Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea in Matematica

DOMINI DI DEDEKIND

Tesi di Laurea in Algebra

Relatore:
Chiar.ma Prof.ssa
Marta Morigi

Presentata da:
Martina Brasini

III Sessione
Anno Accademico 2013/2014

Indice

Introduzione **iii**

1 Nozioni preliminari **1**

1.1 Proprietà generali 1

1.2 Le sequenze esatte corte 3

1.3 I moduli proiettivi 8

1.4 Anello dei quozienti e localizzazione 11

1.5 Estensioni di anelli intere 19

2 Domini di Dedekind **25**

2.1 Gli ideali frazionari 26

2.2 Gli ideali invertibili 28

2.3 Domini di Dedekind e domini a ideali principali 30

2.4 Caratterizzazioni equivalenti di un dominio di Dedekind 36

2.5 Il dominio $\mathbb{Z}[\sqrt{10}]$ 44

Bibliografia **51**

Introduzione

Il presente elaborato si propone di analizzare in modo approfondito la classe dei domini di Dedekind, introducendoli inizialmente come un'estensione della classe dei domini a ideali principali, per poi passare a caratterizzarli mediante proprietà che spaziano in ambiti diversi.
Una volta appurato che esistono molteplici possibilità di definire i domini di Dedekind, la scelta stessa di presentarli come quei domini d'integrità in cui ogni ideale proprio è prodotto di un numero finito di ideali primi, pone inevitabilmente l'accento sullo stretto legame che intercorre tra essi e i domini a ideali principali, in cui è infatti noto che tale proprietà di fattorizzazione per gli ideali sia verificata. Nell'ottica di esplicare tale rapporto, si è rivelato necessario partire dall'introduzione di strumenti, quali le nozioni di ideale frazionario e di ideale invertibile, in grado di delineare in modo efficace le peculiarità della fattorizzazione in ideali primi. In particolare, indagando la connessione di questi nuovi concetti con quelli di ideale massimale e di modulo proiettivo, sono stati così individuati alcuni importanti risultati, tipicamente ottenuti per i domini a ideali principali, che mantengono validità nei domini di Dedekind.
Successivamente l'attenzione è stata focalizzata sulle diverse possibili condizioni equivalenti che possono classificare un dominio di integrità come dominio di Dedekind, che sono state poi raccolte in un teorema riassuntivo finale. Anche in questo contesto gli ideali invertibili e i moduli proiettivi svolgono un ruolo di fondamentale importanza, costituiscono infatti il cardine attorno

a cui ruotano le prime condizioni del teorema. Le ultime due caratterizzazioni invece si basano rispettivamente sulle nozioni di dominio integralmente chiuso e di localizzazione rispetto ad un ideale primo, illustrate nel primo dei due capitoli in cui è articolata la tesi, che apparentemente esulano dal contesto della fattorizzazione di ideali. Quest'ultima osservazione è indicativa del fatto che i domini di Dedekind siano di particolare interesse, non solo come oggetto di studio in sè, ma anche in quanto punto di incontro e di integrazione di diverse competenze.

Capitolo 1

Nozioni preliminari

1.1 Proprietà generali

Definizione 1.1. Sia $(A, \leq)$ un insieme parzialmente ordinato, una *catena di* A è un sottoinsieme non vuoto di A che risulta totalmente ordinato rispetto alla relazione d'ordine $\leq$.

Definizione 1.2. Sia $(A, \leq)$ un insieme parzialmente ordinato e sia B un suo sottoinsieme non vuoto, si definisce *maggiorante di* B *in* A un elemento $a \in A$ tale che $b \leq a$ per ogni $b \in B$.

Definizione 1.3. Sia $(A, \leq)$ un insieme parzialmente ordinato, un elemento $m \in A$ è detto *massimale* se per ogni elemento $a \in A$ che sia confrontabile con m vale $a \leq m$.

Lemma 1.1.1 (Lemma di Zorn)**.** *Sia $A \neq \emptyset$ un insieme parzialmente ordinato; se ogni catena di A ammette un maggiorante in A allora A contiene un elemento massimale.*

Osservazione 1. Sia R un anello, l'insieme di tutti gli ideali $I \neq R$ è parzialmente ordinato rispetto alla relazione di inclusione insiemistica.

Per semplicità di notazione il seguente teorema è enunciato in termini di ideali, anzichè di ideali sinistri/destri, nonostante valga anche per anelli non commutativi; la dimostrazione nel caso non commutativo è analoga.

Teorema 1.1.2. *Sia $R \neq \emptyset$ un anello commutativo unitario, allora in R esiste almeno un ideale massimale; infatti ogni ideale di R, tranne R stesso, è contenuto in un ideale massimale.*

Dimostrazione. Osserviamo preliminarmente che, nel caso in cui gli unici ideali di R siano quello banale ed R stesso, l'ideale banale risulta essere massimale; infatti, essendo R un anello unitario, vale $0_R \neq 1_R$ e quindi l'ideale banale non coincide con R.
A questo punto è lecito supporre che esista almeno un ideale proprio di R non banale; sia dunque $A \neq 0$, $A \underset{\neq}{\subset} R$ un ideale, e sia $\mathscr{S}$ l'insieme di tutti gli ideali B di R tali che $A \subseteq B \underset{\neq}{\subset} R$. Osserviamo che $\mathscr{S}$ è non vuoto, dal momento che $A \in \mathscr{S}$ $(A \neq 0)$, e inoltre risulta essere parzialmente ordinato rispetto alla relazione di inclusione insiemistica; mostriamo allora, al fine di applicare il Lemma di Zorn, che ogni catena di $\mathscr{S}$ ammette maggiorante in $\mathscr{S}$. Sia dunque $\mathscr{C} = \{ C_i \mid i \in I \}$ un sottoinsieme totalmente ordinato di $\mathscr{S}$, i cui elementi sono quindi ideali propri di R che contengono A; verifichiamo che l'insieme $C = \bigcup_{i \in I} C_i$ è ancora un elemento di $\mathscr{S}$. Mostriamo innanzitutto che C è un ideale, presi infatti $a, b \in C$ esistono necessariamente $i, j \in I$ tali che $a \in C_i$, $b \in C_j$, ma per ipotesi deve valere $C_i \subset C_j$ oppure $C_j \subset C_i$, quindi, supponendo che sia verificata la seconda inclusione, troviamo $a, b \in C_i$. Ma allora, essendo C_i un ideale di R, risulta $a - b$, $ra (= ar) \in C_i$ per ogni $r \in R$, e siccome $C_i \subseteq C$ ne viene che anche C è un ideale di R. In particolare vale $A \subseteq C_i \subseteq C$; inoltre, il fatto che $C_i \neq R$ implica che $1_R \notin C_i$ per ogni $i, j \in I$, dunque $C \underset{\neq}{\subset} R$ perché $1_R \notin C$. Pertanto risulta $C \in \mathscr{S}$, e C è chiaramente un maggiorante, quindi possiamo concludere che $\mathscr{S}$ contiene un

elemento massimale; d'altra parte un tale elemento è, per definizione di $\mathscr{S}$, un ideale massimale di R che contiene A. □

1.2 Le sequenze esatte corte

Definizione 1.4. Siano $f : A \longrightarrow B$, $g : B \longrightarrow C$ una coppia di omomorfismi di moduli, si dice che la sequenza di omomomorfismi di moduli $A \xrightarrow{f} B \xrightarrow{g} C$ è *esatta in* B se vale $\operatorname{Im} f = \ker g$.
Una sequenza finita di omomomorfismi di moduli $A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} A_{n-1} \xrightarrow{f_n} A_n$ si dice *esatta* se vale $\operatorname{Im} f_i = \ker f_{i+1}$ per $i = 1, \dots, n-1$.
Una sequenza infinita di omomomorfismi di moduli $\dots \xrightarrow{f_{i-1}} A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \dots$ si dice *esatta* se vale $\operatorname{Im} f_i = \ker f_{i+1}$ per ogni $i \in \mathbb{Z}$.

Spesso con abuso di linguaggio si parla di sequenze esatte di moduli, anzichè di sequenze esatte di omomorfismi di moduli.

Osservazione 2. Per ogni modulo A esistono e sono unici gli omomorfismi di moduli $0 \to A$ e $A \to 0$.

Esempio 1.1. Riportiamo di seguito alcuni esempi di sequenze di omomorfismi di moduli che sono sequenze esatte.
Siano A, B due moduli qualunque, allora le sequenze $0 \to A \xrightarrow{\iota} A \oplus B \xrightarrow{\pi} B \to 0$ e $0 \to B \xrightarrow{\iota} A \oplus B \xrightarrow{\pi} A \to 0$, dove ι e π sono rispettivamente l'iniezione e la proiezione canonica, sono esatte.
Sia C un sottomodulo di D, allora la sequenza $0 \to C \xrightarrow{i} D \xrightarrow{p} D/C \to 0$, dove i e p sono rispettivamente il morfismo di inclusione e l'epimorfismo canonico, è esatta.
Sia $f : A \longrightarrow B$ un omomorfismo di moduli, di definiscono *coimmagine di* f e *cokernel di* f rispettivamente $\operatorname{Coim} f = A/\ker f$ e $\operatorname{Coker} f = B/\operatorname{Im} f$, allora risultano essere esatte le sequenze di moduli $0 \to \ker f \xrightarrow{i} A \xrightarrow{p} \operatorname{Coim} f \to 0$, $0 \to \operatorname{Im} f \xrightarrow{i} B \xrightarrow{p} \operatorname{Coker} f \to 0$ e $0 \to \ker f \xrightarrow{i} A \xrightarrow{f} B \xrightarrow{p} \operatorname{Coker} f \to 0$.

Osservazione 3. L'esattezza di specifiche sequenze di morfismi di moduli può caratterizzare alcune loro importanti proprietà:

(i) la sequenza di omomorfismi di moduli $0 \to A \xrightarrow{f} B$ è esatta se e solo se f è un monomorfismo di moduli;

(ii) la sequenza di omomorfismi di moduli $B \xrightarrow{g} C \to 0$ è esatta se e solo se g è un epimorfismo di moduli;

(iii) se la sequenza di omomorfismi di moduli $A \xrightarrow{f} B \xrightarrow{g} C$ è esatta allora $g \circ f = 0$;

(iv) se la sequenza di omomorfismi di moduli $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ è esatta allora $\operatorname{Coker} f = B/\operatorname{Im} f = B/\ker f = \operatorname{Coim} g \cong C$.

Definizione 1.5. Una sequenza esatta di omomorfismi di moduli della forma $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ è detta *sequenza esatta corta*.

Osservazione 4. Se $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ è una sequenza esatta corta allora f e g sono rispettivamente un monomorfismo e un epimorfismo; dall'osservazione precedente si evince che dire che tale sequenza è una sequenza esatta corta è equivalente a dire che A e C sono rispettivamente un sottomodulo ($A \cong \operatorname{Im} f$) e un modulo quoziente ($C \cong B/\operatorname{Im} f = B/\ker f$) di B.

Lemma 1.2.1 (Il lemma dei cinque)**.** *Sia R un anello, consideriamo il seguente diagramma commutativo di R-moduli ed omomorfismi di R-moduli:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow[f']{} & B' & \xrightarrow[g']{} & C' & \longrightarrow & 0 \end{array}$$

e supponiamo che ciascuna riga sia una sequenza esatta corta, allora:

(i) se α, γ sono monomorfismi allora anche β è un monomorfismo;

(ii) *se α, γ sono epimorfismi allora anche β è un epimorfismo;*

(iii) *se α, γ sono isomorfismi allora anche β è un isomorfismo.*

Dimostrazione. Proviamo che sono verificate le prime due proprietà, dopodichè la terza è una conseguenza immediata.

(i) Supponiamo che α, γ siano monomorfismi e consideriamo $b \in B$ tale che $\beta(b) = 0$; abbiamo $\gamma(g(b)) = g'(\beta(b)) = g'(0) = 0$ e dal momento che γ per ipotesi è iniettiva necessariamente $g(b) = 0$, cioè $b \in \ker g$; dall'esattezza della prima sequenza viene che $\ker g = \operatorname{Im} f$, dunque esiste $a \in A$ tale che $b = f(a)$. Vale $f'(\alpha(a)) = \beta(f(a)) = \beta(b) = 0$, dove f' è iniettiva perché anche la seconda sequenza è esatta e abbiamo supposto che anche α lo sia, pertanto ne segue che $a = 0$, da cui $b = f(a) = f(0) = 0$, complessivamente abbiamo provato che β risulta essere un morfismo iniettivo.

(ii) Supponiamo che α, γ siano epimorfismi; per ogni $b' \in B'$ si ha $g'(b') \in C'$ allora per la suriettività di γ vale $g'(b') = \gamma(c)$ per qualche $c \in C$, a questo punto, poiché l'esattezza della prima sequenza implica la suriettività di g, esisterà un elemento $b \in B$ tale che $g(b) = c$. Dunque abbiamo $g'(b') = \gamma(c) = \gamma(g(b)) = g'(\beta(b))$ ovvero $g'(\beta(b) - b') = 0$ che significa che $(\beta(b) - b') \in \ker g'$; essendo la seconda sequenza esatta sappiamo però che $\ker g' = \operatorname{Im} f'$, di conseguenza $(\beta(b) - b') = f'(a')$ con $a' \in A'$; ora per ipotesi α è un epimorfismo pertanto esiste necessariamente $a \in A$ tale che $\alpha(a) = a'$. Se consideriamo allora l'elemento $b - f(a) \in B$ risulta $\beta(b - f(a)) = \beta(b) - \beta(f(a)) = \beta(b) - f'(\alpha(a)) = \beta(b) - f'(a') = \beta(b) - (\beta(b) - b') = b'$, abbiamo così mostrato che $b' \in B'$ è sempre immagine di un elemento di B cioè che β è un omomorfismo suriettivo.

□

Definizione 1.6. Due sequenze esatte corte $0 \to A \to B \to C \to 0$ e $0 \to A' \to B' \to C' \to 0$ si dicono *isomorfe* se esiste un diagramma commutativo di omomorfismi di moduli della forma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

dove α, β, γ sono isomorfismi.

Teorema 1.2.2. *Sia R un anello e sia $0 \to A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \to 0$ una sequenza esatta corta di R-moduli, allora sono equivalenti le seguenti condizioni:*

(i) esiste un morfismo di R-moduli $h : A_2 \longrightarrow B$ tale che $g \circ h = 1_{A_2}$;

(ii) esiste un morfismo di R-moduli $k : B \longrightarrow A_1$ tale che $k \circ f = 1_{A_1}$;

(iii) la sequenza $0 \to A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \to 0$ è isomorfa alla sequenza esatta corta $0 \to A_1 \xrightarrow{\iota_1} A_1 \oplus A_2 \xrightarrow{\pi_2} A_2 \to 0$ (con la funzione identità su A_1 e A_2); in particolare possiamo osservare che allora vale $B \cong A_1 \oplus A_2$.

Dimostrazione. Mostriamo che le prime due condizioni sono entrambe equivalenti alla terza.

