Lezioni del corso
AL430 - Anelli Commutativi e Ideali

a.a. 2011-2012

Introduzione alla Teoria delle Valutazioni

Stefania Gabelli

Testi di Riferimento

M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

N. Bourbaki, *Algèbre Commutative*, Hermann, Paris, 1961-65.

M. Fontana, *Teoria delle Valutazioni* (appunti raccolti da A. Fabbri), http://www.mat.uniroma3.it/users/fontana/didattica/fontana_didattica.html#dispense

M. Fontana, J. Huckaba, and I. Papick, *Prüfer domains*, Dekker, New York, 1977.

R. Gilmer, *Multiplicative ideal theory*, Dekker, New York, 1972.

P. Ribenboim, *The theory of classical valuations*, Springer-Verlag, New York, 1999.

R.Y. Sharp, *Steps in Commutative Algebra*, London Math. Soc. Student Texts 51, 1990.

Indice

Questi sono gli appunti delle lezioni del corso di Teoria degli Ideali da me tenuto nell'anno accademico 2011-2012. In essi vengono illustrate le prime proprietà degli anelli di valutazione e vengono introdotte alcune classi di domini definibili come intersezione di anelli di valutazioni: domini di Dedekind, di Krull, di Prüfer.

Si presuppone la conoscenza dei concetti di base dell'algebra commutativa: anelli di frazioni, dipendendenza integrale, prime proprietà degli anelli noetheriani. Per approfondimenti e integrazioni si rinvia ai testi di riferimento.

In tutto il corso A sarà un anello commutativo unitario. $\mathrm{Spec}(A)$ denoterà l'insieme degli ideali primi di A e $\mathrm{Max}(A)$ l'insieme degli ideali massimali. Con $\mathcal{U}(A)$ indicheremo il gruppo degli elementi invertibili (o delle unità) di A.

Se A è un *dominio* (cioè non ha zerodivisori), denoteremo con K il suo campo dei quozienti. Un sopra-anello di un dominio A è un dominio B tale che $A \subseteq B \subseteq K$. È evidente che tutti i sopra-anelli di A hanno lo stesso campo dei quozienti K.

Per evitare casi banali, salvo menzione esplicita, supporremo tacitamente che tutti gli anelli considerati non siano campi.

1 Anelli Locali

Diremo che A è un *anello locale* se ha un unico ideale massimale M. In questo caso, il campo quoziente $k(A) := A/M$ si chiama il *campo residuo* di A. Per indicare che A è locale con ideale massimale M si usa anche la notazione $A := (A, M)$ e, se si vuole prendere in considerazione il campo residuo $k := k(A)$, si scrive $A := (A, M, k)$.

Se A ha un numero finito di ideali massimali, si dice che A è *semilocale*.

Proposizione 1.1 *Le seguenti proprietà sono equivalenti:*

(i) *A è un anello locale;*

(ii) *$A \setminus \mathcal{U}(A)$ è un ideale;*

(iii) *$A \setminus \mathcal{U}(A)$ è un ideale massimale.*

Dimostrazione. (i) $\Rightarrow$ (iii) Se $A := (A, M)$, risulta $\mathcal{U}(A) = A \setminus M$ e $M \cap \mathcal{U}(A) = \emptyset$. Da cui $M = A \setminus \mathcal{U}(A)$.

(iii) $\Rightarrow$ (ii) è ovvio.

(ii) $\Rightarrow$ (i) Sia $I = A \setminus \mathcal{U}(A)$. Allora, per ogni $x \notin I$ risulta $(I, x) = A$. Per cui $I := M$ è un ideale massimale. Se poi $N \neq M$ fosse un altro ideale massimale, sarebbe $N \nsubseteq M$, da cui $N \cap \mathcal{U}(A) \neq \emptyset$ e $N = A$, una contraddizione. $\square$

L'intersezione di tutti gli ideali massimali di A si chiama il *radicale di Jacobson* di A e sarà indicato con $\mathrm{Jac}(A)$. Evidentemente A è locale se e soltanto se $\mathrm{Jac}(A)$ è un ideale massimale.

Proposizione 1.2 (1) *$x \in \mathrm{Jac}(A) \Leftrightarrow 1 - xy \in \mathcal{U}(A)$, per ogni $y \in A$.*

(2) *Sia M un ideale massimale di A. Allora M è l'unico ideale massimale di A se e soltanto se $1 + x \in \mathcal{U}(A)$, per ogni $x \in M$.*

Dimostrazione. (1) Sia $x \in \mathrm{Jac}(A)$, $y \in A$. Se $1 - xy \notin \mathcal{U}(A)$, esiste un ideale massimale M con $1 - xy \in M$. Siccome $1 \notin M$, allora $xy \notin M$, ovvero $x \notin M$. Ma $x \in \mathrm{Jac}(A) \subseteq M$, contraddizione.

Viceversa, sia $x \notin \mathrm{Jac}(A)$. Allora $x \notin M$ per qualche ideale massimale M e $(M, x) = A$. Dunque $1 = xy + m$ ($y \in A$, $m \in M$) e $1 - xy \in M$. Perciò $1 - xy \notin \mathcal{U}(A)$.

(2) Sia $A = (A, M)$ e $x \in M = \mathrm{Jac}(A)$. Allora per il punto (1), prendendo $y = -1$ si ha $1 + x \in \mathcal{U}(A)$.

Viceversa, sia $1 + x \in \mathcal{U}(A)$, per ogni $x \in M$. Per $y \notin M$, si ha $(M, y) = A$, da cui $1 = ay + m$ ($a \in A$, $m \in M$) e $ay = 1 + m \in \mathcal{U}(A)$. Allora $y \in \mathcal{U}(A)$ e $\mathcal{U}(A) = A \setminus M$. Perciò $A = (A, M)$. $\square$

Proposizione 1.3 *Sia $A := (A, M)$ un anello locale. Allora A contiene isomorficamente il suo campo residuo $k(A) := \frac{A}{M}$ se e soltanto se esiste un campo F isomorfo a $k(A)$ tale che $A = F + M$ (cioè, ogni elemento di A si scrive come somma di un elemento di F e un elemento di M).*

Dimostrazione. Consideriamo la successione esatta corta

$$0 \longrightarrow M \longrightarrow A \longrightarrow k(A) := \frac{A}{M} \longrightarrow 0.$$

Se esiste un isomorfismo $\alpha : k(A) \longrightarrow F \subseteq A$, allora la composizione $\pi\alpha$ (dove $\pi : A \longrightarrow k(A)$ è la proiezione canonica) è l'identità su $k(A)$; dunque la successione si spezza e $A = F \oplus M$.

Viceversa, se $A = F + M$, poiché $F \cap M = (0)$, si ha $A = F \oplus M$ e $k(A) := \frac{A}{M}$ è isomorfo a F. $\square$

Esempio 1.4 (1) Ogni campo è un anello locale, il cui ideale massimale è l'ideale nullo (0).

(2) L'anello $A := F[[X]] := \{\sum_{i \geq 0} a_i X^i\}$ delle *serie formali* nell'indeterminata X sul campo F è un anello locale con ideale massimale $M := XA$. Infatti una serie $f(X) := \sum_{i \geq 0} a_i X^i$ è invertibile se e soltanto se $a_0 \neq 0$ e dunque $\mathcal{U}(A) = A \setminus XA$. Notiamo che $A = F + XF[[X]]$ e che il campo residuo $k(A)$ è isomorfo ad F.

(3) Se A è un anello e $P \in \operatorname{Spec}(A)$, l'anello delle frazioni $A_P := \{\frac{a}{s}\,; a \in A, s \in A \setminus P\}$ è un anello locale con ideale massimale $P_P = \{\frac{p}{t}\,; p \in P, t \in A \setminus P\}$. Infatti $\frac{a}{s}$ è invertibile se e soltanto se $a \notin P$. L'anello A_P si chiama la *localizzazione* di A in P. Se A è un dominio, l'omomorfismo canonico $A \longrightarrow A_P$ definito da $a \mapsto \frac{a}{1}$ è iniettivo. In questo caso, l'ideale massimale P_P è l'ideale generato da P e viene indicato con PA_P.

Se $A := (A, M)$ e $B := (B, N)$ sono due anelli locali, si dice che B *domina* A se $A \subseteq B$ e $M = N \cap A$ (equivalentemente $M \subseteq N \cap A$). Se B domina A, si ha una inclusione naturale dei campi residui $k(A) \hookrightarrow k(B)$.

Un *omomorfismo locale* è un omomorfismo di anelli $f : (A, M) \longrightarrow (B, N)$ tale che $f(M) \subseteq N$. In questa terminologia, dire che B domina A significa dire che l'inclusione $A \subseteq B$ è un omomorfismo locale.

Esempio 1.5 (1) Siano $A \subseteq B$ due anelli. Se $Q \in \operatorname{Spec}(B)$ e $P := Q \cap A$, l'omomorfismo canonico $A_P \longrightarrow B_Q$, $\frac{a}{s} \mapsto \frac{a}{s}$, è un omomorfismo locale.

(2) Se $P \subsetneq Q$ sono due ideali primi dell'anello A, l'omomorfismo canonico di anelli locali $A_Q \longrightarrow A_P$; $\frac{a}{s} \mapsto \frac{a}{s}$ non è un omomorfismo locale. Infatti $f(Q_Q) = A_P \nsubseteq P_P$.

2 Anelli di Valutazione

Gli anelli di valutazione costituiscono una particolare classe di domini.

Un dominio A con campo delle frazioni K si chiama un *anello di valutazione* o *dominio di valutazione* se, per ogni $x \in K \setminus \{0\}$, si ha che $x \in A$ oppure $x^{-1} \in A$. I campi sono banalmente anelli di valutazione.

Corollario 2.1 *Un dominio di valutazione A è integralmente chiuso.*

Dimostrazione. Sia $x \in K$ intero su A, con relazione di dipendenza integrale $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, $a_i \in A$. Se $x \notin A$, allora $x^{-1} \in A$. Moltiplicando la relazione per x^{1-n} si ottiene $x + (a_{n-1} + \cdots + a_0x^{1-n}) = 0$. Poiché $a_{n-1} + \cdots + a_0x^{1-n} \in A$, allora $-x \in A$, ovvero $x \in A$. $\square$

Un dominio in cui ogni ideale finitamente generato è principale si chiama un *dominio di Bezout*. Per induzione sui generatori, si vede subito che un dominio è di Bezout se e soltanto se ogni ideale generato da due elementi è principale. Notiamo che in un dominio, se $x, y \neq 0$, risulta $\langle x, y\rangle = \langle d\rangle$ se e soltanto se d è un massimo comune divisore di a e b e $d = ax + by$, con $a, b \in A$ (*identità di Bezout*).

Segue dalla definizione che i domini di Bezout noetheriani sono i domini a ideali principali. Vediamo ora che gli anelli di valutazione sono domini di Bezout locali, non necessariamente noetheriani.

Proposizione 2.2 *Le seguenti proprietà sono equivalenti per un dominio A.*

(i) *A è un dominio di valutazione;*

(ii) *Gli ideali (frazionari) principali di A sono linearmente ordinati;*

(iii) *Gli ideali (frazionari) di A sono linearmente ordinati;*

(iv) *A è un dominio di Bezout locale.*

Dimostrazione. (i) $\Rightarrow$ (ii) Siano x, $y \in K \setminus \{0\}$. Se $xy^{-1} \in A$, allora $xA \subseteq yA$. Altrimenti $x^{-1}y \in A$ e quindi $yA \subseteq xA$.

(ii) $\Rightarrow$ (iii) Siano I e J due ideali (frazionari) di A. Se $x \in J \setminus I$, per ogni $y \in I$ si ha $\langle y\rangle \subseteq \langle x\rangle$. Quindi $I \subseteq \langle x\rangle \subseteq J$.

(iii) $\Rightarrow$ (iv) A è locale perché in ogni dominio due ideali massimali che sono comparabili coincidono.

Siano x, $y \in A$. Se $\langle x\rangle \subseteq \langle y\rangle$ si ha $\langle x, y\rangle = \langle y\rangle$. Altrimenti $\langle y\rangle \subseteq \langle x\rangle$ e perciò $\langle x, y\rangle = \langle x\rangle$. Ne segue che A è di Bezout.

(iv) $\Rightarrow$ (ii) Sia M l'ideale massimale di A e siano x, $y \in A \setminus \{0\}$. Supponiamo che $I := \langle x, y\rangle = \langle d\rangle$. Allora $d^{-1}I = A$ e quindi, posto $w := d^{-1}x$, $z := d^{-1}y$, risulta $1 = aw + bz$ per opportuni a, $b \in A$. Siccome $1 \notin M$,

$aw \notin M$ oppure $bz \notin M$. Se $aw \notin M$, allora aw è invertibile in A; quindi $z = z(aw)(aw)^{-1} = w(az)(aw)^{-1} \in \langle w \rangle$. Segue che $\langle z \rangle \subseteq \langle w \rangle$ e dunque $\langle y \rangle \subseteq \langle x \rangle$. Analogamente, se $bz \notin M$ allora $\langle x \rangle \subseteq \langle y \rangle$.

(ii) $\Rightarrow$ (i) Sia $x = \frac{a}{b} \in K$. Gli ideali $\langle a \rangle$ e $\langle b \rangle$ sono comparabili per ipotesi. Se $\langle a \rangle \subseteq \langle b \rangle$, allora $xA \subseteq A$ e $x \in A$. Altrimenti $A \subseteq xA$ e quindi $x^{-1} \in A$. $\square$

Per la corrispondenza tra gli ideali di un anello e quelli di un suo quoziente, si ha subito il seguente corollario.

Corollario 2.3 *Se V è un dominio di valutazione, per ogni ideale primo P l'anello quoziente V/P è un dominio di valutazione.*

Proposizione 2.4 *Sia V un dominio di valutazione. Allora ogni sopra-anello di V è un dominio di valutazione ed è la localizzazione di V rispetto ad un ideale primo. In particolare, i sopra-anelli di V sono linearmente ordinati per inclusione.*

Dimostrazione. Sia R un sopra-anello di V e sia $x \in K \setminus \{0\}$. Se $x \notin R$, allora $x \notin V$; quindi $x^{-1} \in V \subseteq R$. Ne segue che R è un dominio di valutazione. In particolare R è locale. Sia M l'ideale massimale di R e sia $P := M \cap V$. Mostriamo che $V_P = R$. Chiaramente $V_P \subseteq R$. Viceversa, sia $x \in R \setminus V$. Poiché $x^{-1} \in V \subseteq R$, allora x è invertibile in R. Dunque $x^{-1} \in V \setminus M = V \setminus P$. Ne segue che $x = \frac{x}{1} = \frac{1}{x^{-1}} \in V_P$.

Infine, poiché gli ideali primi di V sono linearmente ordinati, anche le sue localizzazioni lo sono. $\square$

Corollario 2.5 *Un dominio di valutazione di dimensione uno non ha sopra-anelli propri.*

Proposizione 2.6 *Sia V un dominio di valutazione. Se P è un primo non principale di V, allora $V_P = (P : P) = (V : P)$.*

Dimostrazione. Mostriamo intanto che $V_P \subseteq (P : P)$. Questo è certamente vero se P è massimale, cioè $V = V_P$; supponiamo quindi che $V \subsetneq V_P$. Sia $x \in V_P \setminus V$. Allora $y := x^{-1} \in V \setminus P$ e dunque $P \subseteq yV$. Segue che $xP \subseteq V$. Inoltre $P = xyP$ e poiché $y \notin P$ risulta $xP \subseteq P$. Quindi $x \in (P : P)$.

Viceversa, $(P : P) \subseteq (V : P) \subseteq V_P$. Infatti, sia $z \in (V : P)$. Poiché V_P è di valutazione, se $z \notin V_P$, si ha $z^{-1} \in PV_P \subseteq P(P : P) \subseteq P$. Dunque $1 = z^{-1}z \in P(V : P)$ and P è invertibile, cioè principale. Una contraddizione. $\square$

Vedremo che un ideale primo principale di un dominio di valutazione è massimale (Corollario 4.2); dunque per la proposizione precedente tutti i sopra-anelli propri di un dominio di valutazione sono del tipo $(P : P)$, con P primo.

2.1 Il Teorema di Krull sulla chiusura integrale

Ogni insieme non vuoto di sottoanelli locali di un campo F è parzialmente ordinato rispetto alla relazione di dominanza. W. Krull ha dimostrato che gli anelli di valutazione con campo dei quozienti K sono precisamente gli elementi massimali dell'insieme di tutti gli anelli locali contenuti propriamente in K. Per vedere questo, ci sarà utile il seguente lemma.

Lemma 2.7 (Lemma (x, x^{-1})) *Sia A un sottoanello di un campo F e sia $I \subseteq A$ un ideale proprio. Allora, per ogni $x \in F \setminus \{0\}$, si ha $I[x] \neq A[x]$ oppure $I[x^{-1}] \neq A[x^{-1}]$.*

Dimostrazione. Supponiamo per assurdo che sia contemporaneamente $I[x] = A[x]$ e $I[x^{-1}] = A[x^{-1}]$. Allora $\sum_{i=0}^{n} a_i x^i = 1 = \sum_{j=0}^{m} b_j x^j$, con $a_i, b_j \in I$. Possamo supporre n e m minimali, con $n \geq m$ (a meno di scambiare x con x^{-1}).

Moltiplicando la seconda uguaglianza per x^n, otteniamo

$$(1 - b_0)x^n = \sum_{j=1}^{m} b_j x^{n-j}.$$

Moltiplicando la prima uguaglianza per $(1 - b_0)$, otteniamo

$$(1 - b_0) = \sum_{i=0}^{n-1} c_i x^i + a_n(1 - b_0)x^n,$$

dove $c_i = a_i(1 - b_0)$. Da cui, sostituendo,

$$1 = b_0 + \sum_{i=0}^{n-1} c_i x^i + a_n \sum_{j=1}^{m} b_j x^{n-j}.$$

Questo contraddice la minimalità di n.

$\square$

Proposizione 2.8 *Sia $A := (A, M)$ un sottoanello locale di un campo F e sia $\mathcal{L}$ l'insieme di tutti i sottoanelli locali propri di F che dominano A. Allora:*

(1) $\mathcal{L}$ ammette un elemento massimale.

(2) Un elemento massimale di $\mathcal{L}$ è un dominio di valutazione.

In particolare, ogni anello locale è dominato da un sopra-anello di valutazione.

Dimostrazione. (1) $\mathcal{L}$ è non vuoto (perché contiene A) ed è parzialmente ordinato per la relazione di dominanza. Applichiamo il Lemma di Zorn. Sia $\{(B_i, N_i)\}_{i\geq 0}$ una catena in $\mathcal{L}$ (dunque B_{i+1} domina B_i per ogni i) e sia $B := \cup B_i$. Allora B è locale con ideale massimale $N := \cup N_i$. Poiché evidentemente B domina A, allora $B \in \mathcal{L}$ e per il Lemma di Zorn $\mathcal{L}$ ha elementi massimali.

(2) Sia (B, N) un sottoanello massimale di F che domina (A, M). Facciamo vedere che, per ogni $x \in F \setminus \{0\}$, risulta $x \in B$ oppure $x^{-1} \in B$. A meno di scambiare x con x^{-1}, possiamo supporre che $N[x] \neq B[x]$ (Lemma 2.7). Sia $\mathcal{N}$ un ideale massimale di $B[x]$ contenente $N[x]$. Allora l'anello locale $B[x]_{\mathcal{N}}$ domina B e quindi, per la massimalità di B, $(B, N) = (B[x]_{\mathcal{N}}, \mathcal{N}B[x]_{\mathcal{N}})$. Dunque $x \in B$. $\square$

Teorema 2.9 (W. Krull, 1932) *Sia $A := (A, M)$ un sottoanello locale di un campo F. Le seguenti proprietà sono equivalenti:*

(i) *A è un dominio di valutazione;*

(ii) *A è un elemento massimale dell'insieme di tutti gli anelli locali contenuti propriamente in F, ordinati con la relazione di dominanza.*

Dimostrazione. (i) $\Rightarrow$ (ii) Supponiamo che $(B, N) \subseteq F$ domini (A, M). Se $x \in B \setminus A$, allora $x^{-1} \in A$ e x^{-1} non è invertibile in A. Allora $x^{-1} \in M \subseteq N$ e $1 = xx^{-1} \in N$. Questo assurdo mostra che $A = B$.

(ii) $\Rightarrow$ (i) segue dalla Proposizione 2.8 (perché ogni anello locale domina almeno se stesso). $\square$

Per la Proposizione 2.8, ogni dominio è contenuto in un anello di valutazione con il suo stesso campo dei quozienti. Mostriamo ora che l'intersezione di tutti i sopra-anelli di valutazione di A è precisamente la chiusura integrale di A. Questo segue dal seguente risultato più generale.

Teorema 2.10 (W. Krull) *Sia A un sottoanello di un campo F. Allora la chiusura integrale di A in F è l'intersezione di tutti gli anelli di valutazione con campo dei quozienti F contenenti A.*

Dimostrazione. Indichiamo con A' la chiusura integrale di A in F.

Sia $\mathcal{V}$ la famiglia degli anelli di valutazione con campo dei quozienti F contenenti A e sia $B := \cap_{V\in\mathcal{V}} V$. Poiché B è integralmente chiuso, allora $A' \subseteq B$.

Viceversa, sia $x \in F \setminus A'$. Mostriamo che $x \notin B$, cioè esiste $V \in \mathcal{V}$ con $x \notin V$. Poniamo $C := A[x^{-1}]$. Notiamo che $x \notin C$, altrimenti, se $x = f(x^{-1})$, moltiplicando per una opportuna potenza di x si otterrebbe una relazione di dipendenza integrale per x. Dunque x^{-1} non è invertibile in C. Sia $N \in \mathrm{Max}(C)$ con $x^{-1} \in N$ e sia $(V, M) \subseteq F$ un dominio di valutazione che domina (C_N, NC_N) (Proposizione 2.8). Allora $x^{-1} \in N \subseteq M$ e perciò x^{-1} non è invertibile in V. In conclusione $x \notin V$. $\square$

3 Anelli di Valutazione Noetheriani

Vogliamo ora caratterizzare i domini di valutazione noetheriani. Il seguente risultato è una versione del Lemma di Nakayama per i domini.

