Q è un ideale primario di un anello commutativo R , il radicale $P = \sqrt{Q}$ di Q in R è R o un suo ideale primo.

Dimostrazione. Siano $a, b \in R$ tali che $ab \in P$, quindi $a^n b^n \in Q$ per un opportuno $n \in \mathbb{N}^+$, e $a \notin P$ dunque, di conseguenza, $a^n \notin Q$. Poiché Q è primario si ha allora $b^n \in P$, e quindi $b \in \sqrt{P} = P$, il che prova l'asserto. \square

Come sappiamo dal [Lemma 3.14](#), se R è unitario il caso $\sqrt{Q} = R$ non si può verificare, quindi ogni ideale primario in un anello commutativo unitario ha radicale primo. Se Q è un ideale primario di un anello commutativo e $P = \sqrt{Q}$, si dice anche che Q è un ideale P -primario.

Sono ovviamente primari tutti gli ideali propri di un anello commutativo R che abbiano R come radicale, caso che si può presentare solo se R non è unitario. Nel caso degli anelli commutativi unitari si verifica invece che sono primari gli ideali con radicale massimale. Questo risultato fornisce un gran numero di esempi interessanti di ideali primari.

Lemma 7.5. Siano R un anello commutativo unitario e $Q \triangleleft R$. Se $P := \sqrt[Q]{Q} \triangleleft R$, allora Q è un ideale primario in R .

Dimostrazione. L'ipotesi comporta che $\bar{P} := P/Q$ è l'unico ideale primo di $\bar{R} := R/Q$, che è quindi un anello locale con ideale massimale \bar{P} . Allora $\bar{R} \setminus \bar{P} = \mathcal{U}(\bar{R})$, per il [Corollario 3.23](#). Dunque, i divisori dello zero in \bar{R} sono tutti contenuti in $\bar{P} = \text{NilRad}(\bar{R})$ e sono quindi nilpotenti, sicché Q è primario. \square

Il risultato analogo non vale nel caso degli anelli non unitari; lo si può verificare con l'[Esempio 7.A.2](#).

Altri due semplici risultati che forniscono ideali primari sono:

Lemma 7.6. Sia R un anello commutativo e siano Q un suo ideale primario e $P = \sqrt{Q}$. Allora, per ogni $a \in R \setminus Q$, $(Q : a)_R$ è un ideale P -primario di R .

Dimostrazione. Come segue dal [Lemma 7.2](#), valgono le inclusioni $Q \subseteq (Q : a)_R \subseteq P$. Di conseguenza, $P = \sqrt{(Q : a)_R}$. Siano ora $r, s \in R$ tali che $rs \in (Q : a)_R$ e $r \notin (Q : a)_R$. Allora $ars \in Q$ e $ar \notin Q$, quindi $s \in \sqrt{Q} = P = \sqrt{(Q : a)_R}$. Concludiamo che $(Q : a)_R$ è P -primario. \square

Lemma 7.7. Siano R un anello commutativo e H, K due ideali primari di R con lo stesso radicale P . Allora anche $H \cap K$ è un ideale P -primario in R .

Dimostrazione. Il [Lemma 3.14](#) fornisce $\sqrt{H \cap K} = \sqrt{H} \cap \sqrt{K} = P$; si tratta dunque solo di provare che $H \cap K$ è primario. Ovviamente $H \cap K \subset R$. Siano $a, b \in R$ tali che $ab \in H \cap K$ e $a \notin H \cap K$. Se $a \notin H$, allora $b \in \sqrt{H} = P$, perché H è primario; alla stessa conclusione si arriva se $a \in H$ e quindi $a \notin K$. Il lemma è così dimostrato. \square

Due esempi importanti Abbiamo detto che gli ideali primari di \mathbb{Z} sono tutte e sole le potenze (ad esponente intero positivo) di ideali primi (lo stesso è vero per tutti gli anelli principali: [Esercizio 7.A.1](#)) e che, negli anelli commutativi unitari, tutti gli ideali con radicale massimale sono primari. Questo potrebbe far supporre che, in ogni anello commutativo unitario, tutti gli ideali con radicale primo siano primari, o magari che la proprietà di essere un ideale primario implichi o sia implicata dalla proprietà di essere potenza di un ideale primo. Nulla di tutto ciò è vero.

Iniziamo da un esempio molto semplice.¹ Siano K un campo, $R = K[x, y]$ un anello di polinomi su K nelle indeterminate x e y ed infine $M = (x, y)$ l'ideale generato in R dalle due

¹ Si veda anche l'[Esercizio 7.A.3](#).

indeterminate. Poiché $R/M \simeq K$, certamente $M \triangleleft R$. Sia H un ideale di R strettamente compreso tra $M^2 = (x^2, xy, y^2)$ ed M , ad esempio: $H = (x, y^2)$. Allora, poiché $M^2 \subseteq H$, si ha $M \subseteq \sqrt{H}$, ma $M \triangleleft R$ e $\sqrt{H} \neq R$ per il Lemma 3.14, quindi $\sqrt{H} = M$ e H è M -primario, per il Lemma 7.5. Infine, dal fatto che $M^2 \subset H \subset M$ segue che H non è una potenza di M , quindi non è una potenza di un ideale primo (non solo perché M è l'unico ideale primo contenente H : se un ideale è potenza di un ideale primo, abbiamo già visto che quest'ultimo è il suo radicale.)

Il secondo esempio è più elaborato. Intendiamo costruire un anello commutativo unitario R ed un suo ideale primo P tali che, per un certo intero $n > 1$, l'ideale P^n non sia primario in R . Piuttosto che limitarci a fornire un esempio 'già pronto', proviamo qui a mostrare in che modo si può procedere per costruirne uno; le stesse tecniche potranno essere adottate in situazioni analoghe per produrre controesempi di altro genere.

Quando si cerca di costruire esempi che soddisfino specifiche condizioni un possibile approccio è quello di considerare la situazione più generale possibile, esaminando le conseguenze delle condizioni richieste in modo da restringere il campo dei possibili esempi a quegli oggetti per i quali queste conseguenze siano soddisfatte. Può anche capitare di osservare che se un esempio del tipo desiderato esiste, ne esiste necessariamente anche uno che verifichi delle proprietà aggiuntive; in questo caso possiamo, come si dice, ridurre il problema limitandoci a considerare solo i potenziali esempi per i quali valgono queste ulteriori proprietà, il che può risultare vantaggioso se (e non è scontato) questa assunzione semplifica la nostra ricerca.

Vediamo cosa significa tutto ciò nel nostro caso. Stiamo cercando un anello commutativo unitario R , un suo ideale primo P e un intero $n > 1$ con le proprietà sopra specificate; ricordando che in questa situazione si ha certamente $P = \sqrt{P^n}$, servono dunque in R elementi a, b tali che $ab \in P^n$, $a \notin P$ e $b \notin P^n$. Essendo P primo, necessariamente si deve avere anche $b \in P$. Inoltre, se supponiamo che un esempio siffatto esista, allora il sottoanello unitario di R generato da $P \cup \{a, b\}$ ha le stesse proprietà richieste per R . Meglio ancora: come è facile verificare, se $ab \in P^n$, esiste un insieme finito $F \subseteq P$ tale che $ab \in F^n$. Se R_1 è il sottoanello unitario di R generato da $F \cup \{a, b\}$ e $P_1 = P \cap R_1$, allora $P_1 \in \text{Spec}(R_1)$, $ab \in P_1^n$, $a \notin P_1$ e $b \notin P_1^n$, quindi R_1 e P_1 (ed n) forniscono un esempio con le proprietà richieste in partenza. Abbiamo così una vantaggiosa riduzione: possiamo limitarci a considerare anelli commutativi unitari R che siano finitamente generati. Ogni tale R è, come sappiamo, isomorfo ad un quoziente di un anello di polinomi su \mathbb{Z} in un insieme finito di indeterminate, quindi ci riduciamo a ragionare su anelli di questo tipo.

D'altra parte, anche dopo le eventuali riduzioni la situazione potrebbe essere considerata ancora troppo complicata. È spesso conveniente cercare un compromesso tra l'analisi della situazione generale e la considerazione di specifici casi particolari in cui il problema assuma una forma semplificata: la generalità garantirebbe che l'esempio, se esiste, non possa sfuggire dalla rete; ma la semplificazione ci può aiutare a trovarlo e riconoscerlo effettivamente.

Tornando al nostro problema specifico, una difficoltà che incontriamo è data dalla condizione $ab \in P^n$: potrebbe essere non facilissimo stabilire se, in un dato anello, un assegnato elemento è o non è somma di un numero non specificato di prodotti di n elementi in un prefissato ideale. Il compromesso che ci permette di semplificare la situazione può essere questo: tentare di costruire un esempio in cui $n = 2$ e ab sia il prodotto di due elementi di P ; se ci riusciamo abbiamo risolto il problema, se non ci riusciamo possiamo riprovare con un'assunzione più debole.

Riassumendo, a questo punto stiamo cercando un anello commutativo unitario R ed un suo ideale primo P costruiti in modo che esistano in R elementi a, b, c, d tali che $a \notin P$ ma $b, c, d \in P$ ed inoltre $ab = cd$ e $b \notin P^2$. Per la riduzione vista sopra, possiamo anche assumere che, come anello unitario, R sia generato da $\{a, b, c, d\}$.

A questo punto R deve essere isomorfo ad un quoziente dell'anello di polinomi a quattro indeterminate $S := \mathbb{Z}[x, y, z, t]$. Possiamo dunque provare a porre $R = S/H$ per un opportu-

no $H \triangleleft S$ e, detto $\varepsilon: S \rightarrow R$ l'epimorfismo canonico, porre $a = x^\varepsilon$, $b = y^\varepsilon$, $c = z^\varepsilon$ e $d = t^\varepsilon$. Imporre $ab = cd$ significa imporre $xy \equiv_H zt$, ovvero $xy - zt \in H$. Dobbiamo quindi richiedere che valga questa condizione. Serve anche fissare un ideale primo P di R , vale a dire: scegliere un ideale primo L di S contenente H e porre $P = L/H$. Come sopra, la condizione $b, c, d \in P$ si traduce nella richiesta $y, z, t \in L$. Dunque, sicuramente servono in S un ideale H tale che $(xy - zt) \subseteq H$ ed un ideale primo L tale che $H + (y, z, t) \subseteq L$; scelti in qualche modo tali H ed L si tratta poi di verificare se le ulteriori condizioni richieste per il nostro esempio sono o meno verificate. È abbastanza ragionevole provare per prima la scelta più semplice: $H = (xy - zt)$ e $L = (y, z, t)$; qui abbiamo tenuto conto di due fatti piuttosto evidenti: $(xy - zt) \subseteq (y, z, t)$ e $S/(y, z, t) \simeq \mathbb{Z}[x]$ è un dominio di integrità, quindi (y, z, t) è primo. Risulta che questa scelta è fortunata: tutte le condizioni richieste sono soddisfatte. Abbiamo infatti:

Proposizione 7.8. *Sia $S = \mathbb{Z}[x, y, z, t]$ un anello di polinomi su \mathbb{Z} nelle quattro indeterminate x, y, z, t , siano $H = (xy - zt) \triangleleft S$ e $R = S/H$. Allora $P := (y, z, t)/H$ è un ideale primo di R e P^2 non è primario in R .*

Dimostrazione. Palesemente $(y, z, t) \supseteq H$, quindi l'ideale P è ben definito, e $R/P \simeq S/(y, z, t) \simeq \mathbb{Z}[x]$ è un dominio di integrità e così P è primo in R . Sia ε l'epimorfismo canonico $S \rightarrow R$ e siano $a = x^\varepsilon$, $b = y^\varepsilon$, $c = z^\varepsilon$ e $d = t^\varepsilon$. Allora $c, d \in P$ e $ab - cd = (xy - zt)^\varepsilon = 0_R$, quindi $ab = cd \in P^2$. D'altra parte $x \notin (y, z, t)$, quindi $a \notin P$. Inoltre, posto $I = (y, z, t)^2 + H$, in modo che $P^2 = I/H$, è chiaro che tutti gli elementi non nulli di I sono polinomi di grado totale (nel senso dell'Osservazione 5.A.1) maggiore di 1, quindi $y \notin I$, ovvero $b \notin P^2$. A questo punto è dimostrato che P^2 non è un ideale primario di R . \square

Esercizi.

7.A.1. Verificare che in un anello principale gli ideali primari sono tutte e sole le potenze ad esponente positivo degli ideali primi.

7.A.2. Sia M un anello non nullo con moltiplicazione costante nulla. Allora nell'anello prodotto diretto $R = M \times \mathbb{Z}_2$ si ha che $M = \text{NilRad}(R)$ è massimale e primo in R , ma l'ideale nullo, pur avendo M come radicale, non è primario. Verificarlo.

È anche chiaro che M è l'unico ideale primo di R e, se M è scelto in modo che il suo gruppo additivo sia privo di sottogruppi massimali (ad esempio, il gruppo additivo razionale ha questa proprietà), allora M è anche l'unico ideale massimale di R .

7.A.3. Si verifichino in dettaglio tutti i passaggi omissi nella discussione del primo degli esempi in "Due esempi importanti" (ad esempio, il fatto che tutte le inclusioni indicate come strette lo siano).

Con riferimento alle notazioni usate per quell'esempio, si osservi anche che M/M^2 può essere riguardato, a meno di cambio degli scalari, come spazio vettoriale su R/M , ovvero su K , di dimensione 2 e che l'applicazione $I \mapsto I/M^2$ dall'insieme degli ideali di R strettamente compresi tra M e M^2 all'insieme dei K -sottospazi di dimensione 1 di M/M^2 è biettiva, il che permette di descrivere facilmente questi ideali.

7.A.4. In un certo senso l'esempio presentato nella [Proposizione 7.8](#) non è ottimale: ne si può ottenere uno come quoziente di un anello di polinomi su \mathbb{Z} con tre indeterminate. Si arriva ad un esempio di questo tipo se, seguendo la procedura discussa prima della proposizione, anziché richiedere che ab sia il prodotto tra due arbitrari elementi di P si assume la condizione più forte che ab sia il quadrato di un elemento di P . Effettuare la costruzione fino a costruire l'esempio richiesto.

Osservare, inoltre, che \mathbb{Z} può essere sostituito in questa costruzione da un qualsiasi dominio di integrità unitario.

7.A.5. Chiamiamo pseudoprimary ogni ideale proprio H di un anello commutativo R che abbia questa proprietà: per ogni $a, b \in R$, se $ab \in H$ allora uno tra a e b appartiene a \sqrt{H} . Trovare un esempio di ideale pseudoprimary ma non primary in un anello commutativo unitario.

7.2 Decomposizioni primarie e decomposizioni primarie minimali

Sia R un anello commutativo e sia $H \triangleleft R$. Informalmente si dice che una decomposizione primaria di H è una rappresentazione

$$H = Q_1 \cap Q_2 \cap \cdots \cap Q_n$$

di H come intersezione di un numero finito ideali primari di R . In modo più preciso, chiamiamo *decomposizione primaria* di H un insieme finito e non vuoto \mathcal{D} di ideali primari di R tale che $H = \bigcap \mathcal{D}$. Si dice che H è *decomponibile* (o decomponibile in ideali primari) se e solo se H ha una decomposizione primaria. Sono ovviamente decomponibili gli ideali primari, e vedremo che in un anello noetheriano tutti gli ideali propri sono decomponibili, ma esistono anelli con ideali propri non decomponibili; alcuni esempi sono tra gli esercizi al termine di questa sezione.

Sono di particolare interesse le decomposizioni di un assegnato ideale con la minima cardinalità possibile. Fissati un anello commutativo R ed un suo ideale decomponibile H , diciamo che una decomposizione primaria \mathcal{D} di H (in R) è irridondante se e solo se nessuna parte propria di \mathcal{D} è una decomposizione primaria di H , vale a dire: o $|\mathcal{D}| = 1$ oppure $H \subset \bigcap (\mathcal{D} \setminus \{Q\})$ per ogni $Q \in \mathcal{D}$. Equivalentemente, \mathcal{D} è irridondante se e solo se $|\mathcal{D}| = 1$ oppure, per ogni $Q \in \mathcal{D}$, si ha $\bigcap (\mathcal{D} \setminus \{Q\}) \not\subseteq Q$. Si dice poi che \mathcal{D} è una decomposizione primaria minimale di H quando \mathcal{D} è irridondante e l'applicazione $Q \in \mathcal{D} \mapsto \sqrt{Q} \in \mathcal{J}(R)$ è iniettiva.

Lemma 7.9. *Siano R un anello commutativo e H un suo ideale decomponibile. Allora H ha una decomposizione primaria minimale in R .*

Dimostrazione. Sia \mathcal{D} una decomposizione primaria di H di cardinalità minima possibile. È chiaro che \mathcal{D} deve essere irridondante. Se esistono $I, J \in \mathcal{D}$ tali che $P := \sqrt{I} = \sqrt{J}$, allora, per il Lemma 7.7, anche $I \cap J$ è P -primary, quindi $(\mathcal{D} \setminus \{I, J\}) \cup \{I \cap J\}$ è una decomposizione primaria di H di cardinalità minore di $|\mathcal{D}|$, contraddicendo la scelta di \mathcal{D} . Questa contraddizione mostra che \mathcal{D} è una decomposizione primaria minimale di H . \square

Consideriamo, ad esempio, le decomposizioni primarie minimali per ideali di \mathbb{Z} . Sia \mathcal{D} un insieme non vuoto di ideali primari di \mathbb{Z} , dunque \mathcal{D} è una decomposizione primaria di $H := \bigcap \mathcal{D}$. Tralasciando il caso banale in cui $\{0\} \in \mathcal{D}$ (in questo caso \mathcal{D} è una decomposizione primaria di $\{0\}$, ed è minimale se e solo se $\mathcal{D} = \{0\}$) abbiamo $\mathcal{D} = \{p_1^{\lambda_1} \mathbb{Z}, p_2^{\lambda_2} \mathbb{Z}, \dots, p_n^{\lambda_n} \mathbb{Z}\}$ per opportuni $n \in \mathbb{N}^+$, numeri primi positivi p_1, p_2, \dots, p_n e interi positivi $\lambda_1, \lambda_2, \dots, \lambda_n$. Allora $H = m\mathbb{Z}$, dove m è un minimo comune multiplo di $p_1^{\lambda_1}, p_2^{\lambda_2}, \dots, p_n^{\lambda_n}$; è chiaro che \mathcal{D} è una decomposizione irridondante di H se e solo se i primi p_i sono a due a due distinti, nel qual caso $m = \prod_{i=1}^n p_i^{\lambda_i}$ e \mathcal{D} è una decomposizione primaria minimale di $m\mathbb{Z}$. Da queste considerazioni e dal teorema fondamentale dell'aritmetica segue molto facilmente che, in \mathbb{Z} , ogni ideale ha una ed una sola decomposizione primaria minimale.

La teoria della decomposizione primaria consiste essenzialmente nel discutere fino a che punto questa proprietà di \mathbb{Z} , o qualche sua versione più debole, si estende al caso di anelli più generali.

7.2.1 Ideali irriducibili per intersezione e decomposizioni primarie in anelli noetheriani

Un ideale H di un anello commutativo R si dice irriducibile per intersezione (o \cap -irriducibile) se e solo se $H \subset R$ e H non è intersezione di due ideali che lo contengano propriamente. Almeno nel caso in cui R è unitario, questo equivale a dire che H è un elemento irriducibile nel monoide $(\mathfrak{J}(R), \cap, R)$. Il [Lemma 2.4](#) implica questo risultato del quale, per ragioni di chiarezza, forniamo anche una dimostrazione esplicita:

Lemma 7.10. *Sia R un anello commutativo noetheriano. Allora ogni ideale proprio di R è intersezione di un insieme finito di ideali \cap -irriducibili in R .*

Dimostrazione. Supponiamo l'asserto falso; allora l'insieme \mathcal{S} degli ideali propri di R che non sono intersezione di un insieme finito di ideali \cap -irriducibili non è vuoto ed ha quindi un elemento massimale H . Poiché H stesso non è allora \cap -irriducibile, si ha $I \cap J = H \subset I, J$ per opportuni $I, J \triangleleft R$. Per la massimalità di H , ora, $I, J \notin \mathcal{S}$, quindi I e J sono entrambi intersezioni di un numero finito di ideali \cap -irriducibili in R , e dunque H ha la stessa proprietà, contraddicendo la definizione di \mathcal{S} . \square

La rilevanza del lemma appena provato nel contesto di questo capitolo è resa evidente dalla proposizione che segue.

Proposizione 7.11. *Siano R un anello commutativo noetheriano e H un suo ideale \cap -irriducibile. Allora H è primario in R .*

Dimostrazione. Per definizione, $H \neq R$. Sia $a \in R \setminus H$ un divisore dello zero modulo H , valga cioè $H \subset I := (H : a)_R$. Basterà provare che a è nilpotente modulo H , ovvero $a \in \sqrt{H}$. Sia R_1 l'anello accresciuto definito da R ; ricordiamo che R_1 è noetheriano, in conseguenza del [Lemma 6.5](#), inoltre $H \triangleleft R_1$. Per ogni $n \in \mathbb{N}^+$, poniamo $K_n = (H : a^n)_{R_1}$. Allora $(K_n)_{n \in \mathbb{N}}$ è una successione crescente di ideali di R_1 , quindi esiste $n \in \mathbb{N}$ tale che $K_n = K_{n+1}$. Sia $J = H + a^n R_1$, l'ideale di R generato da $H \cup \{a^n\}$. Evidentemente $H \subseteq I \cap J$; vogliamo provare che vale l'uguaglianza. Sia $b \in I \cap J$. Allora $b = h + a^n r$ per un opportuno $r \in R_1$. Poiché $b \in I$, si ha $ab \in H$, ovvero $ah + a^{n+1}r \in H$. Ma allora $a^{n+1}r \in H$, dunque $r \in K_{n+1} = K_n$; pertanto $a^n r \in H$ e quindi $b \in H$. Abbiamo dunque $H = I \cap J$; poiché H è \cap -irriducibile e $H \subset I$, allora $H = J$, vale a dire: $a^n \in H$. Pertanto $a \in \sqrt{H}$, come si voleva. \square

L'[Esempio 7.B.10](#) mostra che questo risultato non si estende al caso degli anelli, anche unitari, non noetheriani.

Teorema 7.12. *Negli anelli commutativi unitari noetheriani ogni ideale proprio è decomponibile.*

Dimostrazione. Segue immediatamente dai due enunciati precedenti. \square

Esempi, Osservazioni, Esercizi.

7.B.1. Se K è un campo e $R = K[x, y]$ un anello di polinomi su K a due indeterminate, in R l'insieme $\{(x^2, y), (x, y^2)\}$ è una decomposizione primaria irridondante ma non minimale di $(x, y)^2$.

7.B.2. Verificare che se H è un ideale di un anello commutativo R e R/H è noetheriano, allora H è decomponibile in R .

7.B.3. Variazioni nella terminologia: alcuni autori chiamano *ridotte* le decomposizioni primarie minimali; talvolta, con terminologia che ha origine nella geometria, gli elementi di una decomposizione primaria minimale di un ideale H sono chiamati *componenti* di H , e dei loro radicali si dice che appartengono (!) ad H .

7.B.4. Provare che, per ogni insieme S , nell'anello delle parti di S gli ideali primari sono tutti e soli gli ideali di indice 2, e quindi sono tutti massimali. (Suggerimento: tutti gli elementi dell'anello sono idempotenti. Questo enunciato si estende a tutti gli anelli booleani)

Di conseguenza, gli ideali decomponibili di $\mathcal{P}(S)$ hanno indice finito. Se S è infinito si ottengono così vari esempi di ideali propri non decomponibili, come l'ideale nullo e quello costituito dalle parti finite di S .

7.B.5. Sia $R = \bigoplus_{i \in I} H_i$ un anello commutativo, somma diretta di una famiglia $(H_i)_{i \in I}$ di suoi ideali che siano tutti unitari. Provare che gli ideali primari di R sono tutti e soli quelli della forma $Q \oplus \bigoplus_{i \neq j \in I} H_j$ al variare di i in I e di Q tra gli ideali primari di H_i .

Dedurre che se l'insieme degli $i \in I$ tali che $H_i \neq 0$ è infinito, allora l'ideale nullo di R non è decomponibile.

7.B.6. Sia $(R_i)_{i \in I}$ una famiglia di anelli commutativi unitari non nulli, e sia $R = \prod_{i \in I} R_i$. Dimostrare che se Q è un ideale primario di R e per qualche $i \in I$ l' i -esimo idempotente canonico e_i di R non appartiene a Q , allora Q contiene $\prod_{i \neq j \in I} R_j$. Anche in questo caso, dedurre che se l'insieme degli $i \in I$ tali che $R_i \neq 0$ è infinito, allora l'ideale nullo di R non è decomponibile.

7.B.7. Sia C l'anello delle funzioni continue dall'intervallo reale $I = [0, 1]$ a \mathbb{R} . Ricordando dall'Esercizio 4.B.1 che gli ideali massimali di C sono tutti e soli gli ideali $M_i = \{f \in C \mid i^f = 0\}$ al variare di i in I , dopo aver osservato che per ogni $i, j \in I$, se $i \neq j$ esistono $f \in C \setminus M_i$ e $g \in C \setminus M_j$ tali che $fg = 0$, concludere che ogni ideale primario di C è contenuto in esattamente un ideale massimale e che quindi, in C , l'ideale nullo non è decomponibile.

7.B.8. Verificare che tutti gli ideali primi sono \cap -irriducibili.

7.B.9. Costruire, in un anello commutativo unitario noetheriano, un esempio di ideale primario che non sia \cap -irriducibile.

7.B.10. Fissato un numero primo positivo p , sia P un p -gruppo di Prüfer, riguardato come modulo su \mathbb{Z} , e sia $R = P \times \mathbb{Z}$ la sua idealizzazione. È facile verificare (farlo!) che ogni ideale di R che non contenga P è contenuto in P ed è di conseguenza \cap -irriducibile, ma non è primario.

Si noti che R non è lontanissimo dall'essere noetheriano: R_R è estensione di un R -modulo artiniiano, P , mediante un R -modulo noetheriano, $R/P \simeq \mathbb{Z}$.

7.B.11. Scrivere una decomposizione primaria minimale dell'ideale $(12(x+1)^3) \cap (8, x^2)$ nell'anello di polinomi $\mathbb{Z}[x]$.

7.3 Teoremi di unicità

A differenza di quanto accade per gli ideali di \mathbb{Z} , in generale, anche in un anello commutativo unitario noetheriano, un ideale decomponibile può avere più decomposizioni primarie minimali,

come mostrato dall'[Esempio 7.C.1](#). Valgono però due teoremi, noti come primo e secondo teorema di unicità per decomposizioni primarie minimali, che esprimono forme deboli ma comunque molto utili di unicità. Il primo garantisce che il numero degli ideali primari in una decomposizione primaria minimale di un fissato ideale è indipendente dalla decomposizione, così come l'insieme dei radicali degli ideali primari che vi appaiono.

Teorema 7.13 (Primo teorema di unicità). *Siano R un anello commutativo, H un suo ideale decomponibile e \mathcal{D} una decomposizione primaria minimale di H . Allora, ponendo $\text{Spec}'(R) = \{R\} \cup \text{Spec}(R)$,*

$$\{\sqrt{Q} \mid Q \in \mathcal{D}\} = \{P \in \text{Spec}'(R) \mid (\exists a \in R \setminus H)(P = \sqrt{(H : a)_R})\}. \quad (*)$$

Se \mathcal{D}' è un'altra decomposizione primaria minimale di H , allora $|\mathcal{D}'| = |\mathcal{D}|$ e $\{\sqrt{Q} \mid Q \in \mathcal{D}\} = \{\sqrt{Q} \mid Q \in \mathcal{D}'\}$.

Dimostrazione. Sia $a \in R \setminus H$, allora $\mathcal{D}_a := \{Q \in \mathcal{D} \mid a \notin Q\} \neq \emptyset$. Utilizzando il [Lemma 1.15](#) abbiamo $(H : a)_R = (\bigcap \mathcal{D} : a) = \bigcap_{Q \in \mathcal{D}} (Q : a) = \bigcap_{Q \in \mathcal{D}_a} (Q : a)$ e quindi $\sqrt{(H : a)} = \bigcap_{Q \in \mathcal{D}_a} \sqrt{(Q : a)}$ per il [Lemma 3.14](#). Dal momento che $\sqrt{Q} = \sqrt{(Q : a)} \in \text{Spec}'(R)$ per ogni $Q \in \mathcal{D}$, come mostra il [Lemma 7.6](#), e che gli ideali primi sono \cap -irriducibili ([Esercizio 7.B.8](#)), è facile concludere che $\sqrt{(H : a)} \in \text{Spec}'(R)$ se e solo se esiste $Q \in \mathcal{D}_a$ tale che $\sqrt{(H : a)} = \sqrt{(Q : a)} = \sqrt{Q}$. D'altra parte, per ogni $Q \in \mathcal{D}$ esiste $a \in (\bigcap (\mathcal{D} \setminus \{Q\})) \setminus Q$, perché \mathcal{D} è irridondante. Per un tale a si ha $\mathcal{D}_a = \{Q\}$ e quindi $\sqrt{(H : a)} = \sqrt{(Q : a)} = \sqrt{Q}$, per quanto visto sopra. A questo punto è provata la (*). Il resto dell'enunciato segue facilmente: (*) mostra che l'insieme $\{\sqrt{Q} \mid Q \in \mathcal{D}\}$ non dipende dalla particolare decomposizione primaria minimale \mathcal{D} scelta, e dalla definizione di decomposizione primaria minimale segue che la sua cardinalità è $|\mathcal{D}|$. \square

Nelle notazioni del teorema appena dimostrato, l'insieme $\{\sqrt{Q} \mid Q \in \mathcal{D}\}$ è indicato con $\text{Ass}(H)$ (o $\text{Ass}_R(H)$ se un riferimento all'anello ambiente è necessario) ed i suoi elementi vengono chiamati gli ideali associati all'ideale decomponibile H . Nel caso, importante, in cui R sia un anello commutativo noetheriano (ma non in generale, si veda l'[Esercizio 7.C.6](#)) la descrizione degli associati ad un ideale H di R è ancora più esplicita di quanto mostrato dal [Teorema 7.13](#), infatti in questo caso gli ideali associati ad H sono gli elementi di $\text{Spec}'(R)$ della forma $(H : a)_R$ per un opportuno $a \in R \setminus H$; questo segue dall'[Esercizio 7.C.5](#) e suggerisce una parziale estensione a moduli della nozione di ideale primo associato, brevemente discussa nell'[Osservazione 7.C.7](#).

Tra gli ideali associati ad un ideale decomponibile H di un anello commutativo R si distinguono quelli minimali per inclusione, che vengono chiamati *ideali isolati* associati ad H ; gli altri sono anche noti come ideali *immersi*, questa curiosa terminologia proviene dalla geometria. Evidentemente l'unico caso in cui R sia isolato è quello in cui $\text{Ass}_R(H) = \{R\}$, ovvero $R = \sqrt{H}$, dunque R non è unitario e l'unica decomposizione primaria minimale di H in R è $\{H\}$.

Ricordiamo che, in conseguenza dell'[Esercizio 3.B.4](#), per ogni ideale proprio H di un anello commutativo R , se non è vuota (cosa che non accade mai se R non è unitario), $\text{Var}(H)$ ha elementi minimali. Se H è decomponibile questi sono precisamente i primi isolati associati ad H . Infatti:

Lemma 7.14. *Siano R un anello commutativo e H un suo ideale decomponibile. Allora ogni ideale in $\text{Var}_R(H)$ contiene un ideale primo isolato associato ad H . Di conseguenza gli elementi minimali di $\text{Var}_R(H)$ sono i primi isolati associati ad H e sono così in numero finito.*

Dimostrazione. Sia $P \in \text{Var}(H)$, e sia \mathcal{D} una decomposizione primaria minimale di H . Dal momento che P è primo e $H = \bigcap \mathcal{D} \subseteq P$, esiste $Q \in \mathcal{D}$ tale che $Q \subseteq P$ e quindi $\sqrt{Q} \subseteq P$.

Ovviamente $\sqrt{Q} \neq R$, perché $P \neq R$, e poiché $\sqrt{Q} \in \text{Ass}(H)$ è chiaro che \sqrt{Q} contiene un ideale primo isolato associato a P . La prima parte dell'enunciato è così provata, la seconda segue senza difficoltà. \square

L'unione e l'intersezione tra gli ideali associati ad un ideale decomponibile H descrivono, rispettivamente l'insieme degli elementi di R nilpotenti modulo H e quello degli elementi che sono divisori dello zero modulo H , discussi anche nel [Lemma 7.1](#). Infatti:

Proposizione 7.15. *Siano R un anello commutativo e H un suo ideale decomponibile. Allora $\bigcap \text{Ass}_R(H) = \sqrt{H}$ e $\bigcup \text{Ass}_R(H) = \bigcup \{(H : a)_R \mid a \in R \setminus H\}$ è l'insieme dei elementi di R che sono divisori dello zero modulo H .*

Dimostrazione. Che valga $\bigcap \text{Ass}_R(H) = \sqrt{H}$ segue dal fatto che ogni ideale primo in $\text{Var}(H)$ contiene un primo associato ad H . Proviamo la seconda uguaglianza. Sia $a \in R \setminus H$. Se \mathcal{D} è una decomposizione primaria minimale di H , esiste $Q \in \mathcal{D}$ tale che $a \notin Q$ e $(H : a)_R \subseteq (Q : a)_R \subseteq \sqrt{Q} \in \text{Ass}_R(H)$. Dunque $\bigcup \{(H : a)_R \mid a \in R \setminus H\} \subseteq \bigcup \text{Ass}_R(H)$. Viceversa, sia $b \in \bigcup \text{Ass}_R(H)$. Allora, per il [Teorema 7.13](#), esiste $r \in R \setminus H$ tale che $b \in \sqrt{(H : r)_R}$, quindi $rb^n \in H$ per un opportuno $n \in \mathbb{N}^+$. Fissato un tale r , sia n minimo per la proprietà richiesta; allora $a := rb^{n-1} \notin H$ e $b \in (H : a)_R$. Con questo la dimostrazione è completa. \square

Veniamo infine al secondo teorema di unicità. Essenzialmente questo teorema garantisce che, nel passaggio da una decomposizione primaria all'altra di uno stesso ideale decomponibile, a poter variare sono solo gli ideali primari il cui radicale sia un ideale immerso. Questa situazione sarà poi anche illustrata dall'[Esempio 7.C.1](#). Stabiliamo ancora un po' di terminologia ed una notazione. Se \mathcal{D} è una decomposizione primaria minimale di un ideale decomponibile H in un anello commutativo R e $P \in \text{Ass}_R(H)$, indichiamo con $\mathcal{D}(P)$ l'unico ideale appartenente a \mathcal{D} che abbia P come radicale. Questo ideale $\mathcal{D}(P)$ è anche noto come la P -componente di H .

Teorema 7.16 (Secondo teorema di unicità). *Siano R un anello commutativo, H un suo ideale decomponibile e $P \in \text{Ass}_R(H)$. Se P è isolato (tra gli ideali associati ad H), allora, scelte comunque due decomposizioni primarie minimali \mathcal{D} e \mathcal{D}' di H , si ha $\mathcal{D}(P) = \mathcal{D}'(P)$.*

Dimostrazione. Se $\text{Ass}_R(H) = \{P\}$, allora $\{H\}$ è l'unica decomposizione primaria minimale di H ed in questo caso non c'è nulla da dimostrare. Possiamo allora supporre $\mathcal{J} := \text{Ass}_R(H) \setminus \{P\} \neq \emptyset$ (di conseguenza, anche se osservarlo non è essenziale ai fini della dimostrazione, $P \neq R$ e quindi P è primo). Poiché P è isolato, cioè minimale in $\text{Ass}_R(H)$, per ogni $I \in \mathcal{J}$ si ha $I \not\subseteq P$, possiamo quindi fissare $a_I \in I \setminus P$. Posto $a = \prod_{I \in \mathcal{J}} a_I$ si ha allora $a \in (\bigcap \mathcal{J}) \setminus P$.