$(i) \Rightarrow (iii)$ I morfismi $f : A_1 \longrightarrow B$ e $h : A_2 \longrightarrow B$ inducono un omomorfismo $\varphi : A_1 \oplus A_2 \longrightarrow B$ tale che $\varphi \circ \iota_1 = f$, $\varphi \circ \iota_2 = h$, dove ι_1, ι_2 sono le mappe di iniezione canonica rispettivamente di A_1 e A_2 in $A_1 \oplus A_2$ (cioè $\varphi(a_1, a_2) = f(a_1) + h(a_2)$ per $(a_1, a_2) \in A_1 \oplus A_2$); verifichiamo che tale φ rende commutativo il seguente diagramma di omomorfismi di R-moduli

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{\iota_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1_{A_1}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_{A_2}} & & \\ 0 & \longrightarrow & A_1 & \xrightarrow[f]{} & B & \xrightarrow[g]{} & A_2 & \longrightarrow & 0 \end{array}$$

Segue dalla definizione di φ che $f \circ 1_{A_1} = f = \varphi \circ \iota_1$; inoltre, dal momento che $\pi_2 \circ \iota_2 = 1_{A_2}$ e che per ipotesi abbiamo $g \circ h = 1_{A_2}$, possiamo mostrare che $1_{A_2} \circ \pi_2 = g \circ \varphi$ osservando che il diagramma

$$\begin{array}{ccc} A_1 \oplus A_2 & \xleftarrow{\iota_2} & A_2 \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle 1_{A_2}} \\ B & \underset{h}{\longleftarrow} & A_2 \end{array}$$

in cui sostituiamo a π_2 e g le rispettive mappe inverse ι_2 e h è commutativo; infatti vale $h \circ 1_{A_2} = h = \varphi \circ \iota_2$ per definizione di φ.
La tesi segue dal Lemma dei cinque.

$(ii) \Rightarrow (iii)$ I morfismi $k : B \longrightarrow A_1$ e $g : B \longrightarrow A_2$ inducono un omomorfismo $\psi : B \longrightarrow A_1 \oplus A_2$ tale che $\pi_1 \circ \psi = k$, $\pi_2 \circ \psi = g$, dove π_1, π_2 sono le mappe di proiezione canonica da $A_1 \oplus A_2$ in A_1 e A_2 rispettivamente (cioè risulta $\psi(b) = (k(b), g(b))$ per $b \in B$). Utilizzando l'ipotesi che $k \circ f = 1_{A_1}$ e il fatto che $\pi_1 \circ \iota_1 = 1_{A_1}$ si verifica come nel caso precedente che tale ψ rende commutativo il diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \underset{f}{\longrightarrow} & B & \underset{g}{\longrightarrow} & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1_{A_1}} & & \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle 1_{A_2}} & & \\ 0 & \longrightarrow & A_1 & \xrightarrow{\iota_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \longrightarrow & 0 \end{array}$$

e che quindi ψ è un isomorfismo di R-moduli.

$(iii) \Rightarrow (i), (ii)$ Consideriamo il seguente diagramma commutativo di omomorfismi di R-moduli

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{\iota_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1_{A_1}} & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle 1_{A_2}} & & \\ 0 & \longrightarrow & A_1 & \underset{f}{\longrightarrow} & B & \underset{g}{\longrightarrow} & A_2 & \longrightarrow & 0 \end{array}$$

dove per ipotesi φ è un isomorfismo perché le due sequenze sono esatte, e pertanto vale $\varphi^{-1} \circ \varphi = 1_{A_1 \oplus A_2}$.

Siccome il diagramma commuta, se definiamo $h : A_2 \longrightarrow B$ come $h = \varphi \circ \iota_2$ (dove $\iota_2 : A_2 \longrightarrow A_1 \oplus A_2$ è tale che $\pi_2 \circ \iota_2 = 1_{A_2}$) troviamo che $g \circ h = g \circ \varphi \circ \iota_2 = 1_{A_2}$; analogamente definendo $k : B \longrightarrow A_1$ come $k = \pi_1 \circ \varphi^{-1}$ (dove $\pi_1 : A_1 \oplus A_2 \longrightarrow A_1$ è tale che $\pi_1 \circ \iota_1 = 1_{A_1}$) risulta $k \circ f = \pi_1 \circ \varphi^{-1} \circ f = 1_{A_1}$.

□

Definizione 1.7. Una sequenza esatta corta che soddisfi una delle condizioni equivalenti del teorema è detta *sequenza esatta spezzante*.

1.3 I moduli proiettivi

Utilizziamo la convenzione che, nel caso in cui R sia un anello unitario, la nozione di R-modulo coincida con quella di R-modulo unitario.

Definizione 1.8. Un modulo P su un anello R è detto *proiettivo* se per ogni diagramma di omomorfismi di R-moduli della forma

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow[g]{} & B & \longrightarrow & 0 \end{array}$$

dove la sequenza $A \xrightarrow{g} B \to 0$ è esatta, esiste un omomomorfismo di R-moduli $h : P \longrightarrow A$ che rende commutativo il seguente diagramma

$$\begin{array}{ccccc} & & P & & \\ & \swarrow{\scriptstyle h} & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow[g]{} & B & \longrightarrow & 0 \end{array}$$

Equivalentemente si ha che P è un R-modulo proiettivo se, presi arbitrariamente due omomorfismi di R-moduli $f : P \longrightarrow B$ e $g : A \longrightarrow B$, con g suriettivo, esiste sempre un omomomorfismo di R-moduli $h : P \longrightarrow A$ tale che $g \circ h = f$.

Teorema 1.3.1. *Ogni modulo libero su un anello unitario è proiettivo.*

Dimostrazione. Sia R un anello unitario; consideriamo il seguente diagramma di omomorfismi di R-moduli

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow[g]{} & B & \longrightarrow & 0 \end{array}$$

dove F è un modulo libero su R, mentre A e B sono R-moduli.
Sia X una base per F e sia $\iota : X \longrightarrow F$ il morfismo canonico di inclusione; per ogni $x \in X$ risulta $f \circ \iota(x) \in B$, dunque essendo g suriettiva deve esistere $a_x \in A$ tale che $g(a_x) = f \circ \iota(x)$. Consideriamo la funzione $X \longrightarrow A$ definita da $x \longmapsto a_x$; dal momento che F è un modulo libero, essa induce un omomorfismo di R-moduli $h : F \longrightarrow A$ tale che $h \circ \iota(x) = a_x$ per ogni $x \in X$. Di conseguenza risulta $g \circ h \circ \iota(x) = f \circ \iota(x)$, ma se $g \circ h$ ed f coincidono sugli elementi della base X allora coincidono su tutto F. Dunque abbiamo provato che esiste un omomorfismo h che fa commutare il diagramma, cioè P è proiettivo. □

Teorema 1.3.2. *Sia R è un anello unitario e sia P un R-modulo, allora sono equivalenti:*

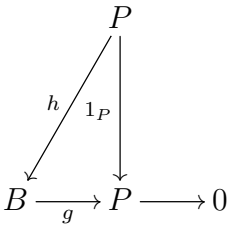
(i) *P è proiettivo;*

(ii) *ogni sequenza corta esatta $0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$ è spezzante, e dunque $B \cong A \oplus P$;*

(iii) esistono un modulo libero F e un R-modulo K tali che $F \cong K \oplus P$.

Dimostrazione. Sia dunque P un R-modulo.

$(i) \Rightarrow (ii)$ Supponiamo che P sia proiettivo; sia $0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$ una sequenza corta esatta (in particolare è quindi esatta la sequenza $B \xrightarrow{g} P \to 0$), allora esiste un omomorfismo $h : P \longrightarrow B$ che rende commutativo il seguente diagramma



Dunque abbiamo provato l'esistenza di un morfismo h tale che $g \circ h = 1_P$, pertanto, per il **Teorema 1.2.2**, la sequenza $0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$ è una sequenza esatta spezzante, e vale quindi $B \cong A \oplus P$.

$(ii) \Rightarrow (iii)$ Ricordando che in generale un qualunque R-modulo è immagine mediante un omomorfismo di un R-modulo libero, possiamo affermare che esiste un epimorfismo $g : F \longrightarrow P$, dove F è un modulo libero su R. Sia $K = \ker g$, in particolare K è un R-modulo contenuto in F, allora la sequenza $0 \to K \xrightarrow{i} F \xrightarrow{g} P \to 0$ risulta essere esatta per costruzione. Ma per ipotesi una tale sequenza corta esatta è necessariamente spezzante, dunque in particolare vale $F \cong K \oplus P$.

$(iii) \Rightarrow (i)$ Per ipotesi $F \cong K \oplus P$, dove F è un modulo libero e K è un R-modulo; denotiamo con π e con ι rispettivamente le composizioni $F \cong K \oplus P \longrightarrow P$, dove la seconda funzione è il morfismo di proiezione canonica, e $P \longrightarrow K \oplus P \cong F$, dove la prima funzione è il morfismo di iniezione canonica. Consideriamo, per una qualunque sequenza esatta

$A \xrightarrow{g} B \longrightarrow 0$, il seguente diagramma di omomorfismi di R-moduli

$$\begin{array}{ccccc} & & F & & \\ & & \downarrow{\scriptstyle \pi} & & \\ & & P & & \\ & & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow[g]{} & B & \longrightarrow & 0 \end{array}$$

Ora, per quanto visto nel teorema precedente, il modulo F essendo un modulo libero è proiettivo, e quindi esiste un omomorfismo $\tilde{h} : F \longrightarrow A$ tale che $g \circ \tilde{h} = f \circ \pi$. Sia ora $h : P \longrightarrow A$ il morfismo $h = \tilde{h} \circ \iota$, risulta allora $g \circ h = g \circ \tilde{h} \circ \iota = f \circ \pi \circ \iota = f$; pertanto possiamo concludere che P è proiettivo.

□

1.4 Anello dei quozienti e localizzazione

Definizione 1.9. Un sottoinsieme $S \neq \emptyset$ di un anello R è detto *parte moltiplicativa* se per ogni $a, b \in S$ risulta $ab \in S$.

Esempio 1.2. Sia R un anello unitario, sono parti moltiplicative di R l'insieme delle unità, e l'insieme costituito da tutti gli elementi che non sono 0-divisori; in particolare allora, in un dominio d'integrità, l'insieme degli elementi non nulli è una parte moltiplicativa.

Teorema 1.4.1. *Sia S una parte moltiplicativa di un anello commutativo R, la relazione definita su $R \times S$ da $(r, s) \sim (r', s') \Leftrightarrow s_1(rs' - r's) = 0$ per qualche $s_1 \in S$ è una relazione d'equivalenza.*
In particolare, se R non ha 0-divisori e $0_R \notin S$, tale relazione si riduce alla seguente: $(r, s) \sim (r', s') \Leftrightarrow rs' - r's = 0$.

Dimostrazione. La relazione sopra definita è una relazione d'equivalenza, in quanto gode delle proprietà seguenti

(i) riflessiva, poiché $(r,s) \sim (r,s)$ per ogni $(r,s) \in R \times S$, dal momento che $rs - rs = 0$;

(ii) simmetrica, perché se $(r,s) \sim (r',s')$ vale $s_1rs' - s_1r's = 0$ per qualche $s_1 \in S$, ma allora $s_1(r's - rs') = 0$, quindi vale $(r',s') \sim (r,s)$;

(iii) transitiva, infatti se $(r,s) \sim (r',s')$, $(r',s') \sim (r'',s'')$, significa che esistono $s_1, s_2 \in S$ tali che $s_1(rs' - r's) = 0$, $s_2(r's'' - r''s') = 0$ (da cui $s_2r''s' = s_2r's''$), ma allora, posto $t = s_1s_2s' \in S$, risulta $t(rs'' - r''s) = s_1[s_2s'rs'' - (s_2s'r'')s] = s_1[s_2s'rs'' - s_2r's''s] = s_1[s_2s''(rs' - sr')] = s_2s''[s_1(rs' - s'r)] = 0$.

□

Osservazione 5. Sotto le ipotesi precedenti, denotando con r/s e con $S^{-1}R$ rispettivamente la classe di equivalenza di $(r,s) \in R \times S$ e l'insieme di tutte le classi di equivalenza di $R \times S$, rispetto alla relazione d'equivalenza $\sim$ sopra definita, valgono le seguenti proprietà:

(i) $r/s = r'/s' \Leftrightarrow s_1(rs' - r's) = 0$ per qualche $s_1 \in S$;

(ii) $tr/ts = r/s$ per ogni $r \in R$ e per ogni $s, t \in S$;

(iii) se $0_R \in S$ allora $S^{-1}R$ è costituito da una sola classe di equivalenza.

Teorema 1.4.2. *Sia S una parte moltiplicativa di un anello commutativo R, allora $S^{-1}R$ risulta essere un anello commutativo unitario, con le operazioni di somma e prodotto definite nel modo seguente: $r/s + r'/s' = (rs' + r's)/ss'$ e $(r/s)(r'/s') = rr'/ss'$.*

Dimostrazione. Verifichiamo innanzitutto che tali operazioni sono ben poste in $S^{-1}R$, cioè che sono indipendenti dal rappresentante della classe di equivalenza scelto ($(rs' + r's)/ss'$ e rr'/ss' sono chiaramente elementi di $S^{-1}R$). Siano $r_1/s_1 = r/s$, $r_1'/s_1' = r'/s'$, proviamo che allora $r/s + r'/s' =$

$(rs' + r's)/ss' = (r_1s'_1 + r'_1s_1)/s_1s'_1 = r_1/s_1 + r'_1/s'_1$ e $(r/s)(r'/s') = rr'/ss' = r_1r'_1/s_1s'_1 = (r_1/s_1)(r'_1/s'_1)$. Ora, per ipotesi esistono $t_1, t_2 \in S$ tali che $t_1(rs_1 - r_1s) = 0$, $t_2(r's'_1 - r'_1s') = 0$; moltiplicando la prima equazione per $t_2s's'_1$ e la seconda per t_1ss_1, e sommando le espressioni trovate, si ottiene $t_1t_2[s's'_1(rs_1 - r_1s) + ss_1(r's'_1 - r'_1s')] = t_1t_2[s_1s'_1(rs' + r's) - ss'(r_1s'_1 + r'_1s_1)] = 0$. Dal momento che $t_1t_2 \in S$ questo significa che vale $s_1s'_1(s'r + sr') = ss'(r_1s'_1 + r'_1s_1)$, da cui $(rs' + r's)/ss' = (r_1s'_1 + r'_1s_1)/s_1s'_1$. In modo analogo si mostra che è ben definito anche il prodotto.

A questo punto è facile verificare che $S^{-1}R$ è un anello commutativo unitario; in particolare l'elemento neutro additivo di $S^{-1}R$ è $0/s$ (con $0/s = 0/s'$ per ogni $s, s' \in S$), e l'elemento inverso additivo di r/s è $-r/s$; mentre l'elemento neutro moltiplicativo è dato da s/s (con $s/s = s'/s'$ per ogni $s, s' \in S$). □

Definizione 1.10. Siano R un anello commutativo e S una sua parte moltiplicativa, allora $S^{-1}R$ è detto *anello dei quozienti o delle frazioni di R rispetto ad S*.

Proposizione 1.4.3. *Sia R un anello commutativo privo di 0-divisori, e sia S una sua parte moltiplicativa tale che $0_R \notin S$, allora $S^{-1}R$ risulta essere un dominio d'integrità.*

In particolare, se S è esattamente l'insieme di tutti gli elementi non nulli di R, $S^{-1}R$ è un campo.