Lemma 3.1 *Sia A un dominio con campo dei quozienti K e siano I, J ideali frazionari non nulli di A. Se I è finitamente generato e $IJ = I$, allora $1 \in J$. In particolare, se $J \subseteq A$, allora $J = A$.*

Dimostrazione. Sia $I = x_1A + \cdots + x_nA$, con $0 \neq x_i \in K$. Se $I = IJ = x_1J + \cdots + x_nJ$, allora per ogni $i = 1, \ldots, n$ possiamo scrivere $x_i = x_1y_{i1} + \cdots + x_ny_{in}$, $y_{ij} \in J$. Da cui $\sum_j(\delta_{ij} - y_{ij})x_j = 0$, dove δ_{ij} è il simbolo di Kronecker. Allora il sistema lineare $\sum_j(\delta_{ij} - y_{ij})X_j = 0$ ha soluzioni non nulle in K e perciò $\det(\delta_{ij} - y_{ij}) = 0$. Ma, calcolando, risulta $\det(\delta_{ij} - y_{ij}) = 1 - z$, con $z \in J$; perciò $1 = z \in J$. $\square$

Teorema 3.2 *Le seguenti proprietà sono equivalenti per un dominio A:*

(i) *A è un dominio di valutazione noetheriano;*

(ii) *A è un dominio di valutazione a ideali principali;*

(iii) *A è un dominio locale a ideali principali;*

(iv) *A è un dominio locale di dimensione uno il cui ideale massimale è principale;*

(v) *Esiste $t \in A$ (*parametro uniformizzante*) tale che, per ogni elemento non nullo $x \in A$ si ha $x = ut^n$, con $u \in \mathcal{U}(A)$ e $n \geq 0$ univocamente determinati;*

(vi) *Esiste $t \in A$ tale che, per ogni ideale non nullo I di A, $I = \langle t^n \rangle$ con $n \geq 0$;*

(vii) *A è un dominio locale e, se M è il suo ideale massimale, tutti e soli gli ideali non nulli di A sono gli ideali M^n, $n \geq 0$;*

(viii) *A è un dominio locale noetheriano integralmente chiuso di dimensione uno.*

Dimostrazione. (i) $\Rightarrow$ (ii) perché un dominio di valutazione è di Bezout, cioè ogni ideale finitamente generato è principale (Proposizione 2.2).

(ii) $\Rightarrow$ (i) e (ii) $\Rightarrow$ (iii) sono evidenti.

(iii) $\Rightarrow$ (iv) perché un dominio a ideali principali ha dimensione uno.

(iv) $\Rightarrow$ (v) Poiché A ha un unico ideale massimale, per il Teorema di Cohen, A è noetheriano. Sia t un generatore dell'ideale massimale M di A. Se $x \in A$ è invertibile, allora $x = xt^0$. Altrimenti $x \in M$, quindi

$x = x_1 t$ con $x_1 \in A$. Se x_1 non è invertibile, possiamo scrivere $x_1 = x_2 t$, con $x_2 \in A$ e dunque $x = x_2 t^2$. Così proseguendo, otteniamo una catena di ideali principali

$$\langle x \rangle \subseteq \langle x_1 \rangle \subseteq \langle x_2 \rangle \subseteq \ldots \subseteq \langle x_k \rangle \subseteq \ldots .$$

Per noetherianità, tale catena staziona, cioè $\langle x_n \rangle = \langle x_{n+1} \rangle$ per qualche intero $n \geq 0$. Allora $x_n = u$ è invertibile e $x = ut^n$ (altrimenti per costruzione $x_n = x_{n+1} t$ e $\langle x_n \rangle \subsetneq \langle x_{n+1} \rangle$).

Per l'unicità, se $x = ut^n = vt^m$, allora $(u - v)t^{n-m} = 0$, da cui $u = v$ e $n = m$.

(v) $\Rightarrow$ (vi) Per ipotesi $x = ut^n \in A$ è invertibile se e soltanto se $n = 0$. Sia I un ideale proprio di A e sia $S := \{k \geq 1\,;\ \text{ tali che } ut^k \in I\}$. Se n è il minimo intero in S, allora $I = \langle t^n \rangle$.

(vi) $\Rightarrow$ (vii) È evidente che A è locale con ideale massimale $M = \langle t \rangle$. Inoltre se $I = \langle t^n \rangle$ allora $I = M^n$.

(vii) $\Rightarrow$ (vi) Si ha $M \neq M^2$, altrimenti $M = M^n$ per ogni $n \geq 1$ e M sarebbe l'unico ideale proprio non nullo del dominio A, il che è impossibile. Sia $t \in M \setminus M^2$. Poiché $\langle t \rangle = M^k$ per qualche $k \geq 1$, allora $k = 1$. Ovvero $M = \langle t \rangle$ e $M^n = \langle t^n \rangle$.

(vi) $\Rightarrow$ (ii) A è evidentemente ad ideali principali. Inoltre gli ideali di A sono linearmente ordinati. Quindi A è un dominio di valutazione per la Proposizione 2.2.

(ii) $\Rightarrow$ (viii) A è evidentemente noetheriano ed ha dimensione uno perché è a ideali principali. Infine A è locale per la Proposizione 2.2 e integralmente chiuso per il Corollario 2.1.

(viii) $\Rightarrow$ (iv) Basta mostrare che l'ideale massimale di A è principale. Sia $x \in A$ un elemento non nullo. Poiché M è l'unico ideale primo non nullo di A, allora l'ideale principale $I := \langle x \rangle$ ha radicale M. Poiché M è finitamente generato, le potenze di M sono tutte distinte (Lemma 3.1). Inoltre I contiene una potenza M^n di M. Perciò, scegliendo n minimale, $M^{n-1} \nsubseteq I$. Sia $y \in M^{n-1} \setminus I$, così che $yM \subseteq M^n \subseteq I$ e $\frac{y}{x} M \subseteq A$. Mostriamo che $\frac{y}{x} M = A$ e dunque $M = \langle \frac{x}{y} \rangle$. Se $\frac{y}{x} M \neq A$, necessariamente $\frac{y}{x} M \subseteq M$ e $\frac{y}{x} \subseteq (M : M)$ è intero su A. Poiché A è integralmente chiuso, allora $\frac{y}{x} \in A$ e $y \in I$. Contraddizione. $\square$

Se $V := (V, M)$ è un un anello di valutazione noetheriano con parametro uniformizzante t, ogni elemento non nullo di V è del tipo ut^n, con $n \geq 0$ e u invertibile unicamente determinati; quindi ogni elemento del campo dei quozienti K è del tipo $\frac{ut^n}{vt^m} = wt^k$, con $w \in \mathcal{U}(A)$ e $k \in \mathbb{Z}$ unicamente determinati.

Esempio 3.3 (1) La localizzazione di $\mathbb{Z}$ in un ideale primo $\langle p \rangle$ è un anello di valutazione noetheriano. Infatti è un dominio locale di dimensione uno con ideale massimale $p\mathbb{Z}_{\langle p \rangle}$ principale.

(2) L'anello delle serie formali $F[[X]]$ è un anello di valutazione noetheriano con parametro uniformizzante X. Infatti se $f(X) := \sum a_i X^i \neq 0$ e n è l'*ordine* di $f(X)$, cioè il minimo intero n tale che $a_n \neq 0$, allora risulta $f(X) = X^n g(X)$, con $g(X) := a_n + a_{n+1}X + \dots$ invertibile.

Il campo dei quozienti di $F[[X]]$ si indica con $F((X))$ e si chiama il *campo delle serie di Laurent*. Se $\varphi(X)$ è una serie di Laurent non nulla, allora $\varphi(X) = \frac{f(X)}{g(X)} = X^k u(X)$, con $k = \operatorname{ord} f - \operatorname{ord} g \in \mathbb{Z}$ e $u(X) \in F[[X]]$ invertibile. L'intero $k := \operatorname{ord} f - \operatorname{ord} g$ si chiama ancora l'ordine di $\varphi(X)$.

(3) I domini di valutazione di dimensione strettamente maggiore di uno non sono noetheriani.

Domini di valutazione di dimensione finita uguale a $d \geq 2$ possono essere costruiti induttivamente "incollando" due domini di valutazione nel modo seguente.

Sia $V := (V, M)$ un dominio di valutazione di dimensione $n \geq 1$ con campo dei quozienti K e campo residuo $k := k(V) = V/M$ e supponiamo che esista un dominio di valutazione $W := (W, N)$ di dimensione $m \geq 1$ con campo dei quozienti k. Se $\pi : V \longrightarrow k$ è la proiezione canonica, allora $R := \pi^{-1}W$ è un dominio di valutazione di dimensione $d := n + m$.

$$\begin{tikzcd} R := \pi^{-1}(W) \arrow[r] \arrow[d] & W \arrow[d, "\iota"'] \\ V \arrow[r, "\pi"] & \frac{V}{M} =: k \end{tikzcd}$$

Notiamo che se $V = k + M$, allora $R = W + M$.

Per vedere che R è un dominio di valutazione di dimensione $n + m$, notiamo che:

(a) M è un ideale di R.

Infatti $M = \pi^{-1}(0) \subseteq \pi^{-1}(W) = R$; inoltre, essendo $R \subseteq V$, si ha $MR \subseteq MV = M$. Notiamo anche che risulta $M = (R :_R V)$, cioè M è il *conduttore* di V in R.

(b) Ogni ideale di R è comparabile con M.

Sia I un ideale di R. Se $I \nsubseteq M$, ogni $a \in I \setminus M$ è invertibile in V. Dunque $a^{-1} \in V$ e $M = a^{-1}(aM) \subseteq aM \subseteq I$.

(c) Gli ideali di R che contengono M sono in corrispondenza biunivoca con gli ideali di W.

Questo segue dal fatto che, poiché π è suriettiva ed ha nucleo M, risulta $W \cong \frac{R}{M}$.

(d) R e V hanno lo stesso campo dei quozienti K.

Infatti, se $a, b \in V \setminus \{0\}$ e $m \in M$, si ha $am, bm \in R$ e $\frac{a}{b} = \frac{ma}{mb}$.

(e) R è un dominio di valutazione.

Infatti, sia $x \in K \setminus R$. Se $x \notin V$, allora $x^{-1} \in V \setminus \mathcal{U}(V) = M \subseteq R$. Se $x \in V$, allora $x + M \in k \setminus \frac{R}{M}$. Poiché $\frac{R}{M} \cong W$ è di valutazione, $x^{-1} + M \in \frac{R}{M}$, da cui $x^{-1} \in R$.

(f) Gli ideali primi di R contenuti in M sono in corrispondenza biunivoca con gli ideali primi di V.

Infatti, poiché R è di valutazione e V è un suo sopra-anello, si ha $V = (M : M) = R_M$.

Ad esempio, se $V := \mathbb{Q}[[X]]$, con ideale massimale $M := X\mathbb{Q}[[X]]$, allora $k = \mathbb{Q}$ e k contiene $W := \mathbb{Z}_{\langle p \rangle}$, $p \geq 2$ primo. La controimmagine di W in $\mathbb{Q}$ è l'anello $R := \mathbb{Z}_{\langle p \rangle} + X\mathbb{Q}[[X]]$ delle serie formali a coefficienti razionali con il termine noto in $\mathbb{Z}_{\langle p \rangle}$. Siccome V e W sono DVR, allora R è un dominio di valutazione di dimensione 2.

I due ideali primi di R sono: l'ideale massimale $N := pR = p\mathbb{Z}_{\langle p \rangle} + X\mathbb{Q}[[X]]$ e l'ideale $M = X\mathbb{Q}[[X]]$.

Notiamo che M non è finitamente generato, equivalentemente principale, come ideale di R. Infatti $(R : M)$ è un ideale frazionario di V e $M(R : M) \subseteq R \subsetneq V$. Dunque $M(R : M) \subseteq M$ e M non può essere principale in R. D'altra parte, vedremo che ogni ideale primo principale di un dominio di valutazione è massimale (Proposizione 4.1).

(4) Domini di valutazione di dimensione uno che non sono noetheriani esistono; essi verranno caratterizzati nel Paragrafo 9.1.

4 Ideali Primari di Anelli di Valutazione

In questo paragrafo V denoterà un *dominio di valutazione*. Vogliamo studiare gli ideali primari di V.

Ricordiamo che un ideale Q di un anello A si dice *primario* se $xy \in Q$ e $x \notin Q$ implica $y^n \in Q$, per qualche $n \geq 1$ (equivalentemente, $y \in \sqrt{Q}$). Gli ideali primi sono chiaramente primari.

È facile vedere che il radicale di un ideale primario Q è un ideale primo P (in questo caso Q si dice *P-primario*). Però il viceversa non è vero. In particolare se P è un ideale primo, si ha $\sqrt{P^n} = P$, ma P^n può non essere primario (a meno che P non sia massimale). Ad esempio sia F un campo e $A := F[X, Y, Z]/(XY - Z^2) =: F[x, y, z]$. Se $P = (x, z)$, l'ideale $P^2 = (x^2, z^2, xz)$ non è primario, infatti, $xy = z^2 \in P^2$, mentre $x \notin P^2$ e $y \notin P$.

Tuttavia vedremo che le potenze di un ideale primo P di V sono ideali P-primari. Notiamo che, poiché gli ideali di V sono linearmente ordinati (Proposizione 2.2), il radicale di ogni ideale proprio di V è un ideale primo.

Proposizione 4.1 *Se $Q \subseteq V$ è P-primario e $x \in V \setminus P$, allora $Q = xQ$.*

Dimostrazione. Se $x \in V \setminus P$, allora $Q \subseteq P \subseteq xV$ e $Q = x(x^{-1}Q)$ con $Q \subseteq x^{-1}Q \subseteq V$. Inoltre, poiché Q è P-primario e $x \notin P$, allora $x^{-1}Q \subseteq Q$. Quindi $Q = xQ$. $\square$

Corollario 4.2 *Se Q è un ideale P-primario finitamente generato, allora P è un ideale massimale. In particolare, un ideale primo principale di V è massimale.*

Dimostrazione. Se $x \in V \setminus P$, si ha $Q = xQ$. Allora, se Q è finitamente generato, ovvero principale, cancellando Q si ottiene $V = xV$. Dunque x è invertibile e P è massimale. $\square$

Corollario 4.3 *Sia $Q \subseteq V$ un ideale primario e P un ideale primo contenente Q. Allora $QV_P = Q$.*

Dimostrazione. Sia $\frac{q}{s} \in QV_P$ con $q \in Q$ e $s \in V \setminus P$. Poiché $Q = sQ$, si ha $q = sq'$, $q' \in Q$. Allora $\frac{q}{s} = q' \in Q$. Il viceversa è ovvio. $\square$

Proposizione 4.4 *Sia $I \subseteq V$ un ideale proprio e $P_0 := \cap_{n \geq 1} I^n$. Allora*

(1) *P_0 è un ideale primo di V.*

(2) *Se $I^k = I^{k+1}$ per qualche $k \geq 1$, allora I è un ideale primo idempotente.*

(3) *Ogni ideale primo contenuto propriamente in I è contenuto in P_0.*

(4) *Se J è un ideale e $I \subsetneq \sqrt{J}$, allora J contiene una potenza di I.*

Dimostrazione. (1) Siano $x, y \in V \setminus P_0$. Dunque $x \notin I^n$ e $y \notin I^m$ per opportuni $n, m \geq 1$. Allora $I^n \subsetneq xV$ e $I^m \subsetneq yV$. Ne segue che $I^{n+m} \subseteq yI^n \subsetneq xyV$. Perciò $xy \notin P_0$ e P_0 è un ideale primo.

(2) Se $I^k = I^{k+1}$ per qualche $k \geq 1$, allora $I^k = P_0$ è un ideale primo. Dunque $I \subseteq P_0 = I^k$ da cui $I = I^k = I^{k+1}$ e $I = I^2 = P_0$ è un ideale primo.

(3) Se P è un ideale primo e $P \subsetneq I$, allora $I^n \nsubseteq P$ per ogni $n \geq 1$ (altrimenti $I \subseteq P$). Da cui $P \subseteq I^n$ per ogni n, cioè $P \subseteq \cap_{n \geq 1} I^n =: P_0$.

(4) Se J non contiene alcuna potenza I^n di I, allora $J \subseteq \cap_{n \geq 1} I^n =: P_0$. Quindi $\sqrt{J} \subseteq P_0 \subseteq I$ e $I \nsubseteq \sqrt{J}$ (altrimenti $I = \sqrt{J}$). $\square$

Proposizione 4.5 *L'insieme degli ideali P-primari di V è moltiplicativamente chiuso. Quindi P^n è un ideale P-primario per ogni $n \geq 1$.*

Se inoltre $P \neq P^2$, ogni ideale P-primario è una potenza di P.

Dimostrazione. Siano Q_1, Q_2 ideali P-primari. Chiaramente $\sqrt{Q_1 Q_2} = P$. Siano $x, y \in V$ tali che $xy \in Q_1 Q_2$ e $x \notin P$. Per far vedere che $Q_1 Q_2$ è primario, dobbiamo mostrare che $y \in Q_1 Q_2$. Per la Proposizione 4.1, si ha $Q_1 = xQ_1$, così che $xyV \subseteq Q_1 Q_2 = xQ_1 Q_2$. Quindi $y \in yV \subseteq Q_1 Q_2$.

Supponiamo ora che $P \neq P^2$ e sia Q un ideale P-primario. Poiché $P^2 \subsetneq P = \sqrt{Q}$, per la Proposizione 4.4(4), Q contiene una potenza di P^2, ovvero di P. Sia $k \geq 1$ il minimo intero positivo tale che $P^k \subseteq Q$ e sia $y \in P^{k-1} \setminus Q$.

Allora $Q \subseteq yV$ e $Q = yI$, con $I := y^{-1}Q \subseteq V$. Poiché Q è P-primario e $y \notin Q$, segue che $I \subseteq P$. Perciò $Q = yI \subseteq yP \subseteq P^{k-1}P = P^k \subseteq Q$, da cui $Q = P^k$. $\square$

Un ideale primo P di V si dice *ramificato* se esiste qualche ideale P-primario di V diverso da P. Se $P \neq P^2$ allora P è ramificato (perché P^2 è P-primario). Osserviamo che, se $P = P^2$, allora P non può essere finitamente generato (Lemma 3.1).

Se P', P sono due ideali primi di un anello A, diciamo che P' e P sono *adiacenti* se $P' \subsetneq P$ e non ci sono altri ideali primi tra P' e P.

Proposizione 4.6 *Sia A un anello e siano P', P due primi adiacenti, $P' \subsetneq P$. Allora P' è l'intersezione di tutti gli ideali P-primari contenenti P'.*

Dimostrazione. Nelle ipotesi date, l'anello $A_P/P'A_P$ è locale di dimensione uno. Dunque non è restrittivo supporre che A sia un dominio locale di dimensione uno con ideale massimale $M = P$ e $P' = (0)$. In questo caso, ogni ideale proprio non nullo di A è M-primario e l'unico elemento di A contenuto in tutti gli ideali non nulli è 0. Infatti ad esempio se $x \in M \setminus \{0\}$, $x \notin x^2A$. $\square$

Proposizione 4.7 *Sia P un ideale primo di V. Le seguenti proprietà sono equivalenti:*

(i) *P è ramificato;*

(ii) *$P = \sqrt{I}$, per qualche ideale $I \subsetneq P$;*

(iii) *P è il radicale di un ideale principale;*

(iv) *P non è l'unione degli ideali primi contenuti propriamente in P;*

(v) *Esiste un ideale primo P' adiacente a P.*

Dimostrazione. (i) $\Rightarrow$ (ii) e (iv) $\Rightarrow$ (v) sono evidenti.

(ii) $\Rightarrow$ (iii) Se $x \in P \setminus I$, allora $I \subseteq xV \subseteq P$ e dunque $P = \sqrt{xV}$.

(iii) $\Rightarrow$ (iv) Se $P = \sqrt{xV}$, allora $x \in P$ e $x \notin P'$, per ogni primo P' contenuto in P.

(v) $\Rightarrow$ (i) segue dalla Proposizione 4.6. $\square$

Corollario 4.8 *V soddisfa la condizione della catena ascendente (acc) sugli ideali primi se e soltanto se ogni ideale primo non nullo è ramificato.*

Dimostrazione. Applichiamo la Proposizione 4.7, (i) $\Leftrightarrow$ (iv).

Supponiamo che valga la acc sugli ideali primi e sia $P \in \mathrm{Spec}(V)$. Consideriamo una catena di ideali primi $P_0 \subseteq P_1 \subseteq \ldots \subseteq P_n \subseteq \ldots$ propriamente contenuti in P. Se la catena stabilizza a P_k, si ha $\cup P_n = P_k \subsetneq P$. Quindi P è ramificato.

Viceversa, supponiamo che non valga la acc sugli ideali primi e sia $P_0 \subseteq P_1 \subseteq \ldots \subseteq P_n \subseteq \ldots$ una catena di ideali primi che non stabilizza. Allora l'unione $P := \cup P_n$ è un ideale primo che non è ramificato. Infatti, è facile vedere che P è primo. Inoltre P è l'unione di tutti gli ideali primi propriamente contenuti in P, perché se $P' \subsetneq P$ e $x \in P \setminus P'$, allora $x \in P_i$ per qualche P_i della catena e $P' \subseteq P_i$. □

Corollario 4.9 *Se P è un ideale primo ramificato di V, l'intersezione degli ideali P-primari di V è un ideale primo adiacente a P.*

Dimostrazione. Per la Proposizione 4.7, esiste un ideale primo P' adiacente a P e, per la Proposizione 4.6, P' è l'intersezione di tutti gli ideali P-primari di V. □

5 Anelli di Valutazione Discreti

Ricordiamo che, se V è un dominio di valutazione e $P \in \mathrm{Spec}(V)$ è tale che $P \neq P^2$, allora P è un primo ramificato (Proposizione 4.5).

