7 Fattorizzazione — Anelli di Dedekind

In questo capitolo rivisiteremo la teoria elementare della divisibilità e della fattorizzazione nei monoidi, per arrivare a discutere un'importante classe di domini di integrità noetheriani, quella degli anelli di Dedekind.

7.1 Richiami sulla fattorizzazione in monoidi commutativi

Ricordiamo un pò 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 $\mathrm{Div}_M(a)$ 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 7.1. *Per ogni $a, b \in M$ sono equivalenti:*
(i) $a \sim_M b$; (ii) $\mathrm{Div}_M(a) = \mathrm{Div}_M(b)$; (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 $\widetilde{M}$. Per brevità, scriveremo spesso $\tilde{a}$ per la classe $[a]_{\sim_M}$ degli elementi associati di 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 $\mathrm{Div}_M(a) = \mathcal{U}(M) \cup [a]_{\sim_M}$ (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 7.A.3). È altrettanto facile verificare che ciascuna delle proprietà di essere invertibile, irriducibile, primo è invariante per il pasaggio 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 $\widetilde{M}$.

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.
F_2): ogni elemento non invertibile di M è prodotto di irriducibili, ed ogni irriducibile è primo.

[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 $(\mathbb{Z}, \cdot)$.

F$_3$): 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.

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

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

7.A.3. Sia P il sottomonoide 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.

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

i) ogni divisore di a è cancellabile;

ii) due qualsiasi fattorizzazioni di a come prodotto di primi in M sono essenzialmente uguali.

7.2 Una caratterizzazione dei monoidi fattoriali in termini di ordinamenti

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 $M/{\sim_M} = \widetilde{M}$ dalla divisibilità in M non è altro che la relazione di divisibilità in $\widetilde{M}$, che è così un ordinamento, in accordo col fatto che $\widetilde{M}$ ha un unico elemento invertibile, il suo elemento neutro $\tilde{1}$ (a questo proposito può essere utile esaminare l'Osservazione 7.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 $\widetilde{M}$. 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 $\widetilde{M}$. Poiché la divisibilità è una relazione d'ordine in $\widetilde{M}$ quest'ultima affermazione equivale a dire che $\tilde{d}$ è l'estremo inferiore di $\{\tilde{a}, \tilde{b}\}$ nell'insieme ordinato $(\widetilde{M}, |)$. 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 $(\widetilde{M}, |)$.

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

Ci occupiamo ora del problema dell'esistenza o meno di un MDC 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 $\widetilde{M}$, ordinato per divisibilità, è un reticolo. Dimostreremo che questa proprietà è non lontana dal caratterizzare i monoidi fattoriali.

L'esistenza di MCD e l'esistenza di mcm in un monoide commutativo non sono affatto condizioni indipendenti tra loro, come stiamo per verificare. 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 $a|b$.

Proposizione 7.2. *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 $\left[\frac{n}{m}\right]e = d$, 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 $a\left[\frac{b}{d}\right] = b\left[\frac{a}{d}\right]$, 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 $n_1\left[\frac{m}{n_1}\right]d = ab = n_1\left[\frac{a}{n_1}\right]b$, da cui $\left[\frac{m}{n_1}\right]d = \left[\frac{a}{n_1}\right]b$. Quindi $e := \left[\frac{m}{n_1}\right]d|b$; 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 $\left[\frac{m}{n_1}\right] = \left[\frac{e}{d}\right]$ 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. □

Può sorprendere la mancanza di simmetria tra le due parti dell'enunciato della Proposizione 7.2: 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 7.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 7.3. *Se M è un monoide commutativo cancellativo, sono equivalenti le proprietà:*
(i) *$\widetilde{M}$, 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: $\widetilde{M}$ è un inf-semireticolo).*
(iii) *Per ogni $a, b \in M$, esiste un mcm tra a e b in M (vale a dire: $\widetilde{M}$ è un sup-semireticolo).*

Assumendo che M sia cancellativo, l'ipotesi che $\widetilde{M}$ sia un reticolo, ovvero che in M ogni coppia di elementi abbia un MCD, implica che ogni irriducibile in M è primo. Il primo passo per la dimostrazione è questo lemma:

Lemma 7.4. *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 $e \sim_M cd$.*

Dimostrazione. Ovviamente dc è un divisore comune ad ac e bc, quindi $dc|e$. Da $e = dc\left[\frac{e}{dc}\right]|ac$ segue, cancellando c, $d\left[\frac{e}{dc}\right]|a$. 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 $e \sim_M cd$. □

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 7.B.5.

Lemma 7.5. *Sia M un monoide cancellativo e supponiamo che $\widetilde{M}$, 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 $\tilde{1} = \tilde{a} \wedge \tilde{p}$, dunque $\tilde{b} = \widetilde{ab} \wedge \widetilde{pb}$, per il Lemma 7.4. Ma p divide sia ab che pb, quindi $p|b$. È così provato che p è primo. □

Lemma 7.6. *Sia M un monoide cancellativo e supponiamo che $\widetilde{M}$, 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, $S \neq \varnothing$ e quindi $\widetilde{S} = \{\tilde{a} \mid a \in S\} \neq \varnothing$. Esiste allora $a \in M$ tale che $\tilde{a}$ sia minimale (rispetto a $|$) in $\widetilde{S}$. 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. □

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

Teorema 7.7. *Sia M un monoide commutativo cancellativo. Allora M è fattoriale se e solo se $\widetilde{M}$, ordinato per divisibilità, è un reticolo a condizione minimale.*

Dimostrazione. Se $\widetilde{M}$ 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 $(\widetilde{M}, |)$ è un

reticolo. Possiamo definire un'applicazione $\tau\colon \widetilde{M} \to \mathbb{N}$, associando a ciascun $\tilde{a} \in \widetilde{M}$ 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 $\tilde{1}^\tau = 0$. Ora, se $\tilde{a}, \tilde{b} \in \widetilde{M}$ 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 $\widetilde{M}$ e $n = \min S^{\vec{\tau}}$, ogni $\tilde{a} \in S$ tale che $\tilde{a}^\tau = n$ è un elemento minimale in S. Questo mostra che $(\widetilde{M}, |)$ verifica la condizione minimale. A questo punto la dimostrazione è completa. □

Corollario 7.8. *Sia M un monoide commutativo cancellativo. Allora M è fattoriale se e solo se $\widetilde{M}$, è fattoriale.*

Dimostrazione. Posto $M_1 = \widetilde{M}$, abbiamo ovviamente $\widetilde{M}_1 \simeq \widetilde{M}$. Dunque, per il Teorema 7.7, $\widetilde{M}$ è fattoriale se e solo se $\widetilde{M}$, ordinato per divisibilità, è un reticolo a condizione minimale, ma, per lo stesso teorema, questo equivale all'essere M fattoriale. □

Infine, richiamiamo un pò di terminologia utile. Se M è fattoriale, i suoi elementi irriducibili sono gli a tali che $\tilde{a}$ sia un *atomo* nel reticolo, cioè un elemento minimale tra quelli diversi dal minimo $\tilde{1}$. Dualmente, in un reticolo con massimo si chiamano *coatomi* gli elementi massimali nel reticolo tra quelli diversi dal massimo.