Dimostrazione. Per il teorema precedente $S^{-1}R$ è un anello commutativo unitario; mostriamo che non ha 0-divisori. Abbiamo la relazione d'equivalenza $r/s = r'/s' \Leftrightarrow rs' - r's = 0$, ne viene $r/s = 0/s \Leftrightarrow rs = 0$, ma dal momento che per ipotesi R non ha 0-divisori e $0_R \notin S$, questo implica che $r = 0$; dunque $(r/s)(r'/s') = rr'/ss' = 0_{S^{-1}R} \Leftrightarrow rr' = 0$, ma allora necessariamente almeno uno tra r ed r' dev'essere nullo, da cui rispettivamente segue che $r/s = 0_{S^{-1}R}$ oppure $r'/s' = 0_{S^{-1}R}$.

Nel caso in cui S sia composto da tutti gli elementi non nulli di R, allora

per ogni $r \neq 0$ l'elemento inverso di $r/s \in S^{-1}R$ è s/r, che appartiene a sua volta a $S^{-1}R$. □

Teorema 1.4.4. *Sia S una parte moltiplicativa di un anello commutativo R, allora*

(i) la funzione $\varphi_S : R \longrightarrow S^{-1}R$ definita da $r \longmapsto rs/s$, con $s \in S$ qualunque, è un omomorfismo di anelli, tale che $\varphi_S(s)$ risulta essere un'unità di $S^{-1}R$ per ogni $s \in S$;

(ii) se R non contiene 0-divisori e $0_R \notin S$, allora il morfismo φ_S è iniettivo.

Dimostrazione. Osserviamo innanzitutto che l'applicazione φ_S è ben posta, in quanto $rs/s = rs'/s'$ per ogni $s, s' \in S$.

(i) Si verifica che φ_S è un morfismo di anelli, e che l'elemento $s/s^2 \in S^{-1}R$ è l'inverso moltiplicativo di $s^2/s = \varphi_S(s) \in S^{-1}R$, per ogni $s \in S$.

(ii) Sia $r \in R$ tale che $\varphi_S(r) = rs/s = 0_{S^{-1}R}$, allora $rs/s = 0/s$, cioè deve valere $rs^2s_1 = 0$ per qualche $s_1 \in S$; ma ora $s^2s_1 \in S$, e quindi per ipotesi $s^2s_1 \neq 0$, dunque necessariamente $r = 0$, dal momento che R non ha 0-divisori.

□

Osservazione 6. Se R è un dominio d'integrità, ed S è una sua parte moltiplicativa tale che $0_R \notin S$, allora il morfismo $\varphi_S : R \longrightarrow S^{-1}R$ immerge R nel suo anello dei quozienti.
Pertanto è lecito identificare il dominio R con la sua immagine mediante φ_S, e considerarlo come sottoanello di $S^{-1}R$.

In questa seconda parte della sezione, benchè la maggior parte dei risultati presentati sia valida sotto condizioni più deboli, si è scelto di limitarsi a considerare il caso in cui R sia un anello commutativo unitario, e di supporre che la parte moltiplicativa S considerata sia tale che $0_R \notin S$.

Teorema 1.4.5. *Sia S una parte moltiplicativa di R; se I è un ideale di R, allora l'insieme $S^{-1}I$ è un ideale di $S^{-1}R$.*

Dimostrazione. È importante notare che se $a/s \in S^{-1}I$ non necessariamente $a \in I$, infatti è sufficiente che esistano $r \in I$, $t \in S$ tali che l'elemento r/t appartenga alla classe di equivalenza a/s; questo significa che deve valere $s_1ta = s_1sr$ per qualche $s_1 \in S$, ma poiché r appartiene all'ideale I, otteniamo in particolare che se $a/s \in S^{-1}I$ allora esiste $t_1 = s_1t \in S$ tale che $t_1a \in I$.
Siano a/s, $a'/s' \in S^{-1}I$, dobbiamo mostrare che $(a/s) - (a'/s') \in S^{-1}I$; per quanto appena osservato esistono $t, t' \in S$ tali che $ta, t'a' \in I$, scriviamo allora $(a/s)-(a'/s') = (ta/ts)-(t'a'/t's') = (tat's'-t'a'ts)/tst's'$, ma dal momento che I è un ideale, poiché $ta, t'a' \in I$ e $t', s', t, s \in R$, risulta $tat's' - t'a'ts \in I$, e sicuramente $tst's' \in S$ perché S è una parte moltiplicativa, dunque tale elemento appartiene a $S^{-1}I$. Allo stesso modo, se $a/s \in S^{-1}I$ e t è un elemento di S tale che $ta \in I$, allora per ogni $r/u \in S^{-1}R$ vale $(r/u)(a/s) = (r/u)(ta/ts) = rta/uts \in S^{-1}I$, infatti $r(ta) \in I$ e $uts \in S$. □

L'ideale $S^{-1}I$ è detto *estensione di I in $S^{-1}R$.*

Proposizione 1.4.6. *Sia S una parte moltiplicativa di R; sia I un ideale di R, allora l'ideale $S^{-1}I$ coincide con tutto $S^{-1}R$ se e solo se $S \cap I \neq \emptyset$.*

Dimostrazione. Supponiamo che $S^{-1}I = S^{-1}R$, allora $\varphi_S^{-1}(S^{-1}I) = R$, e dunque in particolare $\varphi_S(1_R) = a/s$ per qualche $a \in I$, $s \in S$; ora, poiché $\varphi_S(1_R) = 1_Rs/s$, deve esistere $s_1 \in S$ tale che $s_1sa = s_1s^2$, ma $s_1sa \in I$ mentre $s_1s^2 \in S$, e pertanto l'elemento $s_1sa = s_1s^2 \in S \cap I$.
Viceversa, se $S \cap I \neq \emptyset$, possiamo considerare un elemento s appartenente a tale intersezione, ma allora $s/s = 1_{S^{-1}R} \in S^{-1}I$, da cui segue che necessariamente $S^{-1}I = S^{-1}R$. □

Teorema 1.4.7. *Sia S una parte moltiplicativa di R; se J è un ideale di $S^{-1}R$, allora l'insieme $\varphi_S^{-1}(J)$ è un ideale di R.*

Dimostrazione. Siano $a, b \in \varphi_S^{-1}(J)$, allora $\varphi_S(a), \varphi_S(b) \in J$, che è un ideale, quindi $\varphi_S(a-b) = \varphi_S(a) - \varphi_S(b) \in J$, da cui $a - b \in \varphi_S^{-1}(J)$; inoltre per $r \in R$ vale $\varphi_S(r) \in S^{-1}R$ e pertanto, essendo J un ideale di $S^{-1}R$, risulta $\varphi_S(ra) = \varphi_S(r)\varphi_S(a) \in J$ che implica $ra \in \varphi_S^{-1}(J)$. □

L'ideale $\varphi_S^{-1}(J)$ è detto *contrazione di J in R.*

Teorema 1.4.8. *Sia S una parte moltiplicativa di R, siano I un ideale di R e J un ideale di $S^{-1}R$, allora*

(i) $I \subseteq \varphi_S^{-1}(S^{-1}I)$*;*

(ii) sia $I = \varphi_S^{-1}(J)$, risulta $S^{-1}I = J$; in altre parole tutti gli ideali di $S^{-1}R$ sono della forma $S^{-1}I$ con I ideale di R.

Dimostrazione. (i) Se $a \in I$, allora per ogni $s \in S$ vale $as \in I$, di conseguenza $\varphi_S(s) = as/s \in S^{-1}I$, e quindi $a \in \varphi_S^{-1}(S^{-1}I)$; complessivamente si ha l'inclusione $I \subseteq \varphi_S^{-1}(S^{-1}I)$.

(ii) Innanzitutto osserviamo che, avendo definito $I = \varphi_S^{-1}(J)$, dove per ipotesi J è un ideale di $S^{-1}R$, I risulta essere un ideale di R. Consideriamo dunque l'ideale $S^{-1}I$, i cui elementi sono della forma r/s con r tale che $\varphi_S(r) \in J$; per ogni $r/s \in S^{-1}I$ si trova allora che $r/s = (1_R/s)(rs/s) = (1_R/s)\varphi_S(r) \in J$, dal momento che J è un ideale di $S^{-1}R$, e quindi è provata l'inclusione $S^{-1}I \subseteq J$. D'altra parte, preso un qualunque elemento r/s nell'ideale J si ha $\varphi_S(r) = rs/s = (r/s)(s^2/s) \in J$, cioè $r \in \varphi_S^{-1}(J) = I$, ma allora $r/s \in S^{-1}I$; dalla doppia inclusione segue che $J = S^{-1}I$.

□

Lemma 1.4.9. *Sia S una parte moltiplicativa di R, e sia P un ideale primo di R disgiunto da S, allora $S^{-1}P$ è un ideale primo di $S^{-1}R$ e risulta $\varphi_S^{-1}(S^{-1}P) = P$.*

Dimostrazione. Per la **Proposizione 1.4.6**, poiché $S \cap P = \emptyset$, vale $S^{-1}P \neq S^{-1}R$; mostriamo che $S^{-1}P$ è un ideale primo. Supponiamo che $(r/s)(r'/s') \in S^{-1}P$, allora devono esistere $a \in P$, $t \in S$ tali che $rr'/ss' = a/t$, ovvero deve valere l'uguaglianza $s_1trr' = s_1ss'a$, per qualche $s_1 \in S$; dal momento che a appartiene all'ideale P, in particolare ne segue che $s_1trr' \in P$. Ora, siccome P è un ideale primo, il fatto che $s_1t \in S$, che per ipotesi è disgiunto da P, implica che necessariamente $rr' \in P$, e quindi che almeno uno tra r e r' deve appartenere a P. Ma allora si ha che $r/s \in S^{-1}P$ oppure $r'/s' \in S^{-1}P$, che equivale a dire che l'ideale $S^{-1}P$ è primo.
A questo punto verifichiamo che vale l'uguaglianza $\varphi_S^{-1}(S^{-1}P) = P$, dove l'inclusione $P \subseteq \varphi_S^{-1}(S^{-1}P)$ segue dal teorema precedente. Sia dunque $r \in \varphi_S^{-1}(S^{-1}P)$, allora $\varphi_S(r) = rs/s \in S^{-1}P$ e quindi deve valere $rs/s = a/t$ per qualche $a \in P$, $t \in S$, ma questo comporta che deve esistere $s_1 \in S$ tale che $s_1trs = s_1sa \in P$, da cui, essendo $s_1, t, s \in S$ con $S \cap P = \emptyset$, segue che $r \in P$; e questo mostra che vale anche l'inclusione inversa. □

Teorema 1.4.10. *Sia S una parte moltiplicativa di R; c'è una corrispondenza biunivoca tra l'insieme $\mathscr{U}$ degli ideali primi di R disgiunti da S e l'insieme $\mathscr{V}$ degli ideale primi di $S^{-1}R$, data dalla funzione $P \longmapsto S^{-1}P$.*

Dimostrazione. Il lemma precedente assicura che se $P \in \mathscr{U}$ allora $S^{-1}P \in \mathscr{V}$, e che la funzione $\mathscr{U} \longrightarrow \mathscr{V}$, definita da $P \longmapsto S^{-1}P$, è iniettiva; dobbiamo mostrare che tale applicazione è anche suriettiva. Sia dunque J un ideale primo di $S^{-1}R$ e sia $I = \varphi_S^{-1}(J)$, per il **Teorema 1.4.8** risulta $S^{-1}I = J$, pertanto è sufficiente mostrare che tale $I \in \mathscr{U}$; ora, dal momento che J è un ideale primo, vale in particolare $J = S^{-1}I \neq S^{-1}R$, e quindi $I \cap S = \emptyset$, per il **Lemma 1.4.6**. A questo punto rimane solo da provare che l'ideale $I = \varphi_S^{-1}(J)$ è primo, ma se $ab \in I$ per definizione si ha che $\varphi_S(ab) = \varphi_S(a)\varphi_S(b) \in J$, ed essendo J un ideale primo questo implica che necessariamente $\varphi_S(a) \in J$ oppure $\varphi_S(b) \in J$, da cui $a \in I$ oppure $b \in I$. □

Osservazione 7. Sia P un ideale primo di R, allora $R \setminus P$ è una parte moltiplicative di R; infatti, in tal caso, per ogni $a, b \in R$ vale la proprietà $ab \in P \Rightarrow a \in P \ \vee \ b \in P$, la cui contronominale $(a, b \notin P \Rightarrow ab \notin P)$ è una condizione equivalente al fatto che l'insieme $R \setminus P$ sia moltiplicativamente chiuso in R.

Definizione 1.11. Sia R un anello commutativo unitario e sia P un suo ideale primo, si definisce *localizzazione di R in P*, e si denota con R_P, l'anello dei quozienti $S^{-1}R$ dove $S = R \setminus P$.
Inoltre, per ogni ideale I di R, l'ideale $S^{-1}I$ di R_P si denota con I_P.

Teorema 1.4.11. *Sia P un ideale primo di un anello commutativo unitario R, allora*

(i) c'è una corrispondenza biunivoca tra l'insieme degli ideali primi di R contenuti in P e l'insieme degli ideali primi di R_P, data dalla funzione $Q \longmapsto Q_P$;

(ii) l'ideale P_P è l'unico ideale massimale di R_P.

Dimostrazione. Abbiamo definito $R_P = S^{-1}R$, dove $S = R \setminus P$.

(i) Una volta osservato che gli ideali contenuti in P sono esattamente quelli disgiunti da S, la tesi è una conseguenza immediata del teorema precedente.

(ii) Ogni ideale massimale di R_P, è in particolare un ideale primo, ed è quindi della forma Q_P con Q ideale primo di R, $Q \subseteq P$; ora, $Q \subseteq P$ implica $Q_P \subseteq P_P$, e dal momento che P è chiaramente disgiunto da $S = R \setminus P$, per la **Proposizione 1.4.6**, $P_P \neq R_P$. Abbiamo così trovato $Q_P \subseteq P_P \neq R_P$, da cui segue che necessariamente $Q_P = P_P$, perché Q_P è un ideale primo; pertanto P_P è l'unico ideale massimale di R_P.

□

1.5 Estensioni di anelli intere

In questa sezione ogni volta che si fa riferimento ad un anello si sottintende che esso sia commutativo e unitario.

Definizione 1.12. Sia S un anello commutativo unitario, e sia R un suo sottoanello che contiene 1_S, si dice allora che S è una *estensione dell'anello* R.
Diremo brevemente che $R \subseteq S$ è un'estensione di anelli.

Definizione 1.13. Sia $R \subseteq S$ un'estensione di anelli, allora un elemento $s \in S$ è detto *intero su* R se esiste un polinomio monico $f(x) \in R[x]$ avente s come radice.
Se ogni elemento di S è intero su R, allora l'estensione di anelli $R \subseteq S$ è detta *estensione intera*.