Un dominio di valutazione V si chiama

(a) *discreto* se $P \neq P^2$ per ogni ideale primo P ramificato;

(b) *fortemente discreto* se $P \neq P^2$ per ogni ideale primo P non nullo.

Per la corrispondenza tra gli ideali primari di un dominio e quelli di una localizzazione o di un quoziente otteniamo subito il seguente risultato.

Proposizione 5.1 *Se V è un dominio di valutazione (fortemente) discreto, allora per ogni $P \in \mathrm{Spec}(V)$, V_P e V/P sono domini di valutazione (fortemente) discreti.*

Chiaramente fortemente discreto implica discreto. Vediamo ora che in dimensione finita i due concetti sono equivalenti, ed inoltre in dimensione uno sono anche equivalenti alla noetherianità.

Proposizione 5.2 *V è un dominio di valutazione discreto se e soltanto se ogni ideale primario è una potenza del suo radicale.*

Dimostrazione. Supponiamo che ogni ideale P-primario Q sia una potenza di P. Allora, se P è ramificato, $Q = P^n \neq P$, per qualche $n \geq 1$. Dunque necessariamente $P \neq P^2$ e V è discreto.

Viceversa, supponiamo che V sia discreto. Se P è non ramificato, tutti gli ideali P-primari sono uguali a P. Se invece P è ramificato, per ipotesi $P \neq P^2$ e dunque ogni ideale P-primario è una potenza di P (Proposizione 4.5). □

Proposizione 5.3 *Un dominio di valutazione V è fortemente discreto se e soltanto se è discreto e soddisfa la condizione della catena ascendente sugli ideali primi.*

Dimostrazione. Segue dalle definizioni e dal Corollario 4.8. Infatti, se V è fortemente discreto, per ogni ideale primo non nullo P si ha $P \neq P^2$, in particolare P è ramificato e dunque vale la acc sugli ideali primi.

Se viceversa vale la acc sugli ideali primi, ogni primo P non nullo è ramificato. Perciò se V è discreto si ha $P \neq P^2$. □

Corollario 5.4 *Se V ha dimensione finita, V è discreto se e soltanto se è fortemente discreto.*

Proposizione 5.5 *Sia $V := (V, M)$ un dominio di valutazione di dimensione uno. Le seguenti proprietà sono equivalenti:*

(i) $M \neq M^2$;

(ii) *V è fortemente discreto;*

(iii) *V è discreto;*

(iv) *V è noetheriano.*

Dimostrazione. (i) $\Rightarrow$ (ii) perché M è l'unico ideale primo non nullo.

(ii) $\Leftrightarrow$ (iii) per il Corollario 5.4.

(ii) $\Rightarrow$ (iv) M è principale per la Proposizione 5.6. Poiché V ha dimensione uno, V è noetheriano per il Teorema 3.2.

(iv) $\Rightarrow$ (i) perché M è finitamente generato (Lemma 3.1). □

Proposizione 5.6 *Le seguenti proprietà sono equivalenti per un dominio di valutazione V:*

(i) *V è fortemente discreto;*

(ii) *PV_P è principale, per ogni $P \in \mathrm{Spec}(V)$;*

(iii) *Ogni ideale $P \in \mathrm{Spec}(V)$ è ramificato, e se $Q \subsetneq P$ è adiacente a P l'anello V_P/QV_P è un dominio di valutazione noetheriano.*

In particolare, l'ideale massimale di un dominio di valutazione fortemente discreto è principale.

Dimostrazione. (i) $\Rightarrow$ (ii) Sia V fortemente discreto. Se M è l'ideale massimale di V, per definizione $M \neq M^2$. Dunque ogni ideale con radicale uguale a M, essendo M-primario, è una potenza di M (Proposizione 4.5). Ne segue che, se $x \in M \setminus M^2$, si ha $M = xV$. Se poi $P \in \mathrm{Spec}(V)$, poiché V_P è fortemente discreto, allora PV_P è principale.

(ii) $\Rightarrow$ (iii) Se PV_P è principale, PV_P è ramificato e dunque anche P è ramificato. Allora esiste un primo Q adiacente a P (Proposizione 4.7) e l'anello V_P/QV_P ha dimensione uno. Siccome il suo ideale massimale è principale, V_P/QV_P è noetheriano.

(iii) $\Rightarrow$ (i) Per ogni $P \in \mathrm{Spec}(V)$, si ha $PV_P/QV_P \neq P^2V_P/QV_P$. Allora chiaramente $P \neq P^2$ e V è fortemente discreto. $\square$

Daremo in seguito esempi di domini di valutazione di dimensione uno che non sono noetheriani (Paragrafo 9.1) e costruiremo un dominio di valutazione discreto ma non fortemente discreto, necessariamente di dimensione infinita (Paragrafo 10.1).

Esempio 5.7 (1) L'anello di valutazione $V := \mathbb{Z}_{\langle p \rangle} + X\mathbb{Q}[[X]]$ considerato nell'Esempio 3.3(3) è (fortemente) discreto di dimensione due. Infatti l'ideale massimale di V è principale generato da p, mentre l'ideale $P := X\mathbb{Q}[[X]]$ è principale in $V_P = \mathbb{Q}[[X]]_{(X)}$.

(2) L'anello $V := \mathbb{Z}_{\langle p \rangle} + X\mathbb{Q}[[X]]$ è costruito per pullback. Domini di valutazione (fortemente) discreti di dimensione finita maggiore di uno possono essere costruiti iterando questa costruzione. Infatti, è facile vedere che nella situazione dell'Esempio 3.3(3)

$$\begin{array}{ccc} R := \pi^{-1}(W) & \longrightarrow & (W, N) \\ \big\downarrow & & \big\downarrow \iota \\ (V, M) & \xrightarrow{\pi} & \frac{V}{M} =: k \end{array}$$

R è (fortemente) discreto se e soltanto se lo sono sia V che W.

6 Gruppi Ordinati e Gruppi di Divisibilità

Un gruppo abeliano $(G, *)$ è un *gruppo ordinato* se in esso è definita una relazione di ordine, indicata con $\leq$, compatibile con l'operazione, cioè tale che:

$$x \leq x' \, , \, y \leq y' \Rightarrow x * y \leq x' * y'.$$

Un omomorfismo di gruppi ordinati $\alpha : G \longrightarrow G'$ che mantiene l'ordine (cioè tale che se $x \leq y$ risulta $\alpha(x) \leq \alpha(y)$) si dirà un *omomorfismo di ordine.*

Tutti i gruppi considerati in seguito saranno abeliani e useremo principalmente la notazione additiva.

Un elemento g di un gruppo ordinato $(G, +)$ si dice *positivo* se $g \geq 0$ e si dice *negativo* se $g \leq 0$. Notiamo che g è positivo se e soltanto se $-g$ è negativo. Infatti

$$0 \geq g \quad \Leftrightarrow \quad 0 - g = -g \geq g - g = 0.$$

Denotiamo con G_+ l'insieme degli elementi positivi di G e con G_- l'insieme degli elementi negativi. Osserviamo che $0 \in G_+$ e che la somma di due elementi positivi è ancora un elemento positivo (ovvero $G_+ + G_+ = G_+$). Dunque G_+ è un sotto semigruppo di G. Inoltre $G_+ \cap G_- = \{0\}$.

Proposizione 6.1 *Sia G un gruppo abeliano additivo. G è ordinato se e soltanto se esiste un sottoinsieme P di G (detto* sottoinsieme positivo*) tale che*

$$(1)\ \ 0 \in P\,; \quad (2)\ \ P \cap -P = \{0\}\,; \quad (3)\ \ P + P = P.$$

Inoltre un gruppo ordinato G è totalmente ordinato se e soltanto se

$$(4)\ \ G = P \cup -P.$$

Dimostrazione. Se G è ordinato, come visto sopra, l'insieme G_+ dei suoi elementi positivi soddisfa le proprietà (1), (2), (3). Se inoltre G è totalmente ordinato, ogni elemento è confrontabile con 0; quindi vale (4).

Viceversa, se esiste $P \subseteq G$ che soddisfa (1), (2), (3), la relazione su G definita da

$$x \leq y \Leftrightarrow y - x \in P$$

è una relazione di ordinamento compatibile con la somma. Infatti (1) è equivalente alla riflessività, (2) all'antisimmetria e (3) alla transitività. Infine (4) implica che l'ordinamento è totale. Infatti, per $x, y \in G$, si ha $x - y \in P$ (e dunque $y \leq x$) oppure $x - y \in -P$ (e dunque $x \leq y$). $\square$

Quindi, se G è un gruppo abeliano ordinato, il suo ordinamento è univocamente determinato dall'insieme G_+ degli elementi positivi.

Esempio 6.2 (1) Il gruppo nullo è banalmente (totalmente) ordinato, con $P = \{0\} = -P$.

(2) Ogni sottogruppo additivo di $\mathbb{R}$ è totalmente ordinato secondo l'*ordinamento naturale*: $x \leq y \Leftrightarrow y - x \geq 0$.

(3) Se $\{(G_\lambda, \leq_\lambda)\}_{\lambda \in \Lambda}$ è una famiglia di gruppi ordinati, il prodotto diretto $\Pi = \prod_\lambda G_\lambda$ può essere ordinato secondo l'*ordinamento prodotto*, definito da

$$(a_\lambda) \leq (b_\lambda) \quad \Leftrightarrow \quad a_\lambda \leq_\lambda b_\lambda, \text{ per ogni } \lambda \in \Lambda.$$

Il gruppo Π così ordinato si chiama *prodotto cardinale*. In questo caso, $(a_\lambda) \geq 0$ se e soltanto se $a_\lambda \geq_\lambda 0$ per ogni $\lambda \in \Lambda$.

Se Λ è bene ordinato (cioè ogni suo sottoinsieme non vuoto ha un elemento minimale), un altro ordinamento di Π è dato dall'*ordinamento lessicografico*, definito da

$$\begin{aligned}(a_\lambda) \leq (b_\lambda) \quad \Leftrightarrow \quad & (a_\lambda) = (b_\lambda) \text{ oppure} \\ & a_{\lambda_0} <_{\lambda_0} b_{\lambda_0} \text{ se } \lambda_0 \text{ è il minimo indice per cui } a_{\lambda_0} \neq b_{\lambda_0}.\end{aligned}$$

Il gruppo Π così ordinato si chiama *prodotto lessicografico*. In questo caso, $(a_\lambda) \geq 0$ se e soltanto se $(a_\lambda) = (0)$ oppure $a_{\lambda_0} >_{\lambda_0} 0$ se λ_0 è il minimo indice per cui $a_{\lambda_0} \neq 0$.

In modo analogo si possono definire la *somma diretta cardinale* e, se Λ è totalmente ordinato, la *somma diretta lessicografica*.

Notiamo che, se ogni gruppo G_λ è totalmente ordinato, il loro prodotto lessicografico è totalmente ordinato, mentre il prodotto cardinale non lo è. Ad esempio, in $\mathbb{Z} \times \mathbb{Z}$ i due elementi $(0, 1)$ e $(1, 0)$ sono positivi nell'ordinamento prodotto, ma non sono confrontabili (mentre nell'ordinamento lessicografico essi sono positivi e $(0, 1) < (1, 0)$).

Proposizione 6.3 *Un gruppo abeliano non banale totalmente ordinato è privo di torsione; in particolare è infinito.*

Dimostrazione. Sia $g \in G$ un elemento non nullo. Allora $g \in G_+$ oppure $g \in G_-$. Supponiamo che $g \in G_+$ abbia ordine additivo finito $n \geq 2$. Allora $mg \in G_+$ per ogni $m \geq 1$ (perché $G_+ + G_+ = G_+$) e $ng = 0$. Ne segue che $(n-1)g = ng - g = -g \in G_+ \cap G_-$, dunque $(n-1)g = 0$ contro la minimalità di n. Poiché g e $-g$ hanno lo stesso ordine, questo è sufficiente. $\square$

L'insieme $\mathcal{P}(A)$ degli ideali frazionari principali non nulli di un dominio A è un gruppo moltiplicativo parzialmente ordinato secondo la relazione di inclusione

$$xA \leq yA \quad \Leftrightarrow \quad yA \subseteq xA.$$

Se K è il campo dei quozienti di A, indicando con K^* il gruppo moltiplicativo di K, l'applicazione

$$K^* \longrightarrow \mathcal{P}(A), \quad x \mapsto xA$$

è un omomorfismo di gruppi suriettivo con nucleo il gruppo delle unità $\mathcal{U} := \mathcal{U}(A)$ di A. Dunque $\mathcal{P}(A)$ è isomorfo al gruppo quoziente $\Delta(A) := K^*/\mathcal{U}$, secondo la corrispondenza $xA \mapsto x\mathcal{U}$. Scriviamo additivamente l'operazione in $\Delta(A)$, ponendo

$$x\mathcal{U} + y\mathcal{U} = xy\mathcal{U}.$$

Il gruppo $\Delta(A)$ può essere dotato di un ordinamento indotto da quello di $\mathcal{P}(A)$. Precisamente, se $x, y \neq 0$, definiamo

$$x\mathcal{U} \leq y\mathcal{U} \quad \Leftrightarrow \quad yA \subseteq xA \quad \Leftrightarrow \quad x^{-1}y \in A.$$

Notiamo che, secondo questo ordinamento, $x\mathcal{U} \geq 0$ se e soltanto se $x \in A$. Inoltre, se $x, y \in A$, risulta $x\mathcal{U} \leq y\mathcal{U}$ se e soltanto se x divide y in A.

Il gruppo $\Delta(A) := K^*/\mathcal{U}$ così ordinato si chiama il *gruppo di divisibilità* di A.

Proposizione 6.4 *A è un dominio di valutazione se e soltanto se il suo gruppo di divisibilità è totalmente ordinato.*

Dimostrazione. Il gruppo di divisibilità $\Delta(A)$ è ordinatamente isomorfo al gruppo $\mathcal{P}(A)$ degli ideali frazionari principali non nulli e, per la Proposizione 2.2, un dominio A è di valutazione se e soltanto se $\mathcal{P}(A)$ è totalmente ordinato per inclusione. □

Esempio 6.5 Se V è un DVR, il suo gruppo di divisibilità è isomorfo a $\mathbb{Z}$. Infatti ogni ideale di V è principale generato da una potenza del parametro uniformizzante t. Allora $\Delta(V) = \{t^z\mathcal{U}\,; z \in \mathbb{Z}\}$ e l'applicazione

$$\Delta(V) \longrightarrow \mathbb{Z}\,; \quad t^z\mathcal{U} \mapsto z$$

è un isomorfismo di ordine ($t^z\mathcal{U} \leq t^w\mathcal{U} \Leftrightarrow z \leq w$).

7 Valutazioni su un Campo

Ricordiamo che, per definizione, tutti i gruppi ordinati sono abeliani.

Se $(G, *)$ è un gruppo ordinato e α è un simbolo, possiamo estendere l'operazione di G e la sua relazione di ordine all'insieme $G_\alpha := G \cup \{\alpha\}$ ponendo, per ogni $x \in G$:

$$x < \alpha\,; \quad x * \alpha = \alpha * x = \alpha.$$

In notazione additiva, si usa porre $\alpha := \infty$, mentre in notazione moltiplicativa si usa $\alpha := 0$.

Se K è un campo e G è un gruppo additivo totalmente ordinato, una *valutazione su K a valori in G* è un'applicazione

$$v : K \longrightarrow G_\infty := G \cup \{\infty\}$$

tale che

($v1$) $v(x) = \infty$ se e soltanto se $x = 0$;
($v2$) $v(xy) = v(x) + v(y)$, per ogni $x, y \in K$;
($v3$) $v(x + y) \geq \min\{v(x), v(y)\}$.

L'immagine di K^* si chiama il *gruppo dei valori di v*. Sostituendo G con il gruppo dei valori di v, non è restrittivo richiedere che v sia suriettiva. Notiamo che la condizione ($v2$) implica che la restrizione di v al gruppo moltiplicativo K^* di K è un omomorfismo di gruppi.

Le dimostrazioni delle due proposizioni seguenti sono semplici verifiche.

Proposizione 7.1 (1) *Sia $\varphi : F \longrightarrow K$ un isomorfismo di campi. Se $v : K \longrightarrow G$ è una valutazione su K, allora $v\varphi : F \longrightarrow G$ è una valutazione su F.*

(2) *Sia $\alpha : G \longrightarrow G'$ un isomorfismo di gruppi che mantiene l'ordine. Se $v : K \longrightarrow G$ è una valutazione su K, anche $\alpha v : K \longrightarrow G'$ è una valutazione su K.*

Due valutazioni su K, $v : K \longrightarrow G_\infty$ e $v' : K \longrightarrow G'_\infty$ si dicono *equivalenti* se esiste un isomorfismo di ordine $\alpha : G \longrightarrow G'$ tale che $v' = \alpha v$.

Proposizione 7.2 *Sia A un dominio con campo dei quozienti K. Se v è un'omomorfismo del gruppo moltiplicativo A^* a valori in un gruppo totalmente ordinato G che soddisfa la condizione $v(x + y) \geq \min\{v(x), v(y)\}$, allora v si estende ad una valutazione su K a valori in G ponendo*

$$v(0) = \infty\,; \quad v\left(\frac{a}{b}\right) = v(a) - v(b), \quad \textit{se } a, b \neq 0.$$

Proposizione 7.3 *Sia $v : K \longrightarrow G_\infty$ una valutazione. Allora*

(1) $v(1) = 0 = v(-1)$*;*

(2) $v(-x) = v(x)$; $v(x^{-1}) = -v(x)$, *per ogni $x \in K^*$;*

(3) $v(x) > v(y) \Rightarrow v(x + y) = v(y)$, *per ogni $x, y \in K$.*

Dimostrazione. (1) e (2) sono semplici verifiche. Per (3), scrivendo $y = (y + x) - x$, vediamo che

$$v(x + y) \geq \min\{v(x), v(y)\} = v(y) \geq \min\{v(x + y), v(-x)\}.$$

Ma se $\min\{v(x + y), v(-x)\} = v(-x) = v(x)$ sarebbe $v(y) \geq v(x)$. Allora $\min\{v(x + y), v(-x)\} = v(x + y)$ e $v(x + y) = v(y)$. □

Esempio 7.4 (1) Su ogni campo K è possibile definire la *valutazione banale* o *impropria* a valori nel gruppo nullo, definita da $v(x) = 0$ per ogni $x \in K^*$.

(2) Se v è una valutazione su K ed F è un sottocampo di K, la restrizione di v ad F è una valutazione su F. La valutazione v si dice *banale su F* se la sua restizione ad F è banale, ovvero $v(x) = 0$ per ogni $x \in F^*$.

(3) Ogni valutazione su un campo finito è banale. Infatti se G è non banale e totalmente ordinato, G non può essere finito (Proposizione 6.3) ed inoltre se v è una valutazione su K con gruppo dei valori G, v è un omomorfismo suriettivo di K^* su G. Dunque K è infinito.

(4) Se $V := (V, M)$ è un dominio di valutazione noetheriano con parametro uniformizzante t, ogni elemento non nullo del campo dei quozienti K è del tipo $\frac{ut^n}{vt^m} = wt^k$, con $w \in \mathcal{U}(A)$ e $k \in \mathbb{Z}$ unicamente determinati. Allora è possibile definire una valutazione

$$v : K^* \longrightarrow \mathbb{Z}\,; \quad wt^k \mapsto k.$$

Notiamo che se $x \in V$, si ha $v(x) = n$ se e soltanto se $x \in M^n \setminus M^{n+1}$.

Ad esempio, vedendo $\mathbb{Q}$ come il campo dei quozienti di $\mathbb{Z}_{\langle p \rangle}$, $p \geq 2$ primo, possiamo scrivere ogni numero razionale non nullo come $\frac{a}{b}p^k$, dove p non divide né a né b. La valutazione

$$v_p : \mathbb{Q} \longrightarrow \mathbb{Z}_\infty ; \quad 0 \mapsto \infty , 0 \neq x = \frac{a}{b}p^k \mapsto k$$

si chiama *valutazione p-adica*.

Se $V := F[[X]]$ è l'anello delle serie formali sul campo F, il suo campo dei quozienti è il *campo delle serie di Laurent* $F((X))$. Ogni serie di Laurent non nulla si può scrivere come $\varphi(X) := \frac{f(X)}{g(X)} = X^k u(X)$, dove k è l'*ordine* di $\varphi(X)$. Dunque l'ordine definisce una valutazione di $F((X))$ a valori in $\mathbb{Z}$, che è banale su F:

$$\mathrm{ord} : F((X)) \longrightarrow \mathbb{Z}_\infty ; \quad 0 \mapsto \infty , 0 \neq \varphi(X) := X^k u(X) \mapsto k.$$

(5) Se $f(X) \in F[X]$ è un polinomio non nullo, possiamo considerare il suo ordine come serie formale. Allora $\mathrm{ord}\, f = n \geq 0$ se e soltanto se $f(X) = X^n g(X)$, dove $g(X) \in F[X]$ e X non divide $g(X)$. Se $\varphi(X) := \frac{f(X)}{g(X)} \in F(X)$ è una funzione razionale, definiamo poi $\mathrm{ord}\, \varphi = \mathrm{ord}\, f - \mathrm{ord}\, g$. Notiamo che $\mathrm{ord}\, \varphi = z$ se e soltanto se $\varphi(X) = X^z \frac{f_1(X)}{g_1(X)}$ e X non divide né f_1 né g_1.