Esercizi, Esempi, Osservazioni.

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

7.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.

7.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.

Come alcuni dei partecipanti al corso mi hanno fatto notare, si può definire in modo del tutto analogo una struttura con le stesse proprietà sull'insieme $\mathbb{N} \times \mathbb{Z}_2$. In questo caso l'operazione può essere descritta, in modo più sintetico, dall'identità $(u, v) * (s, t) = (u + s, (v + t)0^{u+s})$. Difatti questa struttura è isomorfa ad un quoziente di S.

7.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 $a_0b_0c_0^{-1}d_0^{-1}$ 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 $a := a_0H$, $b := b_0H$, $c := c_0H$, $d := d_0H$, in cui vale l'uguaglianza $ab = cd$. Si provi che ciascuno di a, b, c, d è irriducibile, quindi 1 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 1 è l'unico elemento invertibile di M), ed arrivare alle conclusioni desiderate.

7.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 7.B.4, ma un pò 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 $x_1x_3x_4x_5^{-1}x_6^{-1}$ e $x_2x_3x_4x_5^{-1}x_7^{-1}$. 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 (libero) generato in F da $x_1, \dots, x_7$, e sia $M = PH/H$. Allora M è un monoide commutativo cancellativo. Ponendo $a = x_1x_4H$, $b = x_2x_4H$, $c = x_3H$, si verifichi che $d := x_4H$ 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 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_5H divide ac e bc ma non cd, quindi cd non è un MCD tra ac e bc.

7.3 Applicazioni agli anelli

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 $\varphi\colon a \in R \mapsto aR \in \mathfrak{I}_P(R)$. 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

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

dove abbiamo posto (come faremo d'ora in poi) $\widetilde{R} = R/{\sim_R}$, quoziente del monoide moltiplicativo di R. È anche chiaro che sia $\tilde{\varphi}$ che la sua inversa sono (strettamente) decrescenti, quindi φ è un anti-isomorfismo da $\widetilde{R}$ (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 $\widetilde{R}$, 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

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

Una applicazione piuttosto elegante dell'anti-isomorfismo φ e dei risultatio nella sezione precedente permette di ricavare immediatamente alcuni risultati elementari sugli anelli principali, vediamo come.

Se R è un dominio di integrità unitario, $R^* = R \smallsetminus 0$ è un sottomonoide moltiplicativo di R ed è cancellativo, e $\widetilde{R}^*$ 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). Quindi, dal momento che R è noetheriano, $\mathfrak{I}_P^*(R)$ è un reticolo a condizione massimale; di conseguenza $\widetilde{R}^*$ (anti-isomorfo a $\mathfrak{I}_P^*(R)$) è un reticolo a condizione minimale. Per il Teorema 7.7, 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 fattoriale 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 di chiamano *anelli di Bézout* e verranno brevemente discussi nella sezione 8.1.

Esercizi.

7.C.1. Sia R una anello commutativo unitario. Provare che se R è noetheriano (o, più in generale, verifica la condizione massimale sugli ideali principali), allora ogni elemento non invertibile di R è prodotto di elementi irriducibili.

7.4 Ideali frazionari

In questa sezione, salvo avviso contrario, con R si indicherà un dominio di integrità unitario[3] e $K = Q(R)$ sarà il suo campo dei quozienti.

K ha una ovvia struttura di R-algebra; , quindi di R-modulo; si chiamiano *ideali frazionari* di R gli R-sottomoduli non nulli A di K tali che $(R : A)_R = \mathrm{Ann}_R(A + R/R) \neq 0$, 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:

[3] assumiamo, per definizione, non triviali i domini di integrità, quindi $|R| > 1$.

Lemma 7.9. *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 $0 \neq a \in (R : A)_R$ e $0 \neq b \in (R : B)_R$. 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, $ab \neq 0$ e $Xab \neq 0$, quindi X è un ideale frazionario. Infine, se $0 \neq x \in B$, allora $ax \neq 0$ e $ax(A : B)_K \subseteq R$, quindi $(A : B)_K \in \mathfrak{F}(R)$. □

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 sottomonoide 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 $\mathfrak{F}_P(R)$.

7.10. *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 7.9. □

Il prossimo lemma è tanto semplice quanto utile; esso permette di ridurre molte questioni riguardanti gli ideali frazionari al caso degli ideali interi.

Lemma 7.11. *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 $r^{-1}R \in \mathfrak{U}(\mathfrak{F}(R))$, vediamo che A e A_1 sono associati. Infine, l'applicazione $a \in A \mapsto ar \in A_1$ è un R-isomorfismo. □

Useremo questo lemma per caratterizzare gli ideali frazionari invertibili (cioè gli elementi invertibili di $\mathfrak{F}(R)$). Nelle notazioni del lemma, A è invertibile se e solo se lo è A_1.

Lemma 7.12. *Sia $A \in \mathfrak{F}(R)$. Allora A è invertibile se e solo se $A(R : A)_K = R$. Dunque, se A è invertibile, il suo inverso è $A^{-1} = (R : A)_K$.*

Dimostrazione. Per definizione, $(R : A)_K = \{k \in K \mid Ak \subseteq R\}$, pertanto, se A è invertibile, da $AA^{-1} = R$ segue $A^{-1} \subseteq (R : A)_K$. D'altra parte, da $A(R : A)_K \subseteq R$ moltiplicando per A^{-1} si ottiene $(R : A)_K \subseteq A^{-1}R = A^{-1}$, dunque $A^{-1} = (R : A)_K$. Viceversa, se $A(R : A)_K = R$, allora ovviamente A è invertibile, con inverso $(R : A)_K$. □

Sfrutteremo spesso il precedente lemma in questa formulazione equivalente: A è invertibile se e solo se $1_R \in A(R:A)_K$.