Teorema 1.5.1. *Sia $R \subseteq S$ un'estensione di anelli, e sia $s \in S$, allora sono equivalenti le seguenti condizioni*

(i) *s è intero su R;*

(ii) *$R[s]$ è un R-modulo finitamente generato;*

(iii) *esiste un sottoanello T di S che contiene 1_S e $R[s]$, e che è finitamente generato come R-modulo;*

(iv) *esiste un $R[s]$-sottomodulo B di S, che è finitamente generato come R-modulo, tale che $Ann(B) = \{\, a \in R[s] \mid aB = 0_B \,\} = \{\, 0 \,\}$.*

Dimostrazione. Consideriamo un'estensione di anelli $R \subseteq S$, e un elemento $s \in S$.

$(i) \Rightarrow (ii)$ Per ipotesi esiste un polinomio $f(x) \in R[x]$ monico tale che $f(s) = 0$, sia $deg(f) = n$; ora, ogni elemento di $R[s]$ è della forma $g(s)$ con $g(x) \in R[x]$, e ricordiamo che possiamo sempre scrivere $g(x) =$

$q(x)f(x) + r(x)$, dove $q(x), r(x) \in R[x]$ e vale $deg(r) < deg(f) = n$. Troviamo così che in S vale $g(s) = q(s)f(s) + r(s) = 0 + r(s) = r(s)$, con $r(x) \in R[x]$ tale che $deg(r) < n$, e pertanto $g(s)$ è una combinazione lineare a coefficienti in R di $1_R, s, s^2, \ldots, s^m$, dove $m = deg(r) < n$; complessivamente si ha che $1_R, s, s^2, \ldots, s^{n-1}$ sono generatori di $R[s]$ come modulo su R.

$(ii) \Rightarrow (iii)$ È sufficiente prendere $T = R[s]$; infatti $R[s]$ è banalmente un sottoanello di S che contiene 1_S e $R[s]$, ed è finitamente generato come R-modulo per ipotesi.

$(iii) \Rightarrow (iv)$ dal momento che T è un sottoanello di S che contiene 1_S e $R[s]$, possiamo considerare le estensioni di anelli $R \subseteq R[s] \subseteq T \subseteq S$; sia $B = T$, allora B è un sottoanello di S ed è anche un modulo su $R[s]$, e in particolare è finitamente generato, perché per ipotesi lo è T come R-modulo. Inoltre, poiché $1_S \in B$, se un elemento $a \in R[s]$ è tale che $aB = 0_B$, allora risulta $a = a1_S = 0_B$; complessivamente si ha $Ann(B) = \{\, a \in R[s] \mid aB = 0_B \,\} = \{\, 0 \,\}$.

$(iv) \Rightarrow (i)$ Ricordiamo preliminarmente che, data una matrice quadrata A di ordine n, e indicata con A^* la matrice dei cofattori di A, ovvero la matrice avente come elemento di posto i, j il complemento algebrico dell'elemento di posto i, j di A (cioè $(-1)^{i+j} \det A_{ij}$, dove A_{ij} è la matrice ottenuta da A cancellando la i-esima riga e la j-esima colonna), vale $(A^*)^t \cdot A = \det A \cdot I_n$, ove il simbolo B^t indica la matrice trasposta della matrice B.

Ora, per ipotesi B è un R-modulo finitamente generato, siano $b_1, \ldots, b_n$ i suoi generatori; siccome B è un modulo anche su $R[s]$, in particolare per ogni $i = 1, \ldots, n$ si ha che $sb_i \in B$, e quindi deve essere una combinazione lineare in R dei generatori di B. Siano $r_{ij} \in R$ tali che $sb_i = r_{i1}b_1 + \cdots + r_{in}b_n$, per $i = 1, \ldots, n$, da cui troviamo

$r_{i1}b_1 + \cdots + (r_{ii} - s)b_i + \cdots + r_{in}b_n = 0$; abbiamo allora complessivamente l'identità matriciale $(M - sI_n) \cdot (b_1, \ldots, b_n)^t = (0, \ldots, 0)^t$, dove M è la matrice $M = (r_{ij})$ con $i, j = 1, \ldots, n$. A questo punto, moltiplicando a sinistra per la matrice $((M - sI_n)^*)^t$ e tenendo conto di quanto avevamo osservato inizialmente, otteniamo
$((M - sI_n)^*)^t \cdot (M - sI_n) \cdot (b_1, \ldots, b_n)^t = ((M - sI_n)^*)^t \cdot (0, \ldots, 0)^t$,
quindi $\det(M - sI_n) \cdot (b_1, \ldots, b_n)^t = (0, \ldots, 0)^t$. Sia ora d l'elemento $d = \det(M - sI_n) \in R[s]$, risulta $db_i = 0$ per ogni $i = 1, \ldots, n$, e siccome $b_1, \ldots, b_n$ generano B questo implica $dB = 0$; ma per ipotesi $Ann(B) = \{\, a \in R[s] \mid aB = 0_B \,\} = \{\, 0 \,\}$, e quindi $d = 0$. Sia infine $f(x) \in R[x]$ il polinomio $f(x) = \det(M - xI_n)$, è lecito supporre che $f(x)$ sia monico (perché lo è a meno del segno), per quanto osservato vale $f(s) = \det(M - sI_n) = d = 0$, e di conseguenza s è intero su R.

□

Corollario 1.5.2. *Sia $R \subseteq S$ un'estensione di anelli, se S è finitamente generato come R-modulo allora l'estensione è intera.*

Dimostrazione. Per ogni $s \in S$, l'anello S stesso contiene banalmente sia 1_S che $R[s]$, ed è finitamente generato come modulo su R per ipotesi, pertanto per il teorema precedente s è intero su R; e quindi l'estensione $R \subseteq S$ è intera. □

Teorema 1.5.3. *Sia $R \subseteq S$ un'estensione di anelli, siano $s_1, \ldots, s_t \in S$ interi su R, allora $R[s_1, \ldots, s_t]$ è un R-modulo finitamente generato e un'estensione intera di R.*

Dimostrazione. Osserviamo che chiaramente ciascun s_i, essendo intero su R, è intero su $R[s_1, \ldots, s_{i-1}]$, per ogni $i = 1, \ldots, t$; consideriamo le estensioni di anelli successive $R \subseteq R[s_1] \subseteq R[s_1, s_2] \subseteq \ldots \subseteq R[s_1, \ldots, s_t]$. Ora, dal momento che $R[s_1, \ldots, s_i] = R[s_1, \ldots, s_{i-1}][s_i]$, con s_i intero, per il **Teorema**

1.5.1 si ha che $R[s_1, \ldots, s_i]$ risulta essere finitamente generato come modulo su $R[s_1, \ldots, s_{i-1}]$ per ogni $i = 1, \ldots, t$. Complessivamente ne viene che $R[s_1, \ldots, s_t]$ è un R-modulo finitamente generato; ma allora l'estensione di anelli $R \subseteq R[s_1, \ldots, s_t]$ è intera. □

Teorema 1.5.4. *Siano $R \subseteq S$, $S \subseteq T$ estensioni di anelli intere, allora $R \subseteq T$ è a sua volta un'estensione intera.*

Dimostrazione. Chiaramente $R \subseteq T$ è un'estensione di anelli; mostriamo che ogni elemento di T è intero su R. Sia $t \in T$, poiché l'estensione $S \subseteq T$ è intera, esiste un polinomio monico $f(x) \in S[x]$ tale che $f(t) = 0$; sia $f(x) = \sum_{i=1}^{n} s_i x^i$, in particolare allora $f(x) \in R[s_0, s_1, \ldots, s_n] \subseteq S$, e quindi l'elemento t è intero su $R[s_0, \ldots, s_n]$. Dunque $R[s_0, \ldots, s_n, t]$ è finitamente generato come modulo su $R[s_0, \ldots, s_n]$ (**Teorema 1.5.1**); ma ora $s_0, \ldots, s_n$ sono interi su R, perché lo è l'estensione $R \subseteq S$, e per il teorema precedente $R[s_0, \ldots, s_n]$ è quindi un R-modulo finitamente generato. Pertanto $R[s_0, \ldots, s_n, t]$, e di conseguenza anche $R[t]$, risulta essere a sua volta finitamente generato come R-modulo; possiamo quindi concludere che l'elemento $t \in T$ è intero su R. □

Teorema 1.5.5. *Sia $R \subseteq S$ un'estensione di anelli, e sia $\hat{R}$ l'insieme degli elementi di S interi su R, allora $\hat{R}$ risulta essere un anello, e pertanto è un'estensione intera di R; in particolare $\hat{R}$ contiene tutti i sottoanelli di S che sono estensioni intere di R.*

Dimostrazione. Mostriamo che l'insieme $\hat{R}$ degli elementi di S interi su R è un anello; siano dunque $s, t \in \hat{R} \subseteq S$, in particolare tali elementi appartengono all'anello $R[s, t]$, e dal momento che s e t sono interi su R, l'estensione $R \subseteq R[s, t]$ risulta essere intera. Ma questo significa che tutti gli elementi di $R[s, t]$ sono interi su R, e quindi appartengono a $\hat{R}$; essendo $R[s, t]$ un anello ne viene dunque che $s - t$, $st \in \hat{R}$, e quindi $\hat{R}$ è un sottoanello di S.
A questo punto, le restanti affermazioni sono conseguenze immediate della definizione di $\hat{R}$. □

Definizione 1.14. Sia $R \subseteq S$ un'estensione di anelli, allora l'anello $\hat{R}$ degli elementi di S interi su R è detto *chiusura integrale di R in S*.
Se vale $\hat{R} = R$, si dice che l'anello R è *integralmente chiuso in S*.

Nel caso in cui R sia un dominio d'integrità integralmente chiuso nel suo campo dei quozienti, si può dire semplicemente che R è integralmente chiuso, sottintendendo quale sia l'estensione considerata.

Teorema 1.5.6. *Sia R un dominio d'integrità integralmente chiuso, e sia S una sua parte moltiplicativa tale che $0_R \notin S$, allora anche $S^{-1}R$ risulta essere un dominio d'integrità integralmente chiuso.*

Dimostrazione. Dal momento che R non ha 0-divisori e che $0_R \notin S$, segue dalla **Proposizione 1.4.3** che $S^{-1}R$ è un dominio d'integrità; siano allora $Q(R)$ e $Q(S^{-1}R)$ i campi dei quozienti di R e $S^{-1}R$ rispettivamente. Ricordiamo inoltre che, sotto tali ipotesi, $S^{-1}R$ contiene un sottoanello che è una copia isomorfa di R, con cui è lecito identificare R stesso (**Osservazione 6**); estendendo tale identificazione ai rispettivi campi dei quozienti, si può considerare $Q(R)$ come un sottocampo di $Q(S^{-1}R)$. Si verifica che in realtà i due campi coincidono.
Mostriamo che $S^{-1}R$ è integralmente chiuso; sia dunque $u \in Q(S^{-1}R)$ un elemento intero su $S^{-1}R$, allora deve esistere un polinomio monico a coefficienti in $S^{-1}R$ che si annulla su u, cioè vale $u^n + (r_{n-1}/s_{n-1})u^{n-1} + \cdots + (r_1/s_1)u + (r_0/s_0)$, con $r_i \in R$, $s_i \in S$. Moltiplicando tale equazione per s^n, dove $s = s_0 \cdots s_{n-1} \in S$, troviamo $(su)^n + (s_0 \cdots s_{n-2})r_{n-1}(su)^{n-1} + \cdots + (s_0 s_2 \cdots s_{n-1})r_1 s^{n-2}(su) + (s_1 \cdots s_{n-1})r_0 s^{n-1} = 0$, ovvero un polinomio a coefficienti in R che si annulla in su; pertanto su è intero su R. Abbiamo dunque $su \in Q(S^{-1}R) = Q(R)$, ma per ipotesi R è integralmente chiuso, e quindi necessariamente $su \in R$, da cui segue che $u = su/s \in S^{-1}R$. Complessivamente vale allora $Q(S^{-1}R) = S^{-1}R$, cioè l'anello dei quozienti $S^{-1}R$ è integralmente chiuso. □

Capitolo 2

Domini di Dedekind

Definizione 2.1. Siano $A_1, \ldots, A_n$ sottoinsiemi non vuoti di un anello R, si denota $A_1 \cdots A_n$ l'insieme di tutte le somme finite di elementi della forma $a_1 \cdots a_n$ dove $a_j \in A_j$ per ogni $j = 1, \ldots, n$.
In particolare se $A_1, \ldots, A_n$ sono ideali di R allora l'insieme $A_1 \cdots A_n$ è a sua volta un ideale di R, detto *ideale prodotto degli ideali* $A_1, \ldots, A_n$.

Definizione 2.2. Un ideale P di un anello R è detto *ideale primo* se $P \neq R$ e, ogni volta che l'ideale prodotto AB, di due ideali A, B di R, è contenuto in P, allora necessariamente almeno uno tra A e B deve essere contenuto in P.

Definizione 2.3. Un *Dominio di Dedekind* è un dominio d'integrità in cui ogni ideale proprio si fattorizza come prodotto di un numero finito di ideali primi.

Osservazione 8. I domini a ideali principali godono di tale proprietà di fattorizzazione per gli ideali, mostreremo con un esempio che però non ne sono caratterizzati; pertanto tutti i PID sono in particolare domini di Dedekind, ma questi ultimi non sono necessariamente a ideali principali.

Introduciamo ora il concetto di ideale frazionario, che è essenziale per studiare la classe di domini appena introdotta.

2.1 Gli ideali frazionari

Definizione 2.4. Sia R un dominio d'integrità e sia K il suo campo dei quozienti, un *ideale frazionario di* R è un R-sottomodulo I di K non banale per cui esiste un elemento $a \in R$, $a \neq 0$ tale che $aI \subseteq R$.

Osserviamo che ogni ideale non banale di R è un R-sottomodulo di K contenuto in R stesso, e dunque è ideale frazionario, e che, viceversa, se un ideale frazionario di R è contenuto in R allora è chiaramente un ideale di R.

Osservazione 9. Sia I un ideale frazionario di un dominio R, sia a elemento non nullo di R tale che $aI \subseteq R$, allora aI risulta essere ideale di R.
Si ha inoltre che l'applicazione $\varphi : I \longrightarrow aI$ definita da $x \longmapsto ax$ è un isomorfismo di R-moduli; infatti per ogni $x, y \in I$ e per ogni $h, k \in R$ si ha $\varphi(hx + ky) = a(hx + ky) = hax + kay = h\varphi(x) + k\varphi(y)$, inoltre φ risulta essere banalmente suriettiva, ed anche iniettiva dal momento che per ogni $x \in I$ si ha $ax \in R$ con $a \in R, a \neq 0$. Possiamo dunque affermare che ogni ideale frazionario è isomorfo come R-modulo ad un ideale di R.

Proposizione 2.1.1. *Sia R un dominio d'integrità e sia K il suo campo dei quozienti, allora ogni R-sottomodulo I di K non banale e finitamente generato è un ideale frazionario di R.*

Dimostrazione. Sia I generato dagli elementi $b_1, \ldots, b_n \in K$, vale $I = Rb_1 + \cdots + Rb_n$ dove ogni b_i è un elemento del campo dei quozienti di R e dunque è della forma $b_i = c_i/a_i$ con $c_i, a_i \in R$, $a_i \neq 0$; ponendo $a = a_1 \cdots a_n$ risulta $a \in R$ non nullo e tale che $aI = Ra_2 \cdots a_n c_1 + \cdots + Ra_1 \cdots a_{n-1} c_n \subseteq R$. □

Teorema 2.1.2. *Sia R un dominio d'integrità e sia K il suo campo dei quozienti; allora l'insieme $\mathscr{M}$ degli ideali frazionari di R con l'operazione prodotto definita da $IJ = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I,\, b_i \in J,\, n \in \mathbb{N}^* \right\}$ è un monoide commutativo, avente elemento neutro R.*

Dimostrazione. Osserviamo innanzitutto che l'operazione definita è commutativa dal momento che lo è il prodotto in K, e che risulta $IR = RI = I$ per ogni I ideale frazionario di R.