Si vede subito che l'applicazione

$$\mathrm{ord} : F(X)^* \longrightarrow \mathbb{Z}, ; \quad \varphi(X) \mapsto \mathrm{ord}\, \varphi$$

è un omomorfismo suriettivo di gruppi. Inoltre

$$\mathrm{ord}(\varphi + \psi) \geq \min\{\mathrm{ord}\, \varphi, \mathrm{ord}\, \psi\}.$$

Dunque l'ordine definisce una valutazione su $F(X)$.

Notiamo che invece il grado non definisce una valutazione su $F(X)$, infatti non verifica la proprietà $v3$.

7.1 Costruzione di Valutazioni con Gruppo dei Valori Assegnato

Vogliamo ora mostrare che ogni gruppo totalmente ordinato è il gruppo dei valori di una valutazione.

Se F è un campo e S è un semigruppo abeliano additivo, l'*algebra semigruppo generata da S*, è definita come

$$\begin{aligned} F[S] :=& F[X_g;\, g \in S] \\ =& \left\{ \sum_{g \in S} a_g X_g \;; a_g \in F, a_g = 0 \text{ per quasi tutti gli indici } g \right\} \end{aligned}$$

dove la somma e la moltiplicazione sono definite formalmente dalle relazioni

$$X_0 := 1; \quad X_h X_g = X_{h+g}.$$

Esempio 7.5 (1) Se $S := \mathbb{N} \times \cdots \times \mathbb{N}$ è prodotto diretto finito di n copie di $\mathbb{N}$, l'algebra semigruppo $F[S]$ è isomorfa all'anello dei polinomi in n indeterminate, tramite l'isomorfismo

$$\begin{aligned} &F[S] \longrightarrow F[T_1, \ldots, T_n]; \\ &\sum_{\text{finite},\, h_j \in \mathbb{N}} a_{(h_1,\ldots,h_n)} X_{(h_1,\ldots,h_n)} \mapsto \sum_{\text{finite},\, h_j \in \mathbb{N}} a_{(h_1,\ldots,h_n)} T_1^{h_1} \ldots T_n^{h_n}. \end{aligned}$$

(2) Se $S = \mathbb{Z}$, si ha un isomorfismo

$$F[\mathbb{Z}] \longrightarrow F[T, T^{-1}]; \quad \sum_{\text{finite},\, k \in \mathbb{Z}} a_k X_k \mapsto \sum_{\text{finite},\, k \in \mathbb{Z}} a_k T^k.$$

Sia ora G un gruppo assegnato totalmente ordinato e sia $S \subseteq G$ un semigruppo, $0 \in S$. L'applicazione

$$v_S : F[S] \setminus \{0\} \longrightarrow S\,; \quad f := \sum_{g \in S} a_g X_g \mapsto \min\{g;\ a_g \neq 0\}$$

soddisfa le proprietà $(v2)$ e $(v3)$ di una valutazione e si può quindi estendere ad una valutazione v sul campo dei quozienti K di $F[S]$, ponendo al solito

$$v : K \longrightarrow G_\infty; \ \ 0 \mapsto \infty, \quad \frac{f}{g} \mapsto v_S(f) - v_S(g), \ \text{ con } f, g \neq 0.$$

Il gruppo dei valori di v è allora il sottogruppo di G generato da S (che è detto il *gruppo dei quozienti di S*); in particolare, se $S = G$ è un gruppo, il gruppo dei valori di v è G.

Esempio 7.6 (1) Sia $S := \mathbb{N}$, con l'ordinamento naturale. Identificando $F[\mathbb{N}]$ con l'anello di polinomi $F[T]$, si vede che l'applicazione v_S associa ad ogni polinomio $f(T) \in F[T]$ il suo ordine. Quindi la valutazione indotta su $F(T)$ è l'ordine, con gruppo dei valori $\mathbb{Z}$.

(2) Se $S := \mathbb{N} \times \mathbb{N}$, possiamo identificare $F[S]$ con l'anello dei polinomi in due indeterminate $F[U, V]$. Scriviamo $f(U, V) = f_0(V) + f_1(V)U + \cdots + f_n(V)U^n$ come un polinomio in U a coefficienti in $F[V]$. Se $h = \operatorname{ord}_U f$ è l'ordine di $f(U, V)$ come polinomio in U, si ha $f(U, V) = U^h(f_h(V) + f_{h+1}(V)U + \cdots + f_n(V)U^{n-h})$ con $f_h(V) \neq 0$. Allora, ordinando S lessicograficamente, si ha $v_S(f) = (h, k)$ se e soltanto se $h = \operatorname{ord}_U f$ e $k = \operatorname{ord} f_h$ è l'ordine di $f_h(V)$ in V.

L'applicazione v_S si estende ad una valutazione $F(U, V) \longrightarrow \mathbb{Z} \times \mathbb{Z}$ la cui prima componente è l'ordine rispetto ad U.

(3) Sia $S := \mathbb{R}_+$ il semigruppo additivo dei reali positivi. Gli elementi di $F(S) = F[\{X_\alpha\,;\ \alpha \in \mathbb{R}\,,\ \alpha \geq 0\}]$ sono i "polinomi" del tipo $\sum a_\alpha X_\alpha$, con gli $a_\alpha \in F$ quasi tutti nulli. Dunque possiamo scrivere $f = a_0 X_{\alpha_0} + a_1 X_{\alpha_1} + \cdots + a_n X_{\alpha_n}$, dove $n \geq 0$ e $0 \leq \alpha_0 < \alpha_1 < \cdots < \alpha_n$, ovvero $f = X_{\alpha_0}(a_0 + a_1 X_{\alpha_1 - \alpha_0} + \cdots + a_n X_{\alpha_n - \alpha_0})$. Allora, se $f \neq 0$ si ha $v_S(f) = \alpha_0$.

8 Valutazioni e Anelli di Valutazione

La terminologia *dominio di valutazione* deriva dal fatto che ad ogni dominio di valutazione V si può associare una *valutazione* sul suo campo dei quozienti e viceversa ad ogni valutazione su un campo K resta associato un dominio di valutazione con campo dei quozienti K. Vediamo come.

Ricordiamo che se V è un dominio di valutazione il suo gruppo di divisibilità $\Delta(V) := K^*/\mathcal{U}(V)$ è totalmente ordinato, secondo l'ordinamento

$$x\mathcal{U}(V) \leq y\mathcal{U}(V) \quad \Leftrightarrow \quad yV \subseteq xV \quad \Leftrightarrow \quad x^{-1}y \in V$$

(Proposizione 6.4). Si usa scrivere additivamente l'operazione in $\Delta(V)$, ponendo

$$x\mathcal{U}(V) + y\mathcal{U}(V) = xy\mathcal{U}(V).$$

Teorema 8.1 (1) *Se v è una valutazione su un campo K a valori in G, l'insieme $A_v := \{x \in K\,; v(x) \geq 0\}$ è un anello di valutazione con ideale massimale $M_v := \{x \in K\,; v(x) > 0\}$ e campo dei quozienti K.*

Inoltre l'applicazione

$$\alpha : \Delta(A_v) \longrightarrow G\,; \quad x\mathcal{U}(A_v) \mapsto v(x)$$

è un isomorfismo di ordine.

(2) *Se V è un anello di valutazione con campo dei quozienti K e gruppo di divisibilità $\Delta(V)$, l'applicazione*

$$v : K \longrightarrow \Delta(V)_\infty\,; \quad v(0) = \infty,\, v(x) = x\mathcal{U}(V) \text{ per } x \in K^*$$

è una valutazione su K, il cui anello di valutazione A_v coincide con V.

Inoltre, se v' è una valutazione su K tale che $A_{v'} = V$, allora v e v' sono equivalenti.

Dimostrazione. (1) Si verifica facilmente che A_v è un sottoanello di K. Se poi $x \in K \setminus A_v$, allora $v(x) < 0$. Quindi $v(x^{-1}) = -v(x) > 0$. Ne segue che $x^{-1} \in A_v$ e perciò A_v è un anello di valutazione. In particolare A_v è locale. Poiché un elemento non nullo $x \in A_v$ è invertibile se e soltanto se $x, x^{-1} \in A_v$, ovvero $v(x), v(x^{-1}) = -v(x) > 0$, allora $\mathcal{U}(A_v) = \{x \in A_v; v(x) = 0\} = \{x \in K; v(x) = 0\}$. Dunque l'ideale massimale di A_v è l'ideale $A_v \setminus \mathcal{U}(A_v) = \{x \in K\,; v(x) > 0\} =: M_v$ (Proposizione 1.1).

Il campo dei quozienti di A_v è K. Infatti, se $x \in K \setminus A_v$, allora $x^{-1} \in M_v$ e dunque $x = \frac{1}{x^{-1}}$ appartiene al campo dei quozienti di A_v.

Infine, l'applicazione $\alpha : \Delta(A_v) \longrightarrow G$ è ben definita ed iniettiva. Infatti, se $x\mathcal{U}(A_v) = y\mathcal{U}(A_v)$, si ha $y = xu$ con u invertibile. Allora $v(u) = 0$ e

$v(y) = v(u) + v(x) = v(x)$. Inoltre se $v(x) = v(y)$, allora $v(x) - v(y) = v(xy^{-1}) = 0$. Dunque $xy^{-1} \in \mathcal{U}(A_v)$, ovvero $xA_v = yA_v$. Ne segue che $y = xu$ con u invertibile e $x\mathcal{U}(A_v) = y\mathcal{U}(A_v)$. Inoltre α è un omomorfismo suriettivo perché lo è v ristretto a K^*.

Per vedere che α mantiene l'ordinamento, notiamo che

$$x\mathcal{U}(A_v) \leq y\mathcal{U}(A_v) \Leftrightarrow x^{-1}y \in A_v \Leftrightarrow v(x^{-1}y) = v(y) - v(x) \geq 0 \Leftrightarrow v(x) \leq v(y).$$

(2) L'applicazione v è una valutazione su K. Infatti è un omomorfismo di K^* su $\Delta(V)$ ed inoltre $v(x+y) \geq \min\{v(x), v(y)\}$. Per vedere questo, supponiamo ad esempio che sia $v(x) = x\mathcal{U}(V) \geq y\mathcal{U}(V) = v(y)$. Allora $a := xy^{-1} \in V$ e $(x+y)y^{-1} = (a+1) \in V$. Dunque

$$\min\{v(x), v(y)\} = v(y) = y\mathcal{U}(V) \leq (x+y)\mathcal{U}(V) = v(x+y).$$

Infine $x \in A_v$ se e soltanto se $x\mathcal{U}(V) = v(x) \geq 0 = v(1) = \mathcal{U}(V)$, se e soltanto se $x \in V$. Allora $A_v = V$.

Se poi v' è una valutazione su K a valori in G' tale che $A_{v'} = V$, per la parte (1) l'applicazione $\alpha : \Delta(V) \longrightarrow G'\,, xV \mapsto v'(x)$, è un isomorfismo di ordine tale che $v'(x) = \alpha(v(x))$, per ogni $x \in K^*$. $\square$

L'anello A_v si chiama l'*anello della valutazione* v.

Corollario 8.2 *Due valutazioni su K sono equivalenti se e soltanto se hanno lo stesso anello di valutazione.*

Corollario 8.3 *Sia V un anello di valutazione con campo dei quozienti K. Le seguenti condizioni sono equivalenti.*

(i) *V è noetheriano;*

(ii) *V è l'anello di una valutazione su K a valori in $\mathbb{Z}$;*

(iii) *Il gruppo di divisibilità di V è isomorfo a $\mathbb{Z}$.*

Dimostrazione. (i) $\Rightarrow$ (ii) Se V è noetheriano, con parametro uniformizzante t, tutti i suoi elementi sono del tipo ut^n, con u invertibile e $n \geq 0$. Allora l'applicazione

$$V^* \longrightarrow \mathbb{Z}\,, \quad ut^n \mapsto n$$

si estende ad una valutazione su K a valori in $\mathbb{Z}$.

(ii) $\Rightarrow$ (i) Sia $v : K \longrightarrow \mathbb{Z}_\infty$ una valutazione. Se $t \in K$ è tale che $v(t) = 1$, allora $v(t^n) = n$, per ogni $n \geq 0$. Sia poi $x \in A_v \subseteq K$ tale che $v(x) = v(t^n) = n \geq 0$. Allora $v(x) - v(t^n) = v(xt^{-n}) = 0$. Ne segue che $xt^{-n} = u \in \mathcal{U}(A_v)$ e $x = ut^n$. Dunque A_v è noetheriano, con parametro uniformizzante t.

(ii) $\Leftrightarrow$ (iii) segue dal Teorema 8.1. $\square$

Se V è un anello di valutazione noetheriano, con parametro uniformizzante t, una valutazione su V è determinata dal valore di t. Infatti ogni elemento non nullo del campo dei quozienti K è del tipo ut^k, con $w \in \mathcal{U}(A)$ e $k \in \mathbb{Z}$ unicamente determinati e deve risultare $v(ut^k) = v(u)+kv(t) = kv(t)$.

Allora il gruppo dei valori di v è $G := \{kv(t)\,, k \in \mathbb{Z}\}$ e si ha un isomorfismo $\alpha : G \longrightarrow \mathbb{Z}\,; \quad kv(t) \mapsto k$. La valutazione $v' = \alpha v$ è tale che $v'(t) = 1$ ed ha gruppo dei valori uguale a $\mathbb{Z}$. Essa si chiama la *valutazione normalizzata* di V.

Esempio 8.4 (1) La valutazione p-adica $v_p : \mathbb{Q} \longrightarrow \mathbb{Z}$ è normalizzata e il suo anello di valutazione è $\mathbb{Z}_{\langle p\rangle}$.

(2) La valutazione di ordine $\mathrm{ord} : F((X)) \longrightarrow \mathbb{Z}$ è normalizzata e il suo anello di valutazione è $F[[X]]$.

(3) Sia v è la valutazione su $F(X)$ definita dall'ordine. Per definizione, $\varphi(X) \in F(X)$ ha ordine $n \geq 0$ se e soltanto se $\varphi(x) = X^n \frac{f(X)}{g(X)}$ con X che non divide né $f(X)$ né $g(X)$. Allora l'anello di v è $F[X]_{(X)}$, con ideale massimale $XF[X]_{(X)}$ e campo residuo F.

(4) Consideriamo la valutazione v su $F(X,Y)$ a valori nel prodotto lessicografico $\mathbb{Z} \times \mathbb{Z}$ definita come nell'Esempio 7.6(2).

Per determinare il suo anello di valutazione, osserviamo che dato $(a,b) \in \mathbb{Z} \times \mathbb{Z}$, risulta $(a,b) \geq 0$ se e soltanto se $a > 0$ oppure $a = 0$ e $b \geq 0$.

Sia dunque $\varphi(X,Y) \in F(X,Y)$ non nulla con $v(f) = (a,b)$. Poiché la prima componente di v è l'ordine in X, considerando $\varphi(X,Y)$ come una funzione razionale in X a coefficienti nel campo $F(Y)$ risulta $a := \mathrm{ord}_X \varphi \geq 0$ se e soltanto se, come visto nell'esempio precedente, $\varphi(X,Y) \in F(Y)[X]_{(X)}$. Dunque l'anello di valutazione di v è un sottoanello dell'anello locale $A := F(Y)[X]_{(X)}$. Notiamo che, poiché il campo residuo di A è $F(Y)$, risulta $A = F(Y) + XF(Y)[X]_{(X)}$ (Proposizione 1.3).

Allora, se $a := \mathrm{ord}_X \varphi > 0$, si ha $\varphi(X,Y) \in XF(Y)[X]_{(X)}$. Se poi $a := \mathrm{ord}_X \varphi = 0$, allora $\varphi(X,Y) = \varphi_0(Y) + X\psi(X,Y)$ con $\varphi_0(Y) \in F(Y)$ non nullo e allora ancora $b := \mathrm{ord}\,\varphi_0 \geq 0$ se soltanto se $\varphi_0(Y) \in F[Y]_{(Y)}$. In conclusione, l'anello di v è $R := F[Y]_{(Y)} + XF(Y)[X]_{(X)}$, con ideale massimale $YR = YF[Y]_{(Y)} + XF(Y)[X]_{(X)}$ e campo residuo F.

Notiamo che l'anello di valutazione R è ottenuto per pull-back come nell'Esempio 3.3(3)

$$\begin{tikzcd} R \arrow[r] \arrow[d] & F[Y]_{(Y)} \arrow[d, "\iota"] \\ F(Y)[X]_{(X)} \arrow[r, "\pi"] & \frac{F(Y)[X]_{(X)}}{XF(Y)[X]_{(X)}} = F(Y) \end{tikzcd}$$

(5) L'esempio precedente si può generalizzare nel modo seguente. Sia R un dominio di valutazione ottenuto per pull-back come nell'Esempio 3.3(3)

$$\begin{array}{ccc} R := \pi^{-1}(W) & \longrightarrow & (W, N) \cong \frac{R}{M} \\ \Big\downarrow & & \iota\Big\downarrow \\ (V, M) \cong R_M & \xrightarrow{\pi} & \frac{V}{M} =: k \end{array}$$

in cui V e W sono noetheriani, con valutazione normalizzata v_V e v_W rispettivamente a valori in $\mathbb{Z}$. Allora R è l'anello della valutazione v_R con gruppo dei valori $\mathbb{Z} \times \mathbb{Z}$, ordinato lessicograficamente, definita nel modo seguente.

Poiché il campo dei quozienti di R e V è lo stesso, se $x \in R \setminus \{0\}$, risulta $x = t^n u$, dove t è il parametro uniformizzante di V e $n \geq 0$, $u \in \mathcal{U}(V)$ sono univocamente determinati (Proposizione 3.2). Allora $v_V(x) = n$. Inoltre, poiché $u = \frac{x}{y}$ con $x, y \in R \setminus M$, ponendo $\pi(u) := \pi(x)\pi(y)^{-1}$, resta definita $v_W(\pi(u)) := v_W(\pi(x)) - v_W(\pi(y))$. Si verifica facilmente che l'applicazione $v_R : R^* \longrightarrow \mathbb{Z} \times \mathbb{Z}$ definita da $v_R(x) := (v_V(x), v_W(\pi(u)))$ è una valutazione, che è non negativa su R.

(6) Sia S un semigruppo totalmente ordinato e $F[S] := F[X_g;\, g \in S]$ l'algebra di semigruppo associata. L'applicazione

$$v_S : F[S] \setminus \{0\} \longrightarrow S\,; \quad f := \sum_{g \in S} a_g X_g \mapsto \min\{g;\, a_g \neq 0\}$$

definisce una valutazione sul campo dei quozienti K di $F[S]$ a valori nel gruppo $G := \langle S \rangle$ generato da S (Paragrafo 7.1). L'anello di questa valutazione è l'insieme degli elementi di K a valori non negativi.

Ad esempio sia $S := \mathbb{R}_+$ il semigruppo additivo dei reali positivi. Se $f \in F[S]$ è non nullo, possiamo scrivere $f = X_{\gamma_0}(c_0 + c_1 X_{\gamma_1} + \cdots + c_n X_{\gamma_n})$, dove $n \geq 0$, $c_0 \neq 0$ e $0 < \gamma_1 < \cdots < \gamma_n$. Quindi $v_S(f) = \gamma_0$ (Esempio 7.6.3).

Se $x := \frac{f}{g}$ è un elemento non nullo del campo dei quozienti K di $F[S]$, con $g := X_{\beta_0}(b_0 + b_1 X_{\beta_1} + \cdots + b_m X_{\beta_m})$, $m \geq 0$, $b_0 \neq 0$ e $0 < \beta_1 < \cdots < \beta_m$, l'applicazione $v : K \longrightarrow \mathbb{R}$ definita da $v(x) = v_S(f) - v_S(g) = \gamma_0 - \beta_0$ è una valutazione su K.

Risulta $v(x) \geq 0$ se e soltanto se $\gamma_0 \geq \beta_0$. Dunque $v(x) \geq 0$ se e soltanto se

$$x := \frac{f}{g} = \frac{X_{\gamma_0 - \beta_0}(c_0 + c_1 X_{\gamma_1} + \cdots + c_n X_{\gamma_n})}{b_0 + b_1 X_{\beta_1} + \cdots + b_m X_{\beta_m}}.$$

Notiamo ora che l'ideale M di $F[S]$ generato dagli elementi $\{X_\alpha\}_{\alpha \geq 1}$ è un ideale massimale di $F[S]$ (perché l'anello quoziente $F[S]/M$ è isomorfo al campo F) e che un elemento $a_0 + a_1 X_{\alpha_1} + \cdots + a_k X_{\alpha_k}$, con $0 < \alpha_1 < \cdots < \alpha_k$ sta in M se e soltanto se $a_0 = 0$.

In conclusione, poiché $b_0 + b_1 X_{\beta_1} + \cdots + b_m X_{\beta_m} \notin M$ (perché $b_0 \neq 0$), si ha $v(x) \geq 0$ se e soltanto se $x \in F[S]_M$ e $v(x) > 0$ se e soltanto se $x \in MF[S]_M$. Perciò l'anello della valutazione v è l'anello locale $F[S]_M$, con ideale massimale $MF[S]_M$.

9 Rango di una Valutazione

Se G è un gruppo ordinato, con sottoinsieme positivo G_+, l'ordinamento di G induce un ordinamento su ogni suo sottogruppo H, prendendo come sottoinsieme positivo di H l'insieme $H_+ := G_+ \cap H$. Si vede subito che se G è totalmente ordinato, l'ordinamento indotto su H è ancora totale. Per definire un ordinamento sui sottogruppi quozienti abbiamo bisogno della nozione di sottogrupo isolato.

Un sottoinsieme S di un insieme ordinato X si dice *convesso* se per ogni $s, t \in S$ e $x \in X$, se $s \leq x \leq t$ si ha $x \in S$.

Se G è un gruppo ordinato, un sottogruppo convesso di G si chiama anche un *sottogruppo isolato*.