Proposizione 7.13. *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 7.11 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 $a = \sum_{x\in X} xa^{\alpha_x}$ (come di consueto, questa scrittura sottintende che l'insieme degli $x \in X$ tali che $xa^{\alpha_x} \neq 0$ sia finito). Assumendo $a \neq 0$ e moltiplicando 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 dei 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.

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 $\{a_1, a_2, \dots, a_n\}$ (quindi A è finitamente generato). Inoltre, per ogni $i \in \{1, 2, \dots, n\}$ l'applicazione $\alpha_i \colon a \in A \mapsto ab_i \in R$ 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 $(\alpha_i)_{i\in I}$ costituisce una base duale per $(a_i)_{i\in I}$. Per il lemma della base duale, A è dunque proiettivo. □

Esercizi e Osservazioni.

7.D.1. Il Lemma 7.11 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.

7.D.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?

7.D.3. Costruire, per qualche dominio di integrità unitario R, un ideale frazionario di R contenente R che non sia finitamente generato come R-modulo.

7.D.4. Usando il fatto (non ancora provato) che l'anello di polinomi $\mathbb{Z}[x]$ ad una indeterminata è un anello fattoriale 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 non è invertibile.

7.5 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 7.11 e la Proposizione 7.13, 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 7.13 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 più avanti, 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 7.D.4), ma segue, in modo ancora più semplice, da considerazioni generali, ad esempio dal Teorema 7.15 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 dimostreremo 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 $A, B \in \mathfrak{I}^*(R)$, se A divide B (cioè $B = AC$ per un ideale $C \in \mathfrak{I}^*(R)$), allora $A \supseteq B$. Di conseguenza, due elementi che siano associati in $\mathfrak{I}^*(R)$ devono necessariamente coincidere; in altre parole: la relazione 'essere elementi associati' in $\mathfrak{I}^*(R)$ è la relazione di uguaglianza, sicché $\mathfrak{I}^*(R) \simeq \widetilde{\mathfrak{I}^*(R)}$ e la relazione di divisibilità in $\mathfrak{I}^*(R)$ è una relazione d'ordine. Allora, per il Teorema 7.7, $\mathfrak{I}^*(R)$ è fattoriale se e solo se è cancellativo e $(\mathfrak{I}^*(R), |)$ è un reticolo a condizione minimale. Altra ovvia conseguenza è che R, l'elemento neutro, è l'unico elemento invertibile di $\mathfrak{I}^*(R)$.

Ci tornerà utile, anche più avanti, la seguente osservazione:

Lemma 7.14. *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 $I|J$. □

Teorema 7.15. *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 7.14. 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 7.7.

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 $0 \neq P \in \operatorname{Spec}(R)$. Allora P è un prodotto di ideali massimali di R, ed essendo P primo uno dei fattori di questo prodotto deve essere contenuto in, e quindi coincidere con, P. Dunque P è massimale. □

Corollario 7.16. *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 7.15 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 7.15. Otteniamo così una contraddizione, il che completa la dimostrazione. □

Veniamo ad altre caratterizzazioni degli anelli di Dedekind. Per verificare che un dominio di integrità sia di Dedekind basta verificare che siano invertibili gli ideali primi non nulli. Si ha infatti:

Lemma 7.17. *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 $\mathcal{S} \neq \varnothing$. 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 7.13), 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, siano $a, b \in P$ tali che $ab \in P$ e $a, b \notin P$. Allora P è propriamente contenuto sia in $P + aR$ che in $(P : a)$, dal momento che a quest'ultimo ideale appartiene b. Per la massimalità di P, dunque, 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 nelle ipotesi del Lemma 6.6: per la Proposizione 7.13 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.[4] □

Corollario 7.18. *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 7.17 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. □

Come ulteriore conseguenza, osserviamo che, gli ideali primi in un dominio di integrità unitario determinano anche la proprietà di essere o meno principale.

Corollario 7.19. *Sia R un dominio di integrità unitario. Allora R è un anello principale se e solo se ogni suo ideale primo è principale.*

[4] Una dimostrazione alternativa è suggerita nell'Esercizio 7.E.2

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 7.18. Ma allora ogni ideale non nullo di R è prodotto di ideali primi, quindi principali, e dunque è esso stesso principale. □

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.

La prossima caratterizzazione degli anelli di Dedekind richiede per la sua dimostrazione un lemma il cui enunciato si può confrontare con l'Esercizio 7.A.4 e fornisce una dimostrazione alternativa dell'essenziale unicità delle fattorizzazione in ideali primi in un anello di Dedekind.

Lemma 7.20. *Sia H un ideale invertibile di un dominio di integrità unitario R. Allora le eventuali fattorizzazioni di H in prodotti di ideali primi differiscono tra loro solo per l'ordine dei fattori.*

Dimostrazione. Siano $s, t \in \mathbb{N}$ e $P_1, P_2, \dots, P_s, Q_1, Q_2, \dots, Q_t$ ideali primi di R tali che $H = P_1P_2\cdots P_s = Q_1Q_2\cdots Q_t$. Poiché H è invertibile, ciascuno dei P_i e dei Q_i è invertibile. Sia P un elemento minimale (rispetto all'inclusione) di $\{P_1, P_2, \dots, P_s, Q_1, Q_2, \dots, Q_t\}$. Senza perdere in generalità possiamo assumere $P = P_h$ per un $h \in \{1, 2, \dots, s\}$. Allora $P \supseteq H = Q_1Q_2\cdots Q_t$ e quindi $P \supseteq Q_k$ per un $k \in \{1, 2, \dots, t\}$. Ora, la minimalità di P implica $P = Q_j$. Quindi $P^{-1}H$ è un ideale invertibile di R che si fattorizza come $P^{-1}H = \prod_{i=1,\, i\neq h}^{s} P_i = \prod_{j=1,\, i\neq k}^{t} Q_i$. Facendo induzione sul numero dei fattori, possiamo concludere che queste ultime due fattorizzazioni coincidono a meno dell'ordine dei fattori, e da qui segue la stessa conclusione per le fattorizzazioni $P_1P_2\cdots P_s$ e $Q_1Q_2\cdots Q_t$ di H. □