Sia \mathcal{D} una decomposizione primaria minimale di H in R . Allora $H = \mathcal{D}(P) \cap (\bigcap \{\mathcal{D}(I) \mid I \in \mathcal{J}\})$. Poiché \mathcal{J} è finito ed a appartiene ad ogni $I \in \mathcal{J}$, esiste $\lambda = \lambda(\mathcal{D})$ tale che $a^\lambda \in \mathcal{D}(I)$ per ogni $I \in \mathcal{J}$. Se n è un intero maggiore di λ si ha allora $(H : a^n)_R = (\mathcal{D}(P) : a^n)_R \cap (\bigcap \{(\mathcal{D}(I) : a)_R \mid I \in \mathcal{J}\}) = (\mathcal{D}(P) : a^n)_R \cap R = (\mathcal{D}(P) : a^n)_R$. Ma $a^n \notin P$, perché $a \notin P$, quindi il [Lemma 7.2](#) fornisce $(H : a^n)_R = (\mathcal{D}(P) : a^n)_R = \mathcal{D}(P)$. Se ora \mathcal{D}' è un'altra decomposizione primaria minimale di H in R , scelto n maggiore sia di $\lambda(\mathcal{D})$ che di $\lambda(\mathcal{D}')$, applicando quanto appena provato sia a \mathcal{D} che a \mathcal{D}' , abbiamo $\mathcal{D}(P) = (H : a^n) = \mathcal{D}'(P)$, il che completa la dimostrazione. \square

Esercizi, osservazioni, esempi.

7.C.1. Siano K un campo e $R = K[x, y]$ un anello di polinomi su K . In R si considerino gli ideali $P = (x)$, $M = (x, y)$ e, per ogni $n, m \in \mathbb{N}^+$, $Q_{n,m} = (x^n, xy, y^m)$. Come è chiaro, P è primo ed M è massimale; inoltre M è il radicale di ciascuno degli ideali $Q_{n,m}$, che sono così M -primari. Per fissati $n, m \in \mathbb{N}^+$ si ha poi $Q_{n,m} \cap P = ((x^n, xy) + (y^m)) \cap P = (x^n, xy) + ((y^m) \cap P)$, per il [Lemma 1.8](#). Ora, evidentemente $(y^m) \cap P = (xy^m) \subseteq (xy)$, quindi $Q_{n,m} \cap P = (x^n, xy) =: H_n$ è indipendente dalla scelta di m . Se $n > 1$, gli ideali (primari) $Q_{n,m}$ e P non sono confrontabili ed hanno ovviamente radicali distinti (M e P), quindi, per ogni $m \in \mathbb{N}^+$, $\{Q_{n,m}, P\}$ è una decomposizione primaria minimale di H_n . È anche chiaro che se m e ℓ sono interi positivi distinti si ha $Q_{n,m} \neq Q_{n,\ell}$ (ad esempio perché nell'ovvio isomorfismo tra R/P e $K[y]$ gli ideali $Q_{n,m} + P/P$ e $Q_{n,\ell} + P/P$ corrispondono a $y^m K[y]$ e $y^\ell K[y]$). Dunque, in R , per ogni intero $n > 1$ l'ideale H_n ha infinite decomposizioni primarie minimali.

In questo esempio gli ideali associati all'ideale H_n sono due (entrambi primi): P ed M . Come si vede, $P \subset M$, quindi P è un (l'unico, in effetti) primo isolato, M è l'unico primo immerso. Nelle decomposizioni primarie minimali di H_n qui esibite, la P -componente (cioè l'ideale primario che ha P come radicale) è P stesso. Ciò è in accordo con il secondo teorema di unicità, che garantisce anzi che P appartiene a tutte le decomposizioni primarie minimali di H_n . Invece, essendo M un primo immerso, al variare delle decomposizioni primarie minimali di H_n la M -componente può (anzi, in questo caso evidentemente deve) variare.

7.C.2. Provare che l'intersezione tra due ideali primari I e J è primario se e solo se $\sqrt{I} = \sqrt{J}$ oppure I e J sono confrontabili.

7.C.3. Verificare che, per ogni ideale decomponibile H di un anello commutativo, le decomposizioni primarie minimali di H sono tutte e sole le decomposizioni primarie di H della minima cardinalità possibile.

7.C.4. Sia R un anello commutativo di dimensione (di Krull) 0, oppure un dominio di integrità di dimensione 1. Provare che ogni ideale di R ha al massimo una decomposizione primaria minimale.

Questa osservazione si applica (in modo banale) agli anelli principali, e, come si vedrà più avanti, anche al caso degli anelli artiniani ed a quello degli anelli di Dedekind.

7.C.5. Sia M un premodulo su un anello commutativo R . Verificare che ogni elemento massimale P di $\{\text{Ann}_R(x) \mid 0_M \neq x \in M\}$ è o R o un ideale primo di R ; se R è unitario e M è un R -modulo, allora P è primo.

Dedurre che se H è un ideale di un anello commutativo noetheriano R e P è un ideale associato ad H , allora esiste $a \in R \setminus H$ tale che $P = (H : a)_R$. [*Suggerimento:* $P = \sqrt{Q}$ dove Q è un elemento di una decomposizione primaria minimale \mathcal{D} di H . Applicare quanto provato prima all' R -(pre)modulo D/H , dove $D = \bigcap (\mathcal{D} \setminus \{Q\})$, tenendo presente che $P = \sqrt{(H : a)}$ per un $a \in D$.]

7.C.6. Siano K un campo, $K[X]$ un anello di polinomi nell'insieme infinito di indeterminate X ed M il suo ideale massimale (X) . Scelto, per ogni $x \in X$, un intero $\lambda_x > 1$, l'ideale $Q = (x^{\lambda_i} \mid i \in \mathbb{N})$ è primario, ma il suo radicale M contiene propriamente $(H : a)_R$ per ogni $a \in R \setminus H$. Verificarlo.

7.C.7. Viene definita una nozione di primo associato ad un modulo, che non è sempre sovrapponibile a quella qui definita per ideali decomponibili.

Se M è un modulo su un anello commutativo unitario R , vengono chiamati primi associati ad M gli ideali primi che siano annullatori di un elemento non nullo di M . È chiara la relazione tra questa definizione ed il contenuto dell'[Esercizio 7.C.5](#): se R è noetheriano e $H \triangleleft R$, i primi associati ad H nel senso definito nel testo sono precisamente i primi associati all' R -modulo R/H nel senso appena definito in questa osservazione. L'esempio precedente

7 Decomposizione primaria

mostra che questo non vale per ideali decomponibili di anello commutativo unitario (anche fattoriali) non noetheriani.

7.C.8. Esiste una teoria della decomposizione primaria per moduli noetheriani che corrisponde da vicino a (e nel caso noetheriano generalizza) quella della decomposizione primaria per ideali di un anello commutativo unitario. Per questa teoria si rimanda alla vastissima letteratura disponibile, ci limitiamo qui a dire che se R è un anello commutativo unitario, un R -modulo M è detto coprimario se ogni elemento di R che annulli un elemento non nullo di M appartiene al radicale di $\text{Ann}_R(M)$; un sottomodulo proprio N di M tale che M/N sia coprimario è invece detto primario. Si prova che ogni sottomodulo proprio di un modulo noetheriano è intersezione di un numero finito di sottomoduli primari, e per tali decomposizioni valgono risultati analoghi ai teoremi di unicità dimostrati in questo capitolo.

8 Anelli artiniani

La struttura degli anelli commutativi artiniani è piuttosto ristretta, in particolare nel caso degli anelli unitari che, come vedremo in questo capitolo, se artiniani si descrivono come particolari anelli noetheriani.

8.1 Ideali primi e massimali

Gli anelli commutativi artiniani hanno dimensione di Krull 0. Si ha infatti:

Lemma 8.1. *Sia R un anello commutativo artiniano. Allora:*

- (i) *se R ha un elemento cancellabile a , allora R è unitario e ogni suo elemento cancellabile è invertibile;*
- (ii) *se R è un dominio di integrità, allora R è un campo.*

Dimostrazione. È ovvio che (ii) segue da (i); basterà dunque provare (i). A questo scopo, sia a un elemento cancellabile di R . La successione di ideali $(a^n R)_{n \in \mathbb{N}}$ è decrescente, quindi esiste $n \in \mathbb{N}$ tale che $a^n R = a^{n+1} R$. Per ogni $r \in R$ esiste allora $s \in R$ tale che $a^n r = a^{n+1} s$ e quindi, essendo a cancellabile, $r = as \in aR$. Abbiamo così $R = aR$ ed il [Lemma 3.4](#) mostra che R è unitario e $a \in \mathcal{U}(R)$. A questo punto la dimostrazione è completa. \square

Lemma 8.2. *Sia R un anello commutativo artiniano. Allora R ha solo un numero finito di ideali di indice finito.*

Dimostrazione. Sia \mathcal{J} l'insieme degli ideali di indice finito in R (vale a dire: degli ideali $H \triangleleft R$ tali che R/H sia finito). Allora $R \in \mathcal{J}$, quindi $\mathcal{J} \neq \emptyset$ ed esiste quindi in \mathcal{J} un elemento L minimale rispetto all'inclusione. Per ogni $H \in \mathcal{J}$, evidentemente $R/(H \cap L)$ è finito, dunque $H \cap L \in \mathcal{J}$. Per la minimalità di L , allora $H \cap L = L$, vale a dire, $L \subseteq H$. Abbiamo così provato che \mathcal{J} è l'insieme degli ideali di R contenenti L ; dal momento che R/L è finito, questo insieme è finito. \square

Proposizione 8.3. *Sia R un anello commutativo artiniano. Allora:*

- (i) *ogni ideale primo di R è massimale;*
- (ii) *l'insieme degli ideali massimali di R è finito.*

Dimostrazione. Sia $P \in \text{Spec}(R)$. Allora R/P è un campo, per il [Lemma 8.1](#), quindi $P \triangleleft R$. Ciò prova la (i). Il [Lemma 3.8](#) mostra che ogni ideale massimale di R che non sia primo ha indice finito in R , quindi il [Lemma 8.2](#) implica che R non ha che un numero finito di tali ideali. Resta solo da verificare che $\text{Spec}(R)$ è finito. Assumendo $\text{Spec}(R) \neq \emptyset$, sia \mathcal{J} l'insieme degli ideali che sono intersezione di un numero finito di ideali primi di R e sia H un suo elemento minimale; dunque $H = \bigcap \mathcal{P}$ per un opportuno sottoinsieme finito \mathcal{P} di $\text{Spec}(R)$. Per ogni $P \in \text{Spec}(R)$ si ha $H \cap P \in \mathcal{J}$ e quindi, per la minimalità di H , ricaviamo $J \subseteq P$. Essendo P primo, allora, esiste $Q \in \mathcal{P}$ tale che $Q \subseteq P$, e quindi $P = Q$ perché $Q \triangleleft R$ per (i). Dunque $\text{Spec}(R) = \mathcal{P}$, quindi anche $\text{Spec}(R)$ è finito. Così è provata la (ii). \square

Lemma 8.4. *Sia R un anello commutativo artiniano. Allora $\text{Jac}(R)$ è nilpotente.*

Dimostrazione. Sia $J = \text{Jac}(R)$. La successione $(J^n)_{n \in \mathbb{N}}$ di ideali di R è decrescente, quindi esiste $n \in \mathbb{N}$ tale che $J^n = J^{n+1}$. Ragionando per assurdo, supponiamo $J^n \neq 0$. Sia \mathcal{S} l'insieme degli ideali H di R tali che $H = HJ \neq 0$. Chiaramente $J^n \in \mathcal{S}$, quindi $\mathcal{S} \neq \emptyset$ ed esiste in \mathcal{S} un elemento minimale H . Poiché $HJ^n = H \neq 0$, esiste $h \in H$ tale che $hJ^n \neq 0$. Ovviamente $hJ^n \triangleleft R$ e $(hJ^n)J = hJ^{n+1} = hJ^n$, quindi $hJ^n \in \mathcal{S}$. Ma $hJ^n \subseteq H$, quindi $hJ^n = H$ per la minimalità di H . Poiché $h \in H$, questo mostra in particolare che H è l'ideale generato da h ; in particolare H è finitamente generato e da $HJ = H$ il Lemma di Nakayama (Lemma 3.24) fornisce la contraddizione $H = 0$. \square

Un'ovvia conseguenza è che se R è un anello commutativo artiniano, $\text{Jac}(R) \subseteq \text{NilRad}(R)$ (l'inclusione può essere propria; si veda l'Esempio 8.A.5). Dunque, ricordando la Proposizione 3.22, abbiamo anche:

Corollario 8.5. *Sia R un anello commutativo unitario artiniano. Allora $\text{Jac}(R) = \text{NilRad}(R)$.*

8.2 La struttura degli anelli artiniani unitari

Arriviamo ora alla caratterizzazione degli anelli commutativi unitari artiniani annunciata all'inizio del capitolo.

Teorema 8.6. *Sia R un anello commutativo unitario. Allora R è artiniano se e solo se R è noetheriano e ha dimensione di Krull 0.*

Dimostrazione. Sia R artiniano. Sappiamo dalla Proposizione 8.3 che gli ideali primi di R sono tutti massimali (cioè: R ha dimensione 0) e sono in numero finito; sia J il loro prodotto.¹ Segue dal Lemma 8.4 che vale $J^n = 0$ per un opportuno $n \in \mathbb{N}$. Allora R è annullato da J^n , che è un prodotto di ideali massimali di R , quindi R è noetheriano per il Lemma 6.7. Questo prova che la condizione è necessaria.

Viceversa, sia R un anello noetheriano di dimensione 0. Sia \mathcal{D} una decomposizione primaria minimale dell'ideale nullo di R . Per ogni $Q \in \mathcal{D}$ sia $M_Q = \sqrt{Q}$; per ipotesi, $M_Q \triangleleft R$ ed inoltre, poiché R è noetheriano, il Corollario 3.16 mostra che esiste $n_Q \in \mathbb{N}^+$ tale che $M_Q^{n_Q} \subseteq Q$. Abbiamo allora $\prod_{Q \in \mathcal{D}} M_Q^{n_Q} \subseteq \bigcap \mathcal{D} = 0$.² Applicando di nuovo il Lemma 6.7, concludiamo da ciò che R è artiniano. \square

La dimostrazione di quest'ultimo teorema ha una ulteriore conseguenza: ogni anello commutativo unitario artiniano è, in modo unico, prodotto diretto di un numero finito di anelli locali:

Proposizione 8.7. *Sia R un anello commutativo unitario. Allora R è artiniano se e solo se è isomorfo ad un prodotto diretto finito di anelli locali artiniani.*

Più precisamente, se R è un anello commutativo unitario artiniano, esiste uno ed un solo insieme finito \mathcal{J} di ideali di R che, come anelli, sono locali, tale che $R = \bigoplus_{H \in \mathcal{J}} H$.

Dimostrazione. Se R è isomorfo ad un prodotto diretto del tipo descritto, è ovvio che R è artiniano. Sia, viceversa R artiniano; possiamo ovviamente assumere $R \neq 0$. Allora R è noetheriano e di dimensione zero, quindi il suo ideale nullo 0 è decomponibile e, inoltre, essendo gli ideali primi (ovvero massimali) di R a due a due non confrontabili, tutti gli ideali primi associati a 0

¹ anche se irrilevante per la dimostrazione, notiamo che $J = \text{Jac}(R)$, dal momento che, come è ovvio, gli ideali massimali di R sono a due a due comassimali, quindi il loro prodotto ne è anche l'intersezione.

² probabilmente è un eccesso di scrupolo, ma specifichiamo che il simbolo \prod si riferisce qui alla moltiplicazione tra ideali, non ad un prodotto diretto.

sono isolati. Segue dal secondo teorema di unicità che 0 ha una sola decomposizione primaria minimale in R , chiamiamola \mathcal{D} .

Per ogni $Q \in \mathcal{D}$, il radicale \sqrt{Q} è l'unico ideale massimale di R contenente Q ; pertanto R/Q è un anello locale. Inoltre, se Q_1 e Q_2 sono elementi distinti di \mathcal{D} , da $\sqrt{Q_1} \neq \sqrt{Q_2}$ segue che Q_1 e Q_2 sono comassimali (altrimenti $Q_1 + Q_2$ sarebbe contenuto in un ideale massimale contenente entrambi). Da questo fatto e da $\bigcap \mathcal{D} = 0$ segue che l'omomorfismo $r \in R \mapsto (r + Q)_{Q \in \mathcal{D}} \in \prod_{Q \in \mathcal{D}} (R/Q)$ descritto nel [Lemma 4.11](#) è un isomorfismo, sicché R è, come richiesto, un prodotto diretto di un numero finito di anelli (unitari) artiniani locali.

Resta da provare che, interpretata come somma diretta interna di ideali (locali), questa decomposizione diretta di R è unica. Sia $R = \bigoplus_{H \in \mathcal{J}} H$, dove \mathcal{J} è un insieme finito di ideali di R e ogni $H \in \mathcal{J}$ è un anello locale. Per ogni $H \in \mathcal{J}$ siano J_H l'ideale massimale di H e $Q_H = \sum_{H \neq K \in \mathcal{J}} K$. Dal momento che $J_H = \text{Jac}(H)$ è nilpotente per il [Lemma 8.4](#) e $M_H := Q_H + J_H \triangleleft R$ (ad esempio, perché $R/M_H \simeq H/J_H$), abbiamo $M_H = \sqrt{Q_H}$ e quindi il [Lemma 7.5](#) mostra che Q_H è primario in R . Sia $\mathcal{D}' = \{Q_H \mid H \in \mathcal{J}\}$; è chiaro che $\bigcap \mathcal{D}' = 0$, quindi \mathcal{D}' è una decomposizione primaria di 0 . Notiamo anche l'uguaglianza $H = \bigcap (\mathcal{D}' \setminus \{Q_H\})$, per ogni $H \in \mathcal{J}$. Essa mostra, da una parte, che \mathcal{J} è univocamente determinato da \mathcal{D}' , perché \mathcal{J} risulta essere l'insieme di tutti gli ideali della forma $\bigcap (\mathcal{D}' \setminus \{Q_H\})$ al variare di Q in \mathcal{D}' ; dall'altra parte, la stessa uguaglianza mostra che \mathcal{D}' è irridondante e quindi, evidentemente, minimale. Dunque $\mathcal{D}' = \mathcal{D}$, per quanto osservato all'inizio di questa dimostrazione, sicché \mathcal{D}' è univocamente determinato da R e quindi lo stesso vale per \mathcal{J} . La proposizione è ora dimostrata. \square

Esercizi, Osservazioni, Esempi.

8.A.1. Duplicandone la dimostrazione, generalizzare il [Lemma 8.2](#) provando che ogni pre-modulo artiniano ha solo un numero finito di sottopre-moduli di indice finito.

8.A.2. L'ipotesi che R sia unitario è essenziale per il [Teorema 8.6](#). Ad esempio, un anello che abbia un gruppo abeliano artiniano infinito (come un gruppo di Prüfer) come gruppo additivo e prodotto costante nullo è artiniano ma non noetheriano. Lo stesso discorso vale per l'implicazione inversa: in un anello con prodotto costante nullo non esistono ideali primi; se un tale anello R è infinito ma il suo gruppo additivo è finitamente generato (ad esempio, se è ciclico infinito), allora R è noetheriano e tutti gli ideali primi di R sono massimali, ma R non è artiniano.

8.A.3. Sempre in relazione al [Teorema 8.6](#), va menzionato il fatto che l'ipotesi di commutatività è invece meno rilevante. Infatti questo teorema ha un analogo nella teoria degli anelli unitari non necessariamente commutativi, il teorema di Hopkins-Levitzki che caratterizza gli anelli unitari artiniani come particolari anelli noetheriani (qui gli aggettivi 'artiniano' e 'noetheriano' sono riferiti a condizioni di catena sugli ideali destri).

8.A.4. Dedurre dal [Teorema 8.6](#) che ogni dominio di integrità unitario noetheriano di dimensione 1 (ad esempio, ogni anello principale) ha tutti i quozienti propri artiniani.

8.A.5. Come osservato, in un anello (commutativo) artiniano non unitario, il radicale di Jacobson è sempre contenuto nel nilradicale. Se R è un anello finito non nullo con prodotto costante nullo, allora $\text{Jac } R \subset \text{NilRad } R = R$.

8.A.6. Estendere il [Lemma 8.4](#) dimostrando che in ogni anello commutativo artiniano R il nilradicale è nilpotente. [Suggerimento: assumendo l'asserto falso, ragionando come nella dimostrazione del [Lemma 8.4](#), si può trovare un ideale finitamente generato H di R tale che $HN = H \neq 0$, dove $N = \text{NilRad}(R)$. Il [Lemma 3.27](#) fornisce un elemento di N che agisce come l'identità su H ; usarlo per ottenere $H = 0$.]

8.A.7. L'anello \mathbb{Q}_2 è un anello commutativo unitario noetheriano con un solo ideale massimale e spettro finito, ma non è artiniano. Il suo radicale di Jacobson è ovviamente il

suo ideale massimale, e non coincide col nilradicale (in particolare, non è nilpotente), che è l'ideale nullo. Tutti gli anelli locali noetheriani che non siano campi verificano queste stesse proprietà.

8.A.8. La [Proposizione 8.7](#) riduce lo studio degli anelli commutativi unitari artiniani al caso degli anelli locali. Semplici esempi di anelli commutativi unitari artiniani locali sono i quozienti $K[x]/(x^n)$ dell'anello dei polinomi ad una indeterminata x su un campo K , dove n è un arbitrario intero positivo. (Perché questi anelli sono artiniani e locali?). Questo esempio mostra che, nella situazione in cui R sia un anello commutativo unitario artiniano locale con ideale massimale M il minimo intero positivo n tale che $M^n = 0$ può assumere valori arbitrari.

8.3 Il teorema dell'intersezione di Krull e gli anelli locali noetheriani

Inseriamo qui un classico risultato dovuto a Krull. Benché esso non abbia applicazione diretta agli anelli artiniani, una delle sue conseguenze è che una proprietà di questi, la nilpotenza del radicale di Jacobson, si estende in forma indebolita agli anelli noetheriani.

Iniziamo da un lemma che ha per conseguenza il fatto che, nello studio dei premoduli noetheriani, a meno di effettuare un cambio di scalari ci si può spesso ridurre al caso in cui anche l'anello di scalari sia noetheriano.

Lemma 8.8. *Sia M un premodulo noetheriano sull'anello commutativo R . Allora $R/\text{Ann}_R(M)$ è noetheriano.*

Dimostrazione. Iniziamo a dimostrare il lemma nel caso in cui R sia unitario ed M sia un R -modulo. Certamente $M = FR$ per un suo sottoinsieme finito F . Come mostra la [Proposizione 1.21](#), per ogni $x \in F$ abbiamo $xR \simeq_R R_R/H_x$, dove $H_x = \text{Ann}_R(x)$, quindi R/H_x è noetheriano come R -modulo e dunque come anello. Ma $\text{Ann}_R(M) = \text{Ann}_R(F) = \bigcap_{x \in F} H_x$, quindi segue dal [Lemma 6.5](#) che $R/\text{Ann}_R(M)$ è noetheriano. Passando al caso generale, immergiamo R come ideale nel suo anello accresciuto R_1 . Per il caso precedente, ricordando dal [Lemma 6.6](#) che M resta noetheriano anche come R_1 -modulo, $R_1/\text{Ann}_{R_1}(M)$ è noetheriano. Ma $\text{Ann}_R(M) = R \cap \text{Ann}_{R_1}(M)$, quindi $R/\text{Ann}_R(M)$, come R_1 -modulo, è isomorfo all'ideale $(R + \text{Ann}_{R_1}(M))/\text{Ann}_{R_1}(M)$ di $R_1/\text{Ann}_{R_1}(M)$ ed è quindi noetheriano. Questo significa che $R/\text{Ann}_R(M)$ è noetheriano anche come R -premodulo, quindi come anello. \square

Teorema 8.9 (Teorema dell'intersezione di Krull). *Siano R un anello commutativo, M un R -premodulo noetheriano, $H \triangleleft R$. Allora, se $I = \bigcap_{n \in \mathbb{N}} MH^n$, si ha $IH = I$.*

Dimostrazione. Iniziamo col dimostrare il teorema nel caso particolare in cui R sia noetheriano ed M sia un suo ideale. Supponiamo, per assurdo, $IH \subset I$, e sia $a \in I \setminus IH$. Sia \mathcal{D} una decomposizione primaria minimale di IH in R . Poiché $a \notin IH$, esiste $Q \in \mathcal{D}$ tale che $a \notin Q$ (quindi $Q \neq R$). Ma $aH \subseteq IH \subseteq Q$, quindi $H \subseteq (Q : a)_R$. Dal momento che Q è primario, il [Lemma 7.2](#) prova $H \subseteq \sqrt{Q}$ e quindi, per il [Corollario 3.16](#), vediamo che esiste $n \in \mathbb{N}^+$ tale che $H^n \subseteq Q$. Ma allora $a \in I \subseteq MH^n \subseteq H^n \subseteq Q$, una contraddizione. Il teorema è così provato in questo primo caso.

Passiamo al caso generale. Il [Lemma 8.8](#) mostra che l'anello $\bar{R} := R/\text{Ann}_R(M)$ è noetheriano. Come sappiamo, possiamo riguardare M come premodulo su \bar{R} e, per [Lemma 1.16](#), i suoi \bar{R} -sottopremoduli sono precisamente i suoi R -sottopremoduli. Sia ora $S = M \rtimes \bar{R}$ l'idealizzazione di M (si veda il [Teorema 1.33](#)). Dunque, $S = M + \bar{R}$, dove \bar{R} è un sottoanello di S e $M \triangleleft S$, inoltre $M^2 = 0$ e la moltiplicazione interna di S induce, per restrizione e riduzione, la

moltiplicazione esterna $M \times \bar{R} \rightarrow M$. Gli ideali di S contenuti in M sono esattamente gli \bar{R} - (ovvero gli R -) sottopremoduli di M , dunque M è S -noetheriano. Essendo $S/M \simeq \bar{R}$, concludiamo che anche S è noetheriano.

Sia $\bar{H} = (H + \text{Ann}_R(M))/\text{Ann}_R(M)$. Evidentemente $\bar{H} \triangleleft \bar{R}$ e quindi $H_1 := \bar{H} + M \triangleleft S$. Per ogni $n \in \mathbb{N}$, si ha $MH^n = M\bar{H}^n$; allora da $\bar{H}^n \subseteq H_1^n \subseteq \bar{H}^n + M$ e $MM = 0$ segue $MH_1^n = M\bar{H}^n = MH^n$. Di conseguenza $I = \bigcap_{n \in \mathbb{N}} MH_1^n$. Applicando a S e ad i suoi ideali M e H_1 quanto provato nella prima parte della dimostrazione, abbiamo allora $I = IH_1$. Ma $IH_1 = I(\bar{H} + M) = I\bar{H} = IH$, quindi $I = IH$, come richiesto dall'enunciato. \square

Osserviamo che il teorema dell'intersezione di Krull non vale per moduli non noetheriani, neanche nel caso in cui l'anello degli scalari sia noetheriano; l'Esempio 8.B.2 fornisce un controesempio in cui questo anello è quello degli interi.

Proposizione 8.10. *Sia R un anello commutativo noetheriano, e sia $J = \text{Jac}(R)$. Allora $\bigcap_{n \in \mathbb{N}^+} J^n = 0$ ed R è isomorfo ad un sottoanello unitario di $\prod_{n \in \mathbb{N}^+} (R/J^n)$.*

Dimostrazione. Segue subito dal Teorema 8.9 che se $I = \bigcap_{n \in \mathbb{N}^+} J^n$ allora $IJ = I$. Ma allora il lemma di Nakayama fornisce $I = 0$. Il Lemma 4.11 produce ora un monomorfismo $R \hookrightarrow \prod_{n \in \mathbb{N}^+} (R/J^n)$ di anelli unitari. \square

Il caso più importante della proposizione precedente è quello in cui R è un anello locale; in questo caso $M = \text{Jac}(R)$ è il suo ideale massimale e si hanno due possibilità: o $M^n \neq 0$ per ogni $n \in \mathbb{N}$, nel qual caso R non è artiniano, oppure M è nilpotente, nel qual caso, in conseguenza del Lemma 6.7, R è un anello artiniano. Una versione più generale di questa situazione è suggerita nell'Esercizio 8.B.3.

Esercizi.

8.B.1. Dimostrare che se R è un anello commutativo unitario artiniano infinito, allora R ha un ideale massimale di indice infinito.

8.B.2. Nel teorema dell'intersezione di Krull (8.9) è essenziale l'ipotesi che il modulo M sia noetheriano. Un esempio a riguardo si può ottenere come segue.

Siano p un numero primo e $A = \bigoplus_{i \in \mathbb{N}^+} \langle a_i \rangle$ un gruppo abeliano, dove, per ogni $i \in \mathbb{N}^+$, $\langle a_i \rangle$ è un sottogruppo ciclico di ordine p^i . È facile riconoscere che $\bigcap_{n \in \mathbb{N}} p^n A = 0$; ad esempio perché per ogni $n \in \mathbb{N}$ si ha $p^n A \subseteq \bigoplus_{n < i \in \mathbb{N}} \langle a_i \rangle$. Sia $\Omega = \langle p^{i-1} a_i \mid i \in \mathbb{N}^+ \rangle \leq A$. Non è difficile (ma neanche essenziale) vedere che Ω è precisamente l'insieme degli elementi di A di periodo al più p . Ora,

$$\frac{A}{\Omega} = \frac{\bigoplus_{i \in \mathbb{N}^+} \langle a_i \rangle}{\bigoplus_{i \in \mathbb{N}^+} \langle p^{i-1} a_i \rangle} \simeq \bigoplus_{i \in \mathbb{N}^+} \left(\frac{\langle a_i \rangle}{\langle p^{i-1} a_i \rangle} \right)$$

e ciascuno dei gruppi $\langle a_i \rangle / \langle p^{i-1} a_i \rangle$ è ciclico di ordine p^{i-1} . Dunque $A/\Omega \simeq A$. Sia ora $B = \langle a_1 - p^{i-1} a_i \mid i \in \mathbb{N}^+ \rangle$. È chiaro che $\Omega = B + \langle a_1 \rangle$; inoltre $a_1 \notin B$ (gli elementi di B sono combinazioni lineari dei generatori $a_1 - p^{i-1} a_i$ a coefficienti in \mathbb{Z} , dunque, se $a_1 \in B$ allora $a_1 = \sum_{i \in F} \lambda_i (a_1 - p^{i-1} a_i)$ per una parte finita F di $\mathbb{N}^+ \setminus \{1\}$ e interi λ_i , ma dalla decomposizione di A in somma diretta segue $\lambda_i p^{i-1} a_i = 0$, cioè p divide λ_i , per ogni $i \in F$, una palese contraddizione). Allora $\Omega/B = \langle a_1 + B \rangle$ ha ordine p .

Sia ora $M = A/B$. Riguardiamo M come \mathbb{Z} modulo; posto $H = p\mathbb{Z} \triangleleft \mathbb{Z}$, calcoliamo $I := \bigcap_{n \in \mathbb{N}} MH^n$. Per ogni $n \in \mathbb{N}$, ovviamente, $MH^n = p^n M = (p^n A + B)/B$, quindi $I = I_0/B$, dove $I_0 = \bigcap_{n \in \mathbb{N}} (p^n A + B)$. Va dunque calcolato I_0 . Poiché $A/\Omega \simeq A$, si ha $\Omega/\Omega = 0 = \bigcap_{n \in \mathbb{N}} p^n (A/\Omega) = \bigcap_{n \in \mathbb{N}} (p^n A + \Omega/\Omega)$, quindi $\Omega = \bigcap_{n \in \mathbb{N}} (p^n A + \Omega) \supseteq I_0$, vale a dire: $I \leq \Omega/B$. D'altra parte, per ogni $n \in \mathbb{N}$, dal momento che $a_1 - p^n a_{n+1} \in B$, abbiamo

8 Anelli artiniani

$a_1 + B = p^n(a_{n+1} + B) \in p^n M$, dunque $a_1 + B \in I$. Poiché $\Omega/B = \langle a_1 + B \rangle$, concludiamo $I = \Omega/B$. Ma $|\Omega/B| = p$, quindi $IH = pI = 0 \neq I$. In questo modo abbiamo mostrato che la conclusione del [Teorema 8.9](#) non vale per l'anello \mathbb{Z} , il suo ideale $p\mathbb{Z}$ e lo \mathbb{Z} -modulo M .

8.B.3. Sia R un anello commutativo noetheriano. Provare che R è artiniano se e solo se l'insieme degli ideali massimali di R è finito e $\text{Jac}(R)$ è nilpotente.

9 Anelli di frazioni

In questo capitolo viene presentata l'importante costruzione degli anelli di frazioni, che ha come caso particolarmente significativo quello delle localizzazioni di un anello.

9.1 Posizione del problema e costruzione

Sia S un sottoinsieme non vuoto di un anello commutativo R (in questa sezione considereremo queste notazioni fissate). Lo scopo della costruzione che stiamo per discutere è quello di ottenere un omomorfismo da R ad un anello commutativo unitario in modo che l'immagine di ogni elemento di S risulti invertibile, richiedendo allo stesso tempo che questo omomorfismo sia in un certo senso minimale ed universale per questa proprietà. Possiamo codificare queste richieste in termini di una proprietà universale per un certo tipo di omomorfismi.

Diciamo che un omomorfismo f di anelli da R ad un anello commutativo A è S -*invertivo* se e solo se A è unitario e $s^f \in \mathcal{U}(A)$ per ogni $s \in S$. In accordo con l'uso che abbiamo introdotto definendo (pre)moduli liberi ed algebre libere, diciamo anche che un omomorfismo S -invertivo $f_S: R \rightarrow S^{-1}R$ è universale se e solo se, per ogni anello commutativo unitario A ed ogni omomorfismo S -invertivo $g: R \rightarrow A$ esista uno ed un solo omomorfismo di anelli $\varphi: S^{-1}R \rightarrow A$ tale che $f_S\varphi = g$, cioè questo diagramma sia commutativo:

$$\begin{array}{ccc} R & \xrightarrow{f_S} & S^{-1}R \\ & \searrow g & \swarrow \varphi \\ & & A \end{array}$$

Sottintendendo il riferimento a f_S , chiameremo l'anello commutativo unitario $S^{-1}R$ un anello di frazioni (definito da S e da R). Come già visto per altre proprietà universali, si verifica facilmente che f_S e $S^{-1}R$ sono univocamente definiti a meno di isomorfismi. Più precisamente, se $f': R \rightarrow R'$ è un altro omomorfismo S -invertivo universale, allora esiste un (unico) isomorfismo $\alpha: S^{-1}R \rightarrow R'$ tale che $f' = f_S\alpha$.

Prima di affrontare il problema dell'esistenza di $S^{-1}R$ e f_S , conviene fare alcune esempi ed osservazioni generali.

In alcuni casi il problema ha soluzione banale, o per lo meno già nota:

- se $S \subseteq \mathcal{U}(R)$, allora l'applicazione identica di R è, come si vede senza difficoltà, S -invertivo universale; basta dunque porre $S^{-1}R = R$ e $f_S = \text{id}_R$.
- Se $0_R \in S$ e $f: R \rightarrow A$ è un omomorfismo S -invertivo, allora $A = 0$ è un anello nullo, dal momento che $0_A = 0_R^f$ deve essere invertibile in A . Da ciò segue che ogni tale f è universale, in questo caso.
- Se R è un dominio di integrità e $0_R \notin S$, possiamo definire $S^{-1}R$ come il sottoanello del campo dei quozienti di R generato da $R \cup \{s^{-1} \mid s \in S\}$ e f_S come l'immersione ι di R in questo anello. È infatti facile provare che tale ι è S -invertivo universale ([Esercizio 9.A.1](#)).

Un'osservazione cruciale è la seguente:

Lemma 9.1. *Con le notazioni fissate, indichiamo con S^\bullet e \hat{S} , rispettivamente, la parte chiusa generata e la saturazione di S in (R, \cdot) . Allora per un omomorfismo di anelli $f: R \rightarrow A$ sono*

equivalenti le proprietà di essere S -inversivo, S^\bullet -inversivo, \hat{S} -inversivo. Di conseguenza, per f sono equivalenti le proprietà di essere S -inversivo universale, S^\bullet -inversivo universale, \hat{S} -inversivo universale.