Le seguenti proprietà sono tra le quelle basilari dei sottogruppi isolati.

(a) *Un sottogruppo H di G è isolato se e soltanto se $H_+ = H \cap G_+$ è un sottoinsieme convesso di G_+, se e soltanto se*

$$\textit{per ogni } h \in H \textit{ e } g \in G, 0 \leq g \leq h \textit{ implica } g \in H.$$

Infatti, è evidente che H_+ è convesso se e soltanto se, per ogni $h \in H$ e $g \in G$, $0 \leq g \leq h$ implica $g \in H$. Dunque se H è convesso, lo è anche H_+. Viceversa, sia H_+ convesso e siano $s, t \in H$, $g \in G$ con $s \leq g \leq t$. Se $0 \leq g \leq t$, allora $g \in H_+ \subseteq H$. Se $s \leq g \leq 0$, allora $-s \geq -g \geq 0$ e $-g \in H_+$, da cui $g \in H$.

(b) *L'intersezione di sottogruppi isolati di G è un sottogruppo isolato.*
Questo si verifica subito.

Proposizione 9.1 *Sia G un gruppo ordinato.*

(1) *Se $N \subseteq G$ è un sottogruppo isolato, il gruppo quoziente G/N è ordinato, con sottoinsieme positivo $P := G_+/N$. Inoltre, se G è totalmente ordinato, anche G/N lo è.*

(2) *Un sottogruppo di G è isolato se e soltanto se è il nucleo di un omomorfismo di ordine con dominio G.*

Dimostrazione. (1) Si vede subito che $0 \in P$ e $P + P = P$. Mostriamo che $P \cap -P = \{N\}$. Siano $h, g \in G_+$ tali che $h + N = -g + N$. Allora $h + g \in N$ e $h + g \geq h, g \geq 0$. Poiché N è isolato, allora $h, g \in N$ e $h + N = N = g + N$.

Se poi $G_+ \cup G_- = G$, si ha anche $P \cup -P = G/N$.

(2) Sia $\alpha : G \longrightarrow G'$ un omomorfismo di ordine e sia $\alpha(g) = 0$. Allora, se $0 \leq h \leq g$, risulta $0 \leq \alpha(h) \leq \alpha(g) = 0$, da cui $\alpha(h) = 0$. Ne segue che $\operatorname{Ker} \alpha$ è convesso.

Viceversa, se $N \subseteq G$ è isolato, il gruppo quoziente G/N è ordinato e la proiezione canonica $G \longrightarrow G/N$ è un omomorfismo di ordine. $\square$

Nelle ipotesi e notazioni della proposizione precedente, l'ordinamento definito su G/N dall'insieme positivo $P := G_+/N$ è dato da:

$$a + N \leq b + N \Leftrightarrow a \leq b + n \text{ per qualche } n \in N.$$

Esempio 9.2 (1) Se G è ordinato, il sottogruppo nullo e G sono banalmente isolati.

(2) Sia $G := G_1 \times G_2$ il prodotto lessicografico di due gruppi ordinati. Allora $\{0\} \times G_2$ è un sottogruppo isolato di G e l'isomorfismo canonico $\frac{G}{\{0\}\times G_2} \longrightarrow G_1 \times \{0\}$ è di ordine.

(3) Sia G totalmente ordinato. Se $g \in G$, poniamo $|g| = g$ se $g \geq 0$ e $|g| = -g$ se $g \leq 0$. Dato $x > 0$, sia

$$H_x := \{y \in G;\ nx \geq |y| \text{ per qualche } n \geq 1\}.$$

Si vede subito che H_x è un sottogruppo di G e che è isolato. Infatti, se $0 \leq z \leq y$ con $nx \geq y$, a maggior ragione $nx \geq z$.

Inoltre $x \in H_x$ e se $H \subseteq G$ è un sottogruppo isolato contenente x, allora $H_x \subseteq H$. Infatti, se $y \in H_x$ è tale che $nx \geq |y| \geq 0$, siccome $nx \in H$ e H è convesso, risulta $y \in H$.

Sia ora V un dominio di valutazione con campo dei quozienti K e sia W un suo sopra-anello di valutazione. Allora le unità di V sono anche unità di W, cioè $\mathcal{U}(V) \subseteq \mathcal{U}(W)$ e si ha un omomorfismo suriettivo dei gruppi di divisibilità

$$\pi_W : \Delta(V) := \frac{K^*}{\mathcal{U}(V)} \longrightarrow \frac{K^*}{\mathcal{U}(W)} =: \Delta(W)\,; \quad x\mathcal{U}(V) \mapsto x\mathcal{U}(W)$$

il cui nucleo è $H_W := \mathcal{U}(W)/\mathcal{U}(V)$.

Notiamo che π_W è un omomorfismo di ordine e quindi H_W è un sottogruppo isolato di $\Delta(V)$. Inoltre l'isomorfismo canonico $\Delta(V)/H_W \longrightarrow \Delta(W)$ è un isomorfismo di ordine.

Proposizione 9.3 *Sia V un dominio di valutazione. Allora, con le notazioni precedenti, l'applicazione $\alpha : W \mapsto H_W := \operatorname{Ker} \pi_W$ è un'applicazione biunivoca che mantiene le inclusioni tra l'insieme dei sopra-anelli di V e l'insieme dei sottogruppi isolati di $\Delta(V)$.*

Dimostrazione. Sia $H \subseteq \Delta(V)$ un sottogruppo isolato. Allora il gruppo quoziente $\Delta(V)/H$ è totalmente ordinato e la composizione

$$w : K^* \longrightarrow \Delta(V) \longrightarrow \frac{\Delta(V)}{H}\,; \quad x \mapsto w(x) := x\mathcal{U}(V) + H$$

definisce una valutazione su K il cui anello di valutazione $W := A_w$ contiene V. In questo modo si definisce un'applicazione β che associa ad ogni sottogruppo isolato H di $\Delta(V)$ un sopra-anello W di V tale che $\Delta(W)$ è isomorfo a $\Delta(V)/H$.

Si verifica facilmente che β è l'inversa di α. $\square$

Proposizione 9.4 *Se V è un dominio di valutazione, c'è una corrispondenza biunivoca $P \mapsto H(P) := \mathcal{U}(V_P)/\mathcal{U}(V)$ tra gli ideali primi di V ed i sottogruppi isolati di $\Delta(V)$, che scambia le inclusioni.*

Inoltre, $\Delta(V/P)$ è isomorfo a $H(P)$ e $\Delta(V_P)$ è isomorfo a $\Delta(V)/H(P)$. Infine, se P, Q sono due ideali primi di V, con $P \subseteq Q$, allora $\Delta(V_Q/PV_Q)$ è isomorfo al gruppo quoziente $H(P)/H(Q)$.

Dimostrazione. Poiché ogni sopra-anello di V è una localizzazione di V in un ideale primo, la corrispondenza $P \mapsto V_P$ è una corrispondenza biunivoca tra $\mathrm{Spec}(V)$ e l'insieme dei sopra-anelli di V, che scambia le inclusioni (Proposizione 2.4). Applicando la Proposizione 9.3, otteniamo una corrispondenza biunivoca $P \mapsto V_P \mapsto H(P) := H_{V_P} := \mathcal{U}(V_P)/\mathcal{U}(V)$. Come visto sopra, $\Delta(V_P) \cong \Delta(V)/H(P)$ (Proposizione 9.3).

Osserviamo ora che, se $x \in V \setminus P$, la classe $\overline{x} \in V/P$ è non nulla. Allora, indicando con $\overline{K}$ il campo dei quozienti di V/P, si ha un omomorfismo suriettivo

$$\pi : \mathcal{U}(V_P) \longrightarrow \Delta(V/P) := \overline{K}^*/\mathcal{U}(V/P)\,; \quad \frac{x}{y} \mapsto \frac{\overline{x}}{\overline{y}}\mathcal{U}(V/P).$$

Inoltre $\mathrm{Ker}\,\pi = \mathcal{U}(V)$. Infatti certamente $\mathcal{U}(V) \subseteq \mathrm{Ker}\,\pi$. Viceversa, se $\overline{x} \in \mathcal{U}(V/P)$, allora $x \in V$ e $xy - 1 \in P$, per qualche $y \in V$. Dunque x non può appartenere al massimale di V e perciò $x \in \mathcal{U}(V)$. Ne segue che $\Delta(V/P)$ è isomorfo a $\mathcal{U}(V_P)/\mathcal{U}(V) =: H(P)$.

Se poi $P \subseteq Q$, sostituendo V con V_Q si ottiene che $\Delta(V_Q/PV_Q)$ è isomorfo a $\mathcal{U}(V_P)/\mathcal{U}(V_Q)$, che a sua volta è isomorfo a $H(P)/H(Q)$ (per doppio quoziente). □

Corollario 9.5 *Se G è un gruppo totalmente ordinato, l'insieme dei suoi sottogruppi isolati è totalmente ordinato per inclusione.*

Dimostrazione. Segue dalla proposizione precedente, ricordando che ogni gruppo totalmente ordinato è il gruppo dei valori di una valutazione (Paragrafo 7.1).

Una dimostrazione diretta è la seguente. Siano H e H' due sottogruppi isolati. Se H e H' non sono confrontabili, esistono due elementi positivi $x \in H \setminus H'$ e $x' \in H' \setminus H$. Ma x e x' sono confrontabili in G e, se ad esempio $0 \leq x \leq x'$, essendo H' isolato, risulta $x \in H'$. Contraddizione. □

Il *rango di un gruppo totalmente ordinato* G, che denotiamo con $\mathrm{rg}(G)$, si definisce nel seguente modo: se G ha un numero finito di sottogruppi isolati, $\mathrm{rg}(G)$ è il numero dei sottogruppi isolati non nulli; se G ha un numero infinito di sottogruppi isolati, $\mathrm{rg}(G)$ è infinito. Il *rango di una valutazione o di un anello di valutazione* è il rango del suo gruppo dei valori.

Corollario 9.6 *Se V è un dominio di valutazione, la dimensione ed il rango di V sono uguali.*

Esempio 9.7 (1) Il sottogruppo nullo è l'unico gruppo ordinato di rango zero. Dunque le uniche valutazioni di rango zero sono quelle improprie.

(2) $\mathbb{Z}$ non ha sottogruppi isolati propri, quindi ha rango uno. Infatti se $H := n\mathbb{Z}$, con $0 < n$, è isolato, essendo $0 < 1 \leq n$ si ha che $1 \in H$.

(3) Sia G il prodotto lessicografico di n copie di $\mathbb{Z}$. Si verifica facilmente che, per come è definito l'ordine, tutti e soli i sottogruppi isolati di G sono i sottogruppi $H_i := \{0\} \times \cdots \times \{0\} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$, in cui le prime i componenti sono nulle, $0 \leq i \leq n$. Dunque $\mathrm{rg}(G) = n$.

Infatti, gli H_i sono isolati. Viceversa, sia H isolato e sia $0 < x := (a_1 \ldots, a_n) \in H$. Se a_{i+1} è la prima componente non nulla, ragionando come sopra, si vede che H contiene tutte le n-ple $(0, \ldots, 0, 1, a_{i+2}, \ldots, a_n)$. Dunque $H = H_i$.

(4) Il rango è una funzione additiva, cioè se $N \subseteq G$ è un sottogruppo isolato del gruppo totalmente ordinato G, si ha $\mathrm{rg}(G) = \mathrm{rg}(N) + \mathrm{rg}(G/N)$. In particolare se $G := H \times H'$ è un prodotto lessicografico, si ha $\mathrm{rg}(G) = \mathrm{rg}(H) + \mathrm{rg}(H')$.

Infatti si verifica facilmente che i sottogruppi isolati di G contenenti N sono in corrispondenza biunivoca con i sottogruppi isolati di G/N.

(5) Sia $R := F[Y]_{(Y)} + XF(Y)[X]_{(X)}$ l'anello di valutazione determinato nell'Esempio 8.4(4), il cui gruppo dei valori è il prodotto lessicografico $G := \mathbb{Z} \times \mathbb{Z}$. Allora $\dim(R) = \mathrm{rg}(G) = 2$.

Precisamente, la catena degli ideali primi di R è

$$M := YF[Y]_{(Y)} + P \supseteq P := XF(Y)[X]_{(X)} \supseteq (0),$$

mentre la catena dei sottogruppi isolati di G è

$$(0) \subseteq H_2 := \{0\} \times \mathbb{Z} \subseteq G.$$

L'unico sopra-anello proprio di R è $R_P = F(Y)[X]_{(X)}$, che ha gruppo dei valori $H_1 := \mathbb{Z} \times \{0\}$. Il nucleo della suriezione

$$\Delta(R) \cong G \longrightarrow H_1 \cong \Delta(R_P)$$

è H_2 e nella corrispondenza della Proposizione 9.4

$$P \mapsto R_P \mapsto H(P) = H_2.$$

Notiamo anche che $R/P = F[Y]_{(Y)}$ e che il gruppo dei valori di R/P è proprio $H_2 = H(P)$.

9.1 Valutazioni di Rango Uno

Un dominio di valutazione è noetheriano se e soltanto se il suo gruppo dei valori è isomorfo a $\mathbb{Z}$, in particolare un dominio di valutazione noetheriano ha rango uno (Corollario 8.2). Per dare esempi di domini di valutazione di rango uno non noetheriani, dobbiamo studiare i gruppi totalmente ordinati di rango uno. Mostreremo che questi sono tutti e soli i sottogruppi additivi non nulli di $\mathbb{R}$.

Un ordinamento totale su un gruppo non nullo G si dice *archimedeo* se, dati comunque due elementi $x > 0$, $y \geq 0$, esiste un numero intero $n \geq 1$ tale che $nx \geq y$. Un gruppo G si dice *archimedeo* se è non nullo e totalmente ordinato secondo un ordinamento archimedeo.

È noto che l'ordinamento naturale su $\mathbb{R}$ è archimedeo. Inoltre un teorema di L. O. Hölder asserisce che ogni gruppo archimedeo è isomorfo ad un sottogruppo additivo di $\mathbb{R}$.

Proposizione 9.8 *Sia G un gruppo archimedeo. Le seguenti condizioni sono equivalenti:*

(i) *G è ordinatamente isomorfo a $\mathbb{Z}$;*

(ii) *$G_+ \setminus \{0\}$ ha un minimo elemento;*

(iii) *$G = x\mathbb{Z}$ per qualche $x \in G_+ \setminus \{0\}$.*

Dimostrazione. (i) $\Rightarrow$ (ii) Se $\alpha : \mathbb{Z} \longrightarrow G$ è un isomorfismo di ordine, $\alpha(1)$ è il minimo di $G_+ \setminus \{0\}$.

(ii) $\Rightarrow$ (iii) Supponiamo che $G_+ \setminus \{0\}$ abbia un minimo elemento x. Allora ogni elemento $g \in G_+$ è un multiplo intero di x.

Infatti, per la proprietà archimedea, esiste un minimo intero $n \geq 1$ tale che $nx \geq g$. Allora $nx = g$, altrimenti $nx > g > (n-1)x$ per la minimalità di n e quindi $x > g - (n-1)x > 0$, contro la minimalità di x. Posto $(-n)x = -(nx)$, ne segue che $G = x\mathbb{Z}$.

(iii) $\Rightarrow$ (i) L'applicazione $\mathbb{Z} \longrightarrow G\,;\ k \mapsto kx$, è un isomorfismo di ordine.
$\square$

Proposizione 9.9 *Sia G un gruppo totalmente ordinato. Le seguenti condizioni sono equivalenti:*

(i) *G ha rango uno;*

(ii) *G è archimedeo;*

(iii) *G è ordinatamente isomorfo ad un sottogruppo additivo non nullo di $\mathbb{R}$.*

Dimostrazione. (i) $\Leftrightarrow$ (ii) Ricordiamo che, dato $x \in G$, $x > 0$, l'insieme $H_x := \{y \in G;\ nx \geq |y| \text{ per qualche } n \geq 1\}$ è il più piccolo sottogruppo isolato di G contenente x (Esempio 9.2(3)).

Se G ha rango uno, allora $G = H_x$ per ogni $x > 0$. Quindi G è archimedeo.

Viceversa, se G è archimedeo, allora $G \subseteq H_x$ per ogni $x > 0$. Allora G non ha sottogruppi isolati non banali e perciò ha rango uno.

(ii) $\Rightarrow$ (iii) Sia G un gruppo archimedeo e sia $x_0 \in G$ un elemento positivo fissato. Se $y > 0$, consideriamo l'insieme $S_y := \{\frac{m}{n} \in \mathbb{Q}\,;\ n > 0, mx_0 \leq ny\}$. Per la proprietà archimedea, S_y è non vuoto. Inoltre si vede subito che S_y è propriamente contenuto in $\mathbb{Q}$.

Osserviamo ora che se $\frac{m}{n} \in S_y$ e $\frac{m'}{n'} \leq \frac{m}{n}$, allora anche $\frac{m'}{n'} \in S_y$. Quindi S_y è un sottoinsieme limitato di $\mathbb{R}$ (altrimenti in particolare ogni elemento di $\mathbb{Q}$ sarebbe maggiorato da un elemento di S_y e quindi apparterrebbe a S_y). Ne segue che S_y ha un estremo superiore in $\mathbb{R}$, che indichiamo con $\theta(y)$.

Definiamo ora l'applicazione $\varphi : G \longrightarrow \mathbb{R}$ nel seguente modo: $\varphi(0) = 0$, $\varphi(x_0) = 1$, $\varphi(y) = \theta(y)$ se $y > 0$ e $\varphi(y) = -\theta(-y)$ se $y < 0$.

Si verifica facilmente che φ è un omomorfismo di ordine iniettivo di G nel gruppo additivo dei reali.

(iii) $\Rightarrow$ (ii) perché $\mathbb{R}$ è archimedeo. $\square$

Corollario 9.10 *Una valutazione v ha rango uno se e soltanto se è equivalente ad una valutazione a valori in $\mathbb{R}$.*

Esempio 9.11 (1) Un dominio di valutazione V con gruppo dei valori isomorfo a $\mathbb{R}$ ha rango uno e non è noetheriano (cf. Esempio 8.4(6)).

(2) Sia $G := \mathbb{Z} \times \mathbb{Z}$. Possiamo dotare G di un ordinamento archimedeo immergendo G in $\mathbb{R}$ nel seguente modo. Sia $\alpha \in \mathbb{R}$ un numero irrazionale e definiamo

$$G := \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{R}\,; \quad (m, n) \mapsto m + n\alpha.$$

Questa applicazione è un omomorfismo di gruppi additivi ed è iniettiva perché α è irrazionale. Allora G si identifica ad un sottogruppo di $\mathbb{R}$ e l'ordinamento naturale di $\mathbb{R}$ induce un ordinamento su G.

Con questo ordinamento, G ha dunque rango uno. Inoltre essendo α irrazionale, G non può essere isomorfo a $\mathbb{Z}$ (Proposizione 9.8). Allora un dominio di valutazione con gruppo dei valori G non è noetheriano.

10 Gruppi Discreti e Valutazioni Discrete

Vogliamo ora caratterizzare i domini di valutazione discreti, introdotti nel Paragrafo 5, attraverso i loro gruppi dei valori.

Due sottogruppi isolati H_1 e H_2 di un gruppo ordinato G si dicono *adiacenti* se $H_2 \subsetneq H_1$ e non ci sono sottogruppi isolati di G propriamente contenuti tra H_1 e H_2.

Un gruppo G totalmente ordinato si dice *discreto* se, per ogni coppia di sottogruppi isolati adiacenti $H_2 \subsetneq H_1$, il gruppo quoziente H_1/H_2 è ordinatamente isomorfo a $\mathbb{Z}$.

Diciamo poi che una valutazione v è *discreta (di rango n)* se il suo gruppo dei valori è discreto (di rango n).

Per definizione, un gruppo totalmente ordinato di rango uno è discreto se e soltanto se è ordinatamente isomorfo a $\mathbb{Z}$. Più generalmente si ha:

Proposizione 10.1 *Un gruppo totalmente ordinato di rango finito uguale a $n \geq 1$ è discreto se e soltanto se è ordinatamente isomorfo al prodotto lessicografico di n copie di $\mathbb{Z}$.*

Dimostrazione. Sia G il prodotto lessicografico di n copie di $\mathbb{Z}$. La catena dei sottogruppi isolati di G è

$$H_n = (0) \subseteq H_{n-1} \subseteq \ldots \subseteq H_i \subseteq H_{i-1} \subseteq \ldots H_0 = G,$$

Dove $H_i := \{0\} \times \cdots \times \{0\} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$, ha le prime i componenti nulle. Poiché $H_i/H_{i+1} \cong \mathbb{Z}$ per ogni $0 \leq i \leq n$, G è discreto di rango n.

Viceversa, supponiamo che G sia discreto di rango n e procediamo per induzione su n. Se $n = 1$, allora G è isomorfo a $\mathbb{Z}$. Altrimenti, sia N il sottogruppo isolato massimale di G. N ha rango $n-1$ e dunque, per ipotesi induttiva, è ordinatamente isomorfo al prodotto lessicografico di $n-1$ copie di $\mathbb{Z}$. Inoltre, poiché G è discreto, il gruppo quoziente $H := G/N$ è isomorfo a $\mathbb{Z}$. Allora $G \cong N \times H$ ed è ordinatamente isomorfo al prodotto lessicografico di n copie di $\mathbb{Z}$. □

Ricordiamo che un dominio di valutazione si dice discreto se $P \neq P^2$ per ogni ideale primo P ramificato e si dice fortemente discreto se $P \neq P^2$ per ogni ideale primo P. In dimensione finita questi due concetti sono equivalenti (Paragrafo 5).

Il prossimo risultato mostra che i domini di valutazione fortemente discreti sono esattamente i domini di valutazione il cui gruppo dei valori è discreto.