Teorema 7.21. *Sia R un dominio di integrità unitario. Allora R è un anello di Dedekind se e solo se ogni ideale proprio di R è prodotto di ideali primi.*

Dimostrazione. Una implicazione è già nota (dal Teorema 7.15); abbiamo da provare l'altra. Grazie al Corollario 7.18, ci basterà dimostrare che, in R, se ogni ideale proprio è prodotto di ideali primi allora ogni ideale primo non nullo è invertibile. Assunta la nostra ipotesi, sia $0 \neq Q \in \operatorname{Spec}(R)$ e sia $0 \neq b \in Q$. Per ipotesi, $Q \supseteq bR = P_1P_2\cdots P_n$ per opportuni ideali primi $P_1, P_2, \dots, P_n$, dunque certamente $Q \supseteq P_i$ per qualche $i \in \{1, 2, \dots, n\}$. Ora P_i, in quanto divisore di bR, è certamente invertibile; dunque basterà provare $Q = P_i$. A questo scopo è senz'altro sufficiente dimostrare:

$$\text{ogni ideale primo invertibile di } R \text{ è un ideale massimale.} \tag{$*$}$$

(infatti, se vale $(*)$, allora P_i è massimale, dunque $P_i = Q$). L'obiettivo diventa quindi quello di provare $(*)$.

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 $Q_1, Q_2, \dots, Q_s$ di R, tutti contenenti P, tali che $P + aR = P_1P_2\cdots P_r$ e $P + a^2R = Q_1Q_2\cdots Q_s$. Sia $\bar{\cdot}\colon R \twoheadrightarrow \bar{R} := R/P$ l'epimorfismo canonico. Gli ideali $\bar{P}_i = P_i/P$ e $\bar{Q}_j = Q_j/P$ sono ovviamente ancora primi in $\bar{R}$, e 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 quindi 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 7.20 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 $(P + aR)^2 = P^2 + aP + a^2R$, ricaviamo $P^2 \subseteq P \subseteq P^2 + aR$. Applicando la legge modulare di Dedekind 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 $(*)$. Come già osservato, ciò basta a completare la dimostrazione. □

Corollario 7.22. *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 $P_1, P_2, \dots, P_n \in \operatorname{Spec}(R)$. 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 7.21 possiamo concludere che, se non è nullo, $S^{-1}R$ è di Dedekind.[5] □

Il prossimo obiettivo che ci poniamo è quello di studiare che relazione ci sia tra le proprietà di essere un anello di Dedekind e quella di essere un anello fattoriale. Iniziamo con una ulteriore caratterizzazione di quest'ultima proprietà.

Lemma 7.23. *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 $0 \neq P \in \operatorname{Spec}(R)$ e $0 \neq a \in P$. Allora $a = p_1p_2 \cdots p_r$ per opportuni $r \in \mathbb{N}^+$ ed elementi primi $p_1, p_2, \dots, p_r$ di R. Poiché P è primo, da $p_1p_2 \cdots p_r \in P$ 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 e consideriamo in $(R, \cdot)$ il sottomonoide S generato dagli elementi invertibili e da quelli primi non nulli; dunque S è costituito dagli elementi non nulli di R che siano invertibili oppure prodotto di primi. Intendiamo verificare che S è saturo. Siano $a, b \in R$ tali che $ab \in S$. Allora $ab = up_1p_2 \cdots p_r$ per opportuni $u \in \mathcal{U}(R)$, $r \in \mathbb{N}$ e primi $p_1, p_2, \dots, p_r$. Facendo induzione su r, mostriamo che a e b sono in S. La conclusione è ovvia se $r = 0$. Se $r > 0$, allora p_r divide ab, quindi p_r divide uno tra a e b. Se $p_r | a$, posto $a = p_r a'$ abbiamo $a'b = up_1p_2 \cdots p_{r-1} \in S$ e quindi, per ipotesi di induzione, $a', b \in S$, dunque anche $a = p_r a' \in S$; alla stessa conclusione si perviene assumendo $p_r | b$. Possiamo così concludere che S è effettivamente saturo. Allora, come sappiamo dal Lemma 3.6, $R \setminus S$ è unione di ideali primi. Ma, per ipotesi, $S \cap P \neq \varnothing$ per ogni ideale primo non nullo di R. Di conseguenza $R \setminus S = \{0\}$. Ma allora ogni elemento non nullo e non invertibile di R è prodotto di primi, vale a dire: R è fattoriale. □

Corollario 7.24. *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 $0 \neq pR \in \operatorname{Spec}(R)$ e quindi $pR = P$ per la minimalità di P. □

Proposizione 7.25. *Per un dominio di integrità unitario R sono equivalenti:*
(i) *ogni ideale primo di R è principale.*
(ii) *R è principale;*

[5] per una dimostrazione diversa si veda l'Esercizio 7.E.3.

(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 $0 \neq P \in \operatorname{Spec}(R)$. Se $0 \neq Q \in \operatorname{Spec}(R)$ e $Q \subseteq P$, allora $Q = P$ perché $Q \lhd\cdot R$. Dunque P è minimale tra gli ideali primi non nulli di R e quindi è principale per il Corollario 7.24; ciò prova la (i). A questo punto la dimostrazione è completa. □

Chiudiamo questa sezione con due osservazioni su ideali primari e decomposizioni primarie negli anelli di Dedekind, che ci portano a concludere che le decomposizioni primarie minimali in questi anelli si possono identificare con le fattorizzazioni in prodotti di potenze di primi a due a due distinti.

Proposizione 7.26. *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 proprio non nullo di R, allora H ha, a meno dell'ordine, un'unica decomposizione primaria minimale, precisamente $H = P_1^{\lambda_1} \cap P_2^{\lambda_2} \cap \cdots \cap P_n^{\lambda_n}$, dove $H = P_1^{\lambda_1} P_2^{\lambda_2} \cdots P_n^{\lambda_n}$ è una decomposizione di H in prodotto di ideali primi: per ogni $i, j \in \{1, 2, \ldots, n\}$, $0 \neq P_i \in \operatorname{Spec}(R)$, $\lambda_i \in \mathbb{N}^+$ 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, se $\lambda \in \mathbb{N}^+$, ovviamente $0 = 0^\lambda$ è primo; se poi $0 \neq P \in \operatorname{Spec}(R)$, allora $P = \sqrt{P^\lambda} \lhd\cdot R$ e quindi P^λ è P-primario.