Dimostrazione. Da $S \subseteq S^\bullet \subseteq \hat{S}$ segue che un omomorfismo f di dominio R è S -inversivo se è S^\bullet -inversivo ed è S^\bullet -inversivo se è \hat{S} -inversivo. Viceversa, se $f: R \rightarrow A$ è S -inversivo e $a \in \hat{S}$, allora a è un divisore di un prodotto di elementi di S (si veda quanto nella [sezione 2.3](#)), quindi a^f divide un prodotto di elementi di $S^{\overleftarrow{f}} \subseteq \mathcal{U}(A)$ ed è dunque invertibile in A . Questo prova la prima parte dell'enunciato; la seconda ne è immediata conseguenza. \square

Passiamo ora alla costruzione di $S^{-1}R$. Alla luce del lemma precedente possiamo sostituire S con la parte chiusa che esso genera ed assumere quindi che S sia un sottosemigruppato (cioè una parte chiusa non vuota) di (R, \cdot) . Questo rende più semplice la costruzione, che generalizza quella, già nota, del campo dei quozienti di un dominio di integrità.

Nell'insieme $R \times S$ consideriamo la relazione di equivalenza \sim definita da:

$$(\forall x, y \in R)(\forall s, t \in S) \quad ((x, s) \sim (y, t) \iff (\exists a \in S)(xta = ysa)).$$

Che si tratti effettivamente di una relazione di equivalenza è facile da verificare: le proprietà riflessiva e simmetrica sono ovvie, per la transitività osserviamo che se $x, y, z \in R$ e $s, t, u \in S$ sono tali che $(x, s) \sim (y, t)$ e $(y, t) \sim (z, u)$, allora $xta = ysa$ e $yub = ztb$ per opportuni $a, b \in S$, e quindi $xutab = yusab = ztsab$, dunque $x \sim z$, perché $tab \in S$ (vediamo qui il vantaggio dell'aver assunto che S sia chiusa per moltiplicazione).

Per ogni $x \in R$ e $s \in S$ indichiamo con x/s la classe $[(x, s)]_\sim$, e notiamo subito che $x/s = xt/st$ per ogni $t \in S$. Definiamo come $S^{-1}R$ l'anello di sostegno $(R \times S)/\sim$, con operazioni $+$ (additiva) e \cdot (moltiplicativa) definite ponendo, per ogni $x, y \in R$ e $s, t \in S$:

$$\frac{x}{s} + \frac{y}{t} = \frac{xt + ys}{st} \quad \text{e} \quad \frac{x}{s} \cdot \frac{y}{t} = \frac{xy}{st}.$$

Verifichiamo che queste operazioni sono ben definite. Dal momento che R è commutativo, basta verificare che $(xt + ys)/st = (x't + ys')/s't$ e $xy/st = x'y/s't$ per ogni $x, x', t \in R$ e $s, s', t \in S$ tali che $x/s = x'/s'$. In effetti, sotto quest'ultima condizione, esiste $a \in S$ tale che $xs'a = x'sa$, quindi $(xt + ys)s'ta = (x't + ys')sta$ (dunque $(xt + ys)/st = (x't + ys')/s't$) e $xy'sta = x'y'sta$ (dunque $x/s = x'/s'$); la verifica è così completa.

È chiaro che le operazioni appena definite in $S^{-1}R$ sono entrambe associative e commutative, e che, per ogni $s \in S$, le frazioni $0_R/s$ e s/s sono elementi neutri per $+$ e \cdot , nell'ordine. L'ovvia regola di calcolo $(x/s) + (y/s) = (x + y)/s$ per ogni $x, y \in R$ e $s \in S$ rende semplice verificare sia che $(S^{-1}R, +)$ è un gruppo (ogni $x/s \in S^{-1}R$ ha per opposto $(-x)/s$) che la distributività di \cdot rispetto a $+$: per ogni $x, y, z \in R$ e $s, t, u \in S$,

$$\left(\frac{x}{s} + \frac{y}{t}\right) \cdot \frac{z}{u} = \frac{xt + ys}{st} \cdot \frac{z}{u} = \frac{xtz + ysz}{stu} = \frac{xtz}{stu} + \frac{ysz}{stu} = \frac{xz}{su} + \frac{yz}{tu} = \frac{x}{s} \cdot \frac{z}{u} + \frac{y}{t} \cdot \frac{z}{u}.$$

Abbiamo così strutturato $S^{-1}R$ come anello commutativo unitario. Fissato un elemento $s \in S$, consideriamo l'applicazione

$$f_s: x \in R \mapsto xs/s \in S^{-1}R.$$

Per ogni $x \in R$ e $s, t \in S$ abbiamo $xs/s = xst/st = xt/t$, dunque f_s è indipendente dalla scelta di s . Si riconosce senza difficoltà che f_s un omomorfismo di anelli. Inoltre f_s è S -inversivo, perché, per ogni $s \in S$, si ha che $s^{f_s} = s^2/s$ è invertibile in $S^{-1}R$, con inverso s/s^2 . Resta da provare che f_s è universale. Siano A un anello commutativo unitario e $g: R \rightarrow A$ un omomorfismo S -inversivo di anelli. Dobbiamo dimostrare che esiste uno ed un solo omomorfismo di anelli $\varphi: S^{-1}R \rightarrow A$ tale che $f_s\varphi = g$. Se φ ha questa proprietà, per ogni $x \in R$ e $s \in S$

si deve avere $x^g = x^{fs\varphi} = (xs/s)^\varphi$, quindi anche $(s^2/s)^\varphi = s^g$. Ora, dal momento che s^g è un elemento invertibile di A appartenente a $\text{im } \varphi$, il Lemma 1.1 mostra che φ deve essere un omomorfismo di anelli unitari, quindi $(s/s^2)^\varphi = ((s^2/s)^{-1})^\varphi = ((s^2/s)^\varphi)^{-1} = (s^g)^{-1}$ ed infine $(x/s)^\varphi = (xs/s)^\varphi (s/s^2)^\varphi = x^g (s^g)^{-1}$. Dunque, esiste al più un omomorfismo con le proprietà richieste per φ : l'unico possibile candidato è l'applicazione

$$x/s \in S^{-1}R \mapsto x^g (s^g)^{-1} \in A,$$

ammesso che questa sia ben definita. Per verificare che lo è, iniziamo con l'osservare che, per ogni $s \in S$, esiste $(s^g)^{-1}$ in A , perché g è S -invertivo. Siano poi $x, y \in R$ e $s, t \in S$ tali che $x/s = y/t$, vale a dire: $xta = ysa$ per un opportuno $a \in S$. Allora $x^g t^g a^g = y^g s^g a^g$, ed essendo a^g invertibile e quindi cancellabile in A , $x^g t^g = y^g s^g$; dunque $x^g (s^g)^{-1} = y^g (t^g)^{-1}$. Ciò prova che la nostra applicazione, che d'ora in poi chiamiamo φ , è ben definita. Ovviamente, per ogni $x, y \in R$ e $s, t \in S$, si ha $((x/s) + (y/t))^\varphi = ((x/s) + (y/t))^\varphi = ((xt + ys)/st)^\varphi = (x^g t^g + y^g s^g)(s^g)^{-1}(t^g)^{-1} = x^g (s^g)^{-1} + y^g (t^g)^{-1} = (x/s)^\varphi + (y/t)^\varphi$ e $((x/s) \cdot (y/t))^\varphi = (xy/st)^\varphi = x^g y^g (s^g)^{-1}(t^g)^{-1} = (x/s)^\varphi (y/t)^\varphi$ quindi φ è un omomorfismo di anelli; inoltre $x^{fs\varphi} = (x/1)^\varphi = x^g$, sicché $f_S \varphi = g$.

$$\begin{array}{ccc} R & \xrightarrow{x \mapsto x/1} & S^{-1}R \\ & \searrow f_S & \swarrow \varphi \\ & & A \end{array}$$

$g \swarrow \quad \searrow \swarrow$
 $x/s \quad x^g s^{-g}$

Riassumendo, abbiamo dimostrato che, per ogni anello commutativo unitario R e ogni suo sottoinsieme non vuoto S esistono, e sono unici a meno di isomorfismi, un anello $S^{-1}R$ ed un omomorfismo S -invertivo $f_S: R \rightarrow S^{-1}R$ che sia universale, nel senso definito all'inizio di questa sezione. Chiameremo l'anello $S^{-1}R$ un *anello di frazioni* (ottenuto da R e S) e f_S omomorfismo S -universale (o semplicemente universale). Notiamo ancora che l'omomorfismo φ definito nel corso della verifica è un omomorfismo di anelli unitari, così come lo è f_S se R è unitario.

Supponendo ancora che S sia un sottosemigruppo in (R, \cdot) , osserviamo che $S^{-1}R$ è costituito dalle frazioni x/s al variare di $x \in R$ e $s \in S$, ma $x/s = (xs/s)(s/s^2) = (xs/s)(s^2/s)^{-1}$, dunque $S^{-1}R = \{(s^{f_S})^{-1}x^{f_S} \mid s \in S \wedge x \in R\}$, il che rende in un certo senso conto del simbolo usato per denotare questo anello. Ovviamente la rappresentazione delle frazioni non è, in generale, unica; ad esempio lo zero e l'unità di $S^{-1}R$ si possono rappresentare come $0_R/s$ e s/s per ogni $s \in S$ e, come stiamo per vedere, anche in altri modi.

Lemma 9.2. *Siano R un anello commutativo e S un sottosemigruppo di (R, \cdot) . Allora il nucleo dell'omomorfismo universale $f_S: R \rightarrow S^{-1}R$ è*

$$\ker f_S = \bigcup_{a \in S} \text{Ann}_R(a).$$

Inoltre, per ogni $x \in R$ e $s \in S$:

- (i) $x/s = 0_{S^{-1}R}$ se e solo se $x \in \ker f_S$;
- (ii) $x/s = 1_{S^{-1}R}$ se e solo se $x - s \in \ker f_S$;
- (iii) se x/s è un divisore dello zero in $S^{-1}R$, allora x è un divisore dello zero in R ;
- (iv) x/s è invertibile in $S^{-1}R$ se e solo se x appartiene alla saturazione \hat{S} di S ;
- (v) per ogni $t, u \in S$, sia x/t che xu/t sono associati, in $S^{-1}R$, a x/s ed a $x^{f_S} = xs/s$.

Dimostrazione. Fissiamo $x \in R$ e $s \in S$. Iniziando dalla fine, se $t, u \in S$ si ha: $x/s = (x/t)(t/s) = (xu/t)(t/su)$, e, evidentemente, $t/s, t/su$ sono invertibili in $S^{-1}R$, con inversi s/t e su/t . Da ciò segue la (v), che ha per anche conseguenza: $x \in \ker f_S \iff xs/s = 0_{S^{-1}R} \iff x/s = 0_{S^{-1}R}$, provando così la (i). Ora, $0_{S^{-1}R} = 0_R/s$, quindi $x/s = 0_{S^{-1}R}$ se e solo se esiste $a \in S$ tale che $xa = 0_R$; dal momento che $sa \in S$ questo equivale a $x \in \bigcup_{a \in S} \text{Ann}_R(a)$; otteniamo così la descrizione di $\ker f_S$ nell'enunciato.

Abbiamo $1_{S^{-1}R} = s/s$, quindi $x/s = 1_{S^{-1}R}$ se e solo se $x/s = s/s$, ovvero $x - s \in \ker f_S$; vale dunque (ii). Se invece x/s è un divisore dello zero in $S^{-1}R$, allora esistono $y \in R$ e $t \in S$ tali che $xy/st = (x/s)(y/t) = 0_R/s \neq y/t$, dunque esiste $a \in S$ tale che $xya = 0_R \neq ya$, quindi x è un divisore dello zero in R . Abbiamo così provato (iii).

Resta da provare (iv). Sia x/s invertibile. Allora esistono $y \in R$ e $t \in S$ tali che $xy/st = (x/s)(y/t) = 1_{S^{-1}R} = s/s$, vale a dire: $xysa = ts^2a$ per qualche $a \in S$. Ma allora x divide $ts^2a \in S$, quindi $x \in \hat{S}$. Viceversa, se $x \in \hat{S}$ allora esiste $y \in R$ tale che $xy \in S$, dunque esiste la frazione y/xy e $1_{S^{-1}R} = xys/xys = (x/s)(ys/xy)$ e $x/s \in \mathcal{U}(S^{-1}R)$; si noti che esiste in $S^{-1}R$ la frazione ys/xy proprio perché $xy \in S$. A questo punto la dimostrazione è completa. \square

Esercizi e Osservazioni.

9.A.1. Verificare in dettaglio che, come osservato nella prima parte di questa sezione, quando R è un dominio di integrità e $0_R \notin S$, detto T il sottoanello generato da R e da $\{s^{-1} \mid s \in S\}$ nel campo dei quozienti di R , l'immersione $R \hookrightarrow T$ è un omomorfismo S -inverso universale e dunque $S^{-1}R \simeq T$.

9.A.2. Nel caso in cui R sia un dominio di integrità e $S = R \setminus \{0_R\}$, l'anello di frazioni $S^{-1}R$ si può identificare con il campo dei quozienti di R . In effetti la costruzione che di $S^{-1}R$ abbiamo appena effettuato coincide, in questo caso, proprio con quella usuale del campo dei quozienti, dal momento che, con le notazioni utilizzate per la nostra costruzione, per ogni $x, y \in R$ e $s, t \in S$ si ha $(x, s) \sim (y, t)$ se e solo se $xt = ys$.

Più in generale, vale quest'ultima equivalenza per ogni scelta dell'anello (commutativo) R a condizione che il sottosemigruppo S di (R, \cdot) non contenga divisori dello zero in R . Come segue da uno dei prossimi risultati (**Lemma 9.2**) questa è precisamente la condizione affinché l'omomorfismo universale f_S sia iniettivo.

9.A.3. Riprendendo l'osservazione al punto precedente, la situazione cambia molto nel caso in cui S abbia tra i suoi elementi un divisore dello zero s . In questo caso certamente f_S non può essere iniettivo, perché $\text{Ann}_R(s)$ è contenuto nel nucleo di ogni omomorfismo S -inverso con dominio R . Infatti, se $f: R \rightarrow A$ è un omomorfismo S -inverso e $r \in \text{Ann}_R(s)$, allora $s^f r^f = (0_R)^f = 0_A$, quindi, essendo s^f invertibile, $r^f = 0_A$.

9.A.4. Con le notazioni che stiamo usando (ma qui S è inteso come arbitraria parte non vuota di R), supponiamo che S sia l'unione di due sottoinsiemi T e V . Allora $S^{-1}R$ si può ottenere in due passaggi successivi: costruendo $T^{-1}R$ e poi l'anello di frazioni ottenuto da questo anello e dall'immagine in esso di V . In modo più esplicito, $S^{-1}R \simeq \bar{V}^{-1}(T^{-1}R)$, dove $\bar{V} = V^{\bar{f}_T}$, e, una volta identificato $S^{-1}R$ con $\bar{V}^{-1}(T^{-1}R)$, si ha $f_S = f_T f_{\bar{V}}$.

Per provarlo, si può fare riferimento ai diagrammi commutativi qui disegnati, osservando che f_S è T -inverso, il che permette di usare la proprietà universale per definire φ , e che poi φ risulta \bar{V} -inverso, la qual cosa permette di costruire ψ . Inoltre $f_T f_{\bar{V}}$ è S -inverso, e usando questo fatto si può definire θ . Completare la dimostrazione provando che ψ e θ sono isomorfismi, l'uno inverso dell'altro.

$$\begin{array}{ccc}
 R & \xrightarrow{f_T} & T^{-1}R & \xrightarrow{f_{\bar{V}}} & \bar{V}^{-1}(T^{-1}R) \\
 & \searrow f_S & \downarrow \varphi & \swarrow \psi & \\
 & & S^{-1}R & &
 \end{array}
 \qquad
 \begin{array}{ccc}
 R & \xrightarrow{f_T f_{\bar{V}}} & \bar{V}^{-1}(T^{-1}R) \\
 & \searrow f_S & \swarrow \theta \\
 & & S^{-1}R
 \end{array}$$

9.A.5. Sia R un sottoanello dell'anello commutativo A e $\emptyset \neq S \subseteq R$. Verificare che l'applicazione $x/s \in S^{-1}R \mapsto x/s \in S^{-1}A$ è un omomorfismo iniettivo; si può dunque realizzare $S^{-1}R$ come sottoanello di $S^{-1}A$ e l'omomorfismo S -inverso universale $R \rightarrow S^{-1}R$ come ridotta della restrizione dell'omomorfismo S -inverso universale $A \rightarrow S^{-1}A$.

L'asserto non è del tutto ovvio: la frazione x/s in $S^{-1}R$ e l'omologa frazione x/s in $S^{-1}A$ non sono lo stesso oggetto: se assumiamo S chiusa rispetto alla moltiplicazione in R e quindi a quella in A , la prima è una classe di equivalenza in $R \times S$, la seconda in $A \times S$; anche il fatto che l'applicazione indicata sia ben definita richiede una giustificazione (la si può ottenere utilizzando la proprietà universale discussa in questa sezione, o in altri modi). Quello che viene qui stabilito è che la relazione di equivalenza che definisce l'anello di frazioni su R si può riguardare come indotta via inclusione da quella che definisce $S^{-1}A$.

9.A.6. Abbiamo visto che, in conseguenza del [Lemma 1.1](#), se R è un anello commutativo unitario e S è una parte non vuota di R , allora l'omomorfismo S -inverso universale f_S è universale anche come omomorfismo S -inverso di anelli unitari, nel senso che verifica questa proprietà: per ogni omomorfismo S -inverso g di anelli (commutativi) unitari, esiste uno ed un solo omomorfismo φ di anelli unitari tale che $g = f_S \varphi$. Dunque, se volessimo definire una nozione di anello di frazioni facendo riferimento alla categoria degli anelli unitari piuttosto che a quella degli anelli, non otterremmo niente di diverso da ciò che abbiamo ottenuto.

9.2 Ideali negli anelli di frazioni. Localizzazioni.

Iniziamo con una osservazione piuttosto ovvia:

Lemma 9.3. *Sia R un anello commutativo e sia H un suo ideale primo (risp. primario). Se A è un sottoanello di R che contenga propriamente H , H è un ideale primo (risp. primario) in A .*

Dimostrazione. Ovviamente $H \triangleleft A$. Sia a un divisore dello zero in A/H . Allora a è un divisore dello zero in R/H , quindi a è zero se H è primo in R , nilpotente se H è primario. Da ciò segue l'asserto. \square

Lemma 9.4. *Sia $f: R \rightarrow A$ un omomorfismo di anelli, con R e A entrambi commutativi. Siano B un ideale di A e $H = B^{\overleftarrow{f}}$ la sua antiimmagine mediante f . Allora:*

- (i) $H \triangleleft R$;
- (ii) $\sqrt{H} = (\sqrt{B})^{\overleftarrow{f}}$;
- (iii) se B è primo e $H \neq R$, H è primo;
- (iv) se B è primario e $H \neq R$, H è primario.

Se R e A sono unitari e f è un omomorfismo di anelli unitari, allora $H \subset R$ se $B \subset A$, quindi se B è primo o primario, H ha la stessa proprietà.

Dimostrazione. Componendo f con l'epimorfismo canonico $\nu: A \twoheadrightarrow A/B$ otteniamo un omomorfismo di anelli $f\nu: R \rightarrow A$ di nucleo H . Dunque, $H \triangleleft R$. Per ogni $r \in R$ si ha $r \in \sqrt{H} \iff (\exists n \in \mathbb{N}^+)(r^n \in H) \iff (\exists n \in \mathbb{N}^+)((r^n)^f \in B) \iff (\exists n \in \mathbb{N}^+)((r^f)^n \in B) \iff r^f \in \sqrt{B}$. Sono così provate (i) e (ii). Inoltre R/H è isomorfo al sottoanello $\text{im } f\nu = (\text{im } f + B)/B$ di A/B . Supponiamo $H \neq R$. Allora $B \neq \text{im } f + B$, quindi, come stabilito nel [Lemma 9.3](#), se B è primo (risp. primario) in A/B , allora lo è anche in $\text{im } f + B$, dunque l'isomorfismo $R/H \simeq (\text{im } f + B)/B$ mostra che H è primo (risp. primario) in R .

Infine, se f è un omomorfismo di anelli unitari e $B \neq A$, dal momento che $1_A \notin B$ si ha $1_R \notin H$, il che prova l'ultima parte dell'enunciato. \square

Con le notazioni del [Lemma 9.4](#), H viene talvolta chiamato la contrazione di B rispetto a f . La nozione corrispondente, in termini di immagine anziché di antiimmagine è quella di espansione (chiamata anche estensione, termine che evitiamo per prevenire possibile confusione con la nozione standard di estensione tra moduli): l'espansione di un ideale I di R rispetto ad f

è l'ideale di A generato dall'immagine di I . Va notato che l'immagine di un ideale mediante un omomorfismo (non suriettivo) non è in generale un ideale; ad esempio, se f è l'immersione di \mathbb{Z} in \mathbb{Q} ed I è un ideale non nullo di \mathbb{Z} , l'immagine di I mediante f (cioè I stesso) non è un ideale di \mathbb{Q} . In queste note useremo questa terminologia (parleremo cioè di contrazioni ed espansioni) esclusivamente con riferimento all'omomorfismo universale da un anello ad un suo anello di frazioni.

Fissiamo dunque un anello commutativo R e una sua parte $S \neq \emptyset$; sia $f_S: R \rightarrow S^{-1}R$ il corrispondente omomorfismo S -universale. Per ogni $H \triangleleft R$ e $K \triangleleft S^{-1}R$ chiamiamo *espansione* di H , indicata con H^e , l'ideale di $S^{-1}R$ generato da $H^{\overline{f}_S}$, vale a dire $H^{\overline{f}_S}(S^{-1}R)$, mentre la *contrazione* K^c di K è l'antiimmagine di K mediante f_S . Otteniamo così due applicazioni

$$e: \mathfrak{I}(R) \rightarrow \mathfrak{I}(S^{-1}R), \quad c: \mathfrak{I}(S^{-1}R) \rightarrow \mathfrak{I}(R)$$

tra gli insiemi degli ideali di R e di $S^{-1}R$. La descrizione dettagliata di queste applicazioni è di grande importanza per lo studio degli anelli di frazioni. È ovvio che, considerati $\mathfrak{I}(R)$ e $\mathfrak{I}(S^{-1}R)$ come insiemi ordinati (dalla relazione di inclusione), e e c sono entrambe crescenti.

Lemma 9.5. *Con le notazioni appena fissate, se S è un sottosemigruppato di (R, \cdot) , per ogni $H \triangleleft R$ e $K \triangleleft S^{-1}R$ si ha:*

- (i) $H^e = \{h/s \mid h \in H \wedge s \in S\}$;
- (ii) $K^{ce} = K$;
- (iii) $H^{ec} = \bigcup_{a \in S} (H : a) = \{r \in R \mid (\exists a \in S)(ra \in H)\} \supseteq H$;
- (iv) $H^e \neq S^{-1}R \iff H \cap S = \emptyset \iff \sqrt{H} \cap S = \emptyset \iff (\sqrt{H})^e \neq S^{-1}R$.

Dunque, $ce = \text{id}_{\mathfrak{I}(S^{-1}R)}$; di conseguenza c è iniettiva ed e è suriettiva. Come insieme ordinato, $\mathfrak{I}(S^{-1}R)$ è isomorfo ad un sottoinsieme di $\mathfrak{I}(R)$.

Dimostrazione. Sia $T = \{h/s \mid h \in H \wedge s \in S\}$. Per ogni $h, h' \in H$, $s, s' \in S$ e $r \in R$ si ha $(h/s) - (h'/s') = (hs' - h's)/ss' \in T$ e $(h/s)(r/s') = hr/ss' \in T$, quindi $T \triangleleft S^{-1}R$. È anche chiaro che $H^{\overline{f}_S} \subseteq T \subseteq H^{\overline{f}_S}\{s/s^2 \mid s \in S\} \subseteq H^e$. Dunque $T = H^e$, e la (i) è provata.

Verifichiamo ora la (ii). Banalmente, $(K^c)^{\overline{f}_S} = K^{\overline{f}_S}$ è incluso in K , quindi anche K^{ce} , l'ideale che esso genera in $S^{-1}R$, è incluso in K . Viceversa, sia $k = x/s$ (con $x \in R$ e $s \in S$) un elemento di K . Allora $x^{fs} = xs/s = k(s^2/s) \in K$, quindi $x \in K^c$, sicché, per la (i), $k \in K^{ce}$; otteniamo così la (ii).

Siano ora $r \in R$ e $s \in S$. Abbiamo $r \in H^{ec}$ se e solo se $rs/s \in H^e$. Se $r \in X := \bigcup_{a \in S} (H : a)$, allora $ra \in H$ per qualche $a \in S$, quindi $rs/s = ra/a \in H^e$. Viceversa, se $rs/s \in H^e$, per (i) esistono $h \in H$ e $t \in S$ tali che $rs/s = h/t$, quindi esiste $a \in S$ tale che $rsta = hsa \in H$, dunque $r \in (H : sta) \subseteq X$, dal momento che $sta \in S$. Ciò prova la (iii).

Passiamo alla (iv). Se esiste $s \in H \cap S$, allora $1_{S^{-1}R} = s/s \in H^e$ e $H^e = S^{-1}R$. Viceversa, se $H^e = S^{-1}R$ allora esistono $h \in S$ e $s \in S$ tali che $h/s = 1_{S^{-1}R} = s/s$, per la (i); quindi per un opportuno $a \in S$ si ha $s^2a = hsa$, dunque $s^2a \in S \cap H$. È così provato che H^e è un ideale proprio se e solo se $H \cap S = \emptyset$. Abbiamo così anche $(\sqrt{H})^e \neq S^{-1}R \iff \sqrt{H} \cap S = \emptyset$. Ora, se $\sqrt{H} \cap S$ non è vuoto e s ne è un elemento, una potenza di s apparterrà ad $H \cap S$; dunque $\sqrt{H} \cap S = \emptyset$ se e solo se $H \cap S = \emptyset$. Questo completa la dimostrazione di (iv). La parte rimanente dell'enunciato è conseguenza immediata di (ii) e del fatto che le applicazioni c ed e sono entrambe crescenti. \square

Nella (iii) l'inclusione $H \subset H^{ec}$ può essere stretta. Per convincersene basta pensare al caso dell'ideale nullo: la (iii), insieme al Lemma 9.2, mostra $0^{ec} = \ker f_S$.

Corollario 9.6. *Se un anello commutativo unitario è artiniiano (risp. noetheriano, ad ideali tutti principali, principale) lo stesso vale per ogni suo anello di frazioni non nullo.*

Dimostrazione. Con le notazioni che stiamo usando, l'insieme ordinato $\mathfrak{J}(S^{-1}R)$ si immerge in $\mathfrak{J}(R)$ e quindi verifica le condizioni di catena che valgono in R . Poiché e è suriettiva, ogni ideale di $S^{-1}R$ è della forma H^e per un opportuno $H \triangleleft R$. Se H è principale, detto h un generatore di H è chiaro che $H^e = h^{fs}S^{-1}R$, quindi anche H^e è principale. Infine, nell'ipotesi che $S^{-1}R$ non si annulla, $S^{-1}R$ è un dominio di integrità se lo è R , quindi se R è principale anche $S^{-1}R$ lo è. \square

Per procedere con lo studio di e e c abbiamo ancora bisogno di un lemma, che mostra come, in un certo senso, il passaggio al quoziente ed il passaggio ad un anello di frazioni siano trasformazioni che commutano tra loro.

Lemma 9.7. *Sempre con le stesse notazioni, fissato $H \triangleleft R$ e detto $\nu: R \rightarrow R/H$ l'epimorfismo canonico da R a $R/H = R^{\bar{\nu}}$, si ha $(S^{\bar{\nu}})^{-1}R^{\bar{\nu}} \simeq S^{-1}R/H^e$.*

Dimostrazione. L'immagine $S^{\bar{\nu}}$ di S mediante ν è un sottosemigruppo di $R^{\bar{\nu}}$, e l'omomorfismo $\nu f_{S^{\bar{\nu}}}$ è certamente S -inverso, quindi la proprietà universale di f_S garantisce l'esistenza dell'omomorfismo $\varphi: S^{-1}R \rightarrow (S^{\bar{\nu}})^{-1}R^{\bar{\nu}}$ tale che $f_S\varphi = \nu f_{S^{\bar{\nu}}}$. Di φ abbiamo una descrizione esplicita, ottenuta nel corso della costruzione degli anelli di frazioni e della verifica della proprietà universale: sappiamo che, per ogni $x \in R$ e $s \in S$,

$$\begin{array}{ccc} R & \xrightarrow{\nu} & R^{\bar{\nu}} & \xrightarrow{f_{S^{\bar{\nu}}}} & (S^{\bar{\nu}})^{-1}R^{\bar{\nu}} \\ & \searrow f_S & & \nearrow \varphi: x/s \mapsto x^{\bar{\nu}}/s^{\bar{\nu}} & \\ & & S^{-1}R & & \end{array}$$

$$(x/s)^\varphi = x^{\bar{\nu}}f_{S^{\bar{\nu}}}s^{-\bar{\nu}}f_{S^{\bar{\nu}}} = (x^{\bar{\nu}}s^{\bar{\nu}}/s^{\bar{\nu}})((s^{\bar{\nu}})^2/s^{\bar{\nu}})^{-1} = x^{\bar{\nu}}/s^{\bar{\nu}}.$$

Ora, questa descrizione mostra chiaramente che φ è suriettiva. Inoltre, $\ker \varphi$ è costituito dalle frazioni x/s tali che $x^{\bar{\nu}}/s^{\bar{\nu}}$ sia lo zero di $(S^{\bar{\nu}})^{-1}R^{\bar{\nu}}$. Dunque, tenendo presente che $\bigcup_{a \in S} \text{Ann}_{R^{\bar{\nu}}}(a^{\bar{\nu}})$ è l'immagine mediante ν di $\bigcup_{a \in S} (H : a)_R = H^{ec}$ (si veda il Lemma 9.5 (iii)), ricaviamo dal Lemma 9.2:

$$x/s \in \ker \varphi \iff x \in H^{ec} \iff xs/s \in H^e \iff x/s \in H^e,$$

dal momento che xs/s e x/s sono associati in $S^{-1}R$. Pertanto $\ker \varphi = H^e$. Di conseguenza $(S^{\bar{\nu}})^{-1}R^{\bar{\nu}} \simeq S^{-1}R/\ker \varphi = S^{-1}R/H^e$. \square

Lemma 9.8. *Nella situazione del Lemma 9.5, per ogni $H \triangleleft R$ tale che $H \cap S = \emptyset$:*

- (i) se H è primario, $H^{ec} = H$ e H^e è primario, con radicale $(\sqrt{H})^e$;
- (ii) se H è primo, H^e è primo.

Dimostrazione. Sappiamo dal Lemma 9.5 (iv) che $H^e \subset S^{-1}R$ e, inoltre, $\sqrt{H} \cap S \neq \emptyset$. Supponiamo H primario. Per la (iii) del Lemma 9.5, se $r \in H^{ec}$ allora $rs \in H$ per qualche $s \in S$. Da $\sqrt{H} \cap S = \emptyset$ segue $s \notin \sqrt{H}$, quindi $r \in H$. Abbiamo così $H^{ec} = H$. Per provare che H^e è primario in $S^{-1}R$ consideriamo il quoziente $S^{-1}R/H^e$. Utilizzando le notazioni del Lemma 9.7, $S^{-1}R/H^e \simeq (S^{\bar{\nu}})^{-1}R^{\bar{\nu}}$, quindi per provare che H^e è primario basta verificare che ogni divisore dello zero in $(S^{\bar{\nu}})^{-1}R^{\bar{\nu}}$ è nilpotente. Sia x un divisore dello zero in $(S^{\bar{\nu}})^{-1}R^{\bar{\nu}}$, possiamo scrivere x come $r^{\bar{\nu}}/s^{\bar{\nu}}$ per opportuni $r \in R$ e $s \in S$. Il Lemma 9.2 (iii) garantisce che $r^{\bar{\nu}}$ è un divisore dello zero in $R^{\bar{\nu}}$, e quindi è nilpotente; di conseguenza x è nilpotente. Abbiamo così provato che H^e è primario; in modo analogo ma ancora più diretto vediamo che H^e è primo se H è primo, perché in questo caso $(S^{\bar{\nu}})^{-1}R^{\bar{\nu}}$ è un dominio di integrità. Infine, ancora nell'ipotesi che H sia primario, \sqrt{H} è primo, quindi $(\sqrt{H})^{ec} = \sqrt{H}$, per quanto dimostrato sopra (e perché $\sqrt{H} \cap S \neq \emptyset$). D'altra parte, come segue dal Lemma 9.4 (ii), $(\sqrt{H^e})^c = \sqrt{H^{ec}} = \sqrt{H}$. Abbiamo così $(\sqrt{H^e})^c = (\sqrt{H})^{ec}$; poiché c è iniettiva ne segue $\sqrt{H^e} = (\sqrt{H})^e$, il che completa la dimostrazione.¹ \square

¹ possiamo osservare che quest'ultima parte della dimostrazione fornisce anche una dimostrazione, indipendente dalla precedente ma molto meno diretta, di (ii). Possiamo anche aggiungere che, più in generale, si può dimostrare $\sqrt{H^e} = \sqrt{H}^e$ per ogni ideale H di R (vedi Esercizio 9.B.4)

Teorema 9.9. Siano R un anello commutativo e S un sottosemigruppato di (R, \cdot) , e sia $\mathfrak{I}_S(R)$ l'insieme degli ideali di R disgiunti da S . Allora le applicazioni espansione $e: \mathfrak{I}(R) \rightarrow \mathfrak{I}(S^{-1}R)$ e contrazione $c: \mathfrak{I}(S^{-1}R) \rightarrow \mathfrak{I}(R)$ inducono per restrizione isomorfismi di insiemi ordinati, l'uno inverso dell'altro, tra queste coppie di insiemi:

- l'insieme degli ideali primari di R disgiunti da S e l'insieme degli ideali primari di $S^{-1}R$;
- $\text{Spec}(R) \cap \mathfrak{I}_S(R)$ e $\text{Spec}(S^{-1}R)$;
- per ogni $P \in \text{Spec}(R) \cap \mathfrak{I}_S(R)$, l'insieme degli ideali P -primari di R e l'insieme degli ideali P^e -primari di $S^{-1}R$.

Dimostrazione. Siano rispettivamente \mathcal{Q} e \mathcal{Q}' l'insieme degli ideali primari di R disgiunti da S e quello degli ideali primari di $S^{-1}R$. I lemmi 9.4, 9.5 e 9.8 mostrano che, per ogni $H \in \mathcal{Q}$ e $K \in \mathcal{Q}'$ si ha $H^e \in \mathcal{Q}'$ e $K^c \in \mathcal{Q}$ (dal momento che $K = K^{ce} \subset S^{-1}R$, certamente $K^c \cap S = \emptyset$), inoltre $H^{ec} = H$. Da ciò segue che \mathcal{Q}' è l'immagine di \mathcal{Q} mediante e mentre \mathcal{Q} è l'immagine di \mathcal{Q}' mediante c , e le applicazioni indotte per restrizione e riduzione da e e c tra questi insiemi sono applicazioni biettive, l'una inversa dell'altra. Inoltre gli stessi lemmi provano che queste applicazioni fanno corrispondere ideali primi a ideali primi, quindi inducono biezioni tra $\text{Spec}(R) \cap \mathfrak{I}_S(R)$ e $\text{Spec}(S^{-1}R)$ e, inoltre, conservano i radicali degli ideali, quindi, per ogni ideale primo $P \in \mathcal{Q}$, fanno corrispondere ideali P -primari ad ideali P^e -primari. Infine, sia e che c sono crescenti, quindi tutte queste biezioni sono isomorfismi tra insiemi ordinati. \square

Osserviamo ancora che la funzione espansione conserva intersezioni e prodotti finiti tra ideali (ma non intersezioni infinite, come indicato nell'Esercizio 9.B.6) e somme arbitrarie; la funzione contrazione conserva le intersezioni (arbitrarie).