Proposizione 10.2 *Sia V un dominio di valutazione con gruppo dei valori G. Le seguenti condizioni sono equivalenti:*

(i) *V è un dominio di valutazione fortemente discreto (di dimensione n);*

(ii) *G è un gruppo discreto (di rango n);*

(iii) *V è l'anello di una valutazione discreta (di rango n).*

Dimostrazione. (i) $\Leftrightarrow$ (ii) Per la corrispondenza biunivoca della Proposizione 9.4, se P, Q sono due ideali primi adiacenti di V, con $P \subseteq Q$, allora l'anello di valutazione $W := V_Q/PV_Q$ ha dimensione uno e $\Delta(W)$ è isomorfo al gruppo quoziente dei due sottogruppi isolati adiacenti corrispondenti $H(P)/H(Q)$. Ora V è fortemente discreto se e soltanto se, per ogni coppia di primi adiacenti $P \subseteq Q$, W è noetheriano (Proposizione 5.6), se e soltanto se $H(P)/H(Q)$ è isomorfo a $\mathbb{Z}$, se e soltanto se G è discreto.

(ii) $\Leftrightarrow$ (iii) per definizione. $\square$

Corollario 10.3 *Un dominio di valutazione di rango finito n è (fortemente) discreto se e soltanto se il suo gruppo dei valori è isomorfo al prodotto lessicografico di n copie di $\mathbb{Z}$.*

Dimostrazione. Per le Proposizioni 10.2 e 10.1. $\square$

Corollario 10.4 *Un dominio di valutazione V è noetheriano se e soltanto se è il dominio di una valutazione discreta di rango uno.*

Per il corollario precedente, un dominio di valutazione noetheriano viene brevemente chiamato un *DVR* (*Discrete Valuation Ring*).

10.1 Un dominio di Valutazione Discreto ma non Fortemente Discreto

Sia $\Lambda := \{\pm\frac{1}{n};\ n \geq 1\} \subseteq \mathbb{Q}$ e consideriamo la somma diretta lessicografica $G := \mathbb{Z}^{(\Lambda)}$, con indice in Λ, di copie di $\mathbb{Z}$. Sia poi V l'anello di una valutazione a valori in G.

Mostriamo che V ha un ideale primo P tale che $P = P^2$, mentre, per ogni altro ideale primo Q, si ha $Q \neq Q^2$. Dunque V è discreto, ma non fortemente discreto.

Per vedere questo, usiamo la corrispondenza illustrata nella Proposizione 9.4. Per ogni $n \geq 1$, consideriamo i sottoinsiemi di G

$$H_{\frac{1}{n}} := \{(a_\lambda)\,;\ a_\lambda = 0,\ \text{per ogni } \lambda < \frac{1}{n}\};$$
$$H_{-\frac{1}{n}} := \{(a_\lambda)\,;\ a_\lambda = 0,\ \text{per ogni } \lambda < -\frac{1}{n}\}.$$

Questi sono sottogruppi isolati di G ed inoltre, poiché $-\frac{1}{n} < -\frac{1}{n+1} < \frac{1}{n+1} < \frac{1}{n}$, per ogni $n \geq 1$, si ha

$$H_{\frac{1}{n}} \subsetneq H_{\frac{1}{n+1}} \subsetneq H_{-\frac{1}{n+1}} \subsetneq H_{-\frac{1}{n}}.$$

A questi gruppi corrispondono rispettivamente gli ideali primi di V

$$P_n \supsetneq P_{n+1} \supsetneq P_{-(n+1)} \supsetneq P_{-n}.$$

Poiché, per ogni $n \geq 1$, i gruppi quozienti $H_{\frac{1}{n+1}}/H_{\frac{1}{n}}$ e $H_{-\frac{1}{n}}/H_{-\frac{1}{n+1}}$ sono isomorfi a $\mathbb{Z}$, gli anelli di valutazione $V_{P_n}/P_{n+1}V_{P_n}$ e $V_{P_{-(n+1)}}/P_{-n}V_{P_{-(n+1)}}$ sono noetheriani (Proposizione 5.6). Dunque, per ogni $n \geq 1$, risulta $P_n \neq P_n^2$ e $P_{-n} \neq P_{-n}^2$.

Notiamo ora che anche

$$H := \cap_{n\geq 1} H_{-\frac{1}{n}} = \cup_{n\geq 1} H_{\frac{1}{n}}$$

è un sottogruppo isolato di G (intersezione di sottogruppi isolati), al quale corrisponde un ideale primo di V

$$P := \cap_{n\geq 1} P_n = \cup_{n\geq 1} P_{-n}.$$

Poiché P è unione di una catena di ideali primi, P è non ramificato ed in particolare $P = P^2$ (Proposizione 4.7).

Non è difficile vedere che G non ha altri sottogruppi isolati, e quindi gli unici ideli primi di V sono gli ideali P, P_n, P_{-n}, $n \geq 1$.

Notiamo che V_P è un dominio di valutazione discreto, ma non fortemente discreto, le cui localizzazioni proprie sono tutte fortemente discrete. Infatti gli ideali primi non massimali di V_P sono gli ideali $P_{-n}V_P$, $n \geq 1$, che sono tutti non idempotenti, mentre l'ideale massimale PV_P è idempotente. Invece l'anello quoziente V/P è fortemente discreto, perché tutti e soli i suoi ideali primi sono gli ideali P_n/P, $n \geq 1$, che sono tutti non idempotenti.

Infine V si ottiene come pull-back di V/P in V_P, come nell'Esempio 3.3(3).

11 Valutazioni Essenziali

Se A è un dominio e $V := (V, M)$ è un sopra-anello di valutazione di A, l'deale primo $P := M \cap A$ si chiama il *centro* di V su A. Poiché $A_P \subseteq V$ e $M \cap A_P = PA_P$, allora V domina A_P. Nel caso in cui risulti $V = A_P$, V si chiama un *dominio di valutazione essenziale* per A e la valutazione associata a V si chiama una *valutazione essenziale* su A.

In particolare, se P è un ideale primo di A tale che l'anello A_P sia di valutazione, A_P è un dominio di valutazione essenziale per A.

Per il Teorema di Krull (Teorema 2.9) un dominio integralmente chiuso A è l'intersezione di tutti i suoi sopra-anelli di valutazione. A si chiama un *dominio essenziale* se si può ottenere come intersezione di sopra-anelli di valutazione essenziali. Questo significa dire che esiste una famiglia $\{P_\lambda\}_{\lambda\in\Lambda}$ di ideali primi di A tale che A_{P_λ} sia un dominio di valutazione, per ogni $\lambda \in \Lambda$, ed inoltre $A = \cap_{\lambda\in\Lambda} A_{P_\lambda}$.

Non tutti i sopra-anelli di valutazione di un dominio sono essenziali. Per dare un esempio, introduciamo le *valutazioni P-adiche*.

Un ideale I di un dominio A si dice *P-adico* se sono verificate le seguenti due proprietà:

(P1) Ponendo $I^0 := A$, se $x, y \in A$ sono tali che $x \in I^n \setminus I^{n+1}$ e $y \in I^m \setminus I^{m+1}$, allora $xy \in I^{n+m} \setminus I^{n+m+1}$.

(P2) $\cap_{n\geq 0} I^n = (0)$;

Proposizione 11.1 *Sia M un ideale che verifica la proprietà* (P1). *Allora*

(1) *M è un ideale primo.*

(2) *L'ideale $P := \cap_{n\geq 1} M^n$ è un ideale primo.*

(3) *M^n è un ideale M-primario, per ogni $n \geq 1$.*

Dimostrazione. (1) si ottiene per $n = m = 0$.

(2) Supponiamo che $x, y \notin P$. Allora $x \in M^n \setminus M^{n+1}$ e $y \in M^m \setminus M^{m+1}$ per qualche $n, m \geq 0$. Dunque $xy \notin M^{n+m+1}$ e perciò $xy \notin P$.

(3) Chiaramente $\sqrt{M^n} = M$. Se $xy \in M^n$ e $x \in A \setminus M$, allora $y \in M^k \setminus M^{k+1}$ per qualche $k \geq 1$ (perché M è primo). Poiché $xy \in M^k \setminus M^{k+1}$, deve essere $n \leq k$ e dunque $y \in M^k \subseteq M^n$. Ne segue che M^n è M-primario.
$\square$

Se $M \subseteq A$ è un ideale primo P-adico, l'applicazione

$$A^* \longrightarrow \mathbb{N} \subseteq \mathbb{Z}\,, \quad x \mapsto n \quad \text{ se } x \in M^n \setminus M^{n+1}$$

è ben definita (per la proprietà (P2)) e verifica le proprietà ($v2$) e ($v3$) di una valutazione. Allora essa si estende ad una valutazione v_M sul campo dei quozienti K di A a valori in $\mathbb{Z}$.

La valutazione v_M è dunque una valutazione discreta di rango uno, il cui anello di valutazione è centrato su M. Essa si chiama la *valutazione P-adica* su K (o su A) indotta da M.

Il prossimo risultato mostra che in particolare tutti gli ideali primi invertibili di altezza uno di A sono P-adici ed inducono una valutazione discreta essenziale su A.

Proposizione 11.2 *Sia M un ideale primo invertibile di un dominio A (in particolare principale) e sia $P := \cap_{n\geq 1} M^n$. Allora:*

(1) *M soddisfa la proprietà* (P1).

(2) *Un ideale $Q \subseteq A$ è M-primario se e soltanto se $Q = M^n$, $n \geq 1$.*

(3) *Ogni ideale primario il cui radicale è propriamente contenuto in M è contenuto in P. In particolare P è adiacente a M.*

(4) *L'ideale $\overline{M} := M/P$ è un ideale P-adico di $\overline{A} := A/M$ (in particolare, se $\cap_{n\geq 1} M^n = (0)$, allora M è P-adico).*

(5) *A_M/PA_M è un DVR (in particolare, se $\cap_{n\geq 1} M^n = (0)$, allora A_M è un DVR ed è l'anello della valutazione P-adica v_M, cioè v_M è essenziale per A).*

Dimostrazione. (1) Se M è invertibile, anche tutte le sue potenze lo sono. Siano $x, y \in A^*$ tali che $x \in M^n \setminus M^{n+1}$ e $y \in M^m \setminus M^{m+1}$. Allora esistono due ideali $I, J \subseteq A$, $I, J \nsubseteq P$, tali che $xA = IM^n$, $yA = JM^m$. Dunque $xy \in IJM^{n+m}$ e, poiché $IJ \nsubseteq P$ e M^{n+m} è invertibile, si ha $xy \notin M^{n+m+1}$.

(2) M^n è M-primario, per la proprietà (P1) (Proposizione 11.1(2)).

Viceversa, sia Q un ideale M-primario. Poiché $Q \nsubseteq P$ e $Q \subseteq M$, esiste $n \geq 1$ tale che $Q \subseteq M^n$ e $Q \nsubseteq M^{n+1}$. Allora, per l'invertibilità di M, $Q = IM^n$ con $I \subseteq A$ e $I \nsubseteq M$. Poiché Q è M-primario, ne segue che $M^n \subseteq Q$ e dunque $Q = M^n$.

(3) Supponiamo che $\sqrt{Q} \subsetneq M$. Per l'invertibilità di M, $Q = IM$ con $I \subseteq A$. Poiché Q è primario e $M \nsubseteq \sqrt{Q}$, allora $I \subseteq Q$, così che $Q = IM \subseteq QM \subseteq Q$ e $Q = QM$. Ne segue che $Q = QM^n$, per ogni $n \geq 1$ e dunque $Q \subseteq P$.

(4) $\overline{M}$ soddisfa la proprietà (P1) per il punto (1) e la proprietà (P2) per definizione.

(5) Poiché M è invertibile, per $x \in M \setminus P$ si ha $xA = IM$ con $I \subseteq A$. Passando alle classi modulo P, si ha $\overline{xA} = \overline{IM}$. Dunque $\overline{M}$ è invertibile in $\overline{A}$. Inoltre $\cap_{n\geq 1}\overline{M}^n = \overline{P} = 0$. Allora possiamo supporre che $P = (0)$.

Ora MA_M è principale e $PA_M = (0)$ è adiacente a MA_M per il punto (3). Dunque A_M è un anello locale di dimensione uno il cui ideale massimale è principale e allora è un DVR (Teorema 3.2).

Infine, poiché l'anello della valutazione v_M contiene A_M, esso deve essere uguale ad A_M (Corollario 2.5). □

Corollario 11.3 *Se M è un ideale primo invertibile di un dominio noetheriano, M ha altezza uno e A_M è un DVR.*

Dimostrazione. Segue dalla Proposizione 11.2, tenendo conto che, essendo A noetheriano, risulta $\cap_{n\geq 1}M^n = (0)$ (Teorema dell'Intersezione di Krull). □

Ricordiamo che se $A = \cap_{\lambda\in\Lambda}A_\lambda$ è una intersezione di domini, si dice che questa intersezione ha il *carattere di finitezza* se ogni elemento non nullo $x \in A$ è non invertibile al più in un numero finito di A_λ. Se A è un'intersezione di localizzazioni rispetto a una famiglia di ideali primi $\{P_\lambda\}_{\lambda\in\Lambda}$, cioè $A = \cap_{\lambda\in\Lambda}A_{P_\lambda}$, il carattere di finitezza equivale a dire che ogni elemento non nullo x di A appartiene al più ad un numero finito di ideali primi P_λ.

Proposizione 11.4 *Sia A un dominio a fattorizzazione unica e sia $\{p_\lambda\}_{\lambda\in\Lambda}$ un sistema completo di elementi primi non associati di A.*

(1) *Gli ideali primi di altezza uno di A sono tutti e soli gli ideali principali $P_\lambda := p_\lambda A$, $\lambda \in \Lambda$.*

(2) *P_λ è un ideale P-adico e la valutazione P-adica indotta da P_λ è essenziale per A, per ogni $\lambda \in \Lambda$.*

(3) A_{P_λ} *è un DVR, per ogni* $\lambda \in \Lambda$.

(4) $A = \cap_{\lambda\in\Lambda} A_{P_\lambda}$ *con il carattere di finitezza.*

In particolare A *è un dominio essenziale.*

Dimostrazione. (1) Sia P un ideale primo di altezza uno. Se $x \in P$ è non nullo e p è un elemento primo che divide x, allora $p \in P$ e dunque $pA = P$.

Viceversa, sia p è un elemento primo di A, Se $x \in \cap_{n\geq 0} p^n A$ è non nullo, allora x è diviso da tutte le potenze di p, il che è impossibile perché A è a fattorizzazione unica. Allora (0) è adiacente a pA (Proposizione 11.2(3)) e perciò pA ha altezza uno.

(2) e (3) seguono da (4) e (5) della Proposizione 11.2.

(4) Sia v_λ la valutazione P-adica indotta da P_λ su A. Dunque, se $a \in A$ è non nullo, $v_\lambda(a) = n$ se e soltanto se $a \in p_\lambda^n A \setminus p_\lambda^{n+1} A$, ovvero $a = p_\lambda^n y$ e p_λ non divide y.

Ne segue che ogni x non nullo nel campo dei quozienti K si scrive in modo unico come come $x = u \prod_{\lambda\in\Lambda} p_\lambda^{v_\lambda(x)}$, dove $u \in A$ è invertibile e $v_\lambda \neq 0$ al più per un numero finito di indici λ. Poiché A_{P_λ} è l'anello della valutazione v_λ, si ha che $v_\lambda(x) \geq 0$ se e soltanto se $x \in A_{P_\lambda}$. Quindi $x \in A$ se e soltanto se $v_\lambda(x) \geq 0$ se e soltanto se $x \in A_{P_\lambda}$, per ogni $\lambda \in \Lambda$. Quindi $A = \cap_{\lambda\in\Lambda} A_{P_\lambda}$ con il carattere di finitezza. $\square$

Esempio 11.5 (1) Se $V := (V, M)$ è un DVR, la sua valutazione normalizzata v è la valutazione P-adica su V indotta da M. Infatti, se t è il parametro uniformizzante di V, cioè $M = tV$, e $x \in V^*$, allora $v(x) = n$ se e soltanto se $x = ut^n$ con $u \in \mathcal{U}(V)$, ovvero $x \in M^n \setminus M^{n+1}$ (Esempio 7.4(4)).

(2) Se $p \geq 2$ è un numero primo, l'ideale principale generato da p è un ideale P-adico di $\mathbb{Z}$ e la valutazione su $\mathbb{Q}$ indotta dall'ideale $\langle p\rangle$ è la valutazione p-adica introdotta nell'Esempio 7.4(4). Questa valutazione è essenziale per $\mathbb{Z}$. Infatti il suo anello di valutazione è $\mathbb{Z}_{\langle p\rangle}$.

(3) Sia F un campo e sia $A := F[X]$. Gli ideali primi non nulli di $F[X]$ sono tutti e soli quelli generati dai polinomi irriducibili $p(X)$, $F[X]_{\langle p(X)\rangle}$ è un DVR e $F[X] = \cap F[X]_{\langle p(X)\rangle}$ con il carattere di finitezza. (Proposizione 11.4).

(4) Sia F un campo e sia $A := F[X, Y]$. L'ideale massimale $M := \langle X, Y\rangle$ di A generato dalle indeterminate X, Y è un ideale P-adico.

Infatti, dato $f(X, Y) := \sum a_{ij} X^i Y^j \in F[X, Y]$, possiamo scrivere in modo unico $f(X, Y) = \sum f_k(X, Y)$, dove $f_k(X, Y) = \sum_{i+j=k} a_{ij} X^i Y^j$ è un polinomio omogeneo di grado k. Poiché M^n è generato da tutti i prodotti $X^i Y^j$ con $i + j = n$, allora risulta $f(X, Y) \in M^n \setminus M^{n+1}$ se e soltanto se $n = \min\{k\,; f_k(X, Y) \neq 0\}$. Questo implica che la condizione (P1) è verificata. Inoltre, poiché A è noetheriano, si ha $\cap_{n\geq 1} M^n = (0)$ (Teorema dell'Intersezione di Krull).

Dunque M induce una valutazione P-adica su A, il cui anello di valutazione V contiene propriamente A_M. Infatti V ha dimensione uno, mentre A_M ha dimensione due. Ad esempio, se $\varphi := \varphi(X,Y) := Y^2/X$ risulta $v_M(\varphi) = 2 - 1 = 1$; quindi $\varphi \in V$, ma $\varphi \notin A_M$.

Dunque la valutazione v_M non è essenziale per A. Tuttavia, poiché A è un dominio a fattorizzazione unica, esso è un dominio essenziale (Proposizione 11.4).

Queste considerazioni si estendono ad ogni anello di polinomi su F, anche in infinite indeterminate.

12 Intersezioni di Anelli di Valutazione

Sia K un campo e sia $\{v_\lambda\}_{\lambda \in \Lambda}$ una famiglia di valutazioni su K, con anello di valutazione V_λ. Allora l'intersezione $A := \cap_{\lambda \in \Lambda} V_\lambda$ è un dominio integralmente chiuso in K. Restringendo eventualmente le valutazioni v_λ al campo dei quozienti di A, possiamo poi supporre che K sia il campo dei quozienti di A.

In generale, come abbiamo visto nel paragrafo precedente, una data valutazione v_λ della famiglia non è essenziale per A. In questo paragrafo daremo qualche condizione perché v_λ sia essenziale.

Consideriamo prima intersezioni finite. Abbiamo bisogno di un lemma tecnico.

Lemma 12.1 *Sia A un anello locale. Se $x \in A$ è invertibile, esiste un intero $n \geq 1$ (dipendente da x) tale che, per ogni intero $m \geq 1$ coprimo con n, l'elemento $1 + x + x^2 + \cdots + x^{m-1}$ è invertibile.*

Dimostrazione. Sia $A := (A, M)$ con campo residuo $k := A/M$ e poniamo $\overline{a} := a + M$ per ogni $a \in A$. Allora a è invertibile se e soltanto se $\overline{a} = \overline{0}$.

Supponiamo $\overline{x} = \overline{1}$. Se k ha caratteristica finita, prendiamo n uguale alla caratteristica di k; se k ha caratteristica zero prendiamo $n = 1$. Allora $\overline{1} + \overline{x} + \overline{x}^2 + \cdots + \overline{x}^{m-1} = m\overline{1} \neq \overline{0}$, per ogni m coprimo con n.

Se $\overline{x} \neq \overline{1}$, notiamo che $\overline{1} + \overline{x} + \overline{x}^2 + \cdots + \overline{x}^{m-1} = (\overline{1} - \overline{x}^m)/(\overline{1} - \overline{x})$. Allora, se $\overline{x}$ non è una radice dell'unità in k, prendiamo $n = 1$. Se invece $\overline{x}$ è una radice dell'unità in k di ordine t, prendiamo $n = t$. In questo modo $\overline{x}^m \neq \overline{1}$, per ogni m coprimo con n. □

Proposizione 12.2 *Siano $(V_1, M_1), \ldots, (V_n, M_n)$ anelli di valutazione del campo K inconfrontabili per inclusione (in particolare di rango uno) e sia $A := V_1 \cap \cdots \cap V_n$. Se $P_i := M_i \cap A$ è il centro di V_i su A, $i = 1, \ldots, n$, allora:*

(1) *Le valutazioni V_i sono essenziali per A, cioè $V_i = A_{P_i}$, per ogni $i = 1, \ldots, n$, e dunque $A = A_{P_1} \cap \cdots \cap A_{P_n}$.*

(2) *K è il campo dei quozienti di A.*

(3) *Gli ideali P_i sono tutti e soli gli ideali massimali di A.*

(4) *A è un dominio di Bezout (ogni ideale finitamente generato è principale).*

Dimostrazione. (1) Fissato i, $1 \leq i \leq n$, mostriamo che per ogni $x \in V_i$ esiste $s := s(x) \in A \setminus P_i$ tale che $sx \in A$.