Abbiamo provato la (i); per provare la (ii) sia $0 \neq H \lhd R$ e sia $H = \bigcap_{i=1}^n Q_i$ una decomposizione primaria minimale di H. Ciascuno dei Q_i si può scrivere come $P_i^{\lambda_i}$, 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, anche gli ideali Q_i sono a due a due comassimali, sicché $H = Q_1 Q_2 \cdots Q_n = P_1^{\lambda_1} P_2^{\lambda_2} \cdots P_n^{\lambda_n}$. Questa è una decomposizione di H come prodotto di primi, e come sappiamo questa è unica a meno dell'ordine dei fattori. Da ciò segue l'asserto. □

A proposito di quest'ultimo enunciato, è piuttosto evidente che se $0 \neq P \in \operatorname{Spec}(R)$ e $n, m \in \mathbb{N}$, allora $P^n = P^m$ se e solo se $n = m$. Dovrebbe essere altrettanto chiaro che l'unicità a meno dell'ordine della decomposizione primaria degli ideali di R segue anche, in modo diretto, dal secondo teorema di unicità per decomposizioni primarie e dal fatto che R ha dimensione al più 1.

Esercizi e Osservazioni.

7.E.1. Dedurre la conclusione dell'Esercizio 7.D.4 dal Lemma 7.14, dopo aver provato che H non divide $x\mathbb{Z}[x]$.

7.E.2. Dimostrare in modo alternativo il Lemma 7.17 utilizzando il Lemma 7.14 per provare che, con le notazioni usate nella dimostrazione di 7.17, ogni elemento massimale P di $\mathcal{S}$ è primo. Suggerimento: si tratta di escludere che si possa avere $IJ \subseteq P$ per ideali I, J di R propriamente contenenti P.

7.E.3. Sia R un dominio di integrità unitario, sia $H \lhd R$ e sia $\varnothing \neq S \subseteq R$. 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 7.22.

7.E.4. Abbiamo enunciato il Lemma 7.23 in preparazione alla dimostrazione del Proposizione 7.25 ma, in realtà, delle due implicazioni contenute nel lemma abbiamo utilizzato per la proposizione solo la più immediata.

7.E.5. La dimostrazione del Lemma 7.23 prova che, in un qualsiasi monoide commutativo, l'insieme degli elementi cancellabili che siano invertibili o prodotto di primi costituisce un sottomonoide saturo.

7.E.6. È possibile dimostrare, ma la cosa richiede più teoria di quanta ne abbiamo sviluppato qui, che vale una forma più forte del Teorema 7.15. Si ha infatti che *se R è un dominio di integrità unitario e $\mathfrak{I}^*(R)$ è un monoide fattoriale, allora R è un anello di Dedekind.*

7.6 Ideali in anelli di Dedekind

Il fatto che gli ideali non nulli di un anello di Dedekind costituiscono un monoide fattoriale permette di ragionare su di essi in modo non molto dissimile da come si fa per i numeri interi o, più in generale, sugli elementi di un anello fattoriale. Un'utile osservazione è che massimi comuni divisori e minimi comuni multipli possono essere facilmente interpretati nel monoide degli ideali.

Lemma 7.27. *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 $\mathfrak{I}(R)$. In particolare, I e J sono coprimi (in $\mathfrak{I}(S)$) se e solo se sono comassimali (in R).*

Dimostrazione. L'enunciato segue subito dal fatto, stabilito nel Teorema 7.15 (i), che la relazione di divisibilità in $\mathfrak{I}(R)$ coincide con l'inclusione inversa. Infatti, per questo motivo $I+J$, l'estremo superiore in $(\mathfrak{I}(R),\subseteq)$ tra I e J, è l'estremo inferiore tra I e J rispetto alla divisibilità, cioè l'unico massimo comun divisore nel monoide $\mathfrak{I}(R)$ tra I e J. Inoltre, I e J sono coprimi in $\mathfrak{I}(R)$ se e solo se l'unità R di $\mathfrak{I}(R)$ 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 $\mathfrak{I}(R)$. □

Lemma 7.28. *Sia R un anello di Dedekind e sia $\mathcal{P}$ un insieme finito di ideali primi di R. Allora, per ogni $H\in\mathfrak{I}^*(R)$, si ha $H\supset\bigcup_{P\in\mathcal{P}}HP$.*

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 $P^{-1}Q\lhd R$. Inoltre, l'essenziale unicità delle fattorizzazioni degli ideali di R in prodotto di primi fornisce $H(P^{-1}Q)\supset HQ$, quindi esiste $a_P\in H(P^{-1}Q)\setminus HQ$. Osserviamo anche che, nel monoide $\mathfrak{I}^*(R)$, gli ideali P e $P^{-1}Q$ sono coprimi e $HP\cap H(P^{-1}Q)$ è il minimo comune multiplo tra HP e $H(P^{-1}Q)$, quindi $HP\cap H(P^{-1}Q)=HQ$. 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. □

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 7.29. *Sia R un anello di Dedekind e sia $H\in\mathfrak{I}^*(R)$. Allora l'insieme degli ideali di R contenenti H è finito. In altri termini: $\mathfrak{I}(R/H)$ 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 7.15, in $\mathfrak{I}^*(R)$ 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. □

Ovvia conseguenza del Lemma 7.29 è che *i quozienti propri degli anelli di Dedekind sono tutti artiniani.*

Se H è un ideale non nullo di un anello di Dedekind R, è ovvio che H ha qualche multiplo in $\mathfrak{I}^*(R)$ che è un ideale principale non nullo: scelto comunque $a \in H \smallsetminus 0$, il punto (i) del Teorema 7.15 mostra che $HJ = aR$ per qualche $J \in \mathfrak{I}^*(R)$. Il prossimo lemma mostra che J può essere scelto coprimo con un arbitrario prefissato ideale non nullo.