Mostriamo che per ogni $I, J \in \mathscr{M}$ risulta $IJ \in \mathscr{M}$, ovvero che IJ è a sua volta un R-sottomodulo di K tale che $cIJ \subseteq R$ per qualche $c \in R$, $c \neq 0$. Chiaramente l'insieme $IJ = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I,\, b_i \in J,\, n \in \mathbb{N}^* \right\}$ è un sottoinsieme non vuoto di K, ed è chiuso rispetto al prodotto per elementi dell'anello R; si ha inoltre che se $\sum_{i=1}^{n} v_i w_i$, $\sum_{j=1}^{m} x_j y_j$ sono arbitrari elementi di IJ (cioè $v_i, x_j \in I$, $w_i, y_j \in J$ per ogni $i = 1, \ldots, n$ e $j = 1, \ldots, m$) allora la loro somma appartiene a IJ. Ora per ipotesi I e J sono ideali frazionari, quindi esistono $a, b \in R$ non nulli tali che $aI \subseteq R$, $bJ \subseteq R$; in particolare aI, bJ sono ideali di R. Consideriamo allora $ab(\sum_{i=1}^{n} v_i w_i + \sum_{j=1}^{m} x_j y_j) = \sum_{i=1}^{n} a v_i b w_i + \sum_{j=1}^{m} a x_j b y_j$ che risulta essere somma di due elementi di $(aI)(bJ)$, ma, essendo quest'ultimo un ideale ordinario di R, questo implica che appartiene a sua volta a $(aI)(bJ) = abIJ \subseteq R$. Dunque vale $(\sum_{i=1}^{n} v_i w_i + \sum_{j=1}^{m} x_j y_j) \in IJ$; inoltre abbiamo trovato che, posto $c = ab$, risulta $cIJ \subseteq R$, dove $c \neq 0$ essendo R un dominio di integrità.

Osserviamo infine che tale prodotto è associativo, cioè che per $I, J, H \in \mathscr{M}$ vale $(IJ)H = I(JH)$; ora, ogni elemento del primo insieme è della forma $\sum_{i=1}^{n}(\sum_{j=1}^{m} a_j b_j)c_i = (a_1 b_1 + \cdots + a_m b_m)c_1 + \cdots + (a_1 b_1 + \cdots + a_m b_m)c_n =$ $a_1(b_1 c_1 + \cdots + b_1 c_n) + \cdots + a_m(b_m c_1 + \cdots + b_m c_n) = \sum_{j=1}^{m} a_j(\sum_{i=1}^{n} b_j c_i)$ con $a_j \in I$, $b_j \in J$, $c_i \in H$ ed $n, m \in \mathbb{N}^*$ fissati, ma allora appartiene anche a $I(JH)$; analogamente si mostra che vale l'inclusione inversa.

Complessivamente abbiamo trovato che l'insieme $\mathscr{M}$ è un monoide commutativo rispetto all'operazione di prodotto definita, e che il dominio R è elemento neutro moltiplicativo. □

2.2 Gli ideali invertibili

Definizione 2.5. Un ideale frazionario I di un dominio d'integrità R è *invertibile* se esiste un ideale frazionario J di R tale che $IJ = R$.

Gli ideali frazionari invertibili di R, detti anche semplicemente ideali invertibili, sono dunque quelli che hanno un elemento inverso moltiplicativo nel monoide degli ideali frazionari di R.

Proposizione 2.2.1. *L'ideale inverso di un ideale frazionario invertibile I è unico, e risulta essere $I^{-1} = \{ a \in K \mid aI \subseteq R \}$.*

Dimostrazione. In generale se I è un ideale frazionario di R l'insieme $I^{-1} = \{ a \in K \mid aI \subseteq R \} \subseteq K$ è chiaramente non vuoto, e si ha che presi $x, y \in I^{-1}$ (cioè tali che $xI, yI \subseteq R$), per ogni $h, k \in R$ vale $(hx+ky)I = h(xI)+k(yI) \subseteq R$ cioè $(hx+ky) \in I^{-1}$. Dunque I^{-1} è a sua volta un ideale frazionario di R; osserviamo che risulta inoltre $I^{-1}I = II^{-1} \subseteq R$.
Ora, nel caso in cui l'ideale I sia invertibile esiste un ideale frazionario J tale che $IJ = JI = R$; necessariamente deve valere allora $J \subseteq I^{-1}$, ma dal momento che sono entrambi R-sottomoduli di K si ha $I^{-1} = RI^{-1} = (JI)I^{-1} = J(II^{-1}) \subseteq JR = RJ \subseteq J$, cioè è verificata anche l'inclusione opposta, e pertanto $J = I^{-1}$. □

Osservazione 10. Da tale caratterizzazione di I^{-1} segue che per ogni ideale I di R vale la relazione $R \subseteq I^{-1}$.

Proposizione 2.2.2. *Sia R un dominio d'integrità avente campo dei quozienti K, ogni ideale frazionario invertibile di R è un R-modulo finitamente generato.*

Dimostrazione. Sia I un ideale frazionario invertibile, allora poiché $I^{-1}I = R$ devono esistere $a_i \in I^{-1}, b_i \in I$ tali che $1_R = \sum_{i=1}^{n} a_i b_i$, di conseguenza

possiamo scrivere ogni elemento $c \in I$ come $c = 1_R c = \sum_{i=1}^{n} c a_i b_i$. Ora il fatto che $a_i \in I^{-1} = \{ a \in K \mid aI \subseteq R \}$ comporta che $ca_i \in R$ per ogni $i = 1, \ldots, n$, e quindi, dal momento che per ogni $c \in I$ vale $c = \sum_{i=1}^{n} c_i b_i$ dove $c_i = ca_i \in R$, si ha che $b_1, \ldots, b_n$ sono generatori di I come R-modulo. □

Proposizione 2.2.3. *Siano $I_1, \ldots, I_n$ ideali di un dominio d'integrità R, l'ideale prodotto $I_1 \cdots I_n$ è invertibile se e solo se ogni I_j è invertibile, per $j = 1, \ldots, n$.*

Dimostrazione. Se l'ideale $I_1 \cdots I_n$ è invertibile esiste un ideale frazionario J di R tale che $J(I_1 \cdots I_n) = R$, ma allora per ogni $j = 1, \ldots, n$ si ha che vale $I_j(JI_1 \cdots I_{j-1} I_{j+1} \cdots I_n) = R$, cioè I_j è invertibile.
D'altra parte se gli ideali $I_1, \ldots, I_n$ sono tutti invertibili risulta banalmente $(I_1 \cdots I_n)(I_1^{-1} \cdots I_n^{-1}) = R$ e quindi anche l'ideale prodotto è invertibile. □

Lemma 2.2.4. *Siano I, A, B ideali frazionari di R tali che $IA = IB$; se I è invertibile risulta allora $A = B$.*

Dimostrazione. Se I è invertibile vale $I^{-1}I = R$, ne viene $A = RA = (I^{-1}I)A = I^{-1}(IA) = I^{-1}(IB) = (I^{-1}I)B = RB = B$. □

Proposizione 2.2.5. *Sia I un ideale di un dominio di integrità R tale che $P_1 \cdots P_n = I = Q_1 \cdots Q_m$ dove P_i, Q_j sono ideali primi di R e gli ideali P_i sono invertibili; allora risulta $n = m$ e inoltre, riordinando eventualmente i fattori, vale $P_i = Q_i$ per ogni $i = 1, \ldots, n$.*

Dimostrazione. Si procede per induzione su n.
Per $n = 1$: si ha $P_1 = Q_1 \cdots Q_m$, in particolare vale l'inclusione $Q_1 \cdots Q_m \subseteq P_1$, ma per ipotesi P_1 è ideale primo e quindi necessariamente dovrà essere $Q_j \subseteq P_1$ per qualche $j = 1, \ldots, m$; supponiamo si verifichi per $j = 1$. D'altra parte $P_1 = Q_1 \cdots Q_m \subseteq Q_1$, ne viene l'uguaglianza $P_1 = Q_1$. Dunque abbiamo la relazione $P_1 = Q_1 \cdots Q_m$ con $P_1 = Q_1$ e P_1 invertibile, per il lemma

precedente si ha allora $Q_2 \cdots Q_m = R$, che è l'elemento neutro moltiplicativo, cioè sostanzialmente abbiamo trovato che $m = 1$ e $P_1 = Q_1$.
Supponiamo ora che l'asserto sia valido nel caso in cui gli ideali P_i siano n e mostriamo che allora è valido anche se tali fattori sono $n + 1$.
Sia dunque $P_1 \cdots P_{n+1} = I = Q_1 \cdots Q_{m+1}$ dove $P_1, \ldots, P_{n+1}$ sono ideali primi invertibili e $Q_1, \ldots, Q_{m+1}$ sono ideali primi di R. È lecito supporre, eventualmente riordinando i fattori, che P_1 non contenga strettamente nessun P_i per $i = 2, \ldots, n + 1$. Vale la relazione $Q_1 \cdots Q_{m+1} = P_1 \cdots P_{n+1} \subseteq P_1$ dove per ipotesi P_1 è ideale primo, quindi deve esistere $j \in 1, \ldots, m + 1$ tale che $Q_j \subseteq P_1$; supponiamo sia $Q_1 \subseteq P_1$. Allo stesso modo si ha $P_1 \cdots P_{n+1} = Q_1 \cdots Q_{m+1} \subseteq Q_1$ e poiché anche Q_1 è primo deve valere $P_i \subseteq Q_1$ per qualche $i \in 1, \ldots, n + 1$. Pertanto abbiamo ottenuto $P_i \subseteq Q_1 \subseteq P_1$, ma avendo supposto che nessun P_i sia sottoinsieme proprio di P_1 ne segue che $P_i = Q_1 = P_1$; complessivamente abbiamo $P_1 \cdots P_{n+1} = Q_1 \cdots Q_{m+1}$ con $Q_1 = P_1$ e, dal momento che P_1 è invertibile, questo implica che deve valere $P_2 \cdots P_{n+1} = Q_2 \cdots Q_{m+1}$. A questo punto però gli ideali P_i sono n e dunque, per ipotesi induttiva, deve valere $m + 1 = n + 1$ (da cui $m = n$), con $Q_i = P_i$ per ogni $i = 2, \ldots, n + 1$ dopo aver eventualmente riordinato in modo opportuno i fattori; avendo inoltre $Q_1 = P_1$, troviamo $Q_i = P_i$ per $i = 1, \ldots, n + 1$. □

2.3 Domini di Dedekind e domini a ideali principali

Lemma 2.3.1. *Ogni ideale principale non banale di un dominio d'integrità R è invertibile.*

Dimostrazione. Un tale ideale è della forma $I = (b)$ con $b \neq 0$, se nel campo dei quozienti K di R consideriamo l'elemento $c = 1_R/b$ e definiamo $J = Rc$,

allora J risulta essere un ideale frazionario di R tale che $IJ = R$. □

Osservazione 11. In un dominio a ideali principali ogni ideale diverso da quello banale è dunque invertibile; sappiamo che inoltre un ideale è massimale se e solo se è primo, pertanto possiamo affermare che ogni ideale primo, non banale, di un dominio a ideali principali è sia invertibile che massimale.

Verifichiamo che tale proprietà si conserva nei domini di Dedekind.

Teorema 2.3.2. *Se R è un dominio di Dedekind allora ogni ideale primo non banale di R è invertibile e massimale.*

Dimostrazione. Mostriamo per il momento che ogni ideale primo e invertibile è anche massimale.
Sia P un ideale primo invertibile di R e sia $a \in R \setminus P$; verifichiamo che l'ideale $P + Ra$ coincide con R. Supponiamo per assurdo $P + Ra \neq R$, dal momento che R è dominio di Dedekind l'ideale $P + Ra$ è prodotto di un numero finito di ideali primi, e lo stesso vale per l'ideale $P + Ra^2 \subseteq P + Ra$; siano dunque $P_1, \ldots, P_n, Q_1 \ldots, Q_m$ ideali primi di R tali che $P + Ra = P_1 \cdots P_n$ e $P + Ra^2 = Q_1 \cdots Q_m$. Sia $\pi : R \longrightarrow R/P$ la proiezione canonica, il quoziente R/P risulta essere un dominio d'integrità poiché P è un ideale primo; se consideriamo allora gli ideali principali di R/P generati da $\pi(a)$ e $\pi(a^2)$ possiamo affermare che essi sono invertibili per quanto mostrato nel lemma precedente; utilizzando le fattorizzazioni di $P + Ra$, $P + Ra^2$ si ottengono rispettivamente le identità $(\pi(a)) = \pi(P_1) \cdots \pi(P_n)$ e $(\pi(a^2)) = \pi(Q_1) \cdots \pi(Q_m)$. Osservando che $P \subseteq P_i$, $P \subseteq Q_j$ per ogni $i = 1, \ldots, n$ e per ogni $j = 1, \ldots, m$, si ha che P_i, Q_j risultano essere ideali primi di R che contengono $\ker \pi = P$, ma allora $\pi(P_i)$, $\pi(Q_j)$ sono ideali primi di R/P dal momento che la proiezione canonica è un'applicazione suriettiva; sappiamo inoltre che sono invertibili perché lo sono rispettivamente i loro ideali prodotto $(\pi(a)), (\pi(a^2))$. Ora, siccome π è un morfismo di anelli deve valere $(\pi(a^2)) = (\pi(a))^2$, cioè

$\pi(Q_1)\cdots\pi(Q_m) = (\pi(P_1))^2\cdots(\pi(P_n))^2 = \pi(P_1)\pi(P_1)\cdots\pi(P_n)\pi(P_n)$ ma abbiamo appena mostrato che tutti i fattori sono ideali primi invertibili, quindi per la **Proposizione 2.2.5** necessariamente $m = 2n$ ed eventualmente riordinando si deve avere $\pi(Q_1) = \pi(P_1)$, $\pi(Q_2) = \pi(P_1), \ldots, \pi(Q_{2n-1}) = \pi(P_n)$, $\pi(Q_{2n}) = \pi(P_n)$, cioè in generale $\pi(P_i) = \pi(Q_{2i-1}) = \pi(Q_{2i})$ per $i = 1, \ldots, n$. Ora, P_i, Q_j contengono $\ker\pi$ pertanto $\pi^{-1}(\pi(P_i)) = P_i$, $\pi^{-1}(\pi(Q_j)) = Q_j$, quindi risulta $P_i = \pi^{-1}(\pi(P_i)) = \pi^{-1}(\pi(Q_{2i-1})) = Q_{2i-1}$ e analogamente $P_i = Q_{2i}$ per $i = 1, \ldots, n$; complessivamente si trova allora $P + Ra^2 = Q_1\cdots Q_m = Q_1Q_2\cdots Q_{2n-1}Q_{2n} = P_1P_1\cdots P_nP_n = (P + Ra)^2$.