Supponiamo per semplicità di notazione $i := 1$ e sia $x \in V_1$ non nullo. Distinguiamo il caso in cui l'insieme $J \subseteq \{1, \ldots, n\}$ degli indici j tali che x sia invertibile in V_j sia non vuoto. In questo caso, sia $n_j \geq 1$ l'intero definito come nel Lemma 12.1, per ogni $j \in J$. Allora, se $m \geq 1$ è coprimo con ogni n_j, l'elemento $t := 1 + x + x^2 + \cdots + x^{m-1}$ è invertibile in ogni V_j, $j \in J$. Mostriamo che, scegliendo $m \geq 3$, $s := t^{-1}$ ha le proprietà volute.

Vediamo prima che $s \in A$, ovvero che $s \in V_i$, per ogni $i = 1, \ldots, n$:

(a) Se $x \in M_i$, risulta $t = 1 + m_i$, con $m_i \in M_i$. Dunque $t \notin M_i$ e perciò $t, s \in \mathcal{U}(V_i) \subseteq V_i$.

(b) Se $x \in V_i \setminus M_i = \mathcal{U}(V_i)$, $i \in J$ e dunque $t, s \in \mathcal{U}(V_i) \subseteq V_i$.

(c) Se $x \notin V_i$, allora $s \in M_i \subseteq V_i$. Infatti, $y := x^{-1} \in M_i$ e $y^{m-1}t = y^{m-1}(1+x+x^2+\cdots+x^{m-1}) = 1+y+y^2+\cdots+y^{m-1} := 1+m_i =: u_i \in \mathcal{U}(V_i)$ $(m_i \in M_i)$. Da cui $s = u_i^{-1}y^{m-1} \in M_i$.

Per finire, verifichiamo che $s \in A \setminus P_1$ e che $sx \in A$, ovvero $sx \in V_i$, per ogni $i = 1, \ldots, n$.

Se $x \in V_i$, in particolare $i = 1$, da (a) e (b), otteniamo che $s \in \mathcal{U}(V_i)$. Quindi $s \in A \setminus P_i$ e $sx \in V_i$. Se $x \notin V_i$, allora da (c) $sx = u_i^{-1}y^{m-2} \in M_i \subseteq V_i$.

Supponiamo ora che J sia vuoto. Allora $x \in M_i$ oppure $x \notin V_i$ per $i = 1, \ldots, n$ (e $x \in M_1$). In questo caso, poniamo $t := 1 + x$ e $s := t^{-1}$.

Allora, se $x \in M_i$, $t, s \in \mathcal{U}(V_i) \subseteq V_i$. Se $x \notin V_i$, $y := x^{-1} \in M_i$ e dunque $u := 1 + y \in \mathcal{U}(V_i)$. Poiché $u := (1 + y) = (1 + x)y = ty$ risulta $s := t^{-1} = yu^{-1} \in M_i \subseteq V_i$.

Perciò $s \in A \setminus P_1$ ed infine $sx \in A$. Infatti, se $x \in M_i$, s è invertibile in V_i e $sx \in M_i \subseteq V_i$. Se $x \notin V_i$, $sx = xyu^{-1} = u^{-1} \in \mathcal{U}(V_i) \subseteq V_i$.

(2) Segue subito da (1).

(3) Se gli anelli di valutazione $V_i = A_{P_i}$ sono inconfrontabili per inclusione, anche gli ideali P_i sono inconfrontabili come ideali di A. Sia $S := A \setminus \{P_1 \cup \cdots \cup P_n\}$. Se $a \in S$, allora $a \notin P_i$, per ogni $i = 1, \ldots, n$, e quindi $a^{-1} \in \cap A_{P_i} = A$. Ne segue che ogni ideale proprio di A è contenuto in S e quindi (per il *Prime Avoidance Theorem*) in qualche P_i. Quindi $\mathrm{Max}(A) = \{P_1, \ldots, P_n\}$.

(4) Poiché I è finitamente generato e A_{P_i} è di valutazione, IA_{P_i} è principale per ogni i (Proposizione 2.2). Allora I è invertibile, e anche principale perché $\mathrm{Max}(A) = \{P_1, \ldots, P_n\}$ (Proposizioni 16.17 e 16.16). $\square$

Consideriamo ora intersezioni di domini di valutazione di rango uno con il carattere di finitezza.

Cominciamo dimostrando che le intersezioni di domini con il carattere di finitezza hanno l'utile proprietà di commutare con le localizzazioni.

Lemma 12.3 *Sia A un dominio e sia $\{A_\lambda\}_{\lambda\in\Lambda}$ una famiglia di sopra-anelli di A tali che l'intersezione $A = \cap_{\lambda\in\Lambda} A_\lambda$ abbia il carattere di finitezza.*

Se $S \subsetneq A^*$ è una parte moltiplicativa, allora $A_S = \cap_{\lambda\in\Lambda}(A_\lambda)_S$ e questa intersezione ha il carattere di finitezza.

Dimostrazione. Chiaramente $A_S \subseteq B := \cap_{\lambda\in\Lambda}(A_\lambda)_S$. Mostriamo che $A_S = B$. Sia $x \in B$ non nullo. Poiché B è contenuto nel campo dei quozienti di A, possiamo scrivere $x = \frac{a}{b}$, con $a, b \in A$. Allora $a, b \in A_\lambda$ per ogni λ e quando b è invertibile in A_λ si ha $x \in A_\lambda$. Dunque, se b è invertibile in tutti gli A_λ, $x \in A$. Altrimenti, per il carattere di finitezza, esistono soltanto un numero finito di indici $\lambda_1, \dots, \lambda_n$ tali che $x \notin A_{\lambda_i}$. Ma poiché $x \in (A_{\lambda_i})_S$, esiste $s \in S$ tale che $sx \in A_{\lambda_i}$ per ogni $i = 1, \dots, n$. In conclusione, $sx \in \cap_{\lambda\in\Lambda} A_\lambda = A$ e dunque $x \in A_S$.

Per provare il carattere di finitezza dell'intersezione $\cap_{\lambda\in\Lambda}(A_\lambda)_S$, osserviamo che se a è invertibile in A_λ, allora $x := \frac{a}{b}$ è invertibile in $(A_\lambda)_S$. Infatti, sia $x := \frac{a}{b} = \frac{x_\lambda}{s_\lambda}$, con $x_\lambda \in A_\lambda$ e $s_\lambda \in S$. Poiché $as_\lambda = x_\lambda b$ è invertibile in $(A_\lambda)_S$, allora x_λ è invertibile in $(A_\lambda)_S$ e $x(s_\lambda x_\lambda^{-1}) = 1$ con $s_\lambda x_\lambda^{-1} \in (A_\lambda)_S$. □

Corollario 12.4 *Sia A un dominio con campo dei quozienti K. Supponiamo che $\mathcal{F}$ sia una famiglia di anelli di valutazione di rango uno di K tale che $A = \cap_{V\in\mathcal{F}} V$ con il carattere di finitezza.*

Se $S \subsetneq A^*$ è una parte moltiplicativa, esiste una una sottofamiglia $\mathcal{F}'$ di $\mathcal{F}$ tale che $A_S = \cap_{W\in\mathcal{F}'} W$, con il carattere di finitezza. Inoltre $(W, M) \in \mathcal{F}'$ se e soltanto se $S \cap M = \emptyset$; in particolare, se Q è un ideale primo di A, $(W, M) \in \mathcal{F}'$ se e soltanto se $M \cap A \subseteq Q$.

Dimostrazione. Per il carattere di finitezza dell'intersezione, si ha $A_S = (\cap_{V\in\mathcal{F}} V)_S = \cap_{V\in\mathcal{F}} V_S$ (Lemma 12.3) con il carattere di finitezza. Ma poiché ogni $V \in \mathcal{F}$ ha rango uno, V_S può essere uguale soltanto a V oppure al campo dei quozienti K (Corollario 2.5). Dunque esiste una sottofamiglia $\mathcal{F}'$ di $\mathcal{F}$ tale che $A_S = \cap_{W\in\mathcal{F}'} W$. Inoltre $(W, M) \in \mathcal{F}'$ se e soltanto $W_S = W$, se e soltanto se $S \subseteq \mathcal{U}(W) = W \setminus M$, ovvero $S \cap M = \emptyset$. □

Proposizione 12.5 *Sia A un dominio con campo dei quozienti K. Supponiamo che $\mathcal{F}$ sia una famiglia di anelli di valutazione di rango uno di K tale che $A = \cap_{V\in\mathcal{F}} V$ con il carattere di finitezza.*

(1) *Se W è un dominio di valutazione essenziale per A, $W \in \mathcal{F}$.*

(2) *Se $P \subseteq A$ è un ideale primo di altezza uno, allora A_P è un anello di valutazione essenziale di A e $A_P \in \mathcal{F}$.*

Dimostrazione. (1) Sia W un dominio di valutazione essenziale e sia P il suo centro su A. Allora esiste una sottofamiglia $\mathcal{F}'$ di $\mathcal{F}$ tale che $W = A_P = \cap_{V \in \mathcal{F}'} V$ (Corollario 12.4). Ma W, essendo di valutazione, ha al più un solo sopra-anello di valutazione di rango uno. Quindi $\mathcal{F}'$ ha un solo elemento e necessariamente $\mathcal{F}' = \{W\}$. In particolare, $W \in \mathcal{F}$.

(2) Sia P un ideale primo di altezza uno di A. Allora esiste una sottofamiglia $\mathcal{F}'$ di $\mathcal{F}$ tale che $A_P = \cap_{V \in \mathcal{F}'} V$. Poiché A_P ha dimensione uno, ogni anello di valutazione $V \in \mathcal{F}'$ è centrato su PA_P. Perciò, sempre per il carattere di finitezza, $\mathcal{F}'$ è finita, cioè $A_P = V_1 \cap \cdots \cap V_n$ è intersezione di un numero finito di anelli di valutazione di rango uno, ognuno centrato su PA_P. Ne segue che $A_P = V_1 = \cdots = V_n$ (Proposizione 12.2). In particolare, A_P è un anello di valutazione di A e $A_P \in \mathcal{F}$. $\square$

Indichiamo con $\mathrm{X}_1(A)$ l'insieme degli ideali primi di altezza uno di un dominio A e con $\mathcal{E}$ la famiglia dei domini di valutazione essenziali di A.

Proposizione 12.6 *Sia A un dominio con campo dei quozienti K. Supponiamo che $\mathcal{F}$ sia una famiglia di anelli di valutazione di rango uno di K tale che $A = \cap_{V \in \mathcal{F}} V$ con il carattere di finitezza. Allora:*

(1) *$W \in \mathcal{E}$ se e soltanto se $W \in \mathcal{F}$ ed il centro di W su A è un ideale primo di altezza uno.*

(2) *$\mathcal{E} = \{A_P\,; P \in \mathrm{X}_1(A)\} \subseteq \mathcal{F}$.*

Dimostrazione. Segue dalla Proposizione 12.5. $\square$

Nelle ipotesi della proposizione precedente, se A è un dominio essenziale e $\mathcal{F}'$ è una famiglia di anelli di valutazione essenziali per A tali che $A = \cap_{V \in \mathcal{F}'} V$, deve necessariamente essere $\mathcal{F}' = \mathcal{E} = \{A_P\,; P \in \mathrm{X}_1(A)\} \subseteq \mathcal{F}$. Dunque la famiglia di domini di valutazione essenziali che definisce A è univocamente determinata. Essa si chiama la *famiglia di definizione di A*.

Esempio 12.7 (1) Se $P \subseteq A$ è un ideale primo invertibile di altezza uno, A_P è un DVR essenziale per A (Proposizione 11.2). Ma un dominio di valutazione essenziale di rango uno di A non è necessariamente un DVR. (Basta osservare che ogni dominio di valutazione è essenziale per se stesso).

(2) Se A è un dominio a fattorizzazione unica, per ogni primo $P \subseteq A$ di altezza uno A_P è un DVR essenziale per A e $A = \cap\{A_P\,; P \in \mathrm{X}_1(A)\}$ con il carattere di finitezza (Proposizione 11.4). Quindi A è un dominio essenziale e la sua famiglia di definizione è $\mathcal{E} := \{A_P\,; P \in \mathrm{X}_1(A)\}$ (Proposizione

12.6(3)). Ma un dominio a fattorizzazione unica può avere sopra-anelli di valutazione discreta non essenziali (Esempio 11.5(4)).

(3) Supponiamo che $\mathcal{F}$ sia una famiglia di anelli di valutazione di rango uno di K tale che $A = \cap_{V \in \mathcal{F}} V$ con il carattere di finitezza. Se A ha dimensione uno, allora $\mathcal{F} = \mathcal{E}$ ed A è essenziale (Proposizione 12.6(1)). Ma può accadere che nessun $V \in \mathcal{F}$ sia un DVR.

12.1 Intersezioni Irridondanti

Se $\{A_\lambda\}$ è una famiglia di domini con stesso campo dei quozienti K, diciamo che $\cap_{\lambda \in \Lambda} A_\lambda$ è una *intersezione irridondante* se, per ogni $\lambda \in \Lambda$, $A_\lambda \not\supseteq \cap_{\mu \neq \lambda} A_\mu$. Questo significa che nessuna componente A_λ si può cancellare dall'intersezione, cioè $\cap_{\lambda \in \Lambda} A_\lambda \neq \cap_{\mu \in \Lambda \setminus \{\lambda\}} A_\mu$, per ogni $\lambda \in \Lambda$. Se qualche A_λ si può cancellare, diremo che l'intersezione è *ridondante*.

Supponiamo ora che $\mathcal{F}$ sia una famiglia di anelli di valutazione di rango uno di K tale che $A = \cap_{V \in \mathcal{F}} V$ con il carattere di finitezza. Abbiamo visto che la famiglia dei domini delle valutazioni essenziali di A è $\mathcal{E} = \{A_P\,; P \in \mathrm{X}_1(A)\} \subseteq \mathcal{F}$ (Proposizione 12.6(2)). Dunque, se A è un dominio essenziale, risulta $A = \cap\{A_P\,; P \in \mathrm{X}_1(A)\}$ e quindi, se $\mathcal{E} \subsetneq \mathcal{F}' \subseteq \mathcal{F}$, l'intersezione $A = \cap_{V \in \mathcal{F}'} V$ è ridondante. D'altra parte, l'intersezione $A = \cap\{A_P\,; P \in \mathrm{X}_1(A)\}$ è irridondante. Infatti sia $\Delta \subseteq \mathrm{X}_1(A)$ tale che $A = \cap\{A_P\,; P \in \Delta\}$. Allora per la Proposizione 12.5(2), per ogni $Q \in \mathrm{X}_1(A)$, Deve essere $A_Q = A_P$ per qualche $P \in \Delta$. Dunque $\Delta = \mathrm{X}_1(A)$.

Tuttavia, se non c'è il carattere di finitezza, l'intersezione $A = \cap_{V \in \mathcal{F}} V$ non è sempre irridondante. Ad esempio, se A_M è un DVR per ogni ideale massimale M (ovvero A è *almost Dedekind*), si ha senz'altro $\mathrm{Max}(A) = \mathrm{X}_1(A)$ e $A = \cap\{A_M;\ M \in \mathrm{X}_1(A)\}$, ma R. Gilmer ha dimostrato che questa intersezione è irridondante se e soltanto se c'è il carattere di finitezza (ovvero A è *Dedekind* - vedi il successivo Paragrafo 13).

Ogni intersezione finita si può ridurre ad una intersezione irridondante. Più generalmente il Lemma di Zorn ci assicura che questo è vero per ogni intersezione con il carattere di finitezza.

Proposizione 12.8 *Sia A un dominio con campo dei quozienti K. Supponiamo che $\{A_\lambda\}_{\lambda \in \Lambda}$ sia una famiglia di sopra-anelli di A tale che $A = \cap_{\lambda \in \Lambda} A_\lambda$ con il carattere di finitezza. Allora esiste un sottoinsieme Λ^* di Λ tale che $A = \cap_{\mu \in \Lambda^*} A_\mu$ e l'intersezione sia irridondante.*

Dimostrazione. Consideriamo l'insieme $\mathcal{S}$ di tutti sottoinsiemi Σ di Λ tali che $A = \cap_{\sigma \in \Sigma} A_\sigma$. Poiché $\Lambda \in \mathcal{S}$, $\mathcal{S}$ è non vuoto. Inoltre $\mathcal{S}$ è (parzialmente) ordinato per inclusione. Ordiniamo $\mathcal{S}$ secondo l'ordinamento inverso. Cioè poniamo $\Sigma_1 \leq \Sigma_2 \ \Leftrightarrow\ \Sigma_1 \supseteq \Sigma_2$. Se ogni catena di $\mathcal{S}$ ammette un maggiorante, per il Lemma di Zorn $\mathcal{S}$ ha un elemento massimale. Ovvero esiste un sottoinsieme minimale Σ^* di Λ tale $A = \cap_{\sigma \in \Sigma^*} A_\sigma$ e chiaramente questa intersezione è irridondante.

Sia allora $\{\Sigma_\nu\}$ una catena di $\mathcal{S}$. Mostriamo che l'intersezione $\overline{\Sigma} := \cap \Sigma_\nu$ è un maggiorante della catena, cioè che $A = \cap_{\sigma \in \overline{\Sigma}} A_\sigma$. Ovviamente $A \subseteq \cap_{\sigma \in \overline{\Sigma}} A_\sigma$. Viceversa, sia $x := a/b \in K$. Se b è invertibile in tutti i V_λ, $x \in A$. Siccome per il carattere di finitezza b è non invertibile al più in un numero finito di V_λ, se $x \notin A$ esistono al più un numero finito di domini $A_1, \dots, A_n \in \mathcal{F}$ che non contengono x. Supponiamo che per ogni $i = 1, \dots, n$ esista un insieme Σ_i della catena che non contiene i. Allora il minimo dei Σ_i, diciamo Σ_j, non contiene $\{1, \dots, n\}$. Dunque $x \in \cap_{\sigma \in \Sigma_j} A_\sigma = A$, mentre per ipotesi $x \notin A$. Allora esiste un k, $1 \leq k \leq n$, che è contenuto in tutti i Σ_ν della catena. Ne segue che $k \in \overline{\Sigma} := \cap \Sigma_\nu$ e dunque $x \notin \cap_{\sigma \in \overline{\Sigma}} A_\sigma$. In conclusione $\cap_{\sigma \in \overline{\Sigma}} A_\sigma \subseteq A$. $\square$

13 Domini di Krull

Krull aveva congetturato che la chiusura integrale di un dominio noetheriano fosse sempre intersezione di anelli di valutazione discreta di rango uno con il carattere di finitezza. Questo fatto è stato poi dimostrato da Mori nel caso locale (1952) ed esteso da Nagata al caso generale (1955). Per questo motivo un dominio si chiama un *dominio di Krull* se è intersezione di domini di valutazione discreta di rango uno con il carattere di finitezza.

Una classe importante di domini di Krull non necessariamente noetheriani è data dai domini a fattorizzazione unica (Proposizione 11.4). Per il teorema di Mori-Nagata, tutti i domini noetheriani integralmente chiusi sono di Krull. Diamo ora una dimostrazione diretta di questo fatto.

Proposizione 13.1 *Un dominio A noetheriano e integralmente chiuso è di Krull. Precisamente A_P è un DVR per ogni primo P di altezza uno e $A = \cap\{A_P\,; P \in \mathrm{X}_1(A)\}$, con il carattere di finitezza.*

Dimostrazione. Se $P \in \mathrm{X}_1(A)$, A_P è un dominio locale di dimensione uno noetheriano e integralmente chiuso, quindi è un DVR (Teorema 3.2).

Sia $x \in A$ non nullo e non invertibile e sia $xA = Q_1 \cap \dots \cap Q_n$ una decomposizione primaria ridotta. Mostriamo che l'ideale primo $P_i := \sqrt{Q_i}$ è invertibile, per ogni $i = 1, \dots, n$, ed in particolare ha altezza uno (Corollario 11.3). Poniamo per semplicità di notazione $i = 1$.

Localizzando in P_1, possiamo supporre che P_1 sia massimale. Allora, poiché $P_1 \subseteq P_1(A : P_1) \subseteq A$, se P_1 non è invertibile, risulta $P_1 = P_1(A : P_1)$, da cui $(A : P_1) = (P_1 : P_1)$. Mostriamo che $(A : P_1) \neq (P_1 : P_1)$.

Osserviamo che $xA \subsetneq (xA :_A P_1)$. Infatti, supponiamo per assurdo che $xA = (xA :_A P_1)$. Allora risulta $xA = (xA :_A P_1) = ((xA :_A P_1) :_A P_1) = (xA :_A P_1^2) = \dots = (xA :_A P_1^n)$, per ogni $n \geq 1$. Siccome P_1 è finitamente generato, Q_1 contiene una potenza di P_1. Supponiamo che $P_1^t \subseteq Q_1$. Allora $(Q_1 :_A P_1^t) = A$ e, poiché Q_i è P_i-primario e $P_1^t \nsubseteq P_i$, $(Q_i :_A P_1^t) = Q_i$ per $i = 2, \ldots, n$. In definitiva, $(xA :_A P_1^t) = \cap_{i=1}^n (Q_i :_A P_1^t) = \cap_{i=2}^n Q_i$, contro la minimalità della decomposizione.

Notiamo poi che, essendo P_1 finitamente generato ed A integralmente chiuso, si ha $(P_1 : P_1) = A$. Allora $(A : P_1) \neq A = (P_1 : P_1)$.

Siccome A_{P_i} è un DVR, risulta $xA_{P_i} = Q_i A_{P_i} = P_i^{e_i} A_{P_i}$, $e_i \geq 1$, e quindi $Q_i = P_i^{(e_i)} := P_i^{e_i} A_{P_i} \cap A$. Inoltre $xA_P = A_P$ per ogni P di altezza uno tale che $P \neq P_1, \ldots, P_n$. Dunque $xA = \cap\{xA_P \cap A\,; P \in \mathrm{X}_1(A)\}$.