Lemma 7.30. *Siano R un anello di Dedekind e $H, I \in \mathfrak{I}^*(R)$. Allora esiste $J \in \mathfrak{I}^*(R)$ tale che HJ sia principale e $I + J = R$.*

Dimostrazione. Sia $\mathcal{V} = \mathrm{Var}(I)$, l'insieme degli ideali primi di R contenenti I. Per i lemmi 7.28 e 7.29, esiste $a \in H \smallsetminus \bigcup_{P\in\mathcal{V}} HP$. 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 H. Quindi $I + J = R$ e la dimostrazione è completa.[6] □

Proposizione 7.31. *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 7.30 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. □

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 7.32. *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 $a \in H \smallsetminus 0$ esiste $b \in H$ tale che $H = aR + bR$.*

Dimostrazione. Sia $I/H \lhd R/H$. Allora, per il Lemma 7.30, esiste $J \lhd R$ 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 $a \in H \smallsetminus 0$. 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: $H = aR + bR$. □

Una dimostrazione alternativa per la parte (i) è nell'Osservazione 7.F.1. Una conseguenza di questo stesso enunciato è il prossimo corollario, al quale premettiamo:

Lemma 7.33. *Siano I e J ideali frazionari del dominio di integrità unitario R e supponiamo I invertibile. Allora $(J : I)_{Q(R)} = I^{-1}J$.*

Dimostrazione. Per ogni $k \in Q(R)$ si ha $kI \subseteq J$ se e solo se $kR \subseteq I^{-1}J$, ovvero: $k \in I^{-1}J$. □

[6] 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.

Corollario 7.34. *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 7.32, il quoziente I/IJ è un R-modulo ciclico, quindi isomorfo a $R/\operatorname{Ann}_R(I/IJ)$. Ora, $\operatorname{Ann}_R(I/IJ) = (IJ : I)_R = I^{-1}IJ = J$ per il Lemma 7.14; si ottiene così (i). Poiché $|R/IJ| = |R/I| \cdot |I/IJ|$, la (ii) ne è una ovvia conseguenza. □

Osservazioni.

7.F.1. Si potrebbe esser tentati dal dimostrare il Teorema 7.32 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 7.31. 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 $\mathcal{V} = \operatorname{Var}(H)$, l'insieme dei divisori primi di H, e $S = R \setminus \bigcup \mathcal{V}$. Allora S è un sottomonoide di $(R, \cdot)$ e, per il Corollario 7.22, $S^{-1}R$ è un anello di Dedekind. Inoltre, per il Corollario 4.15, $S^{-1}R$ è semilocale, dunque $S^{-1}R$ è principale, per la Proposizione 7.31. 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 4.9). Di conseguenza, ogni ideale di R/H è principale.

7.F.2. È stato dimostrato che vale anche l'inverso del Teorema 7.32, 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.*

8 Anelli di valutazione, interi su un anello, interi algebrici

Questo capitolo è in senso stretto un prolungamento del precedente. Infatti introduciamo qui alcune classi di domini di integrità unitari allo scopo di provare un'ulteriore caratterizzazione degli anelli di Dedekind e mostrare che gli anelli degli interi nei campi di numeri sono anelli di Dedekind.

8.1 Anelli di Bézout

Come già accennato nella sezione 7.3, 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 7.3 mostrano che questa condizione implica che d sia un massimo comun divisore tra a e b. Quindi possiamo anche dire, in modo un pò informale, che un dominio di integrità unitario è un anello di Bézout se e solo se "in R vale il teorema di Bézout":

Proposizione 8.1. *Sia R un dominio di integrità unitario. Allora R è un anello di Bèzout 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. □

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 $\overline{\mathbb{Z}}$ degli interi algebrici, che sarà introdotto in una delle prossime sezioni; un altro è presentato nell'Esempio 8.A.2; altri ancora sono ottenibili dal Lemma 8.4.

Esempi ed Esercizi.

8.A.1. Provare che un anello di Bézout fattoriale è necessariamente principale.

8.A.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 $f_0 = d_0 h(0)$ e $g_0 = d_0 k(0)$. Se $d_0 \neq 0$, abbiamo $h(0) = f_0/d_0 \in \mathbb{Z}$, quindi $h \in R$ e $d|_R f$; in modo analogo $d|_R g$. 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 divida 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 $dR = fR + gR$.

8.2 Anelli di valutazione

Per definizione, si dice *anello di valutazione* un dominio di integrità unitario R che verifichi una delle seguenti condizioni, tra loro equivalenti (e quindi tutte):

- (AV_1) l'insieme degli ideali di R è totalmente ordinato per inclusione;
- (AV_2) l'insieme degli ideali principali di R è totalmente ordinato per inclusione;
- (AV_3) per ogni $a, b \in R$, si ha $a|_R b$ o $b|_R a$;
- (AV_4) 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 (AV_1) implica (AV_2), ed è anche chiaro che (AV_2), (AV_3) e (AV_4) sono tra loro equivalenti (dire che un elemento $c = a/b$ di K, con $a, b \in K$ appartiene a R significa precisamente dire che, in R, b divide a). Infine, assunta (AV_2), 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 (AV_2). Proviamo così che (AV_2) implica (AV_1) e l'equivalenza delle (AV_{1-4}) è così dimostrata.

Un'altra caratterizzazione degli anelli di valutazione è la seguente.

Proposizione 8.2. *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 (AV_1)) 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'deale 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 (AV_3) ed è dunque un anello di valutazione. □

Uno dei motivi che rendono rilevanti gli anelli di valutazione nel nostro contesto è che sono di valutazione gli anelli di Dedekind locali, vale a dire (vedi Corollario 7.22) le localizzazioni degli anelli di Dedekind. Sia infatti R un anello di Dedekind locale con ideale massimale M. Allora, in conseguenza del Teorema 7.15, M è l'unico ideale primo non nullo di R e tutti gli ideali non nulli di R sono potenze di M: $\mathfrak{I}^*(R) = \{M^n \mid n \in \mathbb{N}\}$. Dunque, $\mathfrak{I}(R)$, ordinato per inclusione, è una catena, quindi R è un anello di valutazione; osserviamo anche che $M^n \neq M^m$ se n e m sono naturali distinti, quindi il tipo d'ordine di $\mathfrak{I}(R)$è il duale dell'ordinale $\omega + 1$. Possiamo anche notare che questi sono difatti anelli principali. Questo segue dalla Proposizione 7.31, oppure dalla seguente conseguenza della Proposizione 8.2:

Corollario 8.3. *Ogni anello di valutazione noetheriano è principale;*

ma anche, più direttamente, dall'osservazione che, per ogni $a \in M \setminus M^2$, si ha $aR \subseteq M$ e $aR \not\subseteq M^2$, quindi $aR = M$, perché $\mathfrak{I}(R)$ è una catena. Dunque $M^n = a^n R$ è principale, per ogni $n \in \mathbb{N}^+$. È del tutto ovvio il viceversa: ogni anello di valutazione che sia principale è un anello di Dedekind locale. Quindi gli anelli di Dedekind locali sono precisamente gli *anelli principali di valutazione*, che sono anche chiamati, con terminologia più tradizionale, *anelli di valutazione discreta*. Alcuni autori escludono da questa definizione i campi (che sono banalmente sia anelli di valutazione che anelli principali); come sempre, includerli o meno nella definizione è questione di gusto; noi li includiamo.