Valgono le inclusioni $P \subseteq P + Ra^2 = (P + Ra)^2 \subseteq P^2 + Ra$, dunque ogni elemento di P è della forma $b = c + ra$ con $c \in P^2$, $r \in R$, osserviamo che allora $ra = b - c$ deve appartenere a sua volta all'ideale primo P, ma per ipotesi $a \notin P$ e quindi questo implica che necessariamente $r \in P$; abbiamo pertanto verificato che ogni elemento $b \in P$ può essere scritto come $b = c+ra$ dove $c \in P^2$, $r \in P$, e poiché chiaramente $P^2 + Pa \subseteq P$ deve valere l'uguaglianza $P = P^2 + Pa = P(P + Ra)$ da cui, essendo P invertibile, ricaviamo $R = P + Ra$ che è assurdo perché contraddice l'ipotesi fatta.

Abbiamo quindi che ogni ideale primo invertibile P di un dominio di Dedekind R è massimale, in quanto preso un qualunque elemento $a \notin P$ l'ideale generato da P e da a è tutto R; a questo punto dobbiamo dimostrare che ogni ideale primo di R, diverso da quello banale, è invertibile.

Sia P un siffatto ideale, e sia $c \in P$, $c \neq 0$ e consideriamo l'ideale generato da c; per ipotesi R è di Dedekind e dunque si ha $(c) = P_1\cdots P_n$ dove i P_i sono ideali primi di R, essendo poi un ideale principale è invertibile e di conseguenza lo sono anche tutti i P_i, ma allora per quanto osservato nella prima parte della dimostrazione tali ideali sono anche massimali. Ora P è un ideale primo di R e vale $P_1\cdots P_n = (c) \subseteq P$, deve pertanto valere $P_j \subseteq P$ per qualche $j \in \{\, 1, \ldots, n \,\}$ tuttavia abbiamo appena osservato che tutti i P_i sono ideali massimali di R e quindi necessariamente $P = P_j$, ed in particolare

allora l'ideale P risulta essere invertibile. □

Osservazione 12. Sia R un dominio d'integrità e sia I un ideale principale di R, sia ad esempio $I = (a)$, allora la funzione $R \longrightarrow I$ definita da $1_R \longmapsto a$ è un morfismo suriettivo di R-moduli, supponendo poi $I \neq 0$, tale applicazione, essendo definita su un dominio, dev'essere necessariamente iniettiva.
Questo ci permette di concludere che in un dominio a ideali principali R ogni ideale non banale è isomorfo come R-modulo a R stesso; in particolare risulta essere allora un R-modulo libero, e quindi proiettivo.

Complessivamente abbiamo visto che, nel caso in cui R sia un dominio a ideali principali, ogni suo ideale non banale è invertibile ed è proiettivo come modulo su R, condizione che mostreremo essere vera anche per i domini di Dedekind, ma che chiaramente non si verifica per un generico dominio d'integrità. Si trova in generale un risultato molto forte di equivalenza delle due proprietà per gli ideali frazionari.

Lemma 2.3.3. *Sia R un dominio d'integrità avente campo dei quozienti K e sia I un ideale frazionario di R, se $f \in \mathrm{Hom_R}(I, R)$ allora per ogni $a, b \in I$ vale $af(b) = bf(a)$.*

Dimostrazione. Un ideale frazionario I di R è un R-sottomodulo del campo dei quozienti, pertanto se $a, b \in I$ allora sono della forma $a = r/s, b = v/t$ con $r, s, v, t \in R, s, t \neq 0$; si ha $sab = (sa)b = rb \in I, tab = (tb)a = va \in I$ e dunque in R vale $tf(sab) = f(stab) = sf(tab)$, di conseguenza, osservando che in particolare $sa, tb \in R$, in K vale $af(b) = saf(b)/s = f(sab)/s = f(tab)/t = tbf(a)/t = bf(a)$. □

Teorema 2.3.4. *Un ideale frazionario di un dominio di integrità R è invertibile se e solo se è un R-modulo proiettivo.*

Dimostrazione. Sia I un ideale frazionario di R.

($\Rightarrow$) Supponiamo che I sia invertibile allora, per la **Proposizione 2.2.2**, è finitamente generato come R-modulo, dunque esistono $b_1, \ldots, b_n \in I$ tali che $I = Rb_1 + \cdots + Rb_n$, e inoltre vale $1_R = \sum_{i=1}^{n} a_i b_i$ per oppurtuni $a_i \in I^{-1}$.

Consideriamo un R-modulo libero F avente una base di cardinalità n, sia ad esempio $\{ e_1, \ldots, e_n \}$, allora la funzione $\pi : F \longrightarrow I$ che manda ciascun elemento e_i della base di F nel generatore b_i del modulo I risulta essere un omomorfismo suriettivo di R-moduli.

Definiamo ora $\xi : I \longrightarrow F$ nel modo seguente: $\xi(c) = ca_1e_1 + \cdots + ca_ne_n$, e osserviamo che ξ è un omomorfismo di moduli. Inoltre risulta $\pi \circ \xi = 1_I$, infatti siccome $a_i \in I^{-1}$ si ha $ca_i \in R$ per ogni $c \in I$ e per ogni $i = 1, \ldots, n$, e quindi vale $\pi(\xi(c)) = \pi(ca_1e_1 + \cdots + ca_ne_n) = \pi(ca_1e_1) + \cdots + \pi(ca_ne_n) = ca_1\pi(e_1) + \cdots + ca_n\pi(e_n) = ca_1b_1 + \cdots + ca_nb_n = c(a_1b_1 + \cdots + a_nb_n) = c1_R = c$.

Possiamo allora affermare che la sequenza esatta corta di omomorfismi di moduli $0 \longrightarrow \ker\pi \xrightarrow{i} F \xrightarrow{\pi} I \longrightarrow 0$ è una sequenza spezzante, dunque il modulo libero F è isomorfo alla somma diretta di R-moduli $\ker\pi \oplus I$, e per il **Teorema 1.3.2** il verificarsi di questa condizione è equivalente al fatto che l'R-modulo I sia proiettivo.

($\Leftarrow$) Supponiamo ora che I come modulo su R sia proiettivo, mostriamo che è un ideale invertibile. Sia $X = \{ b_j \mid j \in J \}$ un insieme (eventualmente infinito) di generatori non nulli del modulo I, consideriamo ora un R-modulo libero F avente base $\{ e_j \mid j \in J \}$, allora la funzione $\phi : F \longrightarrow I$ che manda ciascun elemento e_j della base di F nel generatore b_j di I risulta essere un omomorfismo suriettivo di R-moduli, e siccome I è proiettivo deve esistere un omomorfismo di R-moduli $\psi : I \longrightarrow F$ tale che $\phi \circ \psi = 1_I$.

Per ogni $j \in J$ sia $\pi_j : F \longrightarrow Re_j \cong R$ il morfismo canonico di proiezione sulla j-esima componente, cioè la funzione $r = \sum_{i \in J} r_i e_i \longmapsto r_j$, e sia poi $\theta_j : I \longrightarrow R$ l'omomorfismo di R-moduli dato da $\theta_j = \pi_j \circ \psi$. Sia ora $b_0 \in X$ un fissato generatore di I, per ogni $j \in J$ poniamo $c_j = \theta_j(b_0)$; poiché $\theta_j \in \mathrm{Hom_R}(I, R)$ per il **Lemma 2.3.3** preso $c \in I$ vale $cc_j = c\theta_j(b_0) = b_0\theta_j(c)$; nel campo dei quozienti K di R si ha allora $c(c_j/b_0) = (cc_j)/b_0 = (b_0\theta_j(c))/b_0 = \theta_j(c) \in R$ per ogni $c \in I$ che significa che $c_j/b_0 \in I^{-1}$, e questo per ogni $j \in J$.

Abbiamo definito il morfismo $\psi : I \longrightarrow F$ dove F è un modulo libero su R, dunque ogni $c \in I$ ha per immagine una combinazione lineare finita a coefficienti in R di elementi della base $\{ e_j \mid j \in J \}$ di F, cioè $\psi(c) = \sum_{j \in J_1} r_j e_j$ con $J_1 = \{ j \in J \mid r_j \neq 0 \}$ di cardinalità finita; ora, per ogni $j \in J_1$ risulta $r_j = \pi_j(\psi(c)) = (\pi_j \circ \psi)(c) = \theta_j(c) = cc_j/b_0 \in R$ pertanto possiamo scrivere $\psi(c) = \sum_{j \in J_1} (cc_j/b_0)e_j$. Ne viene che per ogni $c \in I$ non nullo vale $c = 1_I(c) = (\phi \circ \psi)(c) = \phi(\psi(c)) = \phi(\sum_{j \in J_1} (cc_j/b_0)e_j) = \sum_{j \in J_1} (cc_j/b_0)\phi(e_j) = \sum_{j \in J_1} (cc_j/b_0)b_j = c\sum_{j \in J_1} (c_j/b_0)b_j$ da cui si ricava che necessariamente $\sum_{j \in J_1} (c_j/b_0)b_j = 1_R$ e, dal momento che $c_j/b_0 \in I^{-1}$ e che i b_j sono i generatori di I, complessivamente questo implica che $R \subseteq I^{-1}I$, ma sappiamo che in generale vale l'inclusione opposta quindi possiamo concludere che $I^{-1}I = R$.

□

2.4 Caratterizzazioni equivalenti di un dominio di Dedekind

Definizione 2.6. Un *anello a valutazione discreta* è un dominio a ideali principali che ha uno ed un solo ideale primo diverso da quello banale.
(L'ideale nullo è un ideale primo in un dominio d'integrità).

Lemma 2.4.1. *Se R è un dominio d'integrità noetheriano e integralmente chiuso ed ha un unico ideale primo P non banale allora R è un anello a valutazione discreta.*

Dimostrazione. Dobbiamo verificare solamente che un siffatto dominio è PID, cioè che ogni suo ideale proprio è principale.
Mostreremo nell'ordine che valgono i seguenti fatti:

(i) detto K il campo dei quozienti di R si ha che per ogni ideale frazionario I di R l'insieme $\overline{I} = \{\, a \in K \mid aI \subseteq I \,\}$ coincide con R;

(ii) $R \underset{\neq}{\subseteq} P^{-1}$;

(iii) P è invertibile;

(iv) $\bigcap_{n \in \mathbb{N}^*} P^n = 0$;

(v) P è un ideale principale.

Osserviamo ora che ne segue la tesi.
Sia infatti I un generico ideale proprio di R (che è in particolare un anello unitario non vuoto), sappiamo che deve esistere un ideale massimale M che lo contiene; ma se M è massimale allora è anche primo e di conseguenza deve necessariamente coincidere con P, che per ipotesi è l'unico ideale primo non banale di R. Abbiamo dunque ottenuto che P è un ideale massimale (unico) di R e che ogni ideale proprio di R è contenuto in P.

Ora, se vale $\bigcap_{n\in\mathbb{N}^*} P^n = \emptyset$, esiste un indice $m > 0$ tale che $I \subseteq P^m$ ma $I \not\subset P^{m+1}$, possiamo dunque considerare un elemento $b \in I \setminus P^{m+1}$ e in particolare risulta $b \in I \subseteq P^m$. A questo punto, siccome stiamo supponendo che P sia un ideale principale, cioè $P = (a)$ con $a \in R$, $a \neq 0$, possiamo scrivere $P^m = (a)^m = (a^m)$, e dunque b è della forma $b = ua^m$ con $u \notin P = (a)$, perché altrimenti b apparterrebbe all'ideale $(a^{m+1}) = P^{m+1}$. Osserviamo che $u \notin P$ implica necessariamente che u sia un'unità dell'anello, infatti se così non fosse l'ideale (u) sarebbe un ideale proprio di R e, ripetendo il ragionamento fatto per I, si troverebbe $(u) \subseteq P$. Ma ora, se $b = ua^m$, con u unità, risulta $P^m = (a^m) = (ua^m) = (b) \subseteq I$, e poiché valeva per ipotesi l'inclusione opposta ne viene che $I = P^m = (a^m)$, quindi I è principale.
Rimane a questo punto da provare la veridicità delle affermazioni sopra riportate.

(i) Consideriamo l'insieme $\overline{I} = \{\, a \in K \mid aI \subseteq I \,\}$, dove I è un ideale frazionario di R; banalmente vale $R \subseteq \overline{I}$, e si verifica inoltre che $\overline{I}$ è un sottoanello e un R-sottomodulo di K. Ora, poiché I è un ideale frazionario, esiste $\bar{a} \in R$ non nullo tale che $\bar{a}I \subseteq R$; fissiamo arbitrariamente un elemento $b \in I$, $b \neq 0$, per definizione di $\overline{I}$ per ogni $a \in \overline{I}$ vale $ab \in I$, ma allora $\bar{a}(ab) \in R$. Risulta quindi $(\bar{a}b)a = \bar{a}(ab) \in R$ per ogni $a \in \overline{I}$, con $\bar{a}b \in R$, $\bar{a}b \neq 0$, e quindi $\overline{I}$ è a sua volta un ideale frazionario di R. Sappiamo che allora $\overline{I}$ è isomorfo come R-modulo ad un ideale di R; ora, per ipotesi, R è noetheriano e quindi ogni suo ideale è finitamente generato, per quanto appena osservato anche $\overline{I}$ è finitamente generato come R-modulo. Per il **Corollario 1.5.2** l'estensione di anelli $R \subseteq \overline{I}$ è un'estensione intera. Siccome abbiamo supposto R integralmente chiuso, R contiene ogni sottoanello di K che è un'estensione intera di R (**Teorema 1.5.5**), in particolare allora $\overline{I} \subseteq R$, e pertanto $\overline{I}$ coincide con R.

(ii) Mostriamo che $R \underset{\neq}{\subset} P^{-1}$; sappiamo che l'inclusione $R \subseteq J^{-1}$ vale per ogni ideale J di R, sia allora $\mathscr{F}$ l'insieme degli ideali di R per cui vale l'inclusione stretta e verifichiamo che $\mathscr{F} \neq \emptyset$.

Osserviamo che P non può contenere unità di R perché in tal caso, in quanto ideale, dovrebbe contenere tutto l'anello e non sarebbe quindi un ideale proprio. Dunque preso $b \in P$, $b \neq 0$, e posto $J = (b)$, si ha che $1_R/b \in J^{-1} = \{\, a \in K \mid aJ \subseteq R \,\}$ ma $1_R/b \notin R$, perché b non può essere un'unità; vale allora $R \underset{\neq}{\subset} J^{-1}$, e di conseguenza $J \in \mathscr{F}$.

Per ipotesi R è noetheriano quindi ogni insieme non vuoto di suoi sottomoduli ammette elemento massimale; sia dunque M l'elemento massimale di $\mathscr{F}$, proviamo che M è un ideale primo di R.

Siano $b, c \in R$ tali che $bc \in M$ con $b \notin M$, poiché $M \in \mathscr{F}$ vale $R \underset{\neq}{\subset} M^{-1}$, sia allora $a \in M^{-1} \setminus R$; in particolare $a \in M^{-1} = \{\, a \in K \mid aM \subseteq R \,\}$. Si ha quindi $a(bc) \in R$, da cui si ottiene l'inclusione $abcR + c(aM) = ca(bR + M) \subseteq R$, che equivale al fatto che $ca \in (bR + M)^{-1}$. Osserviamo che ca è necessariamente un elemento di R, infatti se così non fosse si avrebbe $(bR + M) \in \mathscr{F}$, che non è possibile dal momento che M è massimale. Ora, poiché $ca \in R$ vale $caR + aM = a(cR + M) \subseteq R$, e quindi $a \in (cR + M)^{-1}$, ma per ipotesi $a \notin R$ quindi l'ideale $cR + M \in \mathscr{F}$; affinchè questo non sia in contrasto con l'ipotesi di massimalità di M deve valere $cR + M = M$, ossia c deve essere un elemento di M.

In questo modo abbiamo mostrato che l'ideale $M \neq \emptyset$ è primo, ne segue che M deve coincidere con P, che è per ipotesi l'unico ideale primo non banale di R, ma allora $P \in \mathscr{F}$ che significa che $R \underset{\neq}{\subset} P^{-1}$.

(iii) Abbiamo osservato all'inizio della dimostrazione che P è (l'unico) ideale massimale di R, allora dalla relazione $P \subseteq PP^{-1} \subseteq R$ deduciamo che necessariamente deve valere $P = PP^{-1}$ oppure $PP^{-1} = R$.

Supponiamo che sia $P = PP^{-1}$, in particolare risulta $P^{-1}P \subseteq P$; de-

finendo allora come sopra $\overline{P} = \{\, a \in K \mid aP \subseteq P \,\}$ vale banalmente $P^{-1} \subseteq \overline{P}$. A questo punto applicando quanto mostrato nei punti precedenti si trova $R \underset{\neq}{\subset} P^{-1} \subseteq \overline{P} = R$, che è assurdo.
Necessariamente allora $PP^{-1} = R$, cioè l'ideale P è invertibile.

(iv) Supponiamo per assurdo che $\bigcap_{n\in\mathbb{N}^*} P^n \neq 0$, allora tale intersezione è a sua volta un ideale frazionario di R.Siano $x \in \bigcap_{n\in\mathbb{N}^*} P^n$ e $a \in P^{-1}$, in particolare $x \in P^{n+1}$ per ogni $n \in \mathbb{N}^*$ e inoltre, per definizione di P^{-1}, vale $aP \subseteq R$, di conseguenza $ax \in aP^{n+1} = aPP^n \subseteq RP^n \subseteq P^n$ per ogni $n \in \mathbb{N}^*$, e quindi $ax \in \bigcap_{n\in\mathbb{N}^*} P^n$. Complessivamente vale dunque l'inclusione $P^{-1} \subseteq \overline{\bigcap_{n\in\mathbb{N}^*} P^n} = \left\{ a \in K \mid a(\bigcap_{n\in\mathbb{N}^*} P^n) \subseteq \bigcap_{n\in\mathbb{N}^*} P^n \right\}$.
Applicando come sopra i risultati (i) e (ii) si giunge alla contraddizione $R \underset{\neq}{\subset} P^{-1} \subseteq \overline{\bigcap_{n\in\mathbb{N}^*} P^n} = R$, che prova l'asserto.

(v) Osserviamo che dev'essere $P^2 \neq P$, perché se fossero uguali si avrebbe $\bigcap_{n\in\mathbb{N}^*} P^n = P \neq 0$. Consideriamo dunque per $a \in P \setminus P^2$ l'ideale non banale di R dato da aP^{-1}; dal momento che P è invertibile non è possibile che valga l'inclusione $aP^{-1} \subseteq P$, perché altrimenti troveremmo che $a \in aR = a(P^{-1}P) = (aP^{-1})P \subseteq PP = P^2$. Ora, per quanto visto all'inizio della dimostrazione, il fatto che $aP^{-1} \not\subset P$ comporta che aP^{-1} non sia un ideale proprio, dunque necessariamente $aP^{-1} = R$.
Così troviamo $P = RP = (aP^{-1})P = a(P^{-1}P) = aR = (a)$, e dunque l'ideale P è principale.

□

Il seguente risultato è di particolare importanza in quanto fornisce diverse caratterizzazioni dei domini di Dedekind.

Teorema 2.4.2. *Sia R un dominio d'integrità, sono equivalenti le condizioni seguenti:*

(i) *R è un dominio di Dedekind;*

(ii) *ogni ideale proprio di R si fattorizza in modo unico come prodotto di un numero finito di ideali primi;*

(iii) *ogni ideale non banale di R è invertibile;*

(iv) *ogni ideale frazionario di R è invertibile;*

(v) *l'insieme di tutti gli ideali frazionari di R è un gruppo rispetto al prodotto;*

(vi) *ogni ideale di R è un R-modulo proiettivo;*

(vii) *ogni ideale frazionario di R è un R-modulo proiettivo;*

(viii) *R è noetheriano, integralmente chiuso ed ogni suo ideale primo non banale è massimale;*

(ix) *R è noetheriano, e per ogni ideale primo P di R non banale la localizzazione R_P di R in P è un anello a valutazione discreta.*

Dimostrazione. Per il **Teorema 2.3.2** e la **Proposizione 2.2.3** vale $(i) \Rightarrow (iii)$, ma allora $(i) \Rightarrow (ii)$, perché se in un dominio di Dedekind ogni ideale proprio è prodotto di un numero finito di ideali primi invertibili segue dalla **Proposizione 2.2.5** che tale fattorizzazione è necessariamente unica; essendo poi l'implicazione inversa banale risulta $(i) \Leftrightarrow (ii)$. Osserviamo che l'equivalenza $(v) \Leftrightarrow (iv)$ è triviale, essendo l'insieme degli ideali frazionari di un dominio d'integrità un monoide commutativo (**Teorema 2.1.2**). Il **Teorema 2.3.4** sancisce poi l'equivalenza $(iv) \Leftrightarrow (vii)$, da cui discende $(iii) \Leftrightarrow (vi)$; inoltre vale $(vi) \Rightarrow (vii)$, in quanto ogni ideale frazionario è isomorfo come R-modulo a un ideale di R (**Osservazione 9**).
Per completare la dimostrazione è sufficiente provare allora che $(iv) \Rightarrow (viii)$, $(viii) \Rightarrow (ix)$ e $(ix) \Rightarrow (i)$.

$(iv) \Rightarrow (viii)$ Supponiamo che ogni ideale frazionario di R sia invertibile, dobbiamo mostrare che R è noetheriano e integralmente chiuso, e che ogni suo ideale primo diverso dall'ideale banale è massimale.

Per il **Proposizione 2.2.2** si ha che ogni ideale frazionario di R essendo invertibile è finitamente generato come R-modulo, ma questa proprietà, ristretta agli ideali, è una caratterizzazione della noetherianità di R.

Sia K il campo dei quozienti di R, sappiamo che se $u \in K$ è intero su R allora per la **Proposizione 1.5.1** $R[u]$ è finitamente generato come R-sottomodulo di K, ed è quindi un ideale frazionario di R (**Proposizione 2.1.1**). Ma allora per ipotesi $R[u]$ è invertibile, cioè vale $R[u]^{-1}R[u] = R$; osservando che $R[u]R[u] = R[u]$ (perché $R[u]$ è un anello che contiene 1_K), troviamo l'identità $R[u] = RR[u] = (R[u]^{-1}R[u])R[u] = R[u]^{-1}(R[u]R[u]) = R[u]^{-1}R[u] = R$ che implica che $u \in R$. Complessivamente questo prova che l'insieme degli elementi di K interi su R, ovvero la chiusura integrale di R nel suo campo dei quozienti, coincide con R stesso, che è quindi integralmente chiuso.

Sia infine $P \neq 0$ un ideale primo di R, sicuramente esiste un ideale massimale M di R tale che $P \subseteq M$. Consideriamo $M^{-1}P$ che a priori è un ideale frazionario di R, siccome per ipotesi ogni ideale frazionario di R è invertibile vale $M^{-1}P \subseteq M^{-1}M = R$, e dunque $M^{-1}P$ è un ideale ordinario di R. Abbiamo quindi che M e $M^{-1}P$ sono due ideali di R tali che $M(M^{-1}P) = (MM^{-1})P = RP = P$, e poiché P è primo necessariamente deve essere $M \subseteq P$ oppure $M^{-1}P \subseteq P$. Osserviamo che non può valere $M^{-1}P \subset P$, infatti in tal caso (ricordando che per ipotesi anche P è invertibile) troveremmo $R \subseteq M^{-1} = M^{-1}R = M^{-1}(PP^{-1}) = (M^{-1}P)P^{-1} \subseteq PP^{-1} = R$, da cui segue che $M^{-1} = R$; ma allora avremmo che anche $M = MR = MM^{-1} = R$, che non è possibile perché M è un ideale massimale. Abbiamo così provato che $M \subseteq P$ e per ipotesi valeva l'inclusione inversa, pertanto risulta

$P = M$, e quindi in particolare P è massimale.

$(viii) \Rightarrow (ix)$ Sia R un dominio d'integrità noetheriano integralmente chiuso e tale che ogni ideale primo $P \neq 0$ di R sia massimale, se mostriamo che la localizzazione R_P di R in P, per ogni P siffatto, è a sua volta un dominio d'integrità noetheriano e integralmente chiuso ed ha un unico ideale primo non banale, allora per il lemma precedente R_P è un anello a valutazione discreta.

Ora R_P è definito come l'anello dei quozienti $S^{-1}R$, dove $S = R \setminus P$, e siccome P è ideale primo S è parte moltiplicativa di R, e $0_R \notin S$; per il **Teorema 1.5.6** poiché R è un dominio d'integrità integralmente chiuso lo è anche R_P.

Dal momento che R per ipotesi è noetheriano, ogni suo ideale è finitamente generato come R-modulo, ma allora gli ideali di R_P, essendo tutti della forma $I_P = \{\, a/s \mid a \in I, s \in S = R \setminus P \,\} = \{\, a/s \mid a \in I, s \notin P \,\}$ dove I è un ideale di R (**Teorema 1.4.8**), sono a loro volta finitamente generati, quindi anche R_P è noetheriano.

Verifichiamo infine che R_P ammette uno ed un solo ideale primo diverso da quello banale. Il **Teorema 1.4.11** asserisce che un ideale $I_P = \{\, a/s \mid a \in I, s \notin P \,\} \neq 0$ di R_P è primo se e solo se l'ideale I è non banale primo e tale che $I \subseteq P$. Allora, poiché per ipotesi ogni ideale primo $I \neq 0$ di R deve essere massimale, necessariamente $I = P$; di conseguenza P_P risulta essere l'unico ideale primo non banale di R_P.

$(ix) \Rightarrow (i)$ Supponiamo che R sia noetheriano e che per ogni ideale primo $P \neq 0$ di R la localizzazione R_P di R in P sia un anello a valutazione discreta, verifichiamo che allora R è un dominio di Dedekind, ovvero che ogni suo ideale proprio è prodotto di un numero finito di ideali primi.

Osserviamo innanzitutto che ogni ideale $I \neq 0$ di R è invertibile, cioè

che vale $II^{-1} = R$. Consideriamo dunque l'ideale frazionario II^{-1}, che essendo contenuto in R risulta essere un ideale ordinario, e supponiamo che sia invece un ideale proprio di R. Sappiamo che allora esiste un ideale massimale che lo contiene, in particolare un tale M è un ideale primo di R e pertanto, per ipotesi, la localizzazione di R in M è un anello a valutazione discreta; dunque l'ideale $I_M = \{\, a/s \mid a \in I, s \notin M \,\}$ di R_M è principale, sia ad esempio $I_M = (a/s)$ con $a \in I$, $s \in R \setminus M$. Ora, dal momento che R è noetheriano l'ideale I è finitamente generato; sia $I = (b_1, \ldots, b_n)$. Per ogni $i = 1, \ldots, n$ risulta $b_i/1_R \in I_M$, che è l'ideale di R_M generato dall'elemento a/s; allora esisteranno $r_i \in R$, $s_i \in R \setminus M$ tali che $b_i/1_R = (r_i/s_i)(a/s)$, da cui otteniamo la relazione $s_i s b_i = r_i a$ per ogni $i = 1, \ldots, n$. Poniamo $t = ss_1 \cdots s_n$, essendo $R \setminus M$ moltiplicativamente chiuso $t \in R \setminus M$. Nel campo dei quozienti di R vale $(t/a)b_i = tb_i/a = ss_1 \cdots s_i \cdots s_n b_i/a = r_i s_1 \cdots s_{i-1} s_{i+1} \cdots s_n \in R$ per $i = 1, \ldots, n$, ed essendo i b_i i generatori di I questo significa che $t/a \in I^{-1}$. Di conseguenza $t = (t/a)a \in I^{-1}I$, che per ipotesi è contenuto nell'ideale massimale M, ma questo è assurdo perché avevamo preso $t \in R \setminus M$. Abbiamo così provato che l'ideale II^{-1} non può essere ideale proprio di R e quindi $II^{-1} = R$.

A questo punto, consideriamo per ogni ideale proprio I di R un ideale massimale M_I tale che $I \subseteq M_I \underset{\neq}{\subset} R$, mentre per $I = R$ poniamo $M_I = M_R = R$; come prima abbiamo che l'ideale frazionario IM_I^{-1} è un ideale di R, in quanto $IM_I^{-1} \subseteq M_I M_I^{-1} \subseteq R$, e chiaramente contiene l'ideale I. Inoltre per $I \neq R$ risulta $I \underset{\neq}{\subset} IM_I^{-1}$, infatti in caso contrario, poiché ogni ideale di R è invertibile, si troverebbe $R = RR = (I^{-1}I)(M_I^{-1}M_I) = I^{-1}(IM_I^{-1})M_I = I^{-1}IM_I = RM_I = M_I$, che non è possibile perché abbiamo scelto M_I massimale. Sia ora S l'insieme di tutti gli ideali di R e sia $f : S \longrightarrow S$ la funzione definita da $I \longmapsto IM_I^{-1}$; osserviamo che, preso un qualunque ideale proprio J,

si ha che $f(J) \in S$; quindi possiamo definire la successione $(J_n)_{n\in\mathbb{N}}$, a valori in S, nel modo seguente $J_0 = J$ e $J_{n+1} = f(J_n)$ per ogni $n \in \mathbb{N}$. In questo modo, siccome vale $I \subseteq f(I) = IM_I^{-1}$ per ogni $I \in S$, troviamo la seguente catena crescente $J = J_0 \subseteq J_1 \subseteq J_2 \subseteq \dots$ di ideali di R. Essendo R noetheriano deve esistere allora $k \in \mathbb{N}$ tale che $J_k = J_{k+1}$, ed è lecito supporre che k sia il più piccolo indice che soddisfa tale condizione, cioè che valga $J = J_0 \underset{\neq}{\subseteq} J_1 \underset{\neq}{\subseteq} \dots \underset{\neq}{\subseteq} J_{k-1} \underset{\neq}{\subseteq} J_k = J_{k+1}$. Ma, denotando M_{J_n} con M_n per ogni $n \in \mathbb{N}$, per definizione di f si ha $J_{k+1} = f(J_k) = J_k M_{J_k}^{-1} = J_k M_k^{-1}$, quindi tale identità può essere verificata solo se $J_k = R$, perché per gli ideali propri abbiamo visto che vale $J_k \underset{\neq}{\subseteq} J_k M_k^{-1}$. Dunque abbiamo $J_k = R$ con $J_k = f(J_{k-1}) = J_{k-1}M_{k-1}^{-1}$, da cui segue $J_{k-1} = J_{k-1}(M_{k-1}^{-1}M_{k-1}) = (J_{k-1}M_{k-1}^{-1})M_{k-1} = RM_{k-1} = M_{k-1}$; otteniamo $M_{k-1} = J_{k-1} \underset{\neq}{\subseteq} J_k = R$ che significa che M_{k-1} è ideale massimale. La minimalità di k assicura che anche $M_0, \dots, M_{k-2}$ siano massimali, infatti se per qualche $j \in \{\, 0, \dots, k-2 \,\}$ si avesse $M_j = R$, ne verrebbe $J_{j+1} = J_j M_j^{-1} = J_j R = J_j$ che non è possibile. Si verifica che vale $M_{k-1} = J_{k-1} = J_{k-2}M_{k-2}^{-1} = (J_{k-3}M_{k-3}^{-1})M_{k-2}^{-1} = \dots = JM_0^{-1}M_1^{-1}\cdots M_{k-2}^{-1}$ e, dal momento che tutti gli M_j sono invertibili, questo implica che $M_{k-1}(M_0 \cdots M_{k-2}) = J(M_0^{-1}\cdots M_{k-2}^{-1})(M_0 \cdots M_{k-2}) = J$, ovvero è possibile fattorizzare l'ideale proprio J di R come prodotto di ideali massimali, e quindi primi. Possiamo allora concludere che R è un dominio di Dedekind.

□

2.5 Il dominio $\mathbb{Z}[\sqrt{10}]$

Utilizziamo ora una delle caratterizzazioni del teorema precedente per mostrare, attraverso un esempio, che non tutti i domini di Dedekind sono a

ideali principali.

Esempio 2.1. Vogliamo mostrare che valgono, per il dominio d'integrità $\mathbb{Z}[\sqrt{10}] = \left\{ a + b\sqrt{10} \mid a, b \in \mathbb{Z} \right\}$, i seguenti fatti:

(i) $\mathbb{Z}[\sqrt{10}]$ è noetheriano;

(ii) $\mathbb{Z}[\sqrt{10}]$ è integralmente chiuso;

(iii) ogni ideale primo non banale di $\mathbb{Z}[\sqrt{10}]$ è massimale;

(iv) $\mathbb{Z}[\sqrt{10}]$ non è un dominio a fattorizzazione unica.

Infatti, in tal caso, $\mathbb{Z}[\sqrt{10}]$ risulta essere un dominio di Dedekind (**Teorema 2.4.2(viii)**), che chiaramente non è però un dominio a ideali principali, non essendo a fattorizzazione unica.

(i) Sappiamo che $\mathbb{Z}[x]$ è un anello noetheriano, allora, siccome il morfismo di valutazione $\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[\sqrt{10}]$ definito da $p(x) \longmapsto p(\sqrt{10})$ è suriettivo, si ha che l'anello $\mathbb{Z}[\sqrt{10}]$ è noetheriano, in quanto è isomorfo al quoziente di $\mathbb{Z}[x]$ modulo $\ker \varphi$.

(ii) Si verifica facilmente che $\mathbb{Q}(\sqrt{10}) = \left\{ r + s\sqrt{10} \mid r, s \in \mathbb{Q} \right\}$ è il campo dei quozienti di $\mathbb{Z}[\sqrt{10}]$; dobbiamo mostrare che se un elemento $u \in \mathbb{Q}(\sqrt{10})$ è intero su $\mathbb{Z}[\sqrt{10}]$, allora appartiene a $\mathbb{Z}[\sqrt{10}]$.
Osserviamo innanzitutto che ogni $u \in \mathbb{Q}(\sqrt{10})$ intero su $\mathbb{Z}[\sqrt{10}]$ è intero anche su $\mathbb{Z}$; infatti l'estensione di anelli $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{10}]$ è chiaramente intera, e lo stesso vale, per il **Teorema 1.5.3**, per $\mathbb{Z}[\sqrt{10}] \subseteq \mathbb{Z}[\sqrt{10}][u]$; pertanto anche $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{10}][u]$ risulta essere un'estensione intera (**Teorema 1.5.4**).
Consideriamo per il momento il caso in cui $u \in \mathbb{Q}$, e verifichiamo che se u è intero su $\mathbb{Z}[\sqrt{10}]$ allora si ha addirittura che $u \in \mathbb{Z} \subseteq$

$\mathbb{Z}[\sqrt{10}][u]$. Sia $u = r/s \in \mathbb{Q}$ con r, s primi tra loro, in particolare u è intero su $\mathbb{Z}$, quindi esiste un polinomio $p(x) \in \mathbb{Z}[x]$ monico che si annulla in u; vale dunque per opportuni coefficienti $a_i \in \mathbb{Z}$ $(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_1(r/s)^1 + a_0 = 0$. Moltiplicando per s^n si trova $r^n + a_{n-1}r^{n-1}s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0$, da cui, portando r^n a secondo membro, segue che necessariamente s deve dividere r^n in $\mathbb{Z}$. Ma allora, dal momento che abbiamo supposto che r ed s siano relativamente primi, s deve essere un'unità, perché $\mathbb{Z}$ è un dominio a fattorizzazione unica, e quindi $u = r/s \in \mathbb{Z}$.

A questo punto possiamo supporre che $u \in \mathbb{Q}(\sqrt{10})$, $u \notin \mathbb{Q}$, e vogliamo mostrare che se u è intero su $\mathbb{Z}[\sqrt{10}]$ allora $u \in \mathbb{Z}[\sqrt{10}]$. Sia $u = r+s\sqrt{10}$, siccome $u \notin \mathbb{Q}$, il polinomio $f(x) = x^2-2rx+r^2-10s^2 \in \mathbb{Q}[x]$, che è chiaramente un polinomio monico che si annulla su u, è irriducibile, perché è di secondo grado e non ha radici in $\mathbb{Q}$. Possiamo scrivere $f(x) = q \cdot f'(x)$, con $q \in \mathbb{Q}$ e $f'(x) \in \mathbb{Z}[x]$ polinomio primitivo; inoltre f' è ancora di secondo grado, irriducibile e tale che $f'(u) = 0$. Ora, per ipotesi, l'elemento u è intero su $\mathbb{Z}[\sqrt{10}]$, e di conseguenza su $\mathbb{Z}$, pertanto esiste un polinomio monico $g(x) \in \mathbb{Z}[x]$ che si annulla in u, e vale $\deg g \geq 2$ dal momento che $u \notin \mathbb{Q}$. Necessariamente allora f' divide g in $\mathbb{Q}[x]$, ed essendo entrambi polinomi primitivi (g è monico), questo implica che f' deve dividere g anche in $\mathbb{Z}[x]$; ne segue che anche f' è un polinomio monico. Abbiamo dunque la relazione $f(x) = q \cdot f'(x)$, dove sia f che f' sono monici, ma questo significa che devono coincidere, e quindi f è in realtà un polinomio a coefficienti in $\mathbb{Z}$.

Abbiamo così trovato che per ogni $u = r + s\sqrt{10}$ intero su $\mathbb{Z}[\sqrt{10}]$ vale $-2r$, $r^2-10s^2 \in \mathbb{Z}$; rimane da verificare che questo implica che $r, s \in \mathbb{Z}$. Sia $n = -2r \in \mathbb{Z}$, nel caso in cui n sia pari risulta banalmente $r \in \mathbb{Z}$, da cui segue che anche $10s^2 \in \mathbb{Z}$, dal momento che abbiamo $r^2 - 10s^2 \in \mathbb{Z}$. Se $s = t/v$, dove $t, v \in \mathbb{Z}$ $(t, v \neq 0)$ sono relativamente primi, abbiamo

che $10t^2/v^2 \in \mathbb{Z}$, che significa che v^2 divide $10t^2$ in $\mathbb{Z}$; siccome abbiamo supposto che t e v non abbiano fattori primi comuni, necessariamente v^2 deve dividere 10, ma questo è possibile solo se v è un'unità, e quindi abbiamo provato che anche $s \in \mathbb{Z}$. Osserviamo infine che supponendo che $n = -2r \in \mathbb{Z}$ sia dispari si arriva ad un assurdo; abbiamo $r = -n/2$, $s = t/v$, con $t, v \in \mathbb{Z}$ primi tra loro, e sappiamo che $n^2/4 - 10t^2/v^2 = m \in \mathbb{Z}$. Ora, v non può essere dispari, infatti in tal caso dalla relazione $v^2n^2 - 40t^2 = 4v^2m$ segue che v^2n^2 deve in particolare essere pari, che è assurdo dal momento che sia n che v sono dispari. Nel caso in cui invece v sia pari, possiamo scrivere $v = 2v'$ per $v' \in \mathbb{Z}$, e dunque otteniamo $(v')^2n^2 - 10t^2 = 4(v')^2m$, da cui ragionando come prima segue che v' è a sua volta un numero pari. Sia dunque $v' = 2v''$, sostituendo nell'identità precedente ricaviamo $2(v'')^2n^2 - 5t^2 = 8(v'')^2m$, e questo implica che t deve essere pari, che è assurdo perché abbiamo supposto che v sia pari e che t, v siano relativamente primi.

(iii) Sia P un ideale primo non banale di $\mathbb{Z}[\sqrt{10}]$, allora $P \cap \mathbb{Z}$ è chiaramente un ideale di $\mathbb{Z}$, e inoltre è primo, perché se $a, b \in \mathbb{Z} \subseteq \mathbb{Z}[\sqrt{10}]$ e vale $ab \in P \cap \mathbb{Z} \subseteq P$, allora per ipotesi si deve avere che $a \in P$ oppure $b \in P$, e pertanto almeno uno tra a e b appartiene a $P \cap \mathbb{Z}$. Ora, siccome $P \neq 0$, possiamo considerare $u \in P$, $u \neq 0$, e sappiamo che esiste un polinomio di secondo grado, monico, a coefficienti in $\mathbb{Z}[x]$ che si annulla in u. Siano dunque $a, b \in \mathbb{Z}$ tali che $u^2 + au + b = 0$, è chiaro che a e b non possono essere entrambi nulli, proviamo che almeno uno appartiene a P. Se $b \neq 0$ dalla relazione $b = -u^2 - au$ segue che b appartiene all'ideale P, d'altra parte se $b = 0$ abbiamo $u^2 + au = u(u + a) = 0$ (con $a \neq 0$), ma avendo supposto $u \neq 0$ questo implica che $u + a = 0$, e quindi $a = -u \in P$. In conclusione abbiamo che $P \cap \mathbb{Z}$ è un ideale primo non banale di $\mathbb{Z}$.

A questo punto dobbiamo mostrare che ogni ideale primo P non banale

di $\mathbb{Z}[\sqrt{10}]$ è massimale, cioè che ogni ideale Q tale che $P \subset Q \subsetneq \mathbb{Z}[\sqrt{10}]$ coincide con P. Consideriamo gli ideali $P \cap \mathbb{Z}$ e $Q \cap \mathbb{Z}$, risulta $P \cap \mathbb{Z} \subset Q \cap \mathbb{Z} \subsetneq \mathbb{Z}$; inoltre, per quanto osservato precedentemente, $P \cap \mathbb{Z}$ è un ideale primo non banale di $\mathbb{Z}$ e di conseguenza è anche massimale, necessariamente deve valere allora $Q \cap \mathbb{Z} = P \cap \mathbb{Z}$. Verifichiamo che questo implica che $Q \subseteq P$; sia $u \in Q$, allora esistono $a, b \in \mathbb{Z}$ tali che $u^2+au+b = 0$, supponiamo $b \neq 0$, come prima risulta $b \in Q \cap \mathbb{Z} = P \cap \mathbb{Z}$, in particolare $b \in P$, e quindi anche $u^2 + au = u(u + a) \in P$. Ora se $u \in P$ abbiamo concluso, altrimenti deve valere $u + a \in P$, ma siccome $P \subset Q$ e per ipotesi $u \in Q$, necessariamente anche a deve appartenere a Q; così abbiamo $a \in Q \cap \mathbb{Z} = P \cap \mathbb{Z} \subseteq P$, con $u + a \in P$, da cui segue che $u \in P$. Se invece $b = 0$, troviamo $u^2 + au = u(u + a) = 0$, da cui si ricava in modo analogo che $u \in P$. Complessivamente abbiamo mostrato che ogni $u \in Q$ appartiene anche a P, ma per ipotesi $P \subset Q$, e quindi P e Q coincidono.

(iv) Per mostrare che $\mathbb{Z}[\sqrt{10}]$ non è un dominio a fattorizzazione unica, è sufficiente verificare che gli elementi irriducibili e quelli primi non coincidono.

Consideriamo la funzione $N : \mathbb{Z}[\sqrt{10}] \longrightarrow \mathbb{Z}$ definita da $(a+b\sqrt{10}) \longmapsto (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$; si verifica che tale applicazione è moltiplicativa, cioè che $N(uv) = N(u)N(v)$ per ogni $u, v \in \mathbb{Z}[\sqrt{10}]$, da cui si ricava facilmente che $N(u) = 0$ se e solo se $u = 0$. Inoltre, se un elemento $u = a + b\sqrt{10}$ è tale che $|N(u)| = 1$, allora risulta $(a + b\sqrt{10})(a - b\sqrt{10}) = 1$ oppure $(a + b\sqrt{10})(-a + b\sqrt{10}) = 1$, in particolare u è quindi invertibile; di conseguenza, per ogni elemento u che non sia un'unità di $\mathbb{Z}[\sqrt{10}]$ vale $|N(u)| \neq 1$.

Ora, in $\mathbb{Z}[\sqrt{10}]$ vale $6 = -1(4 + \sqrt{10})(4 - \sqrt{10})$, osserviamo che l'elemento 2 non è primo in $\mathbb{Z}[\sqrt{10}]$; infatti, chiaramente 2 divide 6, ma 2 non può dividere nè $4 + \sqrt{10}$ nè $4 - \sqrt{10}$, dal momento che in tal caso

si avrebbe $6 = N(4 \pm \sqrt{10}) = N(2)N(v) = 4N(v)$ per qualche $v \in \mathbb{Z}$, che è assurdo.

Mostriamo infine che 2 è un elemento irriducibile in $\mathbb{Z}[\sqrt{10}]$; supponiamo per assurdo che 2 ammetta una fattorizzazione propria, sia $2 = (a + b\sqrt{10})(a - b\sqrt{10})$ con $|N(a + b\sqrt{10})|$, $|N(a - b\sqrt{10})| \neq 1$. Siccome $N(2) = 4$, necessariamente deve valere $N(a \pm b\sqrt{10}) = a^2 - 10b^2 = \pm 2$, che non è possibile perché nessun intero a è tale che a^2 sia congruo a 2 o a -2 modulo 10, e questo conclude la dimostrazione.

Bibliografia

[1] T. W. Hungerford. *Algebra*, Holt, Rinehart and Winston, Inc., New York-Montreal, Que.-London, 1974.

[2] N. Jacobson, *Basic algebra II*, Second edition, W. H. Freeman and Company, New York, 1989.

[3] M. F. Atiyah; I. G. Macdonald. *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.