Chiaramente $A \subseteq \cap\{A_P\,; P \in \mathrm{X}_1(A)\}$. Viceversa, supponiamo che $\xi = \frac{x}{y} \in K \setminus A$ e mostriamo che $\xi \notin A_P$ per qualche $P \in \mathrm{X}_1(A)$. Per quanto visto sopra, $yA = \cap\{yA_P \cap A\,; P \in \mathrm{X}_1(A)\}$. Poiché $x \notin yA$, $x \notin yA_P$ per qualche $P \in \mathrm{X}_1(A)$. Allora $\xi \notin A_P$.

Dunque $A = \cap\{A_P\,; P \in \mathrm{X}_1(A)\}$. Il carattere di finitezza segue dal fatto che ogni $x \in A$ non invertibile ha un numero finito di primi minimali. □

Abbiamo visto che se A è un dominio a fattorizzazione unica oppure un dominio noetheriano integralmente chiuso, A_P è un DVR per ogni primo P di altezza uno e $A = \cap\{A_P\,; P \in \mathrm{X}_1(A)\}$, con il carattere di finitezza. Vogliamo ora dimostrare che questo è vero per tutti i domini di Krull. La dimostrazione è simile a quella della Proposizione 13.1.

Lemma 13.2 *Sia A un dominio di Krull. Allora $(I : I) = A$, per ogni ideale frazionario non nullo I di A.*

Dimostrazione. Sia $\mathcal{F} = \{V_\lambda\}_{\lambda \in \Lambda}$ una famiglia di DVR tale che $A = \cap_{V \in \mathcal{F}} V$ con il carattere di finitezza. Poiché IV_λ è principale, risulta $(IV_\lambda : IV_\lambda) = V_\lambda$, per ogni $\lambda \in \Lambda$. Allora basta far vedere che $(I : I) = \cap_{\lambda \in \Lambda}(IV_\lambda : IV_\lambda)$.

Chiaramente $(I : I) \subseteq \cap_{\lambda \in \Lambda}(IV_\lambda : IV_\lambda)$. Viceversa, siccome V_λ è un DVR, $IV_\lambda = t_\lambda V_\lambda$ è principale. Allora $(IV_\lambda : IV_\lambda) = (t_\lambda V_\lambda : t_\lambda V_\lambda) = V_\lambda$. Dunque, se $x \in (IV_\lambda : IV_\lambda)$ per ogni $\lambda \in \Lambda$, risulta $x \in \cap_{\lambda \in \Lambda} V_\lambda = A \subseteq (I : I)$. □

Proposizione 13.3 *Sia A un dominio di Krull e sia $x \in A$ non nullo e non invertibile. Allora:*

(1) *L'ideale xA ha una decomposizione primaria finita.*

(2) *Se $P_1, \ldots, P_n$ sono gli ideali primi associati a xA, P_i ha altezza uno e A_{P_i} è un DVR, per ogni $i = 1, \ldots, n$.*

(3) *Se $P_1, \ldots, P_n$ sono gli ideali primi associati a xA,*

$$xA = P_1^{(e_1)} \cap \cdots \cap P_n^{(e_n)} = \cap\{xA_P \cap A\,; P \in \mathrm{X}_1(A)\}.$$

Dimostrazione. Sia $\mathcal{F} = \{V_\lambda\}_{\lambda\in\Lambda}$ una famiglia di DVR tale che $A = \cap_{V\in\mathcal{F}} V$ con il carattere di finitezza. Indichiamo con P_λ il centro di V_λ su A.

(1) Siano $V_1, \dots, V_n$ i domini di $\mathcal{F}$ nei quali x non è invertibile. Allora $xA = \cap_{i=1}^n xV_i \cap A$. Poichè V_i ha rango uno, l'ideale xV_i è primario (con radicale l'ideale massimale di V_i) e quindi $Q_i := xV_i \cap A$ è P_i-primario. Allora $xA = \cap_{i=1}^n Q_i$ è una decomposizione primaria finita di xA.

(2) Sia $xA = \cap_{i=1}^n Q_i$ una decomposizione primaria minimale, dove $Q_i := xV_i \cap A$ è P_i-primario. Mostriamo che P_i ha altezza uno. Poniamo per semplicità di notazione $i = 1$.

Osserviamo che $xA \subsetneq (xA :_A P_1)$. Infatti, supponiamo per assurdo che $xA = (xA :_A P_1)$. Allora risulta $xA = (xA :_A P_1) = ((xA :_A P_1) :_A P_1) = (xA :_A P_1^2) = \cdots = (xA :_A P_1^n)$, per ogni $n \geq 1$. Siccome V_1 è un DVR, xV_1 è una potenza del massimale, dunque $Q_1 := xV_1 \cap A$ contiene una potenza di P_1. Supponiamo che $P_1^t \subseteq Q_1$. Allora $(Q_1 :_A P_1^t) = A$ e, poiché Q_i è P_i-primario e $P_1^t \nsubseteq P_i$, $(Q_i :_A P_1^t) = Q_i$ per $i = 2, \dots, n$. In definitiva, $(xA :_A P_1^t) = \cap_{i=1}^n (Q_i :_A P_1^t) = \cap_{i=2}^n Q_i$, contro la minimalità della decomposizione.

Supponiamo ora che P_1 abbia altezza maggiore di uno. Allora $A_{P_1} = \cap_{V'\in F'} V'$, dove $\mathcal{F}' \subseteq \mathcal{F}$ è la famiglia dei domini $V' \in \mathcal{F}$ il cui centro è contenuto in P_1 (Corollario 12.4). Poiché A_{P_1} ha dimensione maggiore di uno, la famiglia $\mathcal{F}'$ deve essere infinita, altrimenti $A_{P_1} \in \mathcal{F}'$ (Proposizione 12.2). Quindi, per il carattere di finitezza, x è invertibile in infiniti $V' \in \mathcal{F}'$.

Sia $V' \in \mathcal{F}'$, con ideale massimale M' e centro $P' = M' \cap A$, tale che $xV' = V'$. Siccome $V' \in \mathcal{F}'$, si ha $P' \subseteq P_1$. Sia $y \in (xA :_A P_1) \setminus xA$. Per ogni $z \in P'$, abbiamo $\frac{y}{x} z \in \frac{y}{x} P_1 \subseteq A$ ed inoltre $\frac{y}{x} z \in M'$ (perché x è invertibile in V'). Dunque $\frac{y}{x} z \in P'$. In conclusione, $\frac{y}{x} \in (P' : P') = A$ (Lemma 13.2) e allora $y \in xA$, contro la scelta di $y \notin xA$. In conclusione P_1, e quindi ogni P_i, ha altezza uno. Allora $V_i = A_{P_i}$, per $i = 1, \dots, n$ (Proposizione 12.6)(1)).

(3) Sia $xA = \cap_{i=1}^n Q_i$ una decomposizione primaria minimale e sia $P_i = \sqrt{Q_i}$, $i = 1, \dots, n$. Poiché P_i ha altezza uno, A_{P_i} è un DVR e $xA_{P_i} = Q_i A_{P_i} = P_i^{e_i}$, con $e_i \geq 1$. Dunque $Q_i = P_i^{e_i} \cap A =: P_i^{(e_i)}$. Inoltre x non appartiene ad alcun primo P di altezza uno diverso dai P_i e dunque $xA_P = A_P$ per $P \neq P_1, \dots, P_n$. Ne segue che

$$xA = \cap_{i=1}^n Q_i = P_1^{(e_1)} \cap \cdots \cap P_n^{(e_n)} = \cap_{i=1}^n (xA_{P_i} \cap A) = \cap \{xA_P \cap A\,;\, P \in \mathrm{X}_1(A)\}.$$

$\square$

Dalla proposizione precedente segue che in un dominio di Krull, come nei domini noetheriani, vale il *Teorema dell'Ideale Principale*: Un ideale primo è minimale su un ideale principale non nullo se e soltanto se ha altezza uno.

Teorema 13.4 *Le seguenti proprietà sono equivalenti per un dominio A:*

(i) *A è di Krull;*

(ii) *A_P è un DVR, per ogni primo $P \subseteq A$ di altezza uno e $A = \cap\{A_P\,; P \in \mathrm{X}_1(A)\}$ con il carattere di finitezza.*

In particolare, ogni dominio di Krull A è essenziale.

Dimostrazione. (i) $\Rightarrow$ (ii) Sia $\mathcal{F}$ una famiglia di DVR tale che $A = \cap_{V \in \mathcal{F}} V$ con il carattere di finitezza. Per la Proposizione 12.5(2), A_P è un DVR, per ogni primo $P \subseteq A$ di altezza uno e $A_P \in \mathcal{F}$. Dunque l'intersezione $B := \cap\{A_P\,; P \in \mathrm{X}_1(A)\}$ ha il carattere di finitezza.

Chiaramente $A \subseteq B$. Viceversa, sia $\frac{x}{y} \in B$ non nullo. Se y è invertibile in A, allora $\frac{x}{y} \in A$. Altrimenti, $yA = \cap\{yA_P \cap A\,; P \in \mathrm{X}_1(A)\}$ (Proposizione 13.3(3)). Ma poiché $\frac{x}{y} \in A_P$, per ogni $P \in \mathrm{X}_1(A)$, allora $x \in \cap\{yA_P \cap A\,; P \in \mathrm{X}_1(A)\} = yA$. Ne segue che $\frac{x}{y} \in A$.

(ii) $\Rightarrow$ (i) segue dalla definizione. $\square$

Proposizione 13.5 *Sia A un dominio di Krull. Allora:*

(1) *Se $S \subsetneq A^*$ è una parte moltiplicativa, A_S è un dominio di Krull.*

(2) *Se X è un'indeterminata su A, $A[X]$ è un dominio di Krull.*

Dimostrazione. (1) segue subito dal Corollario 12.4.

(2) Sia $Q \subseteq A[X]$ un ideale primo di altezza uno. Allora $Q \cap A = (0)$ se e soltanto se $Q = P_f := f(X)K[X] \cap A[X]$, con $f(X) \in K[X]$ un polinomio irriducibile; infatti $K[X]$ è la localizzazione di $A[X]$ nella parte moltiplicativa $A \setminus \{0\}$. In questo caso, $A[X]_{P_f} = K[X]_{\langle f(X) \rangle}$ è un DVR.

Invece $Q \cap A = P \neq (0)$ se e soltanto se P è un ideale primo di altezza uno di A e $Q = P[X]$. Infatti, se $P' \subseteq P$, allora $P'[X] \subseteq P[X]$; quindi se $P[X]$ ha altezza uno, anche P ha altezza uno. Viceversa, sia $P \subseteq A$ di altezza uno e sia $Q' \subseteq P[X]$ un ideale primo non nullo. Mostriamo che $Q' \cap A \neq (0)$. Da cui $Q' = P[X]$. Poiché $A[X]_{P[X]} = A_P[X]_{PA_P[X]}$, $P[X]$ e $PA_P[X]$ hanno la stessa altezza. Allora possiamo localizzare in P e supporre che A sia locale con ideale massimale P.

Consideriamo un polinomio non nullo $f(X) := a_0 + a_1 X + \cdots + a_n X^n \in Q'$. Poiché $A = A_P$ è di valutazione, gli ideali principali $\langle a_i \rangle$ di A sono linearmente ordinati. Quindi esiste un coefficiente $a_j \neq 0$ che divide tutti gli altri coefficienti e possiamo scrivere $f(X) = af'(X)$, con $a := a_j \in A$ e $f'(X) \in A[X] \setminus P[X]$. Ne segue che $f'(X) \notin Q'$ e $a \in Q' \cap A$.

Ora, poiché A è di Krull, A_P è un DVR e dunque PA_P è principale. Ne segue che anche $PA_P[X]$ è principale e $A[X]_{P[X]} = A_P[X]_{PA_P[X]}$ (essendo di dimensione uno) è un DVR.

Notiamo che $\cap\{A[X]_{P_f}; f(X) \in K[X] \text{ irriducibile}\} = K[X]$ e mostriamo che

$$A[X] = \cap_{Q \in \mathrm{X}_1(A[X])} A[X]_Q = K[X] \cap \{\cap_{P \in \mathrm{X}_1(A)} A[X]_{P[X]}\}.$$

Sia $v_{P[X]}$ la valutazione discreta normalizzata di $K(X)$ il cui anello è $A[X]_{P[X]}$. Questa è la valutazione P-adica indotta da $P[X]$, definita su $A[X]^*$ da $v_{P[X]}(f(X)) = n \geq 0$ se e soltanto se $f(X) \in P^n[X] \setminus P^{n+1}[X]$. La restrizione di $v_{P[X]}$ a K è la valutazione P-adica indotta da P, definita su A^* da $v_P(a) = n \geq 0$ se e soltanto se $a \in P^n \setminus P^{n+1}$. Dunque, dato $f(X) := \sum_{i=1}^n a_i X^i \in A[X]$, risulta $f(X) \in P^n[X] \setminus P^{n+1}[X]$ se e soltanto se $v_{P[X]}(f(X)) = n = \min\{v_P(a_i)\}$. In conclusione, la valutazione $v_{P[X]}$ è definita su $K[X]^*$ ponendo $v_{P[X]}(f(X)) = \min\{v_P(a_i)\}$. Allora $f(X) \in A[X]_{P[X]}$ se e soltanto se $v_{P[X]} = \min\{v_P(a_i)\} \geq 0$, se e soltanto se $v_P(a_i) \geq 0$, se e soltanto se $a_i \in A_P$, per ogni $i = 1, \dots, n$. Finalmente, dato $f(X) \in K[X]$, si ha $f(X) \in A[X]_{P[X]}$ per ogni $P \in \mathrm{X}_1(A)$, se e soltanto se $a_i \in A_P$ per ogni $P \in \mathrm{X}_1(A)$, $i = 1, \dots, n$, se e soltanto se $a_i \in A$, $i = 1, \dots, n$, cioè $f(X) \in A[X]$.

Il carattere di finitezza segue da quello di $K[X]$ e di A. □

Un dominio noetheriano integralmente chiuso di dimensione uno si chiama un *dominio di Dedekind*.

Vogliamo far vedere che i domini di Dedekind sono precisamente i domini di Krull di dimensione uno

Proposizione 13.6 *Sia A un dominio e sia $I \subseteq A$ un ideale. Se IA_M è finitamente generato, per ogni $M \in \mathrm{Max}(A)$, e l'intersezione $A = \cap\{A_M\,; M \in \mathrm{Max}(A)\}$ ha il carattere di finitezza, allora I è finitamente generato.*

In particolare, se A_M è noetheriano, per ogni $M \in \mathrm{Max}(A)$, e l'intersezione $A = \cap\{A_M\,; M \in \mathrm{Max}(A)\}$ ha il carattere di finitezza, allora A è noetheriano.

Dimostrazione. Sia I un ideale di A. Vogliamo far vedere che I è finitamente generato. Per ipotesi I è contenuto in un numero finito di ideali massimali $M_1, \dots, M_n$ e $IA_{M_i} = J_i A_{M_i}$ con $J_i \subseteq I$ finitamente generato. Sia $J := J_1 + \cdots + J_n$. Chiaramente $J \subseteq I$ e J è finitamente generato. Se $I = J$ abbiamo finito; altrimenti per la Proposizione 16.7 J è contenuto in qualche ideale massimale diverso da $M_1, \dots, M_n$. Infatti $IA_{M_i} = J_i A_{M_i} \subseteq JA_{M_i} \subseteq IA_{M_i}$, da cui $IA_{M_i} = JA_{M_i}$ per ogni i. Siano $M_1, \dots, M_n, M_{n+1}, \dots M_{n+k}$, $k \geq 1$, gli ideali massimali contenenti J. Poiché $I \not\subseteq M_{n+j}$, allora $I \not\subseteq M_{n+1} \cup \cdots \cup M_{n+k}$ (Prime Avoidance). Sia $x \in I \setminus (M_{n+1} \cup \cdots \cup M_{n+k})$ e $J' := J + xA$. Allora $J \subseteq J' \subseteq I$, gli unici ideali massimali di A contenenti J' sono $M_1, \dots, M_n$ e ancora $IA_{M_i} = JA_{M_i} = J'A_{M_i}$ per ogni i. Ne segue che $I = J'$ è finitamente generato. □

Teorema 13.7 *Le seguenti proprietà sono equivalenti per un dominio A:*

(i) *A è un dominio di Dedekind;*

(ii) *A è un dominio di Krull di dimensione uno;*

(iii) *A_M è un DVR, per ogni $M \in \mathrm{Max}(A)$ e $A = \cap\{A_M;\, M \in \mathrm{Max}(A)\}$ con il carattere di finitezza.*

Dimostrazione. (i) $\Rightarrow$ (ii) segue dalla Proposizione 13.1.

(ii) $\Rightarrow$ (iii) è chiaro.

(iii) $\Rightarrow$ (ii) Poiché A_M ha dimensione uno, per ogni $M \in \mathrm{Max}(A)$, allora A ha dimensione uno. Inoltre A è integralmente chiuso perché è intersezione di domini integralmente chiusi. Infine, la noetherianità segue dalla Proposizione 13.6. □

Corollario 13.8 *Se A è un dominio di Dedekind, A_S è un dominio di Dedekind, per ogni parte moltiplicativa $S \subsetneq A^*$.*

Dimostrazione. A_S è di Krull (Proposizione 13.5) e di dimensione uno. □

Esempio 13.9 (1) Per induzione sul numero delle indeterminate, si ottiene che, se A è di Krull, l'anello di polinomi $A[X_1, \ldots, X_n]$ è un dominio di Krull. Inoltre se A è a fattorizzazione unica (risp., noetheriano integralmente chiuso) anche $A[X_1, \ldots, X_n]$ lo è (per il Lemma di Gauss e il Teorema della base di Hilbert rispettivamente).

(2) Un anello di polinomi in infinite indeterminate a coefficienti in un campo è un dominio a fattorizzazione unica (quindi di Krull) non noetheriano.

(3) Esempi naturali di domini di Dedekind sono gli anelli di interi algebrici di un ampliamento finito del campo $\mathbb{Q}$ dei numeri razionali (Paragrafo 15).

(4) Un anello di polinomi a coefficienti in un dominio di Dedekind A è di Dedekind se e soltanto se $A = K$ è un campo. Altrimenti, $A[X]$ ha dimensione maggiore di uno.

14 Domini di Prüfer

Un dominio A si chiama un *dominio di Prüfer* se A_M è un dominio di valutazione, per ogni ideale massimale M. Poiché per ogni dominio A risulta $A = \cap\{A_M;\, M \in \mathrm{Max}(A)\}$, i domini di Prüfer sono intersezione di una famiglia di domini di valutazione essenziali ed in particolare sono integralmente chiusi.

Teorema 14.1 *Le seguenti proprietà sono equivalenti per un dominio A:*

(i) *A è un dominio di Prüfer;*

(ii) *A_P è un dominio di valutazione, per ogni ideale primo P;*

(iii) *Ogni ideale non nullo finitamente generato di A è invertibile.*

Dimostrazione. (i) $\Rightarrow$ (iii) Se I è finitamente generato, IA_M è pricipale, per ogni ideale massimale M, perché A_M è un dominio di valutazione (Proposizione 2.2). Allora I è invertibile (Proposizione 16.17) .

(iii) $\Rightarrow$ (ii) Sia $J \subseteq A_P$ un ideale finitamente generato. Allora $J = IA_P$, con $I \subseteq A$ finitamente generato. Poiché I è invertibile in A, allora $J = IA_P$ è invertibile e dunque principale (Proposizione 16.16). Ne segue che A_P è di valutazione (Proposizione 2.2).

(ii) $\Rightarrow$ (i) è ovvio. □

Ricordiamo che un dominio si dice *di Bezout* se ogni ideale finitamente generato è principale.

Corollario 14.2 (1) *Un dominio di Bezout è di Prüfer.*

(2) *Un dominio di Püfer semilocale è di Bezout.*

Dimostrazione. (1) perché gli ideali principali sono invertibili.

(2) Un ideale finitamente generato di un dominio di Prüfer è invertibile e un ideale invertibile di un anello semilocale è principale (Proposizione 16.16). □

Corollario 14.3 *Sia A un dominio di Prüfer. Allora:*

(1) *A_S è un dominio di Prüfer, per ogni parte moltiplicativa $S \subseteq A$.*

(2) *A/P è un dominio di Prüfer, per ogni ideale primo $P \subseteq A$.*

Dimostrazione. (1) Se $M \subseteq A_S$ è un ideale primo, si ha $M = QA_S$ per qualche $Q \in \mathrm{Spec}(A)$ e $(A_S)_M = (A_S)_{QA_S} = A_M$ è di valutazione. Allora A è di Prüfer.

(2) Gli ideali primi di A/P sono del tipo Q/P per qualche $Q \in \mathrm{Spec}(A)$. Siccome A_Q è di valutazione, allora $(A/P)_{Q/P} = A_Q/PA_Q$ è di valutazione. □

Mostriamo ora che i domini di Prüfer noetheriani sono precisamente i domini di Dedekind.

Teorema 14.4 *Le seguenti proprietà sono equivalenti per un dominio A:*

(i) *A è un dominio di Dedekind;*

(ii) *A è un dominio di Prüfer noetheriano;*

(iii) *A è un dominio di Prüfer e di Krull;*

(iv) *Ogni ideale non nullo di A è invertibile.*

Dimostrazione. (i) $\Rightarrow$ (ii) Un dominio di Dedekind è di Prüfer per il Teorema 13.7.

(ii) $\Rightarrow$ (iii) Poiché A_M è un dominio di valutazione noetheriano, esso è un DVR, per ogni $M \in \mathrm{Max}(A)$. Dunque A ha dimensione uno e $A = \cap\{A_P\,; P \in \mathrm{X}_1(A)\}$. Inoltre questa intersezione ha il carattere di finitezza perché, per la noetherianità, ogni elemento non invertibile ha un numero finito di primi minimali. In conclusione A è di Krull.