Esempi di anelli di valutazione sono dunque le localizzazioni di $\mathbb{Z}$ discusse nella sezione 4.1. Un'altra fonte di esempi è data dal prossimo lemma: 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 8.4. *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 $(\mathcal{S}, \preceq)$ ha elementi massimali, e 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 $H \lhd A$: 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 $f_1(c) = 1_K$.[1] Ciò contraddice la scelta di n e m; si conclude così la dimostrazione. □

Esercizi, Esempi, Osservazioni.

8.B.1. Verificare che tutti gli anelli di frazioni non nulli di un anello di valutazione sono anelli di valutazione.

8.B.2. Sia R un anello fattoriale in cui gli irriducibili sono tutti associati tra loro. Descriverne 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.

8.B.3. 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 $K \to \hat{G}$, 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) maggiore di 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 $\mathfrak{F}(R)$ dei suoi ideali frazionari è totalmente ordinato dalla relazione $\supseteq$ di inclusione inversa, e, se $K = Q(R)$, l'applicazione $\digamma : k \in K \mapsto kR \in \mathfrak{F}(R)$ è una valutazione. Come è chiaro, l'anello della valutazione $\digamma$ 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.

8.B.4. 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

[1] 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.

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 interessante è questo: 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 $v_p\colon \mathbb{Q}^* \to \mathbb{Z}$ 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?

8.B.5. 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 $r \neq -s$, $(r + s)^v \geq \min\{r^v, s^v\}$. Sege 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.

8.3 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 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 $c^0, c^1, \ldots, c^{n-1}$ (precisamente: $c^n = \sum_{i=0}^{n-1}(-a_i)c^i$). Dunque:

Lemma 8.5. *Se c ed R sono, rispettivamente un elemento ed un sottoanello unitario dell'anello commutativo A, a 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 $\{c^0 = 1_R, c, c^2, \ldots, c^{n-1}\}$.*[2]

Corollario 8.6. *Con le stesse notazioni, se $c \in \mathcal{U}(A)$, allora c è intero su R se e solo se $c \in R[c^{-1}]$.*

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 $c = \sum_{i=0}^{n-1} c^{i-n+1}R \in R[c^{-1}]$. □

Lemma 8.7. *Sia R un sottoanello unitario dell'anello commutativo unitario 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.*

Dimostrazione. Valga (i); allora, come mostra il Lemma 8.5, $c^n \in M := \sum_{i=0}^{n-1} c^i R$, 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 $c^{n+t+1} \in Mc = \sum_{i=1}^{n} c^i R \subseteq M + c^n R = M$. 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 se 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 $i \in \{1, 2, \ldots, n\}$ si ha $u_i c = \sum_{j=1}^{n} u_j r_{ij}$ per opportuni $r_{ij} \in R$. Dunque, posto $\underline{u} = (u_1, u_2, \ldots, u_n)$, 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 $J = I_n c - L$, una matrice a termini in $R[c]$. Moltiplicando per $\operatorname{adj}(J)$[3] si ha $\underline{u}(I_n d) = 0$, dove $d = \det J$. Ovviamente questo significa $u_i d = 0$ per ogni $i \in \{1, 2, \ldots, n\}$, e quindi $Md = 0$, vale a dire: $d \in \operatorname{Ann}_{R[c]}(M)$. Ma M è fedele come $R[c]$-modulo, quindi questo comporta $d = 0$. 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. □

Corollario 8.8. *Sia R un sottoanello unitario dell'anello commutativo unitario 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 8.7. □

[2] qui e più avanti facciamo tacitamente riferimento all'ovvia struttura di A come R-algebra.

[3] $\operatorname{adj}(J)$ è la matrice dei complementi algebrici di J; come nel caso delle matrici quadrate su un campo, si ottiene $J \operatorname{adj}(J) = \operatorname{adj}(J)J = I_n \det J$

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 8.9. *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 due omomorfismi (strutturali) di anelli unitari: $\xi\colon R \to A$, che definisce A come R-algebra e $\rho\colon A \to \mathrm{End}(B,+)$, che definisce la struttura di A-modulo su B. Quindi B è strutturato come R-modulo da $\xi\rho\colon R \to \mathrm{End}(B,+)$. 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 subito $B = Y(XR) = (YX)R$. Quindi B è generato, come R-modulo, dall'insieme finito $\{xy \mid x \in X \wedge y \in Y\}$. □

Lemma 8.10. *Sia A un anello commutativo unitario e sia R un suo sottoanello unitario. Supponiamo che esistano un numero finito di elementi $a_1, a_2, \ldots, a_n \in A$ tali che $A = R[a_1, a_2, \ldots, a_n]$ e, per ogni $i \in \{1, 2, \ldots, n\}$, che a_i sia intero su $R[a_1, a_2, \ldots, a_{i-1}]$. 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 $R_1 := R[a_1, a_2, \ldots, a_{n-1}]$ è finitamente generato come R-modulo. Poiché a_n è intero su R_1, il Lemma 8.7 mostra che A è finitamente generato come R_1-modulo e quindi, grazie al Lemma 8.9, concludiamo che A è finitamente generato come R-modulo. Una diretta applicazione del Lemma 8.9 completa la dimostrazione. □

Corollario 8.11. *Sia R un sottoanello unitario dell'anello commutativo unitario 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 8.10, è un ampliamento intero di R. Dunque $a - b$ e ab sono interi su R, quindi appartengono a $\bar{R}$. L'asserto segue facilmente. □

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 8.12. *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 8.10 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. □

Fissiamo alcune notazioni. La chiusura intera di $\mathbb{Z}$ nel campo complesso (o, equivalentemente, nella chiusura algebrica $\overline{\mathbb{Q}}$ di $\mathbb{Q}$ in $\mathbb{C}$) viene indicata con $\overline{\mathbb{Z}}$ ed è nota come l'*anello degli interi algebrici*. Come abbiamo già osservato, $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$; 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; ciò segue dal prossimo enunciato.