Lemma 9.10. Nelle solite notazioni:

- (i) per ogni $I, J \triangleleft R$, $(IJ)^e = I^e J^e$; $(I \cap J)^e = I^e \cap J^e$
- (ii) per ogni famiglia $(H_i)_{i \in I}$ di ideali di R , $(\sum_{i \in I} H_i)^e = \sum_{i \in I} H_i^e$;
- (iii) per ogni famiglia $(K_i)_{i \in I}$ di ideali di $S^{-1}R$, $(\bigcap_{i \in I} K_i)^c = \bigcap_{i \in I} K_i^c$;

Dimostrazione. Siano $I, J \triangleleft R$. Che $(IJ)^e = I^e J^e$ è chiaro dalla descrizione delle espansioni in Lemma 9.5.² Mentre è altrettanto chiaro, dalla crescita di e , che $(I \cap J)^e \subseteq I^e \cap J^e$, meno ovvia è l'inclusione opposta. Sia $x \in I^e \cap J^e$. Esistono $i \in I$, $j \in J$, $s, t \in S$ tali che $x = i/s = j/t$. Esiste allora $a \in S$ tale che $ita = jsa$; ma da questa uguaglianza traiamo $ita \in I \cap J$ e quindi $x = ita/sta \in (I \cap J)^e$. Abbiamo provato la (ii). Il resto dell'enunciato è ovvio. \square

L'enunciato precedente ci dice che e è un omomorfismo tra reticoli. Lo stesso non vale per c , che non conserva le somme tra ideali (vedi Esercizio 9.B.7).

Esercizi.

9.B.1. Verificare che se $f: R \rightarrow A$ è un omomorfismo suriettivo tra anelli, l'immagine mediante f di un ideale di R è necessariamente un ideale di A .

9.B.2. Nelle notazioni del Lemma 9.5 si ha, per ogni $H \triangleleft R$:

- $H^{ece} = H^e$;
- $H^{ec} = H$ se e solo se H è la contrazione di un ideale di R ;
- se H è generato da un suo sottoinsieme X , allora H^e è generato da $X^{\vec{f}_S}$;
- $S \cap H = \emptyset \iff \hat{S} \cap H = \emptyset$; verificarlo in modo diretto.

Inoltre, e è iniettiva se e solo se $S \subseteq \mathcal{U}(R)$ (vale a dire: e e c descrivono una biezione tra $\mathfrak{I}(R)$ e $\mathfrak{I}(S^{-1}R)$ solo nel caso banale in cui f_S sia un isomorfismo tra R e $S^{-1}R$).

² o da considerazioni più generali, vedi Esercizio 9.B.9.

9.B.3. Siano R un anello commutativo e S un sottosemigruppato di (R, \cdot) . Provare che, per ogni $H \triangleleft R$ e $P \in \text{Spec}(R)$ tale che $P \cap S = \emptyset$, si ha $H \subseteq P \iff H^e \subseteq P^e \iff H^{ec} \subseteq P$, dove ovviamente e e c indicano espansione e contrazione con riferimento all'anello di frazioni $S^{-1}R$.

9.B.4. Provare che, nella notazioni del [Lemma 9.5](#), $(\sqrt{H})^e = \sqrt{H^e}$ per ogni $H \triangleleft R$.

9.B.5. Costruire un esempio di omomorfismo di anelli unitari commutativi $f: R \rightarrow A$ e di un ideale $H \triangleleft R$ tali che $(\sqrt{H})^{\vec{f}} \subset \sqrt{H^{\vec{f}}}$.

I prossimi cinque esercizi sono relativi al [Lemma 9.10](#); le notazioni sono le solite.

9.B.6. Mostrare con un esempio che l'espansione di una intersezione di una famiglia (infinita) $(H_i)_{i \in I}$ di ideali non è necessariamente l'intersezione degli ideali H_i^e . Suggerimento: basta pensare a qualche anello di frazioni di \mathbb{Z} .

9.B.7. Mostrare con un esempio che la contrazione di una somma di due ideali di un anello di frazioni non è necessariamente la somma delle loro contrazioni. Suggerimento: se R è l'anello di polinomi $\mathbb{Z}[x]$ e $S = \{2\}$ ponendo $I = xR$ e $J = (x+2)R$, si ha $I = I^{ec}$ e $J = J^{ec}$, mentre $(I + J)^e = S^{-1}R$.

9.B.8. L'applicazione contrazione non conserva neanche i prodotti tra ideali. Per costruire un controesempio a riguardo, si considerino un gruppo abeliano A di ordine primo p , visto (nell'unico modo possibile) come \mathbb{Z} -modulo e la idealizzazione $R = A \rtimes \mathbb{Z}$. Verificare che il nucleo dell'omomorfismo universale $R \rightarrow \{p\}^{-1}R$ è A , calcolare la contrazione dell'ideale nullo di $\{p\}^{-1}R$ ed il suo quadrato per arrivare alla conclusione. In aggiunta: utilizzando il [Lemma 9.7](#), identificare $\{p\}^{-1}R$.

9.B.9. Sia $f: R \rightarrow A$ un omomorfismo di anelli unitari commutativi. Mostrare che l'applicazione che ad ogni ideale H di R associa l'ideale di A generato da $H^{\vec{f}}$ conserva prodotti e somme (arbitrarie) tra ideali.

9.B.10. In contrasto con quanto notato con l'esercizio precedente, il fatto che la funzione espansione conservi l'intersezione tra ideali è una proprietà specifica dell'omomorfismo naturale da un anello commutativo unitario ad un suo anello di frazioni. Ad esempio, se K è un qualsiasi anello commutativo unitario, e $R = K[x, y]$ è un anello di polinomi a due indeterminate su K , non è difficile trovare un omomorfismo di anelli unitari f da R ad un altro anello commutativo A tale che, posto $I = xR$ e $J = yR$, si abbia che $(I \cap J)^{\vec{f}}$ sia un ideale di A propriamente contenuto in $I^{\vec{f}} \cap J^{\vec{f}}$. Trovare un tale f .

9.B.11. Con riferimento alla situazione descritta nell'[Esercizio 9.A.5](#), mostrare che, una volta identificato $S^{-1}R$ con un sottoanello di $S^{-1}A$ come lì suggerito, chiamando e e c le applicazioni contrazione ed espansione relative a R e $S^{-1}R$, ε e γ quelle relative ad A e $S^{-1}A$, si ha $H^e S^{-1}A = (HA)^\varepsilon$ per ogni $H \triangleleft R$ e $(K \cap S^{-1}R)^c = R \cap K^\gamma$ per ogni $K \triangleleft S^{-1}A$.

9.B.12. Sia R un dominio di integrità e S una sua parte tale che $0_R \notin S \neq \emptyset$. Ricordando che $S^{-1}R$ può essere realizzato come sottoanello del campo dei quozienti $Q(R)$ di R (di cui consideriamo R come sottoanello) con l'immersione $R \hookrightarrow Q(R)$ come omomorfismo naturale, osservare che $K^c = K \cap R$ per ogni $K \triangleleft S^{-1}R$. Questa è l'origine di una notazione (un po' balorda) usata da alcuni autori che indicano tutte le contrazioni di ideali degli anelli di frazioni di un arbitrario anello R come intersezioni con R .

I risultati precedenti hanno una interpretazione molto esplicita alla luce di due osservazioni fatte: ogni anello di frazioni si può riguardare come anello di frazioni definito da un sottosemigruppato saturo ([Lemma 9.1](#)), e i sottosemigruppato (moltiplicativi) saturi in un anello commutativo sono precisamente i complementi delle unioni di ideali primi ([Lemma 3.10](#)).

Sia dunque R un anello commutativo. Per quanto appena notato, ogni anello di frazioni di R è della forma $S^{-1}R$, dove $S = R \setminus \bigcup \mathcal{P}$ per un insieme \mathcal{P} di ideali primi. Il [Teorema 9.9](#) offre

una descrizione dello spettro primo di questo anello: un ideale primo di R è disgiunto da S se e solo se è contenuto nell'unione $\bigcup \mathcal{P}$. Dunque, la funzione contrazione è una biezione, ed anche un isomorfismo di insiemi ordinati, da $\text{Spec}(S^{-1}R)$ all'insieme degli ideali primi di R contenuti in $\bigcup \mathcal{P}$. Un caso particolarmente importante è quello in cui \mathcal{P} sia un singleton, vale a dire: $\mathcal{P} = \{P\}$ per un qualche $P \in \text{Spec}(R)$, e dunque $S = R \setminus P$. Si usa scrivere, in questo caso, R_P per $(R \setminus P)^{-1}R$. Per quanto visto nel caso generale, $\text{Spec}(R_P)$ è isomorfo come insieme ordinato all'insieme $\mathfrak{I}_P(R) = \{Q \in \text{Spec } R \mid Q \subseteq P\}$ degli ideali primi di R contenuti in P . Ovviamente $\mathfrak{I}_P(R)$ ha massimo: questo massimo è P , quindi l'ideale di R_P corrispondente a P , cioè P^e è il massimo (rispetto all'inclusione) in $\text{Spec}(R_P)$. Da questo segue subito che P^e è massimo tra gli ideali propri di R_P : ogni ideale proprio di R_P è contenuto in un ideale massimale, quindi primo, e dunque in P^e . Tenendo presente che R_P è certamente unitario abbiamo così provato:

Corollario 9.11. *Sia R un anello commutativo e sia P un suo ideale primo. Allora R_P è un anello locale, di ideale massimale P^e .*

Gli anelli di frazioni di questa forma sono noti come localizzazioni. Più precisamente, per ogni ideale primo P di un anello commutativo R , l'anello di frazioni $R_P = (R \setminus P)^{-1}R$ è la localizzazione di R a P .

Un importante esempio è dato dalle localizzazioni di \mathbb{Z} , che possiamo rapidamente descrivere tutte. Ricordiamo (Esercizio 9.A.1) che un anello di frazioni non nullo $S^{-1}R$ di un dominio di integrità R si può realizzare come sottoanello del campi dei quozienti di R : se $0 \notin S \neq \emptyset$, allora $S^{-1}R$ è il sottoanello di $Q(R)$ generato da R e da $\{s^{-1} \mid s \in S\}$. Dunque, per ogni ideale primo P di \mathbb{Z} , la localizzazione \mathbb{Z}_P è il sottoanello di \mathbb{Q} generato dai reciproci degli elementi di $\mathbb{Z} \setminus P$. Se $P = \{0\}$ questo è il campo \mathbb{Q} . Se $P \neq \{0\}$, dunque $P = p\mathbb{Z}$ per qualche numero primo positivo p , otteniamo

$$\mathbb{Z}_P = \{n/m \mid n, m \in \mathbb{Z} \wedge p \text{ non divide } m\} =: \mathbb{Q}_{p'},^3$$

come si verifica facilmente. Come si può descrivere $\mathfrak{I}(\mathbb{Q}_{p'})$? Gli ideali primi di $\mathbb{Q}_{p'}$ sono le espansioni degli ideali primi di \mathbb{Z} contenuti in $p\mathbb{Z}$, quindi di $\{0\}$ e $p\mathbb{Z}$. Dunque $\text{Spec}(\mathbb{Q}_{p'}) = \{\{0\}, p\mathbb{Q}_{p'}\}$. Similmente, dal fatto che gli ideali primari non nulli di \mathbb{Z} contenuti in $p\mathbb{Z}$ sono quelli della forma $p^n\mathbb{Z}$ al variare di $n \in \mathbb{N}^+$ ricaviamo che gli ideali primari di $\mathbb{Q}_{p'}$ sono l'ideale nullo e gli ideali della forma $p^n\mathbb{Q}_{p'}$ al variare di $n \in \mathbb{N}^+$. Ci saremmo potuti arrivare anche per altra via: sappiamo che $\mathbb{Q}_{p'}$ è principale (Corollario 9.6) e che gli ideali primari degli anelli principali sono tutte e solo le potenze degli ideali primi. Ma in questo caso di ideali primi ne abbiamo solo due, e le loro potenze sono gli ideali che abbiamo elencato. Osserviamo che questi ideali sono a due a due distinti, vale a dire $p^a\mathbb{Q}_{p'} \neq p^b\mathbb{Q}_{p'} \neq \{0\}$ per ogni coppia di interi positivi distinti a, b ; ciò segue (ad esempio) dal Teorema 9.9. Oltre questi ideali e l'anello stesso, esistono altri ideali in $\mathbb{Q}_{p'}$? Sappiamo che la funzione espansione e è suriettiva, dunque $\mathfrak{I}(\mathbb{Q}_{p'}) = \{H^e \mid H \triangleleft \mathbb{Z}\} = \{(m\mathbb{Z})^e \mid m \in \mathbb{N}\} = \{m\mathbb{Q}_{p'} \mid m \in \mathbb{N}\}$. Sia $m \in \mathbb{N}^+$; possiamo senz'altro scrivere $m = p^n u$ per opportuni $n, u \in \mathbb{N}$ tali che p^n non divida u . Ma allora u è invertibile in $\mathbb{Q}_{p'}$, abbiamo dunque $m\mathbb{Q}_{p'} = p^n\mathbb{Q}_{p'}$. In questo modo arriviamo a concludere che $\mathbb{Q}_{p'}$ non ha ideali oltre a quelli già identificati. In definitiva, $\mathfrak{I}(\mathbb{Q}_{p'})$ è costituito dall'ideale nullo e dagli ideali $p^n\mathbb{Q}_{p'}$ al variare di $n \in \mathbb{N}$ (includiamo così nel conto anche $\mathbb{Q}_{p'} = p^0\mathbb{Q}_{p'}$) che sono, ripetiamo, a due a due distinti. Dunque, $\mathfrak{I}(\mathbb{Q}_{p'})$ è una catena numerabile. Menzioniamo il fatto che questo rende $\mathbb{Q}_{p'}$ un esempio di anello di valutazione (questi anelli saranno discussi nella sezione 10.2). Il fatto che tutti gli ideali non nulli di $\mathbb{Q}_{p'}$ siano potenze del suo ideale

³ usiamo questa notazione che ricorda il fatto che questo sottoanello, quozientato con \mathbb{Z} , costituisce la p' -componente del gruppo additivo \mathbb{Q}/\mathbb{Z} . Altre notazioni usate per questo anello sono $\mathbb{Z}_{p\mathbb{Z}}$, che è quella generale per le localizzazioni ma non è molto comune, \mathbb{Z}_p , che è una 'semplificazione' della precedente ma è terribilmente fuorviante, \mathbb{Q}_p , che non è solo una mescolanza tra le precedenti, ma viene giustificata dal riferimento al campo dei numeri p -adici. La notazione che usiamo qui è particolarmente diffusa tra chi si occupa di teoria di gruppi.

massimale $p\mathbb{Q}_p$ non è un caso; questa è una proprietà comune a tutti gli anelli noetheriani di valutazione.

Tornando agli anelli di frazioni di un dominio di integrità unitario, realizzati come sottoanelli del suo campo dei quozienti, abbiamo:

Proposizione 9.12. *Sia R un dominio di integrità unitario e sia K un suo (fissato) campo dei quozienti. Allora, se per ogni $M \triangleleft R$ indichiamo con R_M la localizzazione di R a M realizzata come sottoanello di K come indicato nella prima sezione di questo capitolo, $R = \bigcap_{M \triangleleft R} R_M$.*

Dimostrazione. Ovviamente $R \subseteq \bigcap_{M \triangleleft R} R_M$, quindi solo l'inclusione opposta è in questione.

Siano $M \triangleleft R$ e $c \in R_M$. Allora $c = a/b$ per opportuni $a \in R$ e $b \in R \setminus M$, dunque $b \in (R : c)_R$. Si ha così $(R : c)_R \not\subseteq M$. Sia ora $c \in \bigcap \{R_M \mid M \triangleleft R\}$. Allora $(R : c)_R$ è un ideale di R non contenuto in alcun ideale massimale di R , dunque $(R : c)_R = R$. Quest'ultima uguaglianza equivale a $c \in R$, dal momento che implica $1_R \in (R : c)_R$, ovvero $c = c1_R \in R$. La dimostrazione è ora completa. \square

Un'altra osservazione a proposito delle localizzazioni riguarda i loro campi residui. A partire da un anello commutativo R e da un suo ideale primo P , è possibile ottenere un campo in modo abbastanza diretto in due modi: il primo è passare al quoziente R/P , che è un dominio di integrità, e quindi al campo dei quozienti $Q(R/P)$ di questo; il secondo è il passaggio alla localizzazione R_P e quindi al suo campo residuo R_P/P^e . Queste due procedure portano essenzialmente allo stesso risultato:

Proposizione 9.13. *Siano R un anello commutativo e P un suo ideale primo. Allora $R_P/P^e \simeq Q(R/P)$.*

Dimostrazione. Basta applicare il Lemma 9.7. Posto $S = R \setminus P$ e $\bar{R} = R/P$, l'immagine di S in \bar{R} è $\bar{S} := \bar{R} \setminus \{0\}$, quindi $Q(R/P) = (\bar{S})^{-1}\bar{R} \simeq S^{-1}R/P^e = R_P/P^e$. \square

Possiamo anche dire qualcosa sugli anelli di frazioni della forma $S^{-1}R$, dove $S = R \setminus \bigcup \mathcal{P}$ per un insieme finito \mathcal{P} di ideali primi. In questo caso, mediante le biezioni espansione e contrazione, $\text{Spec}(S^{-1}R)$ corrisponde all'insieme degli ideali primi di R che siano contenuti in $\bigcup \mathcal{P}$. Ma il Lemma 3.7 mostra che un ideale (primo o non primo) di R è contenuto in $\bigcup \mathcal{P}$ se e solo se è contenuto in un elemento di \mathcal{P} . Dunque l'insieme di questi ideali (che, ripetiamo, come insieme ordinato è isomorfo a $\text{Spec}(S^{-1}R)$) è $\bigcup_{P \in \mathcal{P}} \mathcal{I}_P(R)$. Se ne deduce che gli ideali massimali di $S^{-1}R$, cioè gli elementi massimali di $\text{Spec}(S^{-1}R)$ sono espansioni di ideali primi appartenenti a \mathcal{P} , precisamente degli elementi di \mathcal{P} massimali per inclusione. Se chiamiamo *semilocale* un anello commutativo unitario in cui l'insieme degli ideali massimali è finito, abbiamo provato:

Corollario 9.14. *Sia R un anello commutativo e sia \mathcal{P} un insieme finito di suoi ideali primi. Allora $(R \setminus \bigcup \mathcal{P})^{-1}R$ è un anello semilocale. I suoi ideali massimali sono gli ideali della forma P^e al variare di P nell'insieme degli elementi di \mathcal{P} massimali per inclusione.⁴*

⁴ si badi bene: la richiesta qui non è che questi ideali P siano massimali come ideali di R , ma solo che siano massimali per inclusione tra gli elementi di \mathcal{P} .

Osservazioni ed esercizi.

9.C.1. L'idea di localizzazione è molto semplice da visualizzare in questi termini: scelto un ideale primo P dell'anello commutativo R , il passaggio all'anello di frazioni R_P "rende invertibili" gli elementi di R non in P . In questo modo si ottiene un anello in cui gli elementi esterni ad un certo ideale proprio (P^e) sono invertibili, quindi un anello locale. Cosa cambia se si parte da un ideale non primo al posto di P ?

9.C.2. Verificare che tutti gli anelli di frazioni che siano locali sono localizzazioni. Si tratta di provare che, se R è un anello commutativo e S è un sottomonoido saturo di (R, \cdot) tale che $S^{-1}R$ sia locale, allora $R \setminus S$ è un ideale primo di R .

9.C.3. Realizzare il sottoanello $\mathbb{Q}_2 = \{n/2^m \mid n \in \mathbb{Z} \wedge m \in \mathbb{N}\}$ di \mathbb{Q} come localizzazione di \mathbb{Z} e descriverne gli ideali. Determinare l'ideale di \mathbb{Q}_2 generato da $\{24/13, 36/5\}$ e la sua contrazione in \mathbb{Z} .

9.C.4. Imitando la dimostrazione del [Proposizione 9.12](#), provare che, se H è un ideale proprio di un anello commutativo unitario R , indicando con \mathcal{V} l'insieme degli ideali massimali di R contenenti H e, per ogni $M \in \mathcal{V}$, con e_M e c_M le funzioni espansione e contrazione relative all'anello di frazioni R_M , si ha $H = \bigcap_{M \in \mathcal{V}} H^{e_M c_M}$.

9.3 Decomposizioni primarie in anelli di frazioni

Concludiamo questo capitolo con alcune rapide osservazioni sulle decomposizioni primarie minimali in anelli di frazioni. Esclusi casi banali, l'espansione e la contrazione dell'espansione di un ideale decomponibile è ancora decomponibile; si ha infatti:

Proposizione 9.15. *Siano R un anello commutativo, H un suo ideale decomponibile con decomposizione primaria minimale \mathcal{D} , S un sottosemigruppato di (R, \cdot) e $S^{-1}R$ il corrispondente anello di frazioni, con omomorfismo S -inverso universale $f_S: R \rightarrow S^{-1}R$ ed applicazioni espansione e contrazione $e: \mathfrak{I}(R) \rightarrow \mathfrak{I}(S^{-1}R)$ e $c: \mathfrak{I}(S^{-1}R) \rightarrow \mathfrak{I}(R)$. Sia poi $\mathcal{D}_S = \{Q \in \mathcal{D} \mid Q \cap S = \emptyset\}$. Allora $\mathcal{D}_S \neq \emptyset$ se e solo se $H^e \neq S^{-1}R$ e, se questo accade, \mathcal{D}_S e $\{Q^e \mid Q \in \mathcal{D}_S\}$ sono decomposizioni primarie minimali, rispettivamente, di H^{ec} in R e di H^e in $S^{-1}R$.*

Dimostrazione. Da $H = \bigcap \mathcal{D}$ e dal [Lemma 9.10 \(i\)](#) segue $H^e = \bigcap \{Q^e \in \mathcal{D} \mid Q \in \mathcal{D}\}$. Se ne ricava che vale $H^e = S^{-1}R$ se e solo se $Q^e = S^{-1}R$ per ogni $Q \in \mathcal{D}$, vale a dire, tenendo conto del [Lemma 9.5 \(iv\)](#), se e solo se $\mathcal{D}_S = \emptyset$.

Sia $\mathcal{D}_S \neq \emptyset$. Da quanto appena visto si ottiene $H^e = \bigcap \{Q^e \mid Q \in \mathcal{D}_S\}$. Inoltre, come si ricava dal [Teorema 9.9](#), per ogni $Q_1, Q_2 \in \mathcal{D}_S$, gli ideali Q_1^e e Q_2^e sono primari in $S^{-1}R$ con radicali (primi) distinti, perché \mathcal{D} è minimale e $\sqrt{Q} \cap S = \emptyset$ per ogni $Q \in \mathcal{D}_S$. Passando alle contrazioni, si ha poi $H^{ec} = \bigcap \{Q^{ec} \mid Q \in \mathcal{D}_S\}$. Ma, ancora per il [Teorema 9.9](#), abbiamo $Q^{ec} = Q$ per ogni $Q \in \mathcal{D}_S$, quindi $H^{ec} = \bigcap \mathcal{D}_S$. Evidentemente \mathcal{D}_S è irridondante, perché lo è \mathcal{D} , dunque \mathcal{D}_S è una decomposizione primaria minimale di H^{ec} , come richiesto dall'enunciato. Infine, per ogni $I \in \mathcal{D}_S$ si ha $H^e \neq \bigcap \{Q^e \mid I \neq Q \in \mathcal{D}_S\}$, altrimenti avremmo $H^{ec} = \bigcap (\mathcal{D}_S \setminus \{I\})$, contro quanto appena stabilito, quindi anche $\{Q^e \mid Q \in \mathcal{D}_S\}$ è irridondante ed è così una decomposizione primaria minimale di H^e in $S^{-1}R$. \square

Un caso particolarmente significativo di quest'ultimo enunciato è quello in cui $S = R \setminus P$ per un primo isolato associato ad H .

Corollario 9.16. *Siano R un anello commutativo, H un suo ideale decomponibile e P un ideale primo isolato associato ad H . Allora, per ogni decomposizione primaria minimale \mathcal{D} di H in R , la P -componente di \mathcal{D}^5 è H^{ec} , dove e e c sono le applicazioni espansione e contrazione relative*

⁵ cioè, si ricorda, l'elemento di \mathcal{D} con radicale P .

alla localizzazione di R a P .

Dimostrazione. Posto $S = R \setminus P$, per ogni $Q \in \mathcal{D}$ si ha $Q \cap S = \emptyset$ se e solo se $Q \subseteq P$, cioè se e solo se Q è la P -componente \bar{Q} di \mathcal{D} . Di conseguenza, nelle notazioni della [Proposizione 9.15](#), $\mathcal{D}_S = \{\bar{Q}\}$ e quindi $H^{ec} = \bigcap \mathcal{D}_S = \bar{Q}$. \square

Evidentemente, questo corollario fornisce una dimostrazione alternativa (e di fatto indipendente) del secondo teorema di unicità per decomposizioni primarie ([7.16](#)).

Esercizi.

9.D.1. Il secondo teorema di unicità per decomposizioni primarie viene talvolta enunciato nella forma (apparentemente) più generale che segue.

Se H è un ideale decomponibile di un anello commutativo R , un sottoinsieme non vuoto \mathcal{P} di $\text{Ass}_R(H)$ è detto *isolato* se e solo se è ‘chiuso verso il basso’, cioè se e solo se ogni elemento di $\text{Ass}_R(H)$ contenuto in qualche elemento di \mathcal{P} appartiene esso stesso a \mathcal{P} . Estendere il [Corollario 9.16](#) dimostrando che se \mathcal{P} è isolato l’intersezione tra le P -componenti di una decomposizione primaria minimale di H , al variare di P in \mathcal{P} , è indipendente dalla decomposizione scelta.

10 Ampliamenti interi ed anelli di valutazione

La nozione di elemento intero su un anello è la diretta generalizzazione di quella di elemento algebrico su un campo; nata nell'ambito della teoria dei numeri, svolge un ruolo molto importante in diversi aspetti della teoria degli anelli. In questo capitolo ci limitiamo ad introdurla ed a discutere brevemente la sua connessione con una classe di domini di integrità: gli anelli di valutazione.

10.1 Interi su un anello

Sia R un sottoanello unitario di un anello commutativo unitario A . Un elemento di A si dice *intero* su R se e solo se è radice di un polinomio monico a coefficienti in R . Se R è un campo, quindi, la nozione di intero si riduce a quella di elemento algebrico. Se ogni elemento di A è intero su R si dice che A è un *ampliamento intero* (o integrale) di R .

Qualunque sia R , sono ovviamente interi su R tutti gli elementi di R (ogni $a \in R$ è radice di $x - a$); sono poi interi su \mathbb{Z} l'unità immaginaria $i \in \mathbb{C}$ e più in generale tutte le radici complesse dell'unità nel campo complesso, come anche i numeri reali della forma $\sqrt[m]{n}$ dove $m \in \mathbb{N}^+$ e $n \in \mathbb{Z}$. I numeri complessi che siano interi su \mathbb{Z} vengono chiamati *interi algebrici*. Vedremo ([Corollario 10.10](#)) che *ogni intero algebrico che sia un numero razionale è un numero intero*.

Esaminiamo alcune caratterizzazioni degli interi su un anello. La prima è una riformulazione della definizione: dire che un elemento c è radice di un polinomio in $R[x]$ monico di grado n , della forma cioè $x^n + \sum_{i=0}^{n-1} a_i x^i$, equivale a dire che c^n è una R -combinazione lineare delle potenze c^0, c^1, \dots, c^{n-1} (precisamente: $c^n = \sum_{i=0}^{n-1} (-a_i) c^i$). Dunque:

Lemma 10.1. *Se c ed R sono, rispettivamente un elemento ed un sottoanello unitario dell'anello commutativo A , c è intero su R se e solo se esiste $n \in \mathbb{N}^+$ tale che c^n appartenga all' R -sottomodulo $\sum_{i=0}^{n-1} c^i R$ di A generato da $\{c^0 = 1_R, c, c^2, \dots, c^{n-1}\}$.¹*

Corollario 10.2. *Con le stesse notazioni, se $c \in \mathcal{U}(A)$, allora c è intero su R se e solo se $c \in R[c^{-1}]$.²*

Dimostrazione. Sia $c \in R[c^{-1}]$. Poiché $R[c^{-1}] = \sum_{i \in \mathbb{N}} c^{-i} R$ esiste $n \in \mathbb{N}$ tale che $c = \sum_{i=0}^n c^{-i} R$. Moltiplicando per c^n otteniamo $c^{n+1} = \sum_{i=0}^n c^{n-i} R$, quindi c è intero su R .

Viceversa, se c è intero su R esiste $n \in \mathbb{N}$ tale che $c^n = \sum_{i=0}^{n-1} c^i R$, quindi $c = \sum_{i=0}^{n-1} c^{i-n+1} R \in R[c^{-1}]$. \square

Lemma 10.3. *Sia R un sottoanello unitario dell'anello commutativo A , e sia $c \in A$. Sono allora equivalenti:*

- (i) c è intero su R ;
- (ii) l'anello $R[c]$ è finitamente generato come R -modulo;
- (iii) esiste un $R[c]$ -modulo fedele che, visto come R -modulo per restrizione degli scalari, è finitamente generato.

¹ qui e più avanti facciamo tacitamente riferimento all'ovvia struttura di A come R -algebra.

² Come da uso corrente, $R[c^{-1}]$ indica il sottoanello di A generato da R e c^{-1} .

Dimostrazione. Valga (i); allora, come mostra il [Lemma 10.1](#), $c^n \in M := \sum_{i=0}^{n-1} c^i R$, per un opportuno $n \in \mathbb{N}$. Facendo induzione su t , possiamo facilmente mostrare che $c^{n+t} \in M$ per ogni $t \in \mathbb{N}$; infatti assumendo $c^{n+t} \in M$ si ottiene $c^{n+t+1} \in cM = \sum_{i=1}^n c^i R \subseteq M + c^n R = M$. Pertanto $R[c] = \sum_{i \in \mathbb{N}} c^i R = M$, e vale così (ii).

Che (iii) segua da (ii) è ovvio: basta considerare $R[c]$ come modulo su sé stesso. Resta da provare che (iii) implica (i). Sia $M = \sum_{i=0}^n u_i R$ un $R[c]$ -modulo fedele che sia R -finitamente generato. Per ogni $i \in \{1, 2, \dots, n\}$ si ha $u_i c = \sum_{j=1}^n u_j r_{ij}$ per opportuni $r_{ij} \in R$. Dunque, posto $\underline{u} = (u_1, u_2, \dots, u_n)$, abbiamo $\underline{u}(I_n c) = \underline{u}L$ per una matrice $L = (r_{ji})$ di tipo $n \times n$ su R (I_n indica la matrice identica di rango n su R). Allora $\underline{u}J = 0$, dove $J = I_n c - L$ è una matrice a termini in $R[c]$. Moltiplicando per $\text{adj}(J)$ ³ si ha $\underline{u}(I_n d) = 0$, dove $d = \det J$. Ovviamente questo significa $u_i d = 0$ per ogni $i \in \{1, 2, \dots, n\}$, e quindi $Md = 0$, vale a dire: $d \in \text{Ann}_{R[c]}(M)$. Ma M è fedele come $R[c]$ -modulo, pertanto $d = 0$. Ricordiamo che $J = I_n c - L$, dove L è una matrice a termini in R . Da ciò segue facilmente che, sviluppando il determinante di J , si ha $0 = d = c^n + \sum_{i=0}^{n-1} r_i c^i$ per opportuni elementi r_i di R , quindi c è intero su R . \square

Corollario 10.4. *Sia R un sottoanello unitario dell'anello commutativo A . Se A è finitamente generato come R -modulo, allora A è un ampliamento intero di R .*

Dimostrazione. Per ogni $c \in A$, A stesso verifica la condizione richiesta dalla (iii) del [Lemma 10.3](#). \square

I prossimi risultati sono generalizzazioni dirette (con dimostrazioni molto simili) di analoghi risultati sulle estensioni algebriche dei campi. È utile iniziare con un lemma in cui l'unica cosa a cui fare attenzione è il preciso significato dell'enunciato.

Lemma 10.5. *Sia R un anello commutativo unitario, A una R -algebra commutativa unitaria che sia finitamente generata come R -modulo e B un A -modulo finitamente generato. Allora B è finitamente generato come R -modulo.*

Prima della dimostrazione, definiamo bene le strutture coinvolte. Abbiamo in partenza due omomorfismi di anelli unitari: l'omomorfismo di struttura $\xi: R \rightarrow A$, che definisce A come R -algebra, e l'azione di modulo $\rho: A \rightarrow \text{End}(B, +)$, che definisce la struttura di A -modulo su B . Quindi B è strutturato come R -modulo dall'azione $\xi\rho: R \rightarrow \text{End}(B, +)$; è a questo modulo che si riferisce l'enunciato. Le operazioni esterne sono compatibili tra loro in questo senso: per ogni $r \in R$, $a \in A$ e $b \in B$ si ha: $(ba)r = (b^{a\rho})^{r\xi\rho} = b^{(ar\xi)\rho} = b(ar)$.

Dimostrazione. Per opportuni insiemi finiti $X \subseteq A$ e $Y \subseteq B$ abbiamo $A = XR$ e $B = YA$. Dalle osservazioni appena fatte sulla compatibilità tra le operazioni coinvolte segue facilmente $B = Y(XR) = (YX)R$ (si confronti questa situazione con quella dell'[Esercizio 1.D.2](#)). Quindi B è generato, come R -modulo, dall'insieme finito $\{xy \mid x \in X \wedge y \in Y\}$. \square

Lemma 10.6. *Sia A un anello commutativo unitario e sia R un suo sottoanello unitario. Supponiamo che esistano un numero finito di elementi $a_1, a_2, \dots, a_n \in A$ tali che $A = R[a_1, a_2, \dots, a_n]$ e, per ogni $i \in \{1, 2, \dots, n\}$, che a_i sia intero su $R[a_1, a_2, \dots, a_{i-1}]$. Allora A è un ampliamento intero di R ed è finitamente generato come R -modulo.*

Dimostrazione. Si può ragionare per induzione su n . Il risultato è ovvio per $n = 0$. Supponiamo $n > 0$ e che l'asserto valga per $n - 1$, allora $R_1 := R[a_1, a_2, \dots, a_{n-1}]$ è finitamente generato come R -modulo. Poiché a_n è intero su R_1 , il [Lemma 10.3](#) mostra che A è finitamente generato come R_1 -modulo e quindi, grazie al [Lemma 10.5](#), concludiamo che A è finitamente generato come R -modulo. Una diretta applicazione del [Corollario 10.4](#) completa la dimostrazione. \square

³ $\text{adj}(J)$ è la matrice dei complementi algebrici di J ; come nel caso delle matrici quadrate su un campo, si ottiene $J \text{adj}(J) = \text{adj}(J)J = I_n \det J$

Corollario 10.7. Sia R un sottoanello unitario dell'anello commutativo A . Allora l'insieme \bar{R} degli elementi di A che siano interi su R costituisce un sottoanello unitario di A contenente R .

Dimostrazione. Siano $a, b \in \bar{R}$. Allora $a - b$ e ab appartengono a $R[a, b]$, che, per il [Lemma 10.6](#), è un ampliamento intero di R . Dunque $a - b$ e ab sono interi su R , quindi appartengono a \bar{R} . L'asserto segue facilmente. \square

Questo anello \bar{R} prende il nome di *chiusura intera* (o integrale) di R in A . La chiusura intera di \bar{R} in A coincide con \bar{R} ; in questo consiste la proprietà di transitività per gli ampliamenti interi:

Corollario 10.8. Siano A, B e C anelli commutativi unitari. Se A è un ampliamento intero di B e B è un ampliamento intero di C , allora A è un ampliamento intero di C .

Dimostrazione. Sia $a \in A$. Allora a è intero su B , quindi $f(a) = 0$ per un opportuno polinomio monico $f \in B[x]$. Sia F l'insieme (finito) dei coefficienti non nulli di f , e sia $B_1 = C[F]$. Allora $f \in B_1[x]$, quindi a è intero su B_1 . Dal [Lemma 10.6](#) segue che $B_1[a]$ è un ampliamento intero di C , quindi a è intero su C . Ciò mostra che A è un ampliamento intero di C . \square

Fissiamo alcune notazioni. La chiusura intera di \mathbb{Z} nel campo complesso (o, equivalentemente, nella chiusura algebrica $\bar{\mathbb{Q}}$ di \mathbb{Q} contenuta in \mathbb{C}) viene indicata con $\bar{\mathbb{Z}}$ ed è nota come l'*anello degli interi algebrici*. Come abbiamo già detto, $\mathbb{Q} \cap \bar{\mathbb{Z}} = \mathbb{Z}$; questa proprietà si esprime dicendo che \mathbb{Z} è un anello integralmente chiuso. In generale, un *anello integralmente chiuso* è, per definizione, un dominio di integrità unitario che coincida con la sua chiusura intera nel suo campo dei quozienti. Sono integralmente chiusi \mathbb{Z} e, più in generale, tutti gli anelli fattoriali come stiamo per vedere.

Lemma 10.9. Siano R un anello fattoriale e $f = \sum_{i=0}^n a_i x^i \in R[x]$. Siano u, v due elementi coprimi di R tali che $v \neq 0$ e, nel campo dei quozienti di R , $f(u/v) = 0_R$. Allora, in R , u divide a_0 e v divide a_n .

Dimostrazione. Si ha $0_R = \sum_{i=0}^n a_i u^i / v^i$; moltiplicando per v^n otteniamo $0_R = \sum_{i=0}^n a_i u^i v^{n-i} = a_0 v^n + \sum_{i=1}^n a_i u^i v^{n-i}$. Ne segue che u divide $a_0 v^n$; ma u è coprimo con v^n , dunque $u \mid_R a_0$. Similmente, da $0_R = a_n u^n + \sum_{i=0}^{n-1} a_i u^i v^{n-i}$ deduciamo $v \mid_R a_n$. \square

Corollario 10.10. Gli anelli fattoriali sono integralmente chiusi.

Dimostrazione. Siano R un anello fattoriale e \bar{R} la chiusura intera di R nel suo campo dei quozienti. Sia poi $c \in \bar{R}$. Allora $c = u/v$ per opportuni elementi $u, v \in R$, tra loro coprimi e tali che $v \neq 0_R$; inoltre esiste un polinomio monico $f \in R[x]$ tale che $f(c) = 0_R$. Il [Lemma 10.9](#) comporta che v divida il coefficiente direttore 1_R di f ; ma allora $v \in \mathcal{U}(R)$ e quindi $c \in R$. Pertanto $\bar{R} = R$, quindi R è integralmente chiuso. \square

Concludiamo questa sezione con un importante lemma.

Lemma 10.11. Siano R un anello commutativo unitario e A un suo ampliamento intero. Siano poi P e Q ideali di A tali che P sia primo e $P \subseteq Q$. Se $P \cap R = Q \cap R$, allora $P = Q$.

Dimostrazione. Sia $c \in Q$, e tra i polinomi monici $f \in R[x]$ scegliamone uno di grado minimo per la condizione $f(c) \in P$ (il fatto che c è intero su R garantisce l'esistenza di almeno un tale polinomio). Posto $r = f(0)$, possiamo scrivere $f = xg + r$ per un opportuno g , monico, in $R[x]$; ovviamente $r \in R$ e g ha grado minore di quello di f , quindi $g(c) \notin P$. D'altra parte $f(c) = cg(c) + r$, quindi da $f(c) \in P \subseteq Q$ e $c \in Q$ ricaviamo $r \in Q$. Ma allora $r \in Q \cap R = P \cap R$, dunque $cg(c) = f(c) - r \in P$. Dal momento che P è primo e $g(c) \notin P$, otteniamo così $c \in P$. Dunque $Q = P$. \square

Ci possiamo fermare un attimo sul contenuto di questo lemma. Quello che ne ricaviamo è che se A è un ampliamento intero di R , ogni catena finita di ideali primi di A dà luogo, se intersecata con R , ad una catena di ideali primi di R della stessa lunghezza. Dunque, la dimensione di A non può superare quella di R . In realtà, è possibile dimostrare che le dimensioni di A e di R coincidono; una dimostrazione è suggerita come [Esercizio 10.A.5](#).

Un caso particolare è questo interessante risultato (la cui tesi prescrive che sia A che R abbiano dimensione 0).

Proposizione 10.12. *Sia A un dominio di integrità, ampliamento intero del suo sottoanello (unitario) R . Allora A è un campo se e solo se R è un campo.*

Dimostrazione. Sia A un campo, e sia $0_R \neq r \in R$. Allora r è invertibile in A e, per il [Corollario 10.2](#), dal fatto che c^{-1} è intero su R segue $c^{-1} \in R[c] = R$; dunque $c \in \mathcal{U}(R)$. Vediamo così che R è un campo.

Viceversa, sia R un campo. Sia M un ideale massimale di A . Evidentemente $R \not\subseteq M$, perché $1_R \notin M$, e $R \cap M \triangleleft R$, dunque $R^M = 0 = R \cap 0$, quindi $M = 0$ (vale a dire: A è un campo) per il [Lemma 10.11](#). \square

Esercizi.

10.A.1. $\mathbb{Z}[\sqrt{5}]$ è un esempio di dominio di integrità unitario non integralmente chiuso. Infatti la sezione aurea $\phi = (1 + \sqrt{5})/2$ è nel campo dei quozienti (immerso nel campo complesso) di $\mathbb{Z}[\sqrt{5}]$, ma non in $\mathbb{Z}[\sqrt{5}]$, eppure è radice del polinomio $x^2 - x - 1$, quindi è un intero algebrico e, in particolare, intera su $\mathbb{Z}[\sqrt{5}]$. Questo è un modo un po' indiretto per provare che $\mathbb{Z}[\sqrt{5}]$ non è un anello fattoriale.

10.A.2. Sia A un anello commutativo, ampliamento intero del suo sottoanello unitario R . Se φ è un omomorfismo di anelli unitari di dominio A , allora A^φ è un ampliamento intero di R^φ . Dedurre che per ogni $H \triangleleft A$ l'anello A/H è ampliamento intero di $R + H/H$ (isomorfo a $R/R \cap H$).

10.A.3. Sia A anello commutativo, ampliamento intero del suo sottoanello unitario R , e sia $\emptyset \neq S \subseteq R$. Identificato $S^{-1}R$ con un sottoanello (unitario) di $S^{-1}A$, come indicato nell'[Esercizio 9.A.5](#), verificare che $S^{-1}A$ è un ampliamento intero di $S^{-1}R$.

10.A.4. Sia A un anello commutativo, ampliamento intero del suo sottoanello unitario R . Provare che per ogni $P \in \text{Spec}(R)$ esiste $Q \in \text{Spec}(A)$ tale che $P = R \cap Q$. Lo si può fare seguendo i passi qui suggeriti.

- i) Sia $S = R \setminus P$. Allora $S^{-1}A$ è un ampliamento intero di R_P ([Esercizio 10.A.3](#)); utilizzando l'[Esercizio 9.B.11](#) verificare che se l'espansione di P in R_P è l'intersezione di un ideale primo K di $S^{-1}A$ con R_P , allora P è l'intersezione della contrazione di K in A con R , e vale quindi proprietà richiesta.
- ii) Quanto al punto precedente mostra che è sufficiente provare l'asserto nel caso in cui P sia massimale. Si può allora assumere $P \triangleleft R$, e basta provare che PA è un ideale proprio in A (se lo è, è contenuto in un ideale massimale di A ...).
- iii) Se $PA = A$, allora $PA_1 = A_1$ per un opportuno sottoanello A_1 di A che sia un ampliamento di R finitamente generato come R -modulo. Ragionando per induzione sul numero dei generatori, basta allora provare l'asserto nel caso in cui $A = R[c]$ per un opportuno $c \in A$. Ragionando come al primo passo, si può ulteriormente assumere che R sia locale (con ideale massimale P).
- iv) Ragionando come al primo passo, si vede che si può ulteriormente assumere che R sia locale (con ideale massimale P). Fatta quest'assunzione, sia $f = f_0 + xf_1$ un polinomio di grado minimo tra quelli monici in $R[x]$ di cui c sia radice. Se, per assurdo, $PA = A$,

allora $1_R = g(c)$ per un opportuno polinomio $g = g_0 + xg_1$ a coefficienti in P di grado minore di quello di f . Inoltre, poiché R è locale, $u := cg_1(c) = 1_R - g_0 \in \mathcal{U}(R)$, quindi $c \in \mathcal{U}(A)$ e $c^{-1} = u^{-1}g_1(c)$. Di conseguenza, c è radice del polinomio $h := c^{-1}f = f_0u^{-1}g_1 + f_1 \in R[x]$. Ma h è monico e ha grado minore di quello di f ...

10.A.5. Utilizzando (anche) l'esercizio precedente, provare che se l'anello commutativo A è un ampliamento intero del suo sottoanello unitario R , allora A e R hanno o entrambi dimensione (di Krull) infinita o la stessa dimensione (finita).

10.2 Anelli di Bézout ed anelli di valutazione

Come già accennato nella sezione 3.4, un *anello di Bézout* è, per definizione, un dominio di integrità unitario R in cui ogni ideale finitamente generato è principale. Naturalmente, perché ciò accada, è sufficiente che, scelti comunque $a, b \in R$, l'ideale $aR + bR$ da essi generato sia principale, ovvero: esista $d \in R$ tale che $aR + bR = dR$. Le considerazioni svolte nella sezione 3.4 mostrano che questa condizione implica che d sia un massimo comun divisore tra a e b . Quindi possiamo anche dire, in modo un po' informale, che un dominio di integrità unitario è un anello di Bézout se e solo se "in R vale il teorema di Bézout":

Proposizione 10.13. *Sia R un dominio di integrità unitario. Allora R è un anello di Bézout se e solo se, per ogni $a, b \in R$, esiste in R un divisore comune ad a e b che sia combinazione lineare di a e b a coefficienti in R . Ogni tale d è un massimo comun divisore tra a e b .*

Dimostrazione. Per un elemento d di R , dire che d è un divisore comune ad a e b equivale a dire che dR contiene aR e bR , quindi $aR + bR$; dire che d è combinazione lineare di a e b in R , equivale a dire che, viceversa, $dR \subseteq aR + bR$. Si ottiene così l'enunciato. \square

Sono ovviamente anelli di Bézout gli anelli principali, anzi, è chiaro che gli anelli principali sono precisamente gli anelli di Bézout noetheriani, ma esistono diversi esempi di anelli di Bézout non principali. Uno, anche se non dimostreremo questo fatto, è l'anello \mathbb{Z} degli interi algebrici introdotto nella sezione precedente, un altro è presentato nell'[Esempio 10.B.2](#); tanti altri ancora sono ottenibili dal [Lemma 10.16](#).

Esempi ed Esercizi.

10.B.1. Provare che un anello di Bézout fattoriale è necessariamente principale.

10.B.2. Sia $R = \mathbb{Z} + x\mathbb{Q}[x]$, l'insieme dei polinomi a coefficienti razionali con termine noto intero. Come è facile verificare, R è un sottoanello unitario di $\mathbb{Q}[x]$; meno immediato è che R è un anello di Bézout non principale. Iniziamo dalla seconda proprietà: se p è un intero primo, la successione $(p^{-n}xR)_{n \in \mathbb{N}^+}$ di ideali di R è strettamente crescente, quindi R non è noetheriano. Per provare che R è di Bézout, fissiamo $f, g \in R$; l'obiettivo è quello di trovare in $fR + gR$ un elemento che, in R , sia un divisore comune a f e g . Sia d un MCD in $\mathbb{Q}[x]$ tra f e g . Poiché d è definito a meno di associati, possiamo scegliere un tale d in modo che il suo termine noto d_0 sia un MCD in \mathbb{Z} tra i termini noti f_0 e g_0 di f e g (fare attenzione: questo ovviamente vale se $d_0 \neq 0$, ma vale anche se $d_0 = 0$, perché in questo caso x divide d , quindi f e g e dunque $f_0 = g_0 = 0$). Proveremo che (sicuramente se $d_0 \neq 0$, a meno di raffinare la scelta di d altrimenti) un tale d è proprio l'elemento di $fR + gR$ che stiamo cercando.

Innanzitutto, serve verificare che d divida f e g in R . Esistono $h, k \in \mathbb{Q}[x]$ tali che $f = dh$ e $g = dk$, quindi $f_0 = d_0h(0)$ e $g_0 = d_0k(0)$. Se $d_0 \neq 0$, abbiamo $h(0) = f_0/d_0 \in \mathbb{Z}$, quindi $h \in R$ e $d \mid_R f$; in modo analogo $d \mid_R g$. Iniziamo allora a considerare questo caso e assumiamo

$d_0 \neq 0$, vale a dire: almeno uno tra f_0 e g_0 non è 0. Per fissare le idee, supponiamo $f_0 \neq 0$. Poiché $\mathbb{Q}[x]$ è principale, esistono $\alpha, \beta \in \mathbb{Q}[x]$ tali che $d = \alpha f + \beta g$. Ora, α e β non sono univocamente determinati: per ogni $q \in \mathbb{Q}[x]$, se $\alpha_q = \alpha + qk$ e $\beta_q = \beta - qh$ si ha infatti $d = \alpha_q f + \beta_q g$. Per raggiungere il nostro scopo basterà scegliere q in modo che α_q e β_q siano in R . Ricordando che $h(0) \neq 0$, perché $f_0 \neq 0$, poniamo $q = \beta(0)/h(0)$. Allora $\beta_q(0) = 0$ e quindi, da una parte $\beta_q \in R$, dall'altra $d_0 = \alpha_q(0)f_0$, cioè $\alpha_q(0) = f_0/d_0 \in \mathbb{Z}$ e quindi $\alpha_q \in R$. A questo punto abbiamo dimostrato che, nell'ipotesi $f_0 \neq 0$, $d \in fR + gR$, quindi $dR = fR + gR$. Ovviamente si può procedere in modo analogo nell'ipotesi $g_0 \neq 0$; resta solo da considerare il caso in cui $f_0 = g_0 = 0$, quello cioè in cui sia f che g siano multipli di x in $\mathbb{Q}[x]$. Se $f = g = 0$, ovviamente, non c'è nulla da dimostrare. Nell'altro caso esiste $\lambda \in \mathbb{N}^+$ tale che x^λ divide sia f che g (in $\mathbb{Q}[x]$), ma $x^{\lambda+1}$ non divida almeno uno dei due. Posto $f = x^\lambda f^*$ e $g = x^\lambda g^*$, esiste $\mu \in \mathbb{N}^+$ tale che sia $f_1 := \mu f^*$ che $g_1 := \mu g^*$ sono in R . Dal momento che almeno uno di questi due polinomi ha termine noto non nullo, per il caso precedente si ha $d_1 R = f_1 R + g_1 R$ per un opportuno $d_1 \in R$. Moltiplicando per $(1/\mu)x^\lambda$ (che è in R perché $\lambda > 0$) e ponendo $ds = (1/n)x^\lambda d_1$, otteniamo $dR = fR + gR$.

Per definizione, un *anello di valutazione* è un dominio di integrità unitario R che verifichi una delle seguenti condizioni, tra loro equivalenti (e quindi tutte):

- (AV₁) l'insieme degli ideali di R è totalmente ordinato per inclusione;
- (AV₂) l'insieme degli ideali principali di R è totalmente ordinato per inclusione;
- (AV₃) per ogni $a, b \in R$, si ha $a|_R b$ o $b|_R a$;
- (AV₄) detto K il campo dei quozienti di R , per ogni $c \in K$ si ha $c \notin R \Rightarrow c^{-1} \in R$.

Vediamo perché queste condizioni sono tra loro equivalenti. Ovviamente (AV₁) implica (AV₂), ed è anche chiaro che (AV₂), (AV₃) e (AV₄) sono tra loro equivalenti (dire che un elemento $c = a/b$ di K , dove $a, b \in K$, appartiene a R significa precisamente dire che, in R , b divide a). Infine, assunta (AV₂), se I e J sono due ideali di R tra loro non confrontabili, esistono $a \in I \setminus J$ e $b \in J \setminus I$; poiché $aR \subseteq I$ e $b \notin I$ allora $bR \not\subseteq aR$; similmente $aR \not\subseteq bR$. Otteniamo così due ideali principali di R non confrontabili tra loro, in contraddizione con (AV₂). Proviamo così che (AV₂) implica (AV₁) e l'equivalenza delle (AV₁₋₄) è ora dimostrata.

Sono ovviamente esempi di anelli di valutazione tutti i campi; esempi più interessanti sono dati dalle *localizzazioni di \mathbb{Z}* discusse nella sezione 9.2.

Un'altra caratterizzazione degli anelli di valutazione è la seguente.

Proposizione 10.14. *Gli anelli di valutazione sono tutti e soli gli anelli di Bézout locali.*

Dimostrazione. Sia R un anello di valutazione. Allora R è un dominio di integrità unitario. Se $a, b \in R$, poiché aR e bR sono tra loro confrontabili, uno dei due coincide con $aR + bR$, che è dunque principale. Dunque R è un anello di Bézout. Inoltre R è locale: se avesse due ideali massimali distinti questi non potrebbero essere confrontabili tra loro per inclusione, contro la definizione (si veda (AV₁)) di anello di valutazione.

Viceversa, sia R un anello di Bézout locale, siano a e b due elementi di R e sia d un loro massimo comun divisore. Se $d = 0_R$ allora $a = b = 0_R$ e $a|_R b$. Altrimenti, da $dR = aR + bR$, moltiplicando per l'ideale frazionario $(dR)^{-1}$, otteniamo $R = \alpha R + \beta R$, dove $\alpha, \beta \in R$ e $a = d\alpha$, $b = d\beta$. Ma R è locale, quindi due ideali propri di R non possono essere comassimali; allora uno tra αR e βR coincide con R , vale a dire: uno tra α e β è invertibile. Pertanto d è associato ad uno tra a e b ; si ha allora $a|_R b$ nel primo caso, $b|_R a$ nel secondo. Abbiamo così provato che R verifica la condizione (AV₃) ed è dunque un anello di valutazione. \square

Corollario 10.15. *Ogni anello di valutazione noetheriano è principale.*

Gli anelli principali di valutazione sono anche noti, con terminologia più tradizionale, come *anelli di valutazione discreta* (la ragione sarà chiarita dall'[Osservazione 10.C.4](#)); alcuni autori limitano l'uso di questa espressione al caso degli anelli principali di valutazione che non siano campi (che sono, banalmente, sia anelli di valutazione che anelli principali).

Il prossimo lemma fornisce un metodo (generale, come suggerito dall'[Esercizio 10.C.1](#)) che fornisce esempi di anelli di valutazione: dato un campo K , tra le coppie (A, H) dove A è un sottoanello unitario di K e H ne è un ideale proprio, quelle massimali per inclusione (nel senso più ovvio) sono costituite da un anello di valutazione e dal suo ideale massimale.

Lemma 10.16. *Sia K un campo, sia R un suo sottoanello unitario e sia I un ideale proprio di R . Sia poi \mathcal{S} l'insieme delle coppie (A, H) , dove A è un sottoanello di K contenente R e H è un ideale proprio di A contenente I . Consideriamo \mathcal{S} ordinato dalla relazione \preceq , definita da: per ogni $(A_1, H_1), (A_2, H_2) \in \mathcal{S}$, $(A_1, H_1) \preceq (A_2, H_2)$ se e solo se $A_1 \subseteq A_2$ e $H_1 \subseteq H_2$. Allora (\mathcal{S}, \preceq) è induttivo ed ha elementi massimali; se (V, M) è uno di questi, allora V è un anello di valutazione e M è il suo ideale massimale; inoltre K è il campo dei quozienti di V .*

Dimostrazione. Che \preceq sia una relazione d'ordine è ovvio; quasi altrettanto ovvio è che (\mathcal{S}, \preceq) è un insieme induttivo. Infatti, sia $\{(A_j, H_j) \mid j \in J\}$ una catena non vuota in (\mathcal{S}, \preceq) , e siano $A = \bigcup\{A_j \mid j \in J\}$ e $H = \bigcup\{H_j \mid j \in J\}$. Allora A è un sottoanello di K contenente R ; inoltre $1_A = 1_R \notin H$ e $H \triangleleft A$: che H costituisca un sottogruppo di $(A, +)$ è ovvio; se $h \in H$ e $a \in A$ esiste $j \in J$ tale che $h \in H_j$ e $a \in A_j$, quindi $ha \in H_j \subseteq H$. Dunque $(A, H) \in \mathcal{S}$. Il Lemma di Zorn assicura quindi l'esistenza di qualche elemento massimale in \mathcal{S} . Sia (V, M) un tale elemento massimale; ovviamente M è un ideale massimale in V ; resta da provare che V è di valutazione. Per farlo basterà provare che, per ogni $c \in K$, o $c \in V$ oppure $c^{-1} \in V$; la qual cosa implica anche che K è il campo dei quozienti di V .

Sia $c \in K \setminus V$. La \preceq -massimalità di (V, M) implica $(V[c], MV[c]) \notin \mathcal{S}$, quindi $MV[c] = V[c]$, ovvero $1_R \in MV[c]$. Come è facile verificare, $MV[c] = \{f(c) \mid f \in M[x]\}$, dove abbiamo indicato con $M[x]$ l'ideale generato da M in $V[x]$, che è costituito dai polinomi i cui coefficienti appartengono a M . Esiste dunque $f \in M[x]$ tale che $1_K = f(c)$. Ragionando per assurdo, supponiamo $c^{-1} \in V$. Come nel caso di c , questo comporta l'esistenza di $g \in M[x]$ tale che $1_K = g(c^{-1})$. Posto $n = \nu f$ e $m = \nu g$, supponiamo di aver scelto f e g in modo che $n + m$ abbia il minimo valore possibile. Per fissare le idee, sia $n \geq m$. Se $g = \sum_{i=0}^m a_i x^i$, moltiplicando per c^n entrambi i membri di $1_K = g(c^{-1})$ abbiamo $(1_K - a_0)c^n = \sum_{i=n-m}^{n-1} a_{n-i} c^i$. D'altra parte, $1_K = (1_K - a_0)f(c) + a_0$ e nel secondo membro di questa equazione si può sostituire il termine $(1_K - a_0)c^n$ con $\sum_{i=n-m}^{n-1} a_{n-i} c^i$, grazie all'equazione precedente. Si ottiene in questo modo un polinomio $f_1 \in M[x]$, di grado minore di n , tale che $f_1(c) = 1_K$.⁴ Ciò contraddice la scelta di n e m ; si conclude così la dimostrazione. \square

Non è difficile provare che, come gli anelli fattoriali, anche gli anelli di valutazione sono integralmente chiusi: in questo consiste la prima parte della dimostrazione del prossimo risultato. Il [Lemma 10.16](#) permette in un certo senso di invertire questa osservazione, fornendo una descrizione generale della chiusura intera di un dominio di integrità unitario nel suo campo dei quozienti.

Proposizione 10.17. *Sia R un dominio di integrità unitario e sia K il suo campo dei quozienti. Detto \mathcal{V} l'insieme dei sottoanelli di K contenenti R che siano di valutazione, $\bigcap \mathcal{V}$ è la chiusura intera di R in K .*

⁴ per quanto irrilevante sia, osserviamo che $f_1 = a_0 + (1_K - a_0)(f - bx^n) + b \sum_{i=n-m}^{n-1} a_{n-i} x^i$, dove b è il coefficiente direttore di f .

Dimostrazione. Sia $V \in \mathcal{V}$, e sia $c \in K \setminus V$. Allora $c^{-1} \in V$; ce lo assicura la condizione (AV₄) nella definizione di anello di valutazione. Se c è intero su R , allora $c \in R[c^{-1}]$ per il Corollario 10.2. Ma $R[c^{-1}] \subseteq V$, questa è dunque una contraddizione, sicché c non è intero su R . Abbiamo così provato che la chiusura intera di R in K è contenuta in $\bigcap \mathcal{V}$.

Viceversa, sia $c \in \bigcap \mathcal{V}$. Se c non è intero su R , allora $c \notin A := R[c^{-1}]$. Dunque $H := c^{-1}A$ è un ideale proprio di A , quindi, applicando il Lemma 10.16, otteniamo un sottoanello di valutazione V di R tale che $A \subseteq V$ e H sia contenuto nell'ideale massimale di V . Allora $V \in \mathcal{V}$ e $c^{-1} \notin \mathcal{U}(V)$, dunque $c \notin V$, il che contraddice l'assunzione $c \in \bigcap \mathcal{V}$. Dunque: c è intero su R ; la dimostrazione è così completa. \square

Esercizi, Esempi, Osservazioni.

10.C.1. Sia R un anello di valutazione, I il suo ideale massimale e K il suo campo dei quozienti. Verificare che l'insieme \mathcal{S} definito come nel Lemma 10.16 a partire da K , R e I ha proprio (R, I) come unico elemento. Di conseguenza, ogni anello di valutazione è ottenibile dalla costruzione nel Lemma 10.16.

10.C.2. Verificare che tutti gli anelli di frazioni non nulli di un anello di valutazione sono anelli di valutazione.

10.C.3. Sia R un anello fattoriale in cui gli irriducibili sono tutti associati tra loro. Descrivere gli ideali principali e dedurre che R è un anello principale di valutazione. Un anello con le proprietà qui richieste per R è l'anello delle serie formali $K[[x]]$, per un qualsiasi campo K .

10.C.4. Sia $(G, +, \leq)$ un gruppo abeliano totalmente ordinato, cioè un gruppo abeliano $(G, +)$ su cui è definita una relazione di ordine totale \leq tale che per ogni $g \in G$ l'applicazione $a \in G \mapsto a + g \in G$ sia (strettamente) crescente. Se K è un campo, una *valutazione* da K a G è un omomorfismo v (di gruppi) dal gruppo moltiplicativo K^* di K a G tale che, per ogni $a, b \in K^*$ si abbia $(a + b)^v \geq \min\{a^v, b^v\}$, a condizione che $(a + b)^v$ sia definito, cioè $a \neq -b$. Spesso ci si libera di quest'ultima clausola aggiungendo a G un simbolo $+\infty$ (non appartiene a G) con l'usuale interpretazione convenzionale: si estendono sia l'ordinamento di G che la sua operazione a $\hat{G} = G \cup \{+\infty\}$ in modo che $+\infty$ sia il massimo di \hat{G} e verifichi la proprietà di assorbimento: $g + (+\infty) = (+\infty) + g = +\infty$ per ogni $g \in \hat{G}$; si prolunga poi v ponendo $0_K^v = +\infty$. In questo modo v diventa un'applicazione $K \rightarrow \hat{G}$, ma ovviamente \hat{G} non è più un gruppo.

Si può dimostrare che se v è una valutazione, come sopra descritta, $R_v := \{k \in K \mid k^v \geq 0_G\} \cup \{0_K\}$ è un sottoanello di K (detto l'anello della valutazione v) ed è un anello di valutazione del senso da noi definito. Infatti, per ogni $c \in K^*$, se $c \notin R_v$, cioè $c^v < 0_G$, allora $(c^{-1})^v > 0_G$, quindi $c^{-1} \in R_v$ (in particolare: $K = Q(R_v)$). Si verifica che gli elementi invertibili di R_v sono precisamente quelli che hanno valutazione (cioè immagine mediante v) uguale a 0_G , dunque l'ideale massimale di R_v è $M_v = \{k \in K \mid k^v > 0_G\} \cup \{0_K\}$. La valutazione v descrive la relazione di divisibilità in R_v , nel senso che i divisori di un elemento non nullo a di R_v sono precisamente quegli elementi $b \in R_v$ tali che $b^v \leq a^v$.

Viceversa, se R è un anello di valutazione, nel senso da noi definito, il gruppo $\mathfrak{F}_P(R)$ dei suoi ideali frazionari principali è totalmente ordinato dalla relazione \supseteq di inclusione inversa, e, se $K = Q(R)$, l'applicazione $F : k \in K \mapsto kR \in \mathfrak{F}_P(R)$ è una valutazione. Come è chiaro, l'anello della valutazione F è proprio R .

Possiamo concludere che la nostra definizione di anello di valutazione equivale a quella appena descritta in questa osservazione.

Aggiungiamo ancora: non è difficile provare che gli anelli di valutazione principali sono precisamente quelli che possono essere definiti da valutazioni a valori in \mathbb{Z} . Questa è l'origine del nome anelli di valutazione discreta che per essi si usa.

10.C.5. Facciamo qualche esempio di valutazione e compariamo questi con gli esempi che abbiamo già visto di anelli di valutazione. Iniziamo dall'esempio più banale: ogni campo K è un anello di valutazione; una valutazione che lo descrive come tale è l'omomorfismo nullo da K^* ad un qualsiasi gruppo abeliano totalmente ordinato.

Un esempio più significativo: per ogni intero primo p ed ogni $n \in \mathbb{Z} \setminus \{0\}$, sia $p^{v_p(n)}$ la massima potenza di p che divide n . Si verifichi (per esercizio) che l'applicazione $v_p: \mathbb{Q}^* \rightarrow \mathbb{Z}$ che ad ogni numero razionale non nullo a/b (con a e b interi) associa $v_p(a) - v_p(b)$ è (ben definita e) una valutazione (che \mathbb{Z} sia un gruppo abeliano totalmente ordinato dall'ordinamento usuale dovrebbe essere chiaro). L'anello della valutazione v_p è evidentemente \mathbb{Q}_p .

L'applicazione v_p è la cosiddetta *valutazione p -adica* definita sui razionali ed ha grande importanza, ad esempio, nella costruzione del campo dei numeri p -adici. È noto che le valutazioni p -adiche (una per ciascun primo p) e la valutazione banale (l'omomorfismo nullo) sono (in un senso che andrebbe precisato) essenzialmente le sole valutazioni definite sul campo razionale.

L'idea della valutazione p -adica si può estendere, in modo ovvio, sostituendo a p un un primo in un qualsiasi anello fattoriale R e a \mathbb{Q} il campo $Q(R)$. Ad esempio, per ogni campo K si definisce la valutazione x -adica da $K(x)^*$ a \mathbb{Z} associando ad un rapporto f/g tra due polinomi non nulli a coefficienti in K l'intero $v_x(f) - v_x(g)$, dove $x^{v_x(f)}$ è la massima potenza di x che divide f (cioè la molteplicità di 0_K come radice di f) e $v_x(g)$ è definito similmente. Analogamente si può definire la valutazione x -adica sull'anello dei quozienti di $K[[x]]$ (che è di valutazione, si veda l'esercizio precedente). In entrambi i casi, $v_x(f)$ ha una semplice descrizione in termini dei coefficienti di f , quale?

10.C.6. Scelto comunque un gruppo abeliano totalmente ordinato G , si possono costruire esempi di anelli di valutazione che abbiano il gruppo ordinato degli ideali principali frazionari isomorfo a G . Per farlo si può partire dall'*algebra gruppo* RG costruita su un dominio di integrità unitario R : questa è una R -algebra (commutativa, unitaria) di sostegno l'insieme delle famiglie $(r_g)_{g \in G} \in R^G$ a supporto finito, tali cioè che l'insieme $\{g \in G \mid r_g \neq 0_R\}$, in cui l'addizione è definita come addizione puntuale, il prodotto tra due elementi $(r_g)_{g \in G}$ e $(s_g)_{g \in G}$ è la famiglia $(t_g)_{g \in G}$, dove, per ogni $g \in G$, t_g è definito come $\sum_{h \in G} r_h s_{g-h}$ (questa operazione è abitualmente chiamata *prodotto di convoluzione*); il prodotto esterno tra un $(s_g)_{g \in G} \in RG$ ed un $r \in R$ è $(s_g r)_{g \in G}$. Si lascia a chi legge la verifica che tutto sia correttamente definito. Talvolta si introduce un simbolo aggiuntivo, x , e si indicano gli elementi $(r_g)_{g \in G}$ di RG come $\sum_{g \in G} r_g x^g$; con questa convenzione notazionale le operazioni definite estendono formalmente quelle che usiamo manipolando polinomi, avendosi $x^g x^h = x^{g+h}$ per ogni $g, h \in G$ (non troppo sorprendentemente: per $G = \mathbb{Z}$ $R\mathbb{Z}$ è isomorfo al sottoanello $R[x, x^{-1}] = \{x^{-n} f \mid n \in \mathbb{N} \wedge f \in R[x]\}$ del campo dei quozienti dell'anello di polinomi $R[x]$; una costruzione leggermente diversa condotta a partire dal monoide $(\mathbb{N}, +)$ anziché G fornisce proprio $R[x]$). Se, per ogni $r \in RG \setminus 0$, poniamo $r^v = \min g \in G \mid r_g \neq 0_G$, si verifica facilmente che per ogni $r, s \in RG \setminus 0$ si ha $(rs)^v = r^v s^v$ e, se $r \neq -s$, $(r+s)^v \geq \min\{r^v, s^v\}$. Segue da ciò che, se $K = Q(RG)$ l'applicazione v che a ciascun $r/s \in K^*$ (con $r, s \in RG$) associa $r^v - s^v$ è una valutazione suriettiva a valori in G . Pertanto l'anello di questa valutazione: $\{r/s \mid r, s \in RG \wedge s \neq 0 \wedge s^v \leq r^v\}$ è di valutazione ed ha la proprietà richiesta.

11 Funtori Hom e moduli proiettivi

Vengono qui introdotti, in modo ridotto all'essenziale, alcune nozioni di carattere omologico, allo scopo di introdurre la nozione di modulo proiettivo. Non viene trattata la nozione, duale, di modulo iniettivo.

La teoria verrà svolta solo per moduli e non per premoduli. La ragione è che in questo contesto non siamo interessati all'anello degli scalari su cui i (pre)modulo sono costruiti, quindi non si perde in generalità nel sostituire eventuali premoduli su un anello commutativo R con i corrispondenti moduli sull'anello accresciuto definito da R .

11.1 Sequenze di moduli

Fissiamo, per tutta questa sezione, un anello commutativo unitario R . Per sequenza di moduli si intende una famiglia di omomorfismi di R -moduli $(\alpha_i)_{i \in I}$ indicata in un intervallo I dell'insieme dei numeri interi tale che, per ogni $i \in I$, a meno che i non sia il massimo di I il dominio di α_{i+1} coincida col codominio di α_i (dunque, la richiesta è che omomorfismi consecutivi nella famiglia siano sempre componibili, nell'ordine in cui appaiono). Rappresenteremo una tale sequenza con scritte come

$$\cdots \longrightarrow A_{i-1} \xrightarrow{\alpha_{i-1}} A_i \xrightarrow{\alpha_i} A_{i+1} \xrightarrow{\alpha_{i+1}} A_{i+2} \xrightarrow{\alpha_{i+2}} \cdots \quad (*)$$

dove, chiaramente, abbiamo indicato, per ogni $i \in I$, con A_i il dominio di α_i . Se i è un elemento di I diverso dal suo eventuale minimo, si dice che la sequenza è quasi esatta al livello i (o, informalmente e in modo potenzialmente ambiguo, in [corrispondenza di] A_i) se $\alpha_{i-1}\alpha_i = 0$ (con 0 indichiamo un qualsiasi omomorfismo nullo; in questo caso quello da A_{i-1} a A_{i+1}); ovviamente questo equivale a richiedere $\text{im } \alpha_{i-1} \subseteq \ker \alpha_i$. Una sequenza che sia quasi esatta ad ogni livello (escluso l'eventuale minimo di I) si dice *quasi esatta* o *complesso di catene*. Anche se non è essenziale, osserviamo che ogni sequenza di moduli come in $(*)$ si può riguardare come restrizione di una sequenza indicata in \mathbb{Z} , che è quasi esatta se lo è la sequenza originaria: è sufficiente prolungarla con omomorfismi nulli, ad esempio ponendo $A_n = 0$ per ogni $n \in \mathbb{Z}$ che sia minore di $\min I$ o maggiore di $\max I + 1$ (qualora questi esistano) e, di conseguenza $\alpha_n = 0$, per ogni tale $n \in \mathbb{Z} \setminus I$.

Una sequenza $(\alpha_i)_{i \in I}$ di R -moduli si dice poi *esatta* al livello i se e solo se $\text{im } \alpha_{i-1} = \ker \alpha_i$; la si dice esatta se è esatta ad ogni livello (escluso, come sopra, $\min I$).

Vediamo qualche esempio. Dire che una sequenza come

$$0 \longrightarrow A \longrightarrow 0$$

è esatta significa dire $A = 0$; perché certamente A è il nucleo dell'omomorfismo di destra, quindi dire che la sequenza è esatta (in A) significa dire che A coincide con l'immagine dell'omomorfismo di sinistra, che è il sottomodulo nullo di A . Più in generale, l'esattezza di sequenze della forma

$$0 \longrightarrow A \xrightarrow{\alpha} B \quad \text{o} \quad A \xrightarrow{\beta} B \longrightarrow 0$$

significa che α è un monomorfismo, nel primo caso, o che β è un epimorfismo, nel secondo. Per la prima sequenza abbiamo infatti che l'immagine dell'omomorfismo a sinistra di A è 0 , quindi l'esattezza della sequenza equivale a $\ker \alpha = 0$; per quanto riguarda la seconda invece

sappiamo che l'omomorfismo a destra di B ha per nucleo B stesso, quindi l'esattezza della sequenza equivale a $\text{im } \beta = B$.

Il primo caso interessante è quello delle *sequenze esatte corte*, cioè sequenze della forma

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\gamma} C \longrightarrow 0,$$

dove A , B e C sono moduli arbitrari, che, alla luce di quanto osservato nel paragrafo precedente possiamo scrivere (e scriveremo) in modo più compatto come

$$A \xrightarrow{\alpha} B \xrightarrow{\gamma} C.$$

Le sequenze esatte corte permettono di esprimere in modo preciso la nozione, che abbiamo già [introdotta](#) informalmente, di estensione di moduli. Abbiamo infatti:

Lemma 11.1. *Sia $A \xrightarrow{\alpha} B \xrightarrow{\gamma} C$ una sequenza esatta corta di moduli. Allora, se $A_0 = \text{im } \alpha$, si ha che A_0 è un sottomodulo di B isomorfo ad A e tale che $B/A_0 \simeq C$. Viceversa, scelti comunque un modulo B , un suo sottomodulo A_0 ed isomorfismi $\varphi: A \rightarrow A_0$ e $\psi: B/A_0 \rightarrow C$, gli omomorfismi $\alpha: a \in A \mapsto a^\varphi \in B$ e $\gamma: b \in B \mapsto (b + A_0)^\psi \in C$ definiscono una sequenza esatta corta $A \xrightarrow{\alpha} B \xrightarrow{\gamma} C$.*

Dimostrazione. Per la prima parte dell'enunciato: ovviamente $A_0 \simeq A$; inoltre $A_0 = \ker \gamma$ perché la sequenza data è esatta, quindi $B/A_0 = B/\ker \gamma \simeq \text{im } \gamma = C$. Viceversa, se A_0 , α e γ sono come nella seconda parte dell'enunciato, è evidente che $A \xrightarrow{\alpha} B \xrightarrow{\gamma} C$ è una sequenza esatta corta, dal momento che α è un monomorfismo, γ è un epimorfismo e $A_0 = \text{im } \alpha = \ker \gamma$. \square

D'ora in avanti chiameremo *estensione* di moduli ogni sequenza esatta corta; più precisamente una estensione di un R -modulo A mediante un R -modulo C è, per definizione, una sequenza esatta corta di R -moduli della forma $A \xrightarrow{\alpha} B \xrightarrow{\gamma} C$. In questo contesto ci si riferisce informalmente a B come modulo estensione, giustificando così l'uso che abbiamo già fatto di questo termine.

Come ovvio esempio, se M è un modulo e N un suo sottomodulo, è una estensione (di N mediante M/N) la sequenza $N \hookrightarrow M \xrightarrow{\pi} M/N$, dove π è l'epimorfismo canonico.

Estensioni spezzate Dati comunque due R -moduli A e C è sempre possibile costruire estensioni di A mediante C ; la maniera più facile è costruire la somma diretta (esterna) $B = A \oplus C$ ed usare il monomorfismo $A \hookrightarrow B$ e la proiezione $B \rightarrow C$ canoniche per costruire la sequenza esatta corta richiesta. Le estensioni di questo tipo si caratterizzano in termini degli omomorfismi che le descrivono, come stiamo per vedere.

Un'estensione $A \xrightarrow{\alpha} B \xrightarrow{\gamma} C$ di R -moduli si dice *spezzata* se e solo se esiste un R -omomorfismo $\mu: C \rightarrow B$ tale che $\mu\gamma = \text{id}_C$. Se esiste, un tale μ è ovviamente iniettivo, questo spiega perché μ viene spesso chiamato un *mono spezzante* per l'estensione data. Le estensioni spezzate sono dunque quelle che danno luogo ad un diagramma commutativo di questa forma:

$$\begin{array}{ccccc} & & C & & \\ & & \swarrow \mu & & \searrow \parallel \\ A & \xrightarrow{\alpha} & B & \xrightarrow{\gamma} & C \end{array}$$

Proposizione 11.2. *Sia $\mathcal{E}: A \xrightarrow{\alpha} B \xrightarrow{\gamma} C$ una estensione di moduli. Allora \mathcal{E} è spezzata se e solo se $B = \text{im } \alpha \oplus K$ per un opportuno sottomodulo K di B .*

Dimostrazione. Poniamo $A_0 := \text{im } \alpha$. Supponiamo che \mathcal{E} sia spezzata e chiamiamo μ un suo mono spezzante. Sia $K = \text{im } \mu$. Allora $K \cap A_0 = 0$: infatti, se $k \in K \cap A_0$ allora $k = c^\mu$ per un opportuno $c \in C$, ma allora da $\mu\gamma = \text{id}_C$ e $k \in A_0 = \ker \gamma$ segue $c = c^{\mu\gamma} = k^\gamma = 0_C$,

quindi $k = c^\mu = 0_B$. Inoltre, per ogni $b \in B$ si ha $b^{\gamma\mu\gamma} = 0_C$, quindi $(b - b^{\gamma\mu})^\gamma = 0_C$, cioè $b - b^{\gamma\mu} \in \ker \gamma = A_0$. Allora $b = (b - b^{\gamma\mu}) + b^{\gamma\mu} \in A_0 + \text{im } \mu = A_0 + K$. Con ciò è provato che, se \mathcal{E} è spezzata, allora A_0 è un sommando diretto in B .

Viceversa, supponiamo $B = A_0 \oplus K$ per un opportuno sottomodulo K di B . Detta ζ la restrizione di γ a K , abbiamo $\ker \zeta = K \cap \ker \gamma = K \cap A_0 = 0$, quindi ζ è un monomorfismo. Inoltre $C = \text{im } \gamma = A_0^\gamma + K^\gamma = K^\gamma = \text{im } \zeta$, dal momento che $A_0^\gamma = 0$, quindi ζ è anche suriettiva. Dunque, ζ è un isomorfismo. Sia $\mu = \zeta^{-1}$. Allora $\mu: C \rightarrow B$ e, per ogni $c \in C$, $c^{\mu\gamma} = c^{\mu\zeta} = c$, quindi $\mu\gamma = \text{id}_C$, vale a dire: μ è un mono spezzante per \mathcal{E} , che risulta così spezzata. \square

Le estensioni realizzate come somma diretta possono essere caratterizzare anche in modo duale, in termini cioè di un *epi spezzante*, vale a dire, con le stesse notazioni della proposizione precedente, di un R -omomorfismo $\varepsilon: B \rightarrow A$ tale che $\alpha\varepsilon = \text{id}_A$. Ovviamente ogni tale ε è effettivamente un epimorfismo.

Proposizione 11.3. *Sia $\mathcal{E}: A \xrightarrow{\alpha} B \xrightarrow{\gamma} C$ una estensione di moduli. Allora \mathcal{E} è spezzata se e solo se ammette un epi spezzante*

La dimostrazione è lasciata per esercizio: consiste nel verificare, in modo analogo a quanto fatto per la [Proposizione 11.2](#), che l'estensione data ha un epi spezzante se e solo se $\text{im } \alpha$ è un sommando diretto in B .

Esercizi ed Osservazioni.

11.A.1. Dimostrare la [Proposizione 11.3](#).

11.A.2. Sia $\mathcal{E}: A \xrightarrow{\alpha} B \xrightarrow{\gamma} C$ una estensione di moduli. È chiaro che esiste sempre un'applicazione (iniettiva) $\mu: C \rightarrow B$ tale che $\mu\gamma = \text{id}_C$. La condizione che definisce l'essere \mathcal{E} un'estensione spezzata è che tra tutte le tali possibili applicazioni μ ce ne sia almeno una che sia un omomorfismo di R -moduli. Discorso analogo vale per la nozione di epi spezzante.

11.A.3. Anche per almeno un'altra categoria, quella dei gruppi (e, in verità, per molte altre), hanno senso le nozioni di estensione (come sequenza esatta corta) e di estensione spezzata, e valgono, con dimostrazioni analoghe, risultati corrispondenti a quelli enunciati per le categorie di moduli. C'è però un'importante differenza: l'esistenza di un mono spezzante per una estensione di gruppi equivale al fatto che l'estensione si realizzi come prodotto semidiretto, l'esistenza di un epi spezzante equivale invece ad una decomposizione in prodotto diretto. Quindi, mentre per le estensioni di moduli l'esistenza di un mono spezzante e di un epi spezzante sono proprietà equivalenti, lo stesso non vale per le estensioni di gruppi, per le quali la seconda proprietà è decisamente più forte della prima.

Osserviamo infine che la terminologia relativa alle sequenze di moduli si estende ad un caso molto simile, quello in cui $(\alpha_i)_{i \in I}$ sia un famiglia di omomorfismi di R -moduli a due a due componibili nel verso contrario a quello considerato in (*):

$$\cdots \longrightarrow A_{i+2} \xrightarrow{\alpha_{i+2}} A_{i+1} \xrightarrow{\alpha_{i+1}} A_i \xrightarrow{\alpha_i} A_{i-1} \xrightarrow{\alpha_{i-1}} \cdots \tag{**}$$

Questo caso non differisce da quello considerato prima se non per una ridefinizione degli indici: basta sostituire l'intervallo I con $I^- := \{-i \mid i \in I\}$ per ottenere la sequenza di moduli $(\alpha_{-i})_{i \in I^-}$, il cui studio è ovviamente del tutto equivalente a quello di $(\alpha_i)_{i \in I}$. Si dice che quella rappresentata in (**) è una sequenza quasi esatta, o una sequenza esatta, se la sequenza $(\alpha_{-i})_{i \in I^-}$ ha la stessa proprietà. Nel caso in cui $(\alpha_i)_{i \in I}$ sia quasi esatta, essa prende anche il nome di *complesso di cocatene*.

11.2 I funtori Hom

Siano R un anello commutativo unitario, A e B due R -moduli. L'insieme B^A delle applicazioni da A a B ha una struttura di R -modulo, quella di prodotto diretto di $|A|$ copie di B : $B^A = \prod_{a \in A} B$. L'operazione additiva di B^A non è altro che l'addizione puntuale (per essere chiari: se $f, g \in B^A$, allora $f = (a^f)_{a \in A}$ e $g = (a^g)_{a \in A}$, dunque $f + g = (a^f + a^g)_{a \in A}$ è l'applicazione $a \in A \mapsto a^f + a^g \in B$); il prodotto esterno è invece descritto da $fr: a \in A \mapsto a^f r \in B$ per ogni $f \in B^A$ e $r \in R$.

Sia $\text{Hom}_R(A, B)$ l'insieme degli R -omomorfismi da A a B . Non è difficile verificare che $\text{Hom}_R(A, B)$ è un R -sottomodulo di B^A . Infatti, per ogni $\alpha, \beta \in \text{Hom}_R(A, B)$ e per ogni $r \in R$, sia

$$\alpha + \beta: a \in A \mapsto a^\alpha + a^\beta \in B$$

che

$$\alpha r: a \in A \mapsto a^\alpha r = (ar)^\alpha \in B$$

sono R -omomorfismi, dal momento che, per ogni $x, y \in A$ e $s \in R$ abbiamo:

$$(x + y)^{\alpha + \beta} = (x + y)^\alpha + (x + y)^\beta = x^\alpha + y^\alpha + x^\beta + y^\beta = x^{\alpha + \beta} + y^{\alpha + \beta}$$

e

$$(xs)^{\alpha r} = (xs)^\alpha r = (x^\alpha s)r = x^\alpha(sr) = x^\alpha(rs) = (x^\alpha r)s = x^{\alpha r}s;$$

si noti che qui è essenziale la commutatività di R .

Fissiamo un R -modulo M . Possiamo utilizzare M e le considerazioni appena fatte per associare ad ogni R -modulo A l' R -modulo $A_* = \text{Hom}(M, A)$. Inoltre, se A e B sono R -moduli, ad ogni $\alpha \in \text{Hom}_R(A, B)$ possiamo associare l' R -omomorfismo α_* da A_* a B_* così definito: $\alpha_*: \varphi \in \text{Hom}(M, A) \mapsto \varphi\alpha \in \text{Hom}(M, B)$. Come è evidente, se α e β sono R -omomorfismi componibili (nell'ordine dato), cioè se il dominio di β coincide col codominio di α , allora $(\alpha\beta)_* = \alpha_*\beta_*$; inoltre, se α è l'omomorfismo identico in A allora α_* è l'omomorfismo identico in A_* . In teoria delle categorie, queste proprietà vengono espresse dicendo che questa trasformazione (di moduli in moduli e omomorfismi in omomorfismi) è un funtore covariante (dalla categoria degli R -moduli in sé). Non approfondiremo questi aspetti generali né tenteremo di dare le definizioni formali pertinenti, ci limiteremo ad usare queste espressioni in relazione al nostro specifico esempio, che chiamiamo il *funtore Hom covariante* definito da M , indicato come $\text{Hom}_R(M, -)$, o semplicemente $\text{Hom}(M, -)$ se non è necessario specificare l'anello R .

Lemma 11.4. *Siano R un anello commutativo unitario e sia $\alpha: A \rightarrow B$ un omomorfismo di R -moduli. Sia poi M un R -modulo. Allora l'omomorfismo α_* , immagine di α mediante il funtore $\text{Hom}_R(M, -)$, ha per nucleo $\{\varphi \in \text{Hom}_R(A, B) \mid \text{im } \varphi \subseteq \ker \alpha\}$. Dunque:*

- (i) $\ker \alpha_* \simeq_R (\ker \alpha)_*$, dove quest'ultimo è l'immagine di $\ker \alpha$ mediante $\text{Hom}_R(M, -)$;
- (ii) se α è un monomorfismo, allora anche α_* è un monomorfismo.

Dimostrazione. Sia $\varphi \in \text{Hom}_R(A, B)$. Allora $\varphi^{\alpha_*} = \varphi\alpha$, dunque $\varphi \in \ker \alpha_*$ se e solo se $\varphi\alpha = 0$, ovvero se e solo se $\text{im } \varphi \subseteq \ker \alpha$. Questo prova la prima parte dell'enunciato. Le due conseguenze elencate sono ora ovvie: per ogni $\varphi \in \ker \alpha_*$, risulta ben definita la ridotta φ' di φ a $\ker \alpha$ (perché questo sottomodulo contiene $\text{im } \varphi$); inoltre φ' è un R -omomorfismo e l'applicazione $\varphi \mapsto \varphi'$ da $\ker \alpha_*$ a $\text{Hom}_R(M, \ker \alpha)$ è un R -isomorfismo. Ma $\text{Hom}_R(M, \ker \alpha) = (\ker \alpha)_*$ e così abbiamo provato (i); (ii) segue in modo ancora più ovvio. \square

Il risultato appena provato viene talvolta espresso dicendo che il funtore $\text{Hom}_R(M, -)$ conserva i nuclei. Ne troveremo presto un'altra interpretazione.

La nozione di funtore covariante ne ha una duale, quella di funtore controvariante. Sempre per un fissato R -modulo M , il *funtore Hom controvariante* definito da M , indicato come

$\text{Hom}(-, M)$, è quello che associa ad ogni R -modulo A l' R -modulo $A^* = \text{Hom}_R(A, M)$ e ad ogni R -omomorfismo $\alpha: A \rightarrow B$ l' R -omomorfismo $\alpha^*: \varphi \in B^* \rightarrow \alpha\varphi \in A^*$. Si noti l'“inversione” del verso della freccia (si va da $A \rightarrow B$ a $B^* \rightarrow A^*$); è questo che rende ragione del prefisso “contro” in “controvariante”. Ciò che qualifica $\text{Hom}(-, M)$ come funtore controvariante è il fatto che vale $(\text{id}_A)^* = \text{id}_{A^*}$ per ogni modulo A e $(\alpha\beta)^* = \beta^*\alpha^*$ per ogni coppia di omomorfismi componibili α e β .

A differenza dei funtori Hom covarianti, i funtori Hom controvarianti non conservano i nuclei, ma, come si dice, mandano nuclei in conuclei, ovvero \ker in coker .¹ Per un arbitrario omomorfismo α di codominio B , $\text{coker } \alpha$ è per definizione $B/\text{im } \alpha$.

Lemma 11.5. *Siano R un anello commutativo unitario e sia $\alpha: A \rightarrow B$ un omomorfismo di R -moduli. Sia poi M un R -modulo. Allora l'omomorfismo α^* , immagine di α mediante il funtore $\text{Hom}_R(-, M)$, ha per nucleo $\{\varphi \in \text{Hom}_R(B, M) \mid \text{im } \alpha \subseteq \ker \varphi\}$. Dunque:*

- (i) $\ker \alpha^* \simeq_R (\text{coker } \alpha)^*$, dove quest'ultimo è l'immagine di $\ker \alpha$ mediante $\text{Hom}_R(-, M)$;
- (ii) se α è un epimorfismo, allora α^* è un monomorfismo.

Dimostrazione. Per ogni $\varphi \in B^* = \text{Hom}(B, M)$ si ha $\varphi^{\alpha^*} = \alpha\varphi$, quindi $\varphi \in \ker \alpha^*$ se e solo se $\text{im } \alpha \subseteq \ker \varphi$; otteniamo così la descrizione di $\ker \alpha^*$ richiesta nell'enunciato. Da qui segue immediatamente che α^* è iniettivo se α è suriettivo; vale quindi la (ii). Infine, se $\varphi \in \ker \alpha^*$ allora, poiché $\text{im } \alpha \subseteq \ker \varphi$, è ben definito l' R -omomorfismo $\varphi': x + \text{im } \alpha \in \text{coker } \alpha \mapsto x\varphi \in M$; si vede molto facilmente che la posizione $\varphi \mapsto \varphi'$ definisce un R -isomorfismo da $\ker \alpha^*$ a $(\text{coker } \alpha)^*$, provando così la (i). \square

Osservazioni.

11.B.1. Il fatto che, per due moduli A e B sull'anello commutativo unitario R , $\text{Hom}_R(A, B)$ sia un R -sottomodulo di B^A dipende in modo essenziale dalla commutatività di R . Questa è forse la principale differenza tra la teoria dei moduli su anelli commutativi e l'analoga teoria per anelli arbitrari.

11.B.2. Le categorie di moduli ricadono in una classe piuttosto particolare, quella delle cosiddette categorie abeliane. Tra le proprietà specifiche di queste categorie (senza le quali non sarebbe possibile sviluppare la teoria a cui accenniamo in questo capitolo) sono il fatto che, come abbiamo visto, gli insiemi degli omomorfismi sono muniti di un'operazione che li struttura come gruppi abeliani (nel nostro caso quella di addizione puntuale, che li rende addirittura moduli), che è possibile per i morfismi di queste categorie definire nozioni di \ker , im , coker con le proprietà familiari—ad esempio, la validità del primo teorema di omomorfismo. Una presentazione abbastanza sintetica delle categorie abeliane si trova nel terzo capitolo del terzo volume del libro di Cohn citato tra i riferimenti bibliografici.

11.B.3. Anche i funtori Hom che abbiamo presentato qui hanno una proprietà che li distingue da altri funtori tra categorie abeliane, quella di essere funtori additivi. La proprietà, che si chiede qui di verificare, è questa: per ogni R -modulo M , scelti comunque due R -moduli A e B le applicazioni $\alpha \in \text{Hom}_R(A, B) \mapsto \alpha_* \in \text{Hom}_R(A_*, B_*)$ e $\alpha \in \text{Hom}_R(A, B) \mapsto \alpha^* \in \text{Hom}_R(A^*, B^*)$ sono omomorfismi di gruppi abeliani (anzi, nel nostro caso, addirittura di R -moduli).

11.B.4. Se R è un anello commutativo unitario, il fatto che R_R sia un R -modulo libero su $\{1_R\}$ si traduce nel fatto che, per ogni R -modulo M , $\alpha \in \text{Hom}_R(R_R, M) \mapsto (1_R)^\alpha \in M$ sia un isomorfismo di R -moduli. Verificarlo.

¹ in questo contesto la parola ‘coker’ va accentata sulla seconda sillaba.

11.3 Funtori esatti

Sia F un funtore tra categorie di moduli (cioè, per due anelli commutativi unitari R ed S , un funtore dalla categoria degli R -moduli a quella degli S -moduli). Se F trasforma moduli nulli in moduli nulli e di conseguenza (esercizio!) omomorfismi nulli in omomorfismi nulli,² dal momento che, come ogni funtore, F rispetta la composizione tra morfismi (trasforma un morfismo $\alpha\beta$ in $\alpha^F\beta^F$ se è covariante, in $\beta^F\alpha^F$ se è controvariante), dovrebbe risultare chiaro che F trasforma ogni complesso di catene di R -moduli in un complesso di catene di S -moduli se F è covariante, in un complesso di cocatene se F è controvariante. Si dice che F è *esatto* se e solo F trasforma ogni sequenza esatta in una sequenza esatta. L'esattezza di un funtore si può equivalentemente esprimere in termini di sequenze esatte corte.

Proposizione 11.6. *Sia F un funtore tra categorie di moduli. Allora F è esatto se e solo trasforma sequenze esatte corte in sequenze esatte corte.*

Dimostrazione. Assumiamo che F sia definito nella categoria degli R -moduli (dove R è un anello commutativo unitario) e che sia covariante; la dimostrazione è analoga nel caso controvariante. Dovendo solo provare l'implicazione non ovvia, supponiamo che F trasformi ogni sequenza esatta corta in una sequenza esatta corta. Se 0 è un R -modulo nullo, allora $0 \rightarrow 0 \rightarrow 0 \rightarrow 0 \rightarrow 0$ è una sequenza esatta corta, quindi anche $0^F \rightarrow 0^F \rightarrow 0^F \rightarrow 0^F \rightarrow 0^F$ lo è, sicché 0^F è un modulo nullo (si noti che tutti i morfismi, in entrambe le sequenze, sono identici). Dunque, F trasforma moduli nulli in moduli nulli. Sia $\theta: A \rightarrow B$ un omomorfismo di R -moduli. Se θ è un monomorfismo, allora $0 \rightarrow A \xrightarrow{\theta} B \rightarrow C := \text{coker } \theta \rightarrow 0$ è esatta e quindi risulterà esatta anche $0 \rightarrow a^F \xrightarrow{\theta^F} B^F \rightarrow C^F \rightarrow 0$; dunque θ^F è mono. Se invece θ è epi, allora dall'esattezza di $0 \rightarrow K := \ker \theta \rightarrow A \xrightarrow{\theta} B \rightarrow 0$, segue l'esattezza di $0 \rightarrow K^F \rightarrow A^F \xrightarrow{\theta^F} B^F \rightarrow 0$, sicché θ^F è epi. Vediamo così che F trasforma monomorfismi in monomorfismi ed epimorfismi in epimorfismi.

Sia ora data un'arbitraria sequenza esatta $\mathcal{E}: \dots \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow D \rightarrow \dots$ di R -moduli. Per provare che F è un funtore esatto basterà mostrare che la sequenza ottenuta applicando F ad \mathcal{E} , vale a dire $\mathcal{E}^F: \dots \rightarrow A^F \xrightarrow{\alpha^F} B^F \xrightarrow{\beta^F} C^F \rightarrow D^F \rightarrow \dots$, è esatta. A questo scopo, sarà sufficiente provarne l'esattezza in B^F . Dalla \mathcal{E} ricaviamo

$$\begin{array}{ccccccc} \dots & \longrightarrow & A & \xrightarrow{\alpha} & B & \begin{array}{l} \xrightarrow{\beta_0} \\ \xrightarrow{\beta} \end{array} & C \longrightarrow D \longrightarrow \dots \\ & & \downarrow J & \nearrow \alpha_0 & & & \downarrow I \end{array}$$

dove $I = \text{im } \beta$, $J = A/\ker \alpha$ e l'epimorfismo $A \twoheadrightarrow J$ è quello canonico. Trasformando questi morfismi con F , che come abbiamo visto conserva le proprietà di essere mono o epi, abbiamo

$$\begin{array}{ccccccc} \dots & \longrightarrow & A^F & \xrightarrow{\alpha^F} & B^F & \begin{array}{l} \xrightarrow{\beta_0^F} \\ \xrightarrow{\beta^F} \end{array} & C^F \longrightarrow D^F \longrightarrow \dots \\ & & \downarrow J^F & \nearrow \alpha_0^F & & & \downarrow I^F \end{array}$$

Ora, chiaramente $\text{im } \alpha_0 = \text{im } \alpha$ e $\ker \beta_0 = \ker \beta$, dunque la sequenza $J \xrightarrow{\alpha_0} B \twoheadrightarrow I$ rappresentata nel primo diagramma dalle frecce diagonali è esatta (corta). Per l'ipotesi su F anche la sua

² questa proprietà è verificata dai funtori Hom ai quali siamo qui interessati, ma più in generale da tutti i funtori additivi)

trasformata $J^F \xrightarrow{\alpha_0^F} B^F \xrightarrow{\beta_0^F} I^F$ è esatta, dunque $\text{im } \alpha_0^F = \ker \beta_0^F$. Poiché α^F è composta da un epimorfismo e da α_0^F , sia ha $\text{im } \alpha^F = \text{im } \alpha_0^F$, mentre $\ker \beta^F = \ker \beta_0^F$, dal momento che β^F è composta da un monomorfismo e da β_0^F . Allora $\text{im } \alpha^F = \ker \beta^F$, vale a dire: \mathcal{E}^F è esatta in B^F , come richiesto. Questo conclude la dimostrazione. \square

La rilevanza delle sequenze esatte corte ai fini dell'esattezza di un funtore suggerisce le seguenti definizioni. Un funtore F tra categorie di moduli si dice *esatto a sinistra* se, per ogni sequenza esatta corta $\mathcal{E}: 0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\gamma} C \rightarrow 0$ è esatta $0 \rightarrow A^F \xrightarrow{\alpha^F} B^F \xrightarrow{\gamma^F} C^F$ se F è covariante, o $0 \rightarrow C^F \xrightarrow{\gamma^{\alpha^F}} B^F \xrightarrow{\alpha^F} A^F$ se F è controvariante. Si dice invece che F è *esatto a destra* se, per ogni sequenza esatta corta come \mathcal{E} è esatta $A^F \xrightarrow{\alpha^F} B^F \xrightarrow{\gamma^F} C^F \rightarrow 0$, se F è covariante, o $C^F \xrightarrow{\gamma^{\alpha^F}} B^F \xrightarrow{\alpha^F} A^F \rightarrow 0$, se F è controvariante.

È chiaro che per un funtore covariante (risp. controvariante) F tra categorie di moduli sono equivalenti le proprietà:

- (i) F è esatto a sinistra e trasforma epimorfismi (risp. monomorfismi) in epimorfismi;
- (ii) F è esatto a destra e trasforma monomorfismi (risp. epimorfismi) in monomorfismi;
- (iii) F è esatto a sinistra e a destra;
- (iv) F è esatto.

I funtori Hom non sono in generale esatti (si veda l'Esempio 11.C.4) ma, in conseguenza diretta dei lemmi 11.4 e 11.5, sono esatti a sinistra:

Proposizione 11.7. *Siano R un anello commutativo unitario e M un R -modulo. Allora i funtori $\text{Hom}(M, -)$ e $\text{Hom}(-, M)$ sono entrambi esatti a sinistra.*

Dimostrazione. Sia data una sequenza esatta corta $\mathcal{E}: A \xrightarrow{\alpha} B \xrightarrow{\gamma} C$. Usando per i morfismi le notazioni già introdotte, $\text{Hom}(M, -)$ trasforma \mathcal{E} nella sequenza quasi esatta

$$0 \rightarrow \text{Hom}(M, A) \xrightarrow{\alpha_*} \text{Hom}(M, B) \xrightarrow{\gamma_*} \text{Hom}(M, C) \rightarrow 0.$$

Per provare che $\text{Hom}(M, -)$ è esatto a sinistra dobbiamo verificare che questa sequenza sia esatta in $\text{Hom}(M, A)$ (cioè che α_* sia un monomorfismo) ed in $\text{Hom}(M, B)$ (cioè che $\ker \gamma_*$ sia contenuto in $\text{im } \alpha_*$). Che α_* sia un monomorfismo è stabilito dal Lemma 11.4. Sia poi $\varphi \in \ker \gamma_*$. Dunque, $\varphi \in \text{Hom}(M, B)$ e, per lo stesso Lemma 11.4, abbiamo $\text{im } \varphi \subseteq \ker \gamma = \text{im } \alpha$, quindi possiamo considerare la ridotta φ_0 di φ a $\text{im } \alpha$, e scrivere φ come $\varphi_0 \iota$, dove ι è l'immersione di $\text{im } \alpha$ in B . Similmente, $\alpha = \alpha_0 \iota$, dove α_0 è la ridotta di α a $\text{im } \alpha$ ed è un isomorfismo.

$$\begin{array}{ccccc} & & B & & \\ & \nearrow \varphi & \uparrow \iota & \nwarrow \alpha & \\ M & \xrightarrow{\varphi_0} & \text{im } \alpha & \xleftarrow{\alpha_0^{-1}} & A \end{array}$$

Come il diagramma suggerisce, $\varphi = \varphi_0 \alpha_0^{-1} \alpha = (\varphi_0 \alpha_0^{-1}) \alpha_*$, infatti $\varphi_0 \alpha_0^{-1} \alpha = \varphi_0 \alpha_0^{-1} \alpha_0 \iota = \varphi_0 \iota = \varphi$. Di conseguenza, $\varphi \in \text{im } \alpha_*$, come richiesto, sicché $\text{Hom}(M, -)$ è esatto a sinistra.

La dimostrazione per $\text{Hom}(-, M)$ è analoga: partendo dalla stessa sequenza esatta corta \mathcal{E} introdotta sopra, bisogna dimostrare l'esattezza di

$$0 \rightarrow \text{Hom}(C, M) \xrightarrow{\gamma^*} \text{Hom}(B, M) \xrightarrow{\alpha^*} \text{Hom}(A, M),$$

cioè, essendo già noto che $\gamma^* \alpha^* = 0$ e, per il Lemma 11.5, γ^* è un monomorfismo, bisogna provare $\ker \alpha^* \subseteq \text{im } \gamma^*$. Sia $\varphi \in \ker \alpha^*$. Per il Lemma 11.5, $\ker \gamma = \text{im } \alpha \subseteq \ker \varphi$, quindi è

ben definito l'epimorfismo $\nu: b + \ker \gamma \in B/\ker \gamma \mapsto b + \ker \varphi \in B/\ker \varphi$. Otteniamo così un diagramma commutativo

$$\begin{array}{ccccc}
 & & B & & \\
 & \swarrow \varphi & & \searrow \gamma & \\
 M & \xleftarrow{\varphi_0} & B/\ker \varphi & \xleftarrow{\nu} & B/\ker \gamma & \xrightarrow[\gamma_0]{\sim} & C
 \end{array}$$

dove i due epimorfismi senza nome sono epimorfismi canonici e φ_0 e γ_0 sono ricavati dal primo teorema di omomorfismo. Otteniamo così $\varphi = \gamma\gamma_0^{-1}\nu\varphi_0 = (\gamma_0^{-1}\nu\varphi_0)\gamma^* \in \text{im } \gamma^*$. Ciò completa la dimostrazione. \square

Esercizi, Osservazioni, Esempi.

11.C.1. Se r è un elemento dell'anello commutativo unitario R , si può definire un funtore covariante dalla categoria degli R -moduli in sé associando ad ogni R -modulo A il suo sottomodulo Ar e ad ogni R -omomorfismo $\alpha: A \rightarrow B$ il morfismo $a \in Ar \mapsto a^\alpha \in Br$ indotto per restrizione e riduzione da α . Questo funtore trasforma monomorfismi in monomorfismi ed epimorfismi in epimorfismi, ma, in generale, non è esatto (né a destra né a sinistra).

Ad esempio, scegliendo \mathbb{Z} come R ed un qualsiasi intero maggiore di 1 come r , la sequenza esatta corta $r\mathbb{Z} \hookrightarrow \mathbb{Z} \twoheadrightarrow \mathbb{Z}_r$ (in cui appare l'epimorfismo canonico) viene trasformata da questo funtore in una sequenza non esatta nel termine centrale.

Si lascia a chi legge la verifica della correttezza della definizione del funtore e delle affermazioni fatte.

11.C.2. Verificare che il funtore presentato all'esempio precedente è esatto se e solo se $r^2R = rR$.

11.C.3. I funtori esatti a sinistra o a destra possono equivalentemente essere definiti senza fare riferimento alle sequenze esatte corte. Dovrebbe infatti essere chiaro che un funtore covariante è esatto a sinistra (risp. a destra) se e solo se trasformano ogni sequenza esatta della forma $0 \rightarrow A \rightarrow B \rightarrow C$ (risp. della forma $A \rightarrow B \rightarrow C \rightarrow 0$) in una sequenza esatta della stessa forma. Discorso analogo si può fare per i funtori controvarianti.

11.C.4. Fissato un intero $n > 1$, consideriamo la sequenza esatta corta di gruppi abeliani $\mathcal{E}: n\mathbb{Z} \hookrightarrow \mathbb{Z} \twoheadrightarrow \mathbb{Z}_n$, dove l'epimorfismo è quello canonico. Come è facile verificare, $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}) \simeq \text{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, n\mathbb{Z}) = 0$ (perché gli omomorfismi mandano elementi periodici in elementi periodici), quindi $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, -)$ trasforma \mathcal{E} in $0 \rightarrow 0 \rightarrow 0 \rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_n) \rightarrow 0$, che non è esatta perché $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_n) \neq 0$ (difatti $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_n) \simeq \mathbb{Z}_n$). Vediamo così che $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, -)$ non è un funtore esatto.

Neanche $\text{Hom}_{\mathbb{Z}}(-, \mathbb{Z}_n)$ è esatto. Abbiamo infatti $\text{Hom}_{\mathbb{Z}}(n\mathbb{Z}, \mathbb{Z}_n) \simeq \text{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_n) \simeq \mathbb{Z}_n \simeq \text{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_n)$ (si veda l'Esercizio 11.B.4), quindi la trasformata di \mathcal{E} mediante $\text{Hom}_{\mathbb{Z}}(-, \mathbb{Z}_n)$, cioè la sequenza $0 \rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_n) \rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_n) \rightarrow \text{Hom}_{\mathbb{Z}}(n\mathbb{Z}, \mathbb{Z}_n) \rightarrow 0$ non può essere esatta.

11.4 Moduli proiettivi

La non-esattezza dei funtori Hom covarianti suggerisce l'importantissima nozione di modulo proiettivo. Per definizione, un modulo M sull'anello commutativo unitario R è *proiettivo* se e solo se il funtore $\text{Hom}_R(M, -)$ è esatto, cioè, vista la [Proposizione 11.7](#), esatto a destra. Risulta, come stiamo per vedere, che i moduli proiettivi sono tutti e soli i sommandi diretti dei moduli liberi.

Teorema 11.8. Sia M un modulo sull'anello commutativo unitario R . Sono equivalenti le affermazioni:

- (i) M è proiettivo;
- (ii) il funtore $\text{Hom}_R(M, -)$ trasforma epimorfismi in epimorfismi;
- (iii) vale la proprietà del sollevamento: scelti comunque un epimorfismo $\varepsilon: A \twoheadrightarrow B$ di R -moduli e $\varphi \in \text{Hom}_R(M, B)$, esiste un $\psi \in \text{Hom}_R(M, A)$ tale che $\varphi = \psi\varepsilon$;³
- (iv) ogni sequenza esatta corta della forma $A \twoheadrightarrow B \twoheadrightarrow M$ è spezzata;
- (v) M è sommando diretto di un R -modulo libero.

$$\begin{array}{ccc} & & A \\ & \nearrow \psi & \downarrow \varepsilon \\ M & \xrightarrow{\varphi} & B \end{array}$$

Dimostrazione. L'equivalenza tra (i) e (ii) è ovvia, dal momento che $\text{Hom}_R(M, -)$ è esatto a sinistra e i funtori esatti a sinistra sono esatti se e solo trasformano epimorfismi in epimorfismi. La (iii) non è altro che una riformulazione della (ii): ciò che richiede è che, per ogni epimorfismo $\varepsilon: A \twoheadrightarrow B$ ogni elemento di $\text{Hom}_R(M, B)$ sia immagine mediante ε_* di un elemento di $\text{Hom}_R(M, A)$, cioè che ε_* sia suriettiva. Dunque, (i), (ii) e (iii) sono equivalenti tra loro.

Valga (iii). Per ogni sequenza esatta corta $\mathcal{E}: A \twoheadrightarrow B \xrightarrow{\varepsilon} M$, la (iii) garantisce l'esistenza di un $\psi \in \text{Hom}_R(M, B)$ tale che $\text{id}_M \psi = \varepsilon$. Tale ψ è un mono spezzante per \mathcal{E} , quindi \mathcal{E} è spezzata e vale la (iv).

Per la [Proposizione 4.20](#) esistono un modulo libero F ed un epimorfismo $\varepsilon: F \twoheadrightarrow M$, abbiamo così la sequenza esatta corta $\ker \varepsilon \hookrightarrow F \xrightarrow{\varepsilon} M$. Se vale (iv), allora questa sequenza è spezzata, sicché M è isomorfo ad un sommando diretto di F e vale (v).

Supponiamo infine che valga (v), quindi $F = M \oplus K$ è libero, su una base $X \subset F$, per un qualche R -modulo K . Siano $\mu: M \hookrightarrow F$ e $\pi: F \twoheadrightarrow M$ il monomorfismo e la proiezione canonica rispetto a questa decomposizione diretta. Useremo questi dati per provare la (iii). Siano dati i morfismi $\varepsilon: A \twoheadrightarrow B$ (epi) e $\varphi: M \twoheadrightarrow B$. Per ogni $x \in X$ esiste $a_x \in A$ tale che $x^{\pi\varphi} = a_x^\varepsilon$, dal momento che ε è suriettiva. Allora la proprietà universale dei moduli liberi assicura l'esistenza di un morfismo $\theta: F \rightarrow A$ tale che $x^\theta = a_x$ per ogni $x \in X$. Ma allora $x^{\theta\varepsilon} = x^{\pi\varphi}$ per ogni $x \in X$ e quindi $\theta\varepsilon = \pi\varphi$ perché X genera F .

$$\begin{array}{ccccc} & & F & \overset{\theta}{\dashrightarrow} & A \\ & \nearrow \mu & \downarrow \pi & & \downarrow \varepsilon \\ M & \xlongequal{\quad} & M & \xrightarrow{\varphi} & B \end{array}$$

Sia ora $\psi = \mu\theta$. Allora $\psi\varepsilon = \mu\theta\varepsilon = \mu\pi\varphi = \varphi$. Quindi ψ è un sollevamento di φ lungo ε . La dimostrazione è completa. \square

In termini meno astratti, la condizione di spezzamento in (iv) viene anche espressa in questo modo: se B è un R -modulo ed A/B è un quoziente di B isomorfo ad M , allora A è un sommando diretto in B . Spesso si fa riferimento a questa come alla *proprietà proiettiva* (di M).

Il teorema appena provato garantisce che i moduli liberi sono proiettivi, ma non è difficile trovare esempi di moduli proiettivi che non sono liberi. Infatti, se l'anello commutativo unitario R è somma diretta dei suoi ideali propri H e K , allora, essendo R_R libero, sia H che K sono proiettivi perché verificano la condizione (v) del teorema. Poiché i moduli liberi non nulli sono fedeli mentre $HK = 0$, né H né K sono liberi. Un caso particolare: se a e b sono interi coprimi maggiori di 1, l'anello \mathbb{Z}_{ab} è somma diretta di sui ideali, quello generato da $[a]_{ab}$ (di ordine b) e quello generato da $[b]_{ab}$ (di ordine a); entrambi questi ideali sono \mathbb{Z}_{ab} -proiettivi, ma non liberi.

Va anche detto che esistono importanti tipi di anelli R con la proprietà che ogni R -modulo proiettivo sia libero. Sono tra questi gli anelli principali, perché si può dimostrare che ogni

³ un tale ψ viene spesso detto un *sollevamento* di φ lungo ε . Nella letteratura matematica in inglese la proprietà del sollevamento è nota come *lifting property*.

sottomodulo di un modulo libero su un anello principale è esso stesso libero (si vedano a questo proposito l'Osservazione 11.D.1 e l'esercizio che segue). Ciò vale, in particolare, per i moduli su \mathbb{Z} , ovvero i gruppi abeliani, quindi i gruppi abeliani proiettivi sono precisamente quelli liberi. A livello meno elementare possiamo citare un teorema di Kaplansky che stabilisce che se R è un anello commutativo locale, ogni R -modulo proiettivo è libero (per un caso particolare si veda l'Esercizio 11.D.3), uno di Hyman Bass, secondo il quale ogni modulo proiettivo non finitamente generato su un anello commutativo unitario noetheriano che non abbia idempotenti non banali (cioè che non sia decomponibile in somma diretta di ideali non nulli) è libero ed un teorema, ancora più profondo, dimostrato indipendentemente da Donald Quillen e Andrei Suslin: se R è un anello di polinomi ad un numero finito di indeterminate su un campo, ogni R -modulo proiettivo finitamente generato è libero.

Un'altra conseguenza del Teorema 11.8 è che una somma diretta è proiettiva se e solo se lo sono i sommandi che vi appaiono:

Corollario 11.9. Sia $(A_i)_{i \in I}$ una famiglia di moduli sull'anello commutativo unitario R . Allora $\coprod_{i \in I} A_i$ è proiettivo se e solo se A_i è proiettivo per ogni $i \in I$.

Dimostrazione. Se $\coprod_{i \in I} A_i$, allora, per il Teorema 11.8, esiste un R -modulo B tale che $F := B \amalg \coprod_{i \in I} A_i$ sia libero. Ma allora, per ogni $i \in I$, si ha $F \simeq A_i \amalg B \amalg \coprod_{i \neq j \in I} A_j$, quindi, per lo stesso teorema, A_i è proiettivo. Viceversa, se ciascuno dei moduli A_i è proiettivo, per ogni $i \in I$ esiste un modulo B_i tale che $F_i := A_i \amalg B_i$ sia libero. Ma $F := \coprod_{i \in I} F_i$ è libero, essendo una somma diretta di moduli isomorfi a R_R , e $F \simeq \coprod_{i \in I} A_i \amalg \coprod_{i \in I} B_i$, quindi $\coprod_{i \in I} A_i$ è proiettivo. \square

Corollario 11.10. Siano A e B sottomoduli di un modulo M . Allora esiste una sequenza esatta corta

$$A \xrightarrow{x \mapsto (x,x)} A \amalg B \xrightarrow{(a,b) \mapsto a-b} A + B.$$

Inoltre, se $A + B$ è proiettivo:

- (i) $A \amalg B \simeq (A \cap B) \amalg (A + B)$;
- (ii) A e B sono proiettivi se e solo se $A \cap B$ è proiettivo.

Dimostrazione. Considerata la somma diretta (esterna) $A \amalg B$, è chiaro che $\varepsilon: (a,b) \in A \amalg B \mapsto a - b \in A + B$ è un epimorfismo, di nucleo $\{(x,x) \mid x \in A \cap B\}$. Da ciò segue che, effettivamente, quella indicata nell'enunciato è una sequenza esatta corta. Se $A + B$ è proiettivo, questa sequenza è spezzata per il Teorema 11.8, quindi $A \amalg B \simeq (A \cap B) \amalg (A + B)$ e vale la (i). La (ii) segue dalla (i) e dal Corollario 11.9. \square

Abbiamo infine un'ulteriore caratterizzazione dei moduli proiettivi, legata alla nozione di base duale, probabilmente familiare dalla teoria degli spazi vettoriali di dimensione finita.

Sia X un insieme di generatori di un modulo M sull'anello commutativo unitario R . Una base duale per X (o per meglio dire, per la coppia (X, M)) è una famiglia $(\alpha_x)_{x \in X}$ di R -omomorfismi da M a R_R che verifica queste due proprietà per ogni $a \in M$:

- (i) l'insieme $\{x \in X \mid a^{\alpha_x} \neq 0_M\}$ è finito;
- (ii) $a = \sum_{x \in X} x a^{\alpha_x}$,

dove la somma in (ii) è ben definita essendo effettivamente estesa solo all'insieme finito descritto in (i).

Lemma 11.11. Siano M un modulo sull'anello commutativo unitario R ed X un suo insieme di generatori. Allora M è proiettivo se e solo se esiste per (X, M) una base duale.

Dimostrazione. Assumiamo che M sia proiettivo e verifichiamo l'esistenza di una base duale per (X, M) . Iniziamo col supporre che M sia un modulo libero su X . Per ogni $x \in X$ definiamo come α_x l'unico R -omomorfismo $M \rightarrow R_R$ che manda x in 1_R ed ogni $y \in X \setminus \{x\}$ in 0_R . Dal momento che $M = \bigoplus_{x \in X} xR$, ogni $a \in M$ si può scrivere, in modo unico, come $a = \sum_{x \in X} x a_x$, dove ciascuno degli a_x è in R e $\{x \in X \mid a_x \neq 0_M\}$ è finito. Evidentemente, per ogni $x \in X$, si ha $a^{\alpha_x} = a_x$. Da ciò segue che $(\alpha_x)_{x \in X}$ è una base duale.⁴

Passiamo ora al caso in cui M sia un modulo proiettivo arbitrario, generato da X . Consideriamo un modulo libero F su X ; possiamo supporre $X \subseteq F$. Per la proprietà universale dei moduli liberi, esiste un epimorfismo $\pi: F \rightarrow M$ tale che $x^\pi = x$ per ogni $x \in X$. D'altra parte, poiché M è proiettivo e quindi l'estensione $\ker \pi \hookrightarrow F \xrightarrow{\pi} M$ è spezzata, esiste un monomorfismo $\mu: M \rightarrow F$ tale che $\mu\pi = \text{id}_M$. Per quanto visto sopra, (X, F) ha una base duale $(\alpha_x)_{x \in X}$. Allora, per ogni $a \in M$, l'insieme $\{x \in X \mid a^{\mu\alpha_x} \neq 0_M\}$ è finito e $a^\mu = \sum_{x \in X} x a^{\mu\alpha_x}$. Applicando π deduciamo da questa uguaglianza $a = a^{\mu\pi} = \sum_{x \in X} x^\pi a^{\mu\alpha_x} = \sum_{x \in X} x a^{\mu\alpha_x}$, dove la combinazione lineare è, in questo caso, calcolata in M . Vediamo così che $(\mu\alpha_x)_{x \in X}$ è una base duale per (X, M) . La condizione è dunque necessaria.

Proviamo ora la sufficienza. Supponiamo che $(\alpha_x)_{x \in X}$ sia una base duale per (X, M) ; verificheremo per M la proprietà del sollevamento. Siano $\varepsilon: A \rightarrow B$ un epimorfismo e $\varphi: M \rightarrow B$ un omomorfismo di R -moduli. Per ogni $x \in X$ esiste (e fissiamo) $a_x \in A$ tale che $x^\varphi = a_x^\varepsilon$. Per ogni $a \in M$ l'insieme $\{x \in X \mid a^{\alpha_x} \neq 0_M\}$ è finito e quindi è ben definita l'applicazione

$$\psi: a \in M \mapsto \sum_{x \in X} a_x a^{\alpha_x} \in A.$$

Come è facile verificare, ψ è un R -omomorfismo. Inoltre, per ogni $a \in M$, si ha

$$a^{\psi\varepsilon} = \left(\sum_{x \in X} a_x a^{\alpha_x} \right)^\varepsilon = \sum_{x \in X} a_x^\varepsilon a^{\alpha_x} = \sum_{x \in X} x^\varphi a^{\alpha_x} = \left(\sum_{x \in X} x a^{\alpha_x} \right)^\varphi = a^\varphi.$$

Pertanto $\psi\varepsilon = \varphi$; ciò prova che la condizione (iii) del Teorema 11.8 è verificata, quindi M è proiettivo. \square

Esempi, Osservazioni, Esercizi.

11.D.1. Non è difficile provare che se tutti gli ideali di un anello commutativo unitario R sono liberi come R -moduli, allora R è principale (farlo come esercizio; un passaggio essenziale è l'osservazione che R è integro perché tutti i suoi ideali non nulli sono fedeli). Nell'esercizio che segue viene anche suggerito come provare che, viceversa, se R è principale ed F è un R -modulo libero, ogni sottomodulo di F è libero. Si giustifica così l'affermazione fatta nel testo che tutti i moduli proiettivi su un anello principale sono liberi.

Aggiungiamo che, più in generale, si può dimostrare che se R è un anello principale ogni sottomodulo di una somma diretta di R -moduli ciclici è esso stesso una somma diretta di moduli ciclici, ma la relativa dimostrazione è meno elementare.

11.D.2. Sia F un modulo libero sull'anello principale R . Provare, ragionando come segue, che ogni sottomodulo di F è libero. Innanzitutto, a questo scopo, si può assumere senza perdere in generalità che F sia una somma diretta $\bigoplus_{i < \alpha} A_i$, dove α è un ordinale e ciascuno degli A_i sia un R -modulo isomorfo a R_R . Per ogni ordinale $\beta \leq \alpha$, sia $F_\beta = \bigoplus_{i < \beta} A_i \leq F$. Osservare che, per ogni $\beta < \alpha$, o $F_{\beta+1} = F_\beta$ oppure $F_{\beta+1} \simeq F_\beta \oplus R_R$, (qui è utile la proprietà proiettiva). Fatto questo, la conclusione segue facilmente.

⁴ Nel caso in cui R sia un campo e quindi M sia uno spazio vettoriale di base X , questa è la consueta base duale di M incontrata in corsi elementari di algebra lineare che, se M ha dimensione finita, costituisce una base dello spazio duale $\text{Hom}(M, R_R)$.

11.D.3. Provare questo caso particolare del teorema di Kaplansky menzionato nel testo: se R è un anello commutativo locale, ogni R -modulo proiettivo M finitamente generato è libero. Suggerimento: detto n il minimo numero di generatori richiesti per M , esiste un R -modulo P tale che $F := M \oplus P$ sia libero di rango n . Se $J \triangleleft R$, ragionare sullo (R/J) -spazio vettoriale F/FJ per ottenere $P = 0$.

11.D.4. Oltre a quella di modulo proiettivo è di grande importanza anche la nozione duale, cioè quella di modulo iniettivo. Per definizione, un modulo M è iniettivo se e solo se il funtore $\text{Hom}(-, M)$ è esatto, cioè conserva i monomorfismi. Per i moduli iniettivi vale, almeno in parte una caratterizzazione come quella data nel [Teorema 11.8](#): M è iniettivo se e solo se vale la duale della proprietà del sollevamento (in sostanza: ogni omomorfismo $A \rightarrow M$ si prolunga a qualsiasi modulo contenente A come sottomodulo), ovvero se e solo se M è sommando diretto di ogni modulo di cui sia sottomodulo (questa è la duale della proprietà proiettiva).

Così come i moduli proiettivi sono legati alla nozione di modulo libero, i moduli iniettivi sono legati alla nozione di modulo divisibile (un R -modulo è divisibile quando $M = Mr$ per ogni $r \in R \setminus 0$ ⁵). Infatti, se R è un dominio di integrità unitario, ogni R -modulo iniettivo è divisibile; il viceversa vale se R è un anello principale o anche, più in generale, se R è un anello di Dedekind. Ad esempio, questo significa che i gruppi abeliani iniettivi sono precisamente quelli divisibili.

I moduli iniettivi non saranno più discussi in queste note; per informazioni più dettagliate si rimanda ad un qualsiasi testo di algebra.

⁵ alcuni autori utilizzano definizioni differenti di divisibilità; le differenze riguardano il caso in cui r sia un divisore dello zero

12 Anelli di Dedekind

In questo capitolo introdurremo un'importante classe di domini di integrità noetheriani, quella degli anelli di Dedekind.

12.1 Ideali frazionari

In questa sezione, salvo avviso contrario, con R si indicherà un dominio di integrità unitario e $K = Q(R)$ sarà il suo campo dei quozienti.

K ha una ovvia struttura di R -algebra, quindi di R -modulo; si chiamano *ideali frazionari* di R gli R -sottomoduli non nulli A di K tali che $(R : A)_R = \text{Ann}_R(A + R/R) \neq 0$, tali cioè che $Ar \subseteq R$ per qualche $r \in R \setminus 0$. È facile verificare che questa condizione equivale all'essere $(R : A)_K \neq 0$. Gli ideali frazionari di R che siano contenuti in R sono esattamente gli ideali non nulli di R , e si chiamano in questo contesto *ideali interi*. Indichiamo con $\mathfrak{F}(R)$ e $\mathfrak{I}^*(R)$, rispettivamente, l'insieme degli ideali frazionari e quello degli ideali interi di R .

Se $A \in \mathfrak{F}(R)$, ogni R -sottomodulo non nullo A_0 di A è ancora un ideale frazionario, dal momento che $(R : A)_R \subseteq (R : A_0)_R$. Si ha anche:

Lemma 12.1. *Se $A, B \in \mathfrak{F}(R)$, allora $A \cap B$, AB , $A + B$, $(A : B)_K \in \mathfrak{F}(R)$.*

Dimostrazione. È chiaro che le parti di K prese in esame sono tutte R -sottomoduli di K . Siano $0_R \neq a \in (R : A)_R$ e $0_R \neq b \in (R : B)_R$. Allora, se X è uno tra $A \cap B$, AB e $A + B$, si ha $Xab \subseteq R \cap X$ e, poiché R è un dominio di integrità, $ab \neq 0_R$ e $Xab \neq 0$, quindi X è un ideale frazionario. Infine, $0 \neq ab \subseteq (A : B)_K$ e, se $0_R \neq x \in B$, allora $ax \neq 0_R$ e $ax(A : B)_K \subseteq R$, quindi $(A : B)_K \in \mathfrak{F}(R)$. \square

È particolarmente significativo il fatto che $\mathfrak{F}(R)$ sia stabile rispetto alla moltiplicazione (tra parti di K). Questo, unitamente all'osservazione che $AR = A$ per ogni R -sottomodulo A di K , garantisce che $\mathfrak{F}(R)$, munito dell'operazione di moltiplicazione tra ideali frazionari, sia un monoide commutativo di elemento neutro R . È a questa struttura di monoide che faremo implicitamente riferimento nel nostro studio di $\mathfrak{F}(R)$. Osserviamo subito che $\mathfrak{I}^*(R)$ costituisce un sottomonoido di $\mathfrak{F}(R)$.

Gli R -sottomoduli ciclici non nulli di K sono ideali frazionari—ad essi ci si riferisce come ideali frazionari principali. La cosa è piuttosto ovvia: per ogni $k \in K \setminus 0$ si ha $k^{-1} \in (R : kR)_K$, quindi $(R : kR)_K \neq 0$. Più precisamente, gli ideali frazionari principali sono elementi invertibili in $\mathfrak{F}(R)$: con le notazioni fissate, l'inverso di kR è proprio $k^{-1}R$. Possiamo riguardare questa osservazione come conseguenza di una considerazione più generale: indicando con K^* il gruppo moltiplicativo di K , l'applicazione

$$k \in K^* \longmapsto kR \in \mathfrak{F}(R)$$

è un omomorfismo di monoidi; la sua immagine è l'insieme degli ideali frazionari principali di R , quindi costituisce un sottogruppo del gruppo degli invertibili di $\mathfrak{F}(R)$. Indicheremo questo sottogruppo con $\mathfrak{F}_P(R)$.

12.2. *Ogni R -sottomodulo finitamente generato e non nullo di K è un ideale frazionario.*

Dimostrazione. Ogni R -sottomodulo finitamente generato è somma di un numero finito di ideali frazionari principali, quindi l'asserto segue dal [Lemma 12.1](#). \square

Il prossimo lemma è tanto semplice quanto utile; esso permette di ridurre molte questioni riguardanti gli ideali frazionari al caso degli ideali interi.

Lemma 12.3. *Per ogni $A \in \mathfrak{F}(R)$ esistono un ideale intero A_1 ed un ideale frazionario principale U tali che $A = A_1U$. Di conseguenza, A_1 è sia R -isomorfo che associato in $\mathfrak{F}(R)$ ad A .*

Dimostrazione. Per definizione, esiste $r \in R \setminus 0$ tale che $A_1 := Ar \subseteq R$. Essendo $A_1 \neq 0$, abbiamo $A_1 \in \mathfrak{I}^*(R)$; ovviamente $A = A_1(r^{-1}R)$ e quindi, dal momento che $r^{-1}R \in \mathcal{U}(\mathfrak{F}(R))$, vediamo che A e A_1 sono associati. Infine, l'applicazione $a \in A \mapsto ar \in A_1$ è un R -isomorfismo. \square

Caratterizziamo ora gli ideali frazionari invertibili, cioè gli elementi invertibili di $\mathfrak{F}(R)$.

Lemma 12.4. *Siano A un ideale frazionario di R e L un R -sottomodulo di K . Allora:*

- (i) *se A è invertibile, $(L : A)_K = LA^{-1}$ e, in particolare, $A^{-1} = (R : A)_K$;*
- (ii) *sono equivalenti:*
 - a) *A è invertibile;*
 - b) *$A(R : A)_K = R$;*
 - c) *$1_R \in A(R : A)_K$.*

Dimostrazione. Sia A invertibile. Ovviamente $L = ALA^{-1}$, quindi $LA^{-1} \subseteq (L : A)_K$. D'altra parte $A(L : A)_K \subseteq L$ e quindi, moltiplicando per A^{-1} , $(L : A)_K \subseteq LA^{-1}$. Abbiamo così $(L : A)_K = LA^{-1}$. Ponendo $L = R$ se ne ricava $(R : A)_K = RA^{-1} = A^{-1}$. Vale dunque la (i).

La (ii) ne è immediata conseguenza: la (b) è ovviamente equivalente a (c) e comporta che A abbia $(R : A)_K$ come inverso. \square

Proposizione 12.5. *Sia $A \in \mathfrak{F}(R)$. Allora A è invertibile in $\mathfrak{F}(R)$ se e solo se A è proiettivo come R -modulo. Inoltre, se A è invertibile allora A è finitamente generato come R -modulo.*

Dimostrazione. Supponiamo A proiettivo. Il [Lemma 12.3](#) mostra che A è isomorfo ad un ideale intero che risulta invertibile se e solo se A è invertibile. Dunque, senza perdere in generalità, possiamo assumere che A stesso sia intero. Sia X un insieme di generatori di A e sia $(\alpha_x)_{x \in X}$ una corrispondente base duale, quindi per ogni $a \in A$ si ha che $\{x \in X \mid a^{\alpha_x} \neq 0_R\}$ è finito e $a = \sum_{x \in X} xa^{\alpha_x}$. Assumendo $a \neq 0_R$ e moltiplicando (in K) per a^{-1} abbiamo anche $1_R = \sum_{x \in X} xy_x$, dove $y_x = a^{-1}a^{\alpha_x}$ per ogni $x \in X$. Per ogni $c \in A$ e $x \in X$ si ha poi $ca^{\alpha_x} = (ca)^{\alpha_x} = ac^{\alpha_x}$, perché α_x è un omomorfismo di R -moduli, dunque $cy_x = ca^{-1}a^{\alpha_x} = aa^{-1}c^{\alpha_x} = c^{\alpha_x} \in R$. Ciò mostra che ciascuno degli elementi y_x è in $(R : A)_K$. Allora $1_R = \sum_{x \in X} xy_x \in A(R : A)_K$, quindi $A(R : A)_K = R$ e A invertibile per il [Lemma 12.4](#).

Viceversa, sia A invertibile. Esistono allora $n \in \mathbb{N}$ ed elementi $a_1, \dots, a_n \in A$ e $b_1, \dots, b_n \in A^{-1}$ tali che $1_R = \sum_{i=1}^n a_i b_i$. Per ogni $a \in A$ si ha $a = \sum_{i=1}^n a_i(ab_i)$, dove ciascuno degli elementi ab_i è in R , perché $b_i \in A^{-1} = (R : A)_K$. Pertanto $A = \sum_{i=1}^n a_i R$, vale a dire: A è generato da $X := \{a_1, a_2, \dots, a_n\}$ (quindi A è finitamente generato). Inoltre, per ogni $i \in \{1, 2, \dots, n\}$ l'applicazione $\alpha_i: a \in A \mapsto ab_i \in R$ è un omomorfismo di R -moduli. Avendo già osservato che $a = \sum_{i=1}^n a_i a^{\alpha_i}$ per ogni $a \in R$, concludiamo che gli omomorfismi α_i permettono di definire una base duale per X e quindi, per il [Lemma 11.11](#), A è proiettivo. \square

Esercizi e Osservazioni.

12.A.1. Il [Lemma 12.3](#) offre una descrizione esplicita degli ideali frazionari: ogni ideale frazionario si ottiene moltiplicando un ideale intero per l'inverso (in K) di un elemento non nullo di R .

12.A.2. Se R è noetheriano, ogni ideale frazionario di R è finitamente generato come R -modulo, quindi noetheriano. Possiamo dedurre che l'insieme degli ideali frazionari di R (ordinato per inclusione) è a condizione massimale?

12.A.3. Costruire, per qualche dominio di integrità unitario R , un ideale frazionario di R contenente R che non sia finitamente generato come R -modulo.

12.A.4. Ricordando dalla [sezione 5.2](#) che l'anello di polinomi $\mathbb{Z}[x]$ ad una indeterminata è un anello fattoriale (noetheriano) in cui sia 2 che x sono irriducibili, mostrare che, posto $H = 2\mathbb{Z}[x] + x\mathbb{Z}[x]$, si ha $(\mathbb{Z}[x] : H)_{Q(\mathbb{Z}[x])} = \mathbb{Z}[x]$, quindi H è un ideale (finitamente generato) non invertibile.

12.A.5. Sia R un dominio di integrità unitario e supponiamo che $\mathcal{I}^*(R)$ sia un monoide cancellativo. Provare che R è integralmente chiuso. Suggerimento: se c è un elemento di $K = Q(R)$ che sia intero su R , allora $R[c]$ è un ideale frazionario

12.2 Anelli di Dedekind

Per definizione, un anello di Dedekind è un dominio di integrità unitario che verifica una delle seguenti condizioni, che, come mostrano il [Lemma 12.3](#) e la [Proposizione 12.5](#), sono tra loro equivalenti:

- * ogni ideale di R è proiettivo;
- * ogni ideale non nullo di R è invertibile;
- * ogni ideale frazionario di R è invertibile;
- * $\mathfrak{F}(R)$ è un gruppo.

La [Proposizione 12.5](#) mostra anche che *tutti gli anelli di Dedekind sono noetheriani*. Avendo già osservato che gli ideali principali non nulli di un dominio di integrità sono sempre invertibili, concludiamo che tutti gli anelli principali sono di Dedekind. Dunque, quella degli anelli di Dedekind è una classe di domini di integrità intermedia tra quella degli anelli principali e quella degli anelli noetheriani. Come si vedrà nel ??, gli anelli degli interi algebrici in estensioni finite del campo razionale forniscono esempi di anelli di Dedekind che spesso non sono principali (un anello di questo tipo è $\mathbb{Z}[\sqrt{-5}]$); altri importanti esempi appaiono in geometria algebrica, come anelli di coordinate di curve affini. $\mathbb{Z}[x]$ è invece un esempio di dominio di integrità unitario noetheriano che non è di Dedekind; questo è facile da dimostrare direttamente (vedi [Esercizio 12.A.4](#)), ma segue, in modo ancora più semplice, da considerazioni generali, ad esempio dal [Teorema 12.7](#) perché l'ideale generato da x in questo anello è primo ma non massimale.

Gli anelli di Dedekind ammettono varie, interessanti caratterizzazioni. La prima che dimostriamo coinvolge il fatto che il monoide degli ideali interi di ogni anello di Dedekind è fattoriale. A questo proposito, osserviamo subito che, qualunque sia il dominio di integrità unitario R , la relazione di divisibilità in R comprende quella di inclusione inversa, nel senso che, per ogni $A, B \in \mathcal{I}^*(R)$, se A divide B (cioè $B = AC$ per un ideale $C \in \mathcal{I}^*(R)$), allora $A \supseteq B$. Di conseguenza, due elementi che siano associati in $\mathcal{I}^*(R)$ devono necessariamente coincidere; in altre parole: la relazione 'essere elementi associati' in $\mathcal{I}^*(R)$ è la relazione di uguaglianza, sicché, nelle notazioni del [Capitolo 2](#), $\mathcal{I}^*(R) \simeq \widetilde{\mathcal{I}^*(R)}$ e la relazione di divisibilità in $\mathcal{I}^*(R)$ è una relazione d'ordine. Allora, per il [Teorema 2.5](#), $\mathcal{I}^*(R)$ è fattoriale se e solo se è cancellativo e $(\mathcal{I}^*(R), |)$ è

un reticolo a condizione minimale. Altra ovvia conseguenza è che l'elemento neutro, R , è l'unico elemento invertibile di $\mathfrak{I}^*(R)$.

Ci tornerà utile, anche più avanti, la seguente osservazione:

Lemma 12.6. *Siano I e J ideali non nulli del dominio di integrità unitario R e supponiamo I invertibile. Allora I divide J in $\mathfrak{I}^*(R)$ se e solo se $I \supseteq J$.*

Dimostrazione. Come appena osservato, $I \supseteq J$ se $I|J$. Viceversa, $J = I(I^{-1}J)$ e, se $I \supseteq J$, allora $I^{-1}J = (R : I)_K J \subseteq R$, dunque $I^{-1}J \in \mathfrak{I}^*(R)$ e $I|J$. \square

Teorema 12.7. *Sia R un anello di Dedekind. Allora $\mathfrak{I}^*(R)$ è un monoide fattoriale. Inoltre,*

- (i) *la relazione di divisibilità in $\mathfrak{I}^*(R)$ coincide con l'inclusione inversa. Vale a dire: per ogni $I, J \in \mathfrak{I}^*(R)$, I divide J in $\mathfrak{I}^*(R)$ se e solo se $I \supseteq J$;*
- (ii) *gli ideali primi non nulli in R sono massimali (cioè: R ha dimensione di Krull al più 1);*
- (iii) *ogni ideale proprio e non nullo di R è prodotto di ideali primi. Tale decomposizione è unica, a meno dell'ordine dei fattori.*

Dimostrazione. La (i) segue immediatamente dal [Lemma 12.6](#). Per ulteriore conseguenza, $\mathfrak{I}^*(R)$, come insieme ordinato (per divisibilità), è anti-isomorfo a $(\mathfrak{I}^*(R), \subseteq)$, che è un sottoreticolo del reticolo degli ideali di R , perché l'intersezione di due ideali non nulli di R è ancora non nullo. Ora, R è noetheriano—l'abbiamo visto [sopra](#)—quindi $(\mathfrak{I}^*(R), |)$ è un reticolo a condizione minimale. Infine, $\mathfrak{I}^*(R)$ è un monoide cancellativo, in quanto sottomonoide del gruppo $\mathfrak{F}(R)$, dunque $\mathfrak{I}^*(R)$ è fattoriale per il [Teorema 2.5](#).

Gli elementi irriducibili in $\mathfrak{I}^*(R)$ sono gli atomi del reticolo $(\mathfrak{I}^*(R), |)$; ovviamente questi devono coincidere con i coatomi del reticolo $(\mathfrak{I}^*(R), \subseteq)$, il duale di $(\mathfrak{I}^*(R), |)$, cioè con gli ideali massimali di R . Abbiamo così che ogni elemento di $\mathfrak{I}^*(R)$, ad eccezione dell'unico invertibile R , si scrive in un unico modo, a meno dell'ordine dei fattori, come prodotto di ideali massimali di R ; vale dunque (iii). Per completare la dimostrazione basta mostrare che vale la (ii). Sia $0 \neq P \in \text{Spec}(R)$. Allora P è un prodotto di ideali massimali di R , ed essendo P primo uno dei fattori di questo prodotto deve essere contenuto in P , e quindi coincidere con P . Dunque P è massimale. \square

Corollario 12.8. *Sia R un anello di Dedekind. Allora $\mathfrak{F}(R)$ è un gruppo abeliano libero sulla base dell'insieme degli ideali primi di R non nulli.*

Dimostrazione. Sia $A \in \mathfrak{F}(R)$. Esiste $r \in R \setminus 0$ tale che $Ar \in \mathfrak{I}^*(R)$. Dal [Teorema 12.7](#) segue che sia rR che Ar sono prodotti di ideali primi non nulli, quindi $A = (Ar)(rR)^{-1}$ è prodotto di ideali primi ed inversi di ideali primi. Dunque l'insieme degli ideali primi non nulli di R genera $\mathfrak{F}(R)$. Supponiamo ora che questi ideali primi non nulli non siano tra loro indipendenti, quindi che esistano ideali primi P_1, P_2, \dots, P_n non nulli ed a due a due distinti, ed interi non nulli $\lambda_1, \lambda_2, \dots, \lambda_n$ tali che $\prod_{i=1}^n P_i^{\lambda_i} = R$ (ricordiamo che R è l'elemento neutro di $\mathfrak{I}^*(R)$). Non si perde in generalità nell'assumere, per un certo intero non negativo $s \leq n$, che $\lambda_1, \lambda_2, \dots, \lambda_s > 0$ e $\lambda_{s+1}, \lambda_{s+2}, \dots, \lambda_n < 0$. Si ha allora $H := \prod_{i=1}^s P_i^{\lambda_i} = \prod_{i=s+1}^n P_i^{-\lambda_i}$, quindi H risulta essere un ideale non nullo di R con due fattorizzazioni essenzialmente diverse in prodotto di ideali primi. Questo è escluso dal [Teorema 12.7](#). Otteniamo così una contraddizione, il che completa la dimostrazione. \square

Segue del [Teorema 12.7](#) anche una semplice descrizione degli ideali primari e delle decomposizioni primarie minimali di ideali negli anelli di Dedekind; come [già osservato](#) nel caso di \mathbb{Z} (ma più in generale lo stesso discorso si sarebbe potuto adattare a tutti gli anelli principali, per i quali la descrizione degli ideali primari è analoga, come indicato nell'[Esercizio 7.A.1](#)) le decomposizioni primarie minimali in questi anelli si possono identificare con le fattorizzazioni in prodotti di potenze di (ideali) primi a due a due distinti.

Proposizione 12.9. *Sia R un anello di Dedekind. Allora:*

- (i) *gli ideali primari di R sono tutte e solo le potenze degli ideali primi con esponenti positivi;*
- (ii) *se H è un ideale non banale di R , allora H ha, a meno dell'ordine dei fattori, un'unica decomposizione primaria minimale, ovvero $\mathcal{D} = \{P_1^{\lambda_1}, P_2^{\lambda_2}, \dots, P_n^{\lambda_n}\}$, dove $H = P_1^{\lambda_1} P_2^{\lambda_2} \dots P_n^{\lambda_n}$ è una fattorizzazione di H in prodotto di potenze di ideali primi a due a due distinti; più precisamente: per ogni $i, j \in \{1, 2, \dots, n\}$, $0 \neq P_i \in \text{Spec}(R)$, $\lambda_i \in \mathbb{N}^+$ e, se $i \neq j$, allora $P_i \neq P_j$.*

Dimostrazione. Iniziamo dalla (i). Sia Q un ideale primario di R . Se $Q = 0$ allora Q è (potenza di) primo. Se $Q \neq 0$, invece, $P = \sqrt{Q}$ è un ideale massimale, in quanto ideale primo non nullo di R , quindi è l'unico ideale primo di R contenente Q , vale a dire: l'unico divisore primo di Q in $\mathfrak{I}^*(R)$. Pertanto Q è una potenza di P . Viceversa, sia $\lambda \in \mathbb{N}^+$. Ovviamente $0 = 0^\lambda$ è primo; se poi $0 \neq P \in \text{Spec}(R)$, allora $P = \sqrt{P^\lambda} \triangleleft R$ per il [Teorema 12.7](#), quindi P^λ è P -primario. La (i) è così dimostrata.

Per provare la (ii), sia $0 \neq H \triangleleft R$ e sia $\mathcal{D} = \{Q_1, Q_2, \dots, Q_n\}$ una decomposizione primaria minimale di H , dove gli ideali Q_i sono a due a due distinti. Come segue da (i), per ogni $i \in \{1, 2, \dots, n\}$ abbiamo $Q_i = P_i^{\lambda_i}$, dove $P_i = \sqrt{Q_i}$ e $\lambda_i \in \mathbb{N}^+$. Essendo i radicali P_i a due a due distinti e quindi comassimali in R , anche gli ideali Q_i sono a due a due comassimali, sicché $H = Q_1 Q_2 \dots Q_n = P_1^{\lambda_1} P_2^{\lambda_2} \dots P_n^{\lambda_n}$. Questa è una fattorizzazione di H come prodotto di primi e, come sappiamo dal [Teorema 12.7](#), questa è unica a meno dell'ordine dei fattori. Da ciò segue l'asserto. \square

A proposito di quest'ultimo enunciato, è anche evidente che se $0 \neq P \in \text{Spec}(R)$ e $n, m \in \mathbb{N}$, allora $P^n = P^m$ se e solo se $n = m$. Inoltre, poiché gli anelli di Dedekind hanno dimensione al più 1, l'unicità della decomposizione primaria si può anche far seguire, in modo diretto, dall'[Esercizio 7.C.4](#).

12.2.1 Alcune caratterizzazioni e loro conseguenze

Presentiamo qui altre tre caratterizzazioni degli anelli di Dedekind. Le prime due portano immediatamente ad alcune conseguenze strutturali; la terza avrà conseguenze molto importanti che verranno discusse in un capitolo successivo.

Invertibilità di primi

Per verificare che un dominio di integrità unitario sia di Dedekind basta verificare che siano invertibili gli ideali primi non nulli. Si ha infatti:

Lemma 12.10. *Sia R un dominio di integrità unitario. Allora l'insieme degli ideali non invertibili di R ha elementi massimali rispetto all'inclusione, e ciascuno di essi è un ideale primo.*

Dimostrazione. Sia \mathcal{S} l'insieme degli ideali di R che non sono invertibili; tra questi c'è l'ideale nullo, quindi $\mathcal{S} \neq \emptyset$. L'unione di una qualsiasi catena di elementi di \mathcal{S} è ancora un elemento di \mathcal{S} : se non lo fosse sarebbe un ideale finitamente generato (per la [Proposizione 12.5](#)), quindi dovrebbe essere il massimo della catena stessa, dunque un elemento di \mathcal{S} . Pertanto \mathcal{S} è induttivo ed il Lemma di Zorn assicura l'esistenza di elementi massimali in \mathcal{S} . Sia P uno di essi, dobbiamo mostrare che P è un ideale primo. Ovviamente $P \neq R$, dal momento che $R \notin \mathcal{S}$. Ragionando per assurdo, supponiamo che P non sia primo. Allora esiste $a \in R \setminus P$ tale che $(P : a)_R \neq P$, dunque P è propriamente contenuto sia in $P + aR$ che in $(P : a)$ e, per la massimalità di P , né $P + aR$ né $(P : a)$ sono in \mathcal{S} . Questi due ideali sono dunque invertibili. Poiché gli ideali principali sono invertibili, è di conseguenza invertibile anche $(P : a)aR = P \cap aR$. Siamo così in condizione di utilizzare il [Corollario 11.10](#): per la [Proposizione 12.5](#) sia $P + aR$ che $P \cap aR$

sono proiettivi, dunque P è proiettivo e di conseguenza invertibile. Questa è una contraddizione, perché fornisce $P \notin \mathcal{S}$. È così provato che P è primo.¹ \square

Corollario 12.11. *Sia R un dominio di integrità unitario. Allora R è di Dedekind se e solo se ogni suo ideale primo non nullo è invertibile.*

Dimostrazione. Il [Lemma 12.10](#) garantisce che R ha un ideale massimale P tra quelli non invertibili, e questo è certamente primo. Se ogni ideale primo non nullo di R è invertibile, allora $P = 0$ e quindi ogni ideale non nullo di R è invertibile, dunque R è di Dedekind. L'implicazione inversa è ovvia. \square

Ulteriore conseguenza di questo corollario è che gli ideali primi in un dominio di integrità unitario determinano anche la proprietà di essere o meno un anello principale.

Corollario 12.12. *Sia R un dominio di integrità unitario. Allora R è un anello principale se e solo se ogni suo ideale primo è principale.*

Dimostrazione. Gli ideali principali non nulli sono invertibili, quindi, se ogni ideale primo di R è principale, allora R è di Dedekind per il [Corollario 12.11](#). Ma allora ogni ideale non nullo di R è prodotto di ideali primi, quindi principali, e dunque è esso stesso principale. \square

In effetti la conclusione di quest'ultimo corollario vale non solo nell'ipotesi che R sia integro. Infatti è stato dimostrato (R. Gilmer, 1969) che *se R è un anello commutativo unitario ed ogni ideale primo di R è principale, tutti gli ideali di R sono principali*. Questo risultato non vale per anelli non unitari, come è facile riconoscere considerando anelli commutativi a prodotto costante nullo.

Il [Corollario 12.12](#) ha sua volta altri sviluppi; come stiamo per vedere utilizzando quel poco di teoria degli anelli di Dedekind già sviluppata è possibile, ad esempio, anche caratterizzare gli anelli principali tra quelli fattoriali.

Proposizione 12.13. *Per un dominio di integrità unitario R sono equivalenti:*

- (i) ogni ideale primo di R è principale;
- (ii) R è principale;
- (iii) R è fattoriale e di Dedekind;
- (iv) R è fattoriale ed ha dimensione al più 1.

Dimostrazione. Le implicazioni (i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) sono già note. Valga la (iv) e sia $0 \neq P \in \text{Spec}(R)$. Se $0 \neq Q \in \text{Spec}(R)$ e $Q \subseteq P$, allora $Q = P$ perché $Q \triangleleft R$. Dunque P è minimale tra gli ideali primi non nulli di R e quindi è principale per il [Corollario 3.12](#); ciò prova la (i). A questo punto la dimostrazione è completa. \square

Vediamo così, in particolare, che per un anello di Dedekind le proprietà di essere un anello fattoriale e di essere un anello principale sono equivalenti. Questo fatto è di gran significato, ad esempio, per la teoria dei numeri; ci torneremo [più avanti](#).

Prodotti di primi

Passiamo ora ad un'altra caratterizzazione: dimostreremo che ogni dominio di integrità unitario in cui tutti gli ideali propri siano prodotti di ideali primi è un anello di Dedekind. A questo scopo introduciamo un lemma che prova l'unicità della fattorizzazione di un ideale in prodotto di ideali primi che siano cancellabili.

¹ Una dimostrazione alternativa è suggerita nell'[Esercizio 12.B.3](#)

Lemma 12.14. *Siano R un anello commutativo ed H un suo ideale proprio. Allora le eventuali fattorizzazioni di H in prodotto di ideali primi che siano cancellabili in $\mathfrak{I}(R)$ sono essenzialmente uguali, vale a dire: differiscono tra loro solo per l'ordine dei fattori.*

Dimostrazione. Supponiamo $H = P_1 P_2 \cdots P_s = Q_1 Q_2 \cdots Q_t$, dove $s, t \in \mathbb{N}$ e $P_1, P_2, \dots, P_s, Q_1, Q_2, \dots, Q_t$ sono ideali primi di R che siano elementi cancellabili nel semigruppato (moltiplicativo) degli ideali di R . Sia P un elemento minimale di $\{P_1, P_2, \dots, P_s, Q_1, Q_2, \dots, Q_t\}$ (rispetto all'inclusione). Senza perdere in generalità possiamo assumere $P = P_h$ per un $h \in \{1, 2, \dots, s\}$. Allora $P \supseteq H = Q_1 Q_2 \cdots Q_t$ e quindi $P \supseteq Q_k$ per un $k \in \{1, 2, \dots, t\}$. Ora, la minimalità di P implica $P = Q_k$. Poiché P è cancellabile rispetto al prodotto tra ideali, abbiamo anche $H_1 := \prod_{i=1, i \neq h}^s P_i = \prod_{i=1, i \neq k}^t Q_i$. Ragionando per induzione sul numero $s + t$ dei fattori coinvolti nelle fattorizzazioni, possiamo assumere che queste ultime due fattorizzazioni dell'ideale H_1 differiscano tra loro solo per l'ordine dei fattori, e da ciò si ricava subito la stessa conclusione per le due fattorizzazioni originali di H . \square

Questo lemma si applica, in particolare, al caso in cui R sia un dominio di integrità unitario ed H ne sia un ideale invertibile. In questo caso, infatti, se $H = P_1 P_2 \cdots P_s$ dove ciascuno dei P_i è un ideale primo di R , allora anche i P_i , essendo divisori di H in $\mathfrak{I}^*(R)$, saranno ideali invertibili di R , e quindi certamente cancellabili in $\mathfrak{I}(R)$.

Teorema 12.15. *Sia R un dominio di integrità unitario. Allora R è un anello di Dedekind se e solo se ogni ideale non nullo di R è prodotto di ideali primi.*

Dimostrazione. Una implicazione è già nota dal [Teorema 12.7](#); proveremo l'altra. Supponiamo dunque che ogni ideale di R sia prodotto di ideali primi. Supponiamo anche di sapere che:

$$\text{ogni ideale primo invertibile di } R \text{ è un ideale massimale.} \quad (*)$$

Siano P un ideale primo non nullo di R e $a \in P \setminus 0$. Per ipotesi, $aR = P_1 P_2 \cdots P_n$ per opportuni ideali primi P_1, P_2, \dots, P_n . Essendo aR invertibile, anche i suoi divisori P_i sono invertibili, e quindi massimali per (*). Inoltre $P \supseteq aR = P_1 P_2 \cdots P_n$, quindi esiste $i \in \{1, 2, \dots, n\}$ tale che $P \supseteq P_i$. Ma abbiamo appena osservato che P_i è massimale, quindi $P = P_i$; come ulteriore conseguenza, P è invertibile. Abbiamo provato che, se, oltre l'ipotesi, vale (*), ogni ideale primo non nullo di R è invertibile, quindi R è di Dedekind per il [Corollario 12.11](#).

Basterà allora provare (*). A questo scopo, sia P un ideale primo ed invertibile di R . Se P non è massimale esiste $a \in R \setminus P$ tale che $P + aR \neq R$. Per ipotesi, gli ideali $P + aR$ e $P + a^2R$ sono entrambi prodotti di ideali primi: esistono dunque ideali primi P_1, P_2, \dots, P_r e Q_1, Q_2, \dots, Q_s , tutti contenenti P , tali che $P + aR = P_1 P_2 \cdots P_r$ e $P + a^2R = Q_1 Q_2 \cdots Q_s$. Indichiamo con $\bar{}$ le immagini mediante l'epimorfismo canonico $R \rightarrow \bar{R} := R/P$. Gli ideali $\bar{P}_i = P_i/P$ e $\bar{Q}_j = Q_j/P$ sono ovviamente ancora primi, ed si ha $\bar{a}\bar{R} = \bar{P}_1 \bar{P}_2 \cdots \bar{P}_r$ e $\bar{a}^2\bar{R} = \bar{Q}_1 \bar{Q}_2 \cdots \bar{Q}_s$. Dunque, l'ideale (principale, e dunque invertibile) $\bar{a}^2\bar{R}$ del dominio di integrità \bar{R} ha due fattorizzazioni in prodotto di primi: quella appena data e quella ricavabile dalla fattorizzazione di $\bar{a}\bar{R}$, cioè $\bar{a}^2\bar{R} = (\bar{a}\bar{R})^2 = \bar{P}_1^2 \bar{P}_2^2 \cdots \bar{P}_r^2$. Per il [Lemma 12.14](#) queste due fattorizzazioni possono differire solo per l'ordine dei fattori, quindi $s = 2r$ e, a meno di riordinare gli ideali Q_j , possiamo assumere, per ogni $i \in \{1, 2, \dots, r\}$, $\bar{P}_i = \bar{Q}_{2i-i} = \bar{Q}_{2i}$. Ma, ricordiamo, sia gli ideali P_i che i Q_j contengono P , quindi, $\bar{P}_i = \bar{Q}_j$ è, per ogni scelta degli indici, equivalente a $P_i = Q_j$. La conclusione è che, per ogni $i \in \{1, 2, \dots, r\}$, si ha $P_i = Q_{2i-i} = Q_{2i}$, ne segue $P + a^2R = \prod_{j=1}^{2r} Q_j = (\prod_{i=1}^r P_i)^2 = (P + aR)^2$. Dal momento che $(P + aR)^2 = P^2 + aP + a^2R \subseteq P^2 + aR$, ricaviamo $P^2 \subseteq P \subseteq P^2 + aR$. Applicando la legge modulare di Dedekind ([Lemma 1.8](#)), otteniamo ancora $P = P^2 + (P \cap aR)$. Essendo P primo, $P \cap aR = aP$. Allora $P = P^2 + aP = P(P + aR)$ e quindi, moltiplicando per P^{-1} , $R = P + aR$, contrariamente a quanto assunto. Questa contraddizione prova (*) e completa così la dimostrazione. \square

Corollario 12.16. *Ogni anello di frazioni non nullo di un anello di Dedekind è un anello di Dedekind.*

Dimostrazione. Sia $S^{-1}R$ un anello di frazioni dell'anello di Dedekind R . Ogni ideale proprio di $S^{-1}R$ è l'espansione di un ideale di R , ha quindi la forma H^e per un opportuno ideale proprio H di R . Poiché R è di Dedekind, $H = P_1P_2\cdots P_n$ per opportuni $P_1, P_2, \dots, P_n \in \text{Spec}(R)$. Allora $H^e = P_1^e P_2^e \cdots P_n^e$, e ciascuno degli ideali P_i^e o è primo in $S^{-1}R$ oppure coincide con $S^{-1}R$ (e in questo caso non contribuisce alla fattorizzazione). Dunque, H^e è prodotto di ideali primi in $S^{-1}R$. Per il [Teorema 12.15](#) possiamo concludere che, se non è nullo, $S^{-1}R$ è di Dedekind.² \square

Esercizi e Osservazioni.

12.B.1. Dedurre la conclusione dell'[Esercizio 12.A.4](#) dal [Lemma 12.6](#), dopo aver provato che H non divide $x\mathbb{Z}[x]$.

12.B.2. È possibile dimostrare, ma la cosa richiede più teoria di quanta ne abbiamo sviluppato qui, che vale una forma più forte del [Teorema 12.7](#). Si ha infatti che se R è un dominio di integrità unitario e $\mathfrak{J}^*(R)$ è un monoide fattoriale, allora R è un anello di Dedekind.

12.B.3. Dimostrare in modo alternativo il [Lemma 12.10](#) utilizzando il [Lemma 12.6](#) per provare che, con le notazioni usate nella dimostrazione del [Lemma 12.10](#), ogni elemento massimale P di \mathfrak{S} è primo. Suggerimento: si tratta di escludere che si possa avere $IJ \subseteq P$ per ideali I, J di R propriamente contenenti P .

12.B.4. Il [Lemma 12.14](#) si può equivalentemente riformulare così: se R è un anello commutativo e H un ideale cancellabile in $\mathfrak{J}(R)$, allora H ha, a meno dell'ordine dei fattori, al massimo una fattorizzazione in prodotto di ideali primi. Questo perché, come osservato nell'[Esercizio 2.C.4](#), gli elementi cancellabili in un semigrupp commutativo costituiscono una parte chiusa satura.

12.B.5. Sia R un dominio di integrità unitario, sia $H \triangleleft R$ e sia $\emptyset \neq S \subseteq R$. Provare che se H è invertibile, allora l'espansione di H in $S^{-1}R$ è invertibile (come ideale di $S^{-1}R$). Ricavare una dimostrazione alternativa del [Corollario 12.16](#).

Un teorema di Emmy Noether

Passiamo ora ad un terzo, importantissimo, teorema di caratterizzazione degli anelli di Dedekind come domini di integrità unitari noetheriani, integralmente chiusi e di dimensione al più 1. Questo risultato è essenzialmente dovuto ad Emmy Noether, che iniziò negli anni venti del novecento lo studio sistematico degli anelli di Dedekind. In realtà la procedura seguita da Noether è inversa rispetto a quella seguita in queste note: lei assunse una variante di questa proprietà (precisamente quella di essere un dominio di integrità noetheriano, integralmente chiuso a quozienti propri artiniani) come definizione degli anelli di Dedekind e ne dedusse le proprietà di invertibilità e di fattorizzazione per i loro ideali.

Premettiamo all'enunciato del teorema di Noether una semplice osservazione generale sugli ideali degli anelli noetheriani.

Lemma 12.17. *Sia R un anello commutativo unitario noetheriano. Allora ogni ideale non nullo di R contiene un prodotto di ideali primi non nulli.*

² per una dimostrazione diversa si veda l'[Esercizio 12.B.5](#).

Dimostrazione. Sia $0 \neq H \triangleleft R$. Se $H = R$ è chiaro che H contiene un ideale primo. Se invece $H \neq R$, allora H ha una decomposizione primaria $\mathcal{D} = \{Q_1, Q_2, \dots, Q_n\}$ (Teorema 7.12) e, per il Corollario 3.16, per ciascun i , se $P_i = \sqrt{Q_i}$, esiste $\lambda_i \in \mathbb{N}$ tale che $P_i^{\lambda_i} \subseteq Q_i$. Dunque $H \supseteq Q_1 Q_2 \cdots Q_n \supseteq P_1^{\lambda_1} P_2^{\lambda_2} \cdots P_n^{\lambda_n}$, la qual cosa prova l'asserto dal momento che ciascuno degli ideali P_i è primo. \square

Teorema 12.18. *Per un dominio di integrità unitario noetheriano R sono equivalenti:*

- (i) R è di Dedekind;
- (ii) ogni localizzazione di R ad un ideale massimale è un anello di valutazione;
- (iii) R è integralmente chiuso ed ha dimensione al più 1.

Dimostrazione. Indichiamo con K il campo dei quozienti di R . Se R è di Dedekind e $S^{-1}R$ è una sua localizzazione non nulla, allora anche $S^{-1}R$ è un anello di Dedekind, per il Corollario 12.16, ed ha un unico ideale massimale M . Ma allora tutti gli ideali non banali di $S^{-1}R$ sono potenze di M e quindi sono confrontabili tra loro. Per questo motivo $S^{-1}R$ è un anello di valutazione; è così provato che (i) implica (ii).

Supponiamo ora che valga (ii). Segue immediatamente dalle proposizioni 9.12 e 10.17 che la chiusura intera di R in K è proprio R , vale a dire: R è integralmente chiuso. Se poi $0 \neq P \in \text{Spec}(R)$ e $P \subseteq M \triangleleft R$, allora il Teorema 9.9 mostra che l'espansione P^e di P nella localizzazione R_M di R a M è un ideale primo non nullo in R_M . Ma R_M è per ipotesi un anello noetheriano di valutazione (ricordiamo dal Corollario 9.6 che gli anelli di frazioni degli anelli noetheriani sono essi stessi noetheriani) e quindi un anello principale, come mostrato dal Corollario 10.15. Allora P^e è massimale in R_M , dunque coincide con M^e , l'unico ideale massimale di R_M . Ma allora, sempre per il Teorema 9.9, $P = M$. Abbiamo così provato che ogni ideale primo non nullo di R è massimale, ovvero: R ha dimensione al più 1. È pertanto vero che (ii) implica (iii).

Supponiamo infine che valga (iii). Sia $0 \neq P \in \text{Spec}(R)$; in accordo col Corollario 12.11, per provare che R è di Dedekind basta verificare che P è invertibile. Ragionando per assurdo, supponiamo che ciò non sia vero, dunque $P(R : P)_K \neq R$. Per ipotesi, P è massimale e ovviamente $P \subseteq P(R : P)_K \subseteq R$, dunque $P(R : P)_K = P$. Allora, per ogni $c \in (R : P)_K$, si ha $Pc \subseteq P$, vale a dire: la moltiplicazione in K induce per restrizione un'operazione esterna che struttura P come modulo su $R[c]$. Questo modulo è ovviamente fedele e, visto come R -modulo, cioè come ideale di R , è finitamente generato perché R è noetheriano. È così soddisfatta per c ed R la condizione (iii) del Lemma 10.3, quindi c è intero su R . Ma R è integralmente chiuso, dunque $c \in R$. Abbiamo provato: $(R : P)_K = R$. Fissiamo ora $a \in P \setminus 0$. Per il Lemma 12.17 esistono $n \in \mathbb{N}^+$ ed ideali primi non nulli P_1, P_2, \dots, P_n di R tali che $P_1 P_2 \cdots P_n \subseteq aR$; possiamo supporre che n sia il minimo intero positivo con questa proprietà. Dal momento che $P_1 P_2 \cdots P_n \subseteq P$, almeno uno degli ideali P_1, \dots, P_n , supponiamo sia P_n , è incluso in P . Ma $P_n \triangleleft R$, perché R ha dimensione (al più) 1, quindi $P_n = P$. Da $P_1 P_2 \cdots P_{n-1} P \subseteq aR$ ricaviamo $a^{-1} P_1 P_2 \cdots P_{n-1} P \subseteq R$, ovvero $a^{-1} P_1 P_2 \cdots P_{n-1} \subseteq (R : P)_K = R$ e quindi $P_1 P_2 \cdots P_{n-1} \subseteq aR$, contraddicendo così la minimalità di n . Questa contraddizione completa la dimostrazione. \square

12.3 Ideali in anelli di Dedekind

Il fatto che gli ideali non nulli di un anello di Dedekind costituiscono un monoide fattoriale permette di operare su di essi con tecniche elementari di uso frequente in aritmetica. Un esempio viene dall'utile osservazione che massimi comuni divisori e minimi comuni multipli possono essere facilmente interpretati nel monoide degli ideali di questi anelli.

Lemma 12.19. Sia R un anello di Dedekind e siano I e J due suoi ideali. Allora $I + J$ e $I \cap J$ sono, rispettivamente, il massimo comun divisore ed il minimo comune multiplo tra I e J in $\mathfrak{J}(R)$. In particolare, I e J sono coprimi (in $\mathfrak{J}(S)$) se e solo se sono comassimali (in R). Inoltre, per ogni $L \triangleleft R$ si ha $L(I \cap J) = LI \cap LJ$.

Dimostrazione. L'enunciato è conseguenza dal fatto che, come banalmente segue da [Teorema 12.7](#) (i), la relazione di divisibilità in $\mathfrak{J}(R)$ coincide con l'inclusione inversa. Infatti per questo motivo $I + J$, l'estremo superiore in $(\mathfrak{J}(R), \subseteq)$ tra I e J , è l'estremo inferiore tra I e J rispetto alla divisibilità, cioè l'unico massimo comun divisore nel monoide $\mathfrak{J}(R)$ tra I e J . Inoltre, I e J sono coprimi in $\mathfrak{J}(R)$ se e solo se l'unità R di $\mathfrak{J}(R)$ è il loro massimo comun divisore, ovvero, per quanto appena visto, se e solo se $I + J = R$, cioè se e solo se I e J sono ideali comassimali. In modo duale si prova che $I \cap J$ è il minimo comune multiplo tra I e J in $\mathfrak{J}(R)$. Infine, l'uguaglianza $L(I \cap J) = LI \cap LJ$ è ovvia se uno tra gli ideali I, J, L è nullo; nell'altro caso segue da proprietà immediate dei minimi comuni multipli in monoidi fattoriali: il prodotto tra L ed un minimo comune multiplo tra I e J è un minimo comune multiplo tra LI e LJ . \square

Lemma 12.20. Sia R un anello di Dedekind e sia \mathcal{P} un insieme finito di ideali primi di R . Allora, per ogni $H \in \mathfrak{J}^*(R)$, si ha $H \supseteq \bigcup_{P \in \mathcal{P}} HP$.

Dimostrazione. Ovviamente $H \supseteq \bigcup_{P \in \mathcal{P}} HP$; occorre solo provare che quest'inclusione è stretta. Possiamo chiaramente assumere che \mathcal{P} non contenga l'ideale nullo. Sia $Q = \prod_{P \in \mathcal{P}} P$, il prodotto degli ideali in \mathcal{P} . Per ogni $P \in \mathcal{P}$ si ha $P^{-1}Q \subseteq R$ (notiamo che $P^{-1}Q$ è il prodotto degli ideali in \mathcal{P} diversi da P) e quindi $P^{-1}Q \triangleleft R$. Inoltre, l'essenziale unicità delle fattorizzazioni degli ideali di R in prodotto di primi fornisce $H(P^{-1}Q) \supseteq HQ$, quindi esiste $a_P \in H(P^{-1}Q) \setminus HQ$. Osserviamo anche che, nel monoide $\mathfrak{J}^*(R)$, gli ideali P e $P^{-1}Q$ sono coprimi, quindi il [Lemma 12.19](#) fornisce $HP \cap H(P^{-1}Q) = H(P \cap P^{-1}Q) = HQ$. Di conseguenza $a_P \notin HP$; d'altra parte $a_P \in HP'$ per ogni $P' \in \mathcal{P} \setminus P$, dal momento che per tali P' si ha $P^{-1}Q \subseteq P'$.

Sia ora $a = \sum_{I \in \mathcal{P}} a_I$; ovviamente $a \in H$. Scelto comunque $P \in \mathcal{P}$, gli addendi a_I che definiscono a sono tutti in HP ad eccezione di a_P , che non vi appartiene; se ne ricava $a \notin HP$. Dunque $a \in H \setminus \bigcup_{P \in \mathcal{P}} HP$; con ciò il lemma è provato. \square

Uno dei casi in cui è possibile applicare il precedente lemma è quello in cui \mathcal{P} è la varietà di un ideale non nullo. Abbiamo infatti:

Lemma 12.21. Sia R un anello di Dedekind e sia $H \in \mathfrak{J}^*(R)$. Allora l'insieme degli ideali di R contenenti H è finito. In altri termini: $\mathfrak{J}(R/H)$ è finito.

Dimostrazione. In un monoide fattoriale, ogni elemento ha, a meno di associati, solo un numero finito di divisori. Dal momento che, come mostra il [Teorema 12.7](#), in $\mathfrak{J}^*(R)$ i divisori di H sono precisamente gli ideali che lo contengono e la relazione 'essere elementi associati' è l'identità, questo basta a provare l'asserto. \square

Ovvia conseguenza del [Lemma 12.21](#) è che *i quozienti propri degli anelli di Dedekind sono tutti artiniani*, cosa che del resto è vera per tutti i domini di integrità unitari noetheriani di dimensione al più uno (si veda l'[Esercizio 8.A.4](#)).

Se H è un ideale non nullo di un anello di Dedekind R , è ovvio che H ha qualche multiplo in $\mathfrak{J}^*(R)$ che è un ideale principale non nullo: scelto comunque $a \in H \setminus 0$, il punto (i) del [Teorema 12.7](#) mostra che $HJ = aR$ per qualche $J \in \mathfrak{J}^*(R)$. Il prossimo lemma mostra che J può essere scelto coprimo con un arbitrario prefissato ideale non nullo.

Lemma 12.22. Siano R un anello di Dedekind e $H, I \in \mathfrak{J}^*(R)$. Allora esiste $J \in \mathfrak{J}^*(R)$ tale che HJ sia principale e $I + J = R$.

Dimostrazione. Sia $\mathcal{V} = \text{Var}(I)$, l'insieme degli ideali primi di R contenenti I . Per i lemmi 12.20 e 12.21, esiste $a \in H \setminus \bigcup_{P \in \mathcal{V}} HP$. Ora, $HJ = aR$ per un opportuno $J \in \mathfrak{I}^*(R)$. Se $I + J$ fosse un ideale proprio, esisterebbe un ideale massimale P contenente $I + J$; si avrebbe allora $I \subseteq P$ e quindi $P \in \mathcal{V}$, ma anche $J \subseteq P$ e quindi $aR = HJ \subseteq HP$, in contraddizione con la scelta di a . Quindi $I + J = R$ e la dimostrazione è completa.³ \square

Proposizione 12.23. *Sia R un anello di Dedekind semilocale (cioè con solo un numero finito di ideali primi). Allora R è un anello principale.*

Dimostrazione. Sia $H \in \mathfrak{I}^*(R)$, sia \mathcal{S} l'insieme degli ideali primi non nulli di R e sia $I = \prod_{P \in \mathcal{S}} P$. Per il Lemma 12.22 esiste $J \in \mathfrak{I}^*(R)$ tale che HJ sia principale e $I + J = R$. Quest'ultima condizione e la scelta di I comportano che J non è contenuto in alcun ideale primo di R , quindi $J = R$, dunque $H = HJ$ è principale. Ciò mostra che R è un anello principale. \square

Arriviamo ora ad un importante risultato: in un arbitrario anello di Dedekind i quozienti propri sono tutti anelli ad ideali principali e gli ideali sono sempre generati da al più due elementi, uno dei quali può essere scelto in modo arbitrario.

Teorema 12.24. *Siano R un anello di Dedekind e H un ideale non nullo di R . Allora:*

- (i) ogni ideale di R/H è principale;
- (ii) per ogni $a \in H \setminus 0$ esiste $b \in H$ tale che $H = aR + bR$.

Dimostrazione. Sia $I/H \triangleleft R/H$. Allora, per il Lemma 12.22, esiste $J \triangleleft R$ tale che IJ sia principale e $R = H + J$. Allora $I = IR = IH + IJ \subseteq H + IJ$, ma $H \subseteq I$, quindi $I = H + IJ$. Allora $I/H = (IJ + H)/H$ è un ideale principale. È così provata la (i).

Sia ora $a \in H \setminus 0$. Allora R/aR è un anello ad ideali principali, per quanto appena provato. Dunque esiste $b \in R$ tale che H/aR sia generato da $b + aR$, vale a dire: $H = aR + bR$. \square

Una dimostrazione alternativa per la parte (i) è nell'Osservazione 12.C.1. Una conseguenza di questo stesso enunciato è il prossimo corollario.

Corollario 12.25. *Siano $I, J \in \mathfrak{I}^*(R)$, dove R è un anello di Dedekind. Allora*

- (i) $I/IJ \simeq_R R/J$;
- (ii) $|R/IJ| = |R/I| \cdot |R/J|$.

Dimostrazione. Per il Teorema 12.24, il quoziente I/IJ è un R -modulo ciclico, quindi isomorfo a $R/\text{Ann}_R(I/IJ)$. Ora, $\text{Ann}_R(I/IJ) = (IJ : I)_R = I^{-1}IJ = J$ per il Lemma 12.4; si ottiene così (i). Poiché $|R/IJ| = |R/I| \cdot |I/IJ|$, la (ii) ne è una ovvia conseguenza. \square

³ L'ultimo passo si potrebbe esprimere, più sinteticamente così: i divisori primi di J moltiplicati per H dividono aR , quindi tali divisori non possono essere in \mathcal{V} , dunque I e J sono coprimi in $\mathfrak{I}^*(R)$, ovvero comassimali.

Osservazioni.

12.C.1. Si potrebbe esser tentati dal dimostrare il [Teorema 12.24](#) ragionando (per la parte (i)) in questo modo: sappiamo che R/H ha un numero finito di ideali, quindi è certamente semilocale; allora i suoi ideali sono principali per la [Proposizione 12.23](#). Naturalmente quest'argomentazione è fallace: non è vero (a meno che H non sia primo) che R/H sia un anello di Dedekind. Però qualcosa di questa idea si può salvare ragionando in questo modo: siano $\mathcal{V} = \text{Var}(H)$, l'insieme dei divisori primi di H , e $S = R \setminus \bigcup \mathcal{V}$. Allora S è un sotto-monoide di (R, \cdot) e, per il [Corollario 12.16](#), $S^{-1}R$ è un anello di Dedekind. Inoltre, per il [Corollario 9.14](#), $S^{-1}R$ è semilocale, dunque $S^{-1}R$ è principale, per la [Proposizione 12.23](#). D'altra parte, $S = \{r \in R \mid r + H \in \mathcal{U}(R/H)\}$ è l'insieme degli elementi di R che sono invertibili modulo H . Di conseguenza, R/H è isomorfo ad un quoziente di $S^{-1}R$ (anche se non è necessario, si può osservare che $R/H = (S + H/R)^{-1}(R/H) \simeq S^{-1}R/H^e$, per il [Lemma 9.7](#)). Di conseguenza, ogni ideale di R/H è principale.

12.C.2. È stato dimostrato che vale anche l'inverso del [Teorema 12.24](#), vale a dire: *un dominio di integrità unitario R è di Dedekind se e solo se in ogni suo quoziente proprio ha tutti gli ideali principali.*

13 Argomenti vari

13.1 Condizioni minimale e condizione massimale per insiemi ordinati

Sia (S, \preccurlyeq) un insieme ordinato. Si dice che (S, \preccurlyeq) verifica la *condizione minimale* se e solo se \preccurlyeq verifica una di queste condizioni, tra loro equivalenti:

- (i) ogni parte non vuota di S ha elementi minimali rispetto a \preccurlyeq ;¹
- (ii) ogni catena in (S, \preccurlyeq) è ben ordinata;
- (iii) ogni catena non vuota in (S, \preccurlyeq) ha minimo;
- (iv) ogni successione decrescente da (\mathbb{N}, \leq) a (S, \preccurlyeq) è definitivamente costante, vale a dire: ha immagine finita;²
- (v) non esistono successioni strettamente decrescenti da (\mathbb{N}, \leq) a (S, \preccurlyeq) .

Il fatto che queste condizioni siano effettivamente equivalenti tra loro è molto semplice da provare; l'unica implicazione forse non totalmente ovvia è quella da (v) a (i), che si può verificare così: se una parte non vuota X di S non ha elementi \preccurlyeq -minimali si può definire ricorsivamente una successione strettamente decrescente $(a_n)_{n \in \mathbb{N}} \in S^{\mathbb{N}}$, a valori in X , scegliendo a_0 in modo arbitrario in X e, supposto (per un arbitrario $n \in \mathbb{N}$) definito $a_n \in X$, scegliendo come a_{n+1} un qualsiasi elemento di X tale che $a_{n+1} \prec a_n$; un tale elemento esiste certamente altrimenti a_n sarebbe minimale in (X, \preccurlyeq) . Ciò prova che la negazione di (i) implica la negazione di (v).

Si definisce in modo duale la *condizione massimale*: dire che (S, \preccurlyeq) verifica la condizione massimale significa dire che l'insieme ordinato duale (S, \succcurlyeq) verifica la condizione minimale, ovvero che (S, \preccurlyeq) verifica queste condizioni, tra loro equivalenti:

- (i) ogni parte non vuota di S ha elementi massimali rispetto a \preccurlyeq ;
- (ii) ogni catena non vuota in (S, \preccurlyeq) ha massimo;
- (iii) ogni successione crescente da (\mathbb{N}, \leq) a (S, \preccurlyeq) è definitivamente costante;
- (iv) non esistono successioni strettamente crescenti da (\mathbb{N}, \leq) a (S, \preccurlyeq) .

Ci si riferisce informalmente a ciascuna delle due condizioni minimale e massimale appena definite, come ad una 'condizione di catena'.

È ovvio che tutti gli insiemi ordinati finiti verificano sia la condizione minimale che la condizione massimale (ma non vale il viceversa: qualsiasi insieme, ordinato dalla relazione di uguaglianza, verifica sia la condizione minimale che quella massimale), che ogni sottoinsieme ordinato³ di un insieme ordinato che verifichi una condizione di catena verifica la stessa condizione, che gli insiemi ben ordinati siano precisamente gli insiemi totalmente ordinati a condizione minimale. Sono esempi di insiemi ordinati a condizione minimale quelli dei naturali ordinati dall'ordinamento naturale o per divisibilità.

Lo studio delle strutture in cui insiemi di sottostrutture, ordinati per inclusione dei sostegni, verifichino una condizione di catena è di grande importanza in quasi ogni settore dell'algebra.

¹ vale a dire; \preccurlyeq è una relazione ben fondata.

² in termini ancora più espliciti, dire che una successione $(a_n)_{n \in \mathbb{N}}$ è definitivamente costante significa che esiste $n \in \mathbb{N}$ tale che $a_{n+t} = a_n$ per ogni $t \in \mathbb{N}$.

³ cioè ordinato dall'ordinamento indotto.