Lemma 8.13. *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 $0_R = \sum_{i=0}^{n} a_i u^i / v^i$, dunque $0_R = \sum_{i=0}^{n} a_i u^i v^{n-i} = a_0 v^n + v^n \sum_{i=1}^{n} a_i u^i v^{n-i}$. Ne segue che u divide $a_0 v^n$; ma u è coprimo con v^n, dunque $u|_R\, a_0$. Similmente, da $0_R = a_n u^n \sum_{i=1}^{n-1} a_i u^i v^{n-i}$ deduciamo $v|_R\, a_n$. □

Corollario 8.14. *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 8.13 comporta che v divida il coefficiente direttore 1_R di f; ma allora $v \in \mathcal{U}(R)$ e quindi $c \in R$. Ciò mostra $\bar{R} = R$; quindi R è integralmente chiuso. □

Non è difficile provare che anche gli anelli di valutazione sono integralmente chiusi: in questo consiste la prima parte della dimostrazione del prossimo risultato. Il Lemma 8.4 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 8.15. *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.*

Dimostrazione. Sia $V \in \mathcal{V}$, e sia $c \in K \setminus V$. Allora $c^{-1} \in V$; ce lo assicura la condizione (AV_4) nella definizione di anello di valutazione. Se c sia intero su R, allora $c \in R[c^{-1}]$ per il Corollario 8.6. 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 8.4, 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. □

Useremo nella prossima sezione questo importante lemma:

Lemma 8.16. *Sia A un anello commutativo unitario, ampliamento intero del suo sottoanello unitario R. Siano P e Q ideali primi di A tali che $P \subseteq Q$. 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 $g(c) \notin P$, ricaviamo $c \in P$. Dunque $Q = P$. □

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 (ma non lo faremo qui) che le dimensioni di A e di R coincidono.

Esercizi.
8.C.1. Sia R un dominio di integrità unitario. Se il suo campo dei quozienti ne è un ampliamento intero, allora R è un campo.
8.C.2. Sia A un anello commutativo unitario, ampliamento intero del suo sottoanello unitario R. Se φ è un omomorfismo di anelli unitari di dominio A, allora $A^{\vec{\varphi}}$ è un ampliamento intero di $R^{\vec{\varphi}}$. Come si può interpretare questa osservazione in termini di quozienti?
8.C.3. $\mathbb{Z}[\sqrt{5}]$ 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 pò indiretto per provare che $\mathbb{Z}[\sqrt{5}]$ non è un anello fattoriale.
8.C.4. Sia R un dominio di integrità unitario e supponiamo che $\mathfrak{I}^*(R)$ 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 ....

8.4 Il teorema di Noether e gli anelli degli interi algebrici dei campi di numeri

Siamo ora in grado di dimostrare un'importante 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 E. 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 invertiblità e di fattorizzazione per i loro ideali.

Premettiamo all'enunciato del teorema di Noether una semplice osservazione generale sugli ideali degli anelli noetheriani.

Lemma 8.17. *Sia R un anello commutativo unitario noetheriano. Allora ogni ideale non nullo di R contiene un prodotto di ideali primi non nulli.*

Dimostrazione. Sia $0 \neq H \lhd R$. Se $H = R$ è chiaro che H contiene un ideale primo; altrimenti H ha una decomposizione primaria, dunque $H = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ dove ciascuno dei Q_i è un ideale primario. 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 $H \subseteq Q_1 Q_2 \cdots Q_n \subseteq P_1^{\lambda_1} P_2^{\lambda_2} \cdots P_n^{\lambda_n}$, la qual cosa prova l'asserto. □

Teorema 8.18. *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. Come già visto nella sezione 8.2, le localizzazioni degli anelli di Dedekind sono anelli di valutazione, quindi (i) implica (ii). Supponiamo poi che valga (ii). Se $0 \neq P \in \mathrm{Spec}(R)$ e $P \subseteq M \lhd\cdot R$, allora il Teorema 4.11 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 4.8 che gli anelli di frazioni degli anelli noetheriani sono essi stessi noetheriani) e quindi un anello principale. 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 4.11, $P = M$. Abbiamo così provato che ogni ideale primo non nullo di R è massimale, ovvero: R ha dimensione al più 1. Per completare la verifica di (iii) occorre provare che R è integralmente chiuso. Consideriamo, per ogni ideale massimale M di R, la corrispondente localizzazione R_M come sottoanello (unitario) di K contenente R. Per un fissato $M \lhd\cdot R$, sia $c \in R_M$. Allora $c = a/b$ per opportuni $a \in R$ e $b \in R \setminus M$, dunque $b \in (R : c)_R$. Si ha così $(R : c) \not\subseteq M$. Sia ora $c \in \bigcap\{R_M \mid M \lhd\cdot R\}$. 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 $c = 1_R\, c \in R$. Abbiamo così provato $\bigcap\{R_M \mid M \lhd\cdot R\} = R$. La Proposizione 8.15 implica ora che la chiusura intera di R in K è proprio R, vale a dire: R è integralmente chiuso. Abbiamo così provato che (ii) implica (iii).[4]

Supponiamo infine che valga (iii). Sia $0 \neq P \in \mathrm{Spec}(R)$; per provare che R è di Dedekind basta verificare che P è invertibile (Corollario 7.18). 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 8.7, 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 8.17 esistono $n \in \mathbb{N}^+$ ed ideali primi non nulli $P_1, P_2, \ldots, P_n$ 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 $P_1, \ldots, P_n$, supponiamo sia P_n, è incluso in P. Ma $P_n \lhd\cdot R$, 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. □

Esercizi.

8.D.1. Duplicando il ragionamento in un passo della dimostrazione del Teorema 8.18, 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:
- $H = \bigcap\{H^{e_M c_M} \mid M \in \mathcal{V}\}$;
- se R è un dominio di integrità, considerando tutte le localizzazioni R_M come sottoanelli di $Q(R)$ contenenti R, si ha $H = \bigcap\{H^{e_M} \mid M \in \mathcal{V}\}$.

[4] si può osservare, a proposito di questa dimostrazione, che non abbiamo usato l'intera Proposizione 8.15, ma solo la parte più più semplice del suo enunciato: il fatto che gli anelli di valutazione sono integralmente chiusi. Questo significa che il Lemma 8.4 non è realmente richiesto per la dimostrazione del Teorema 8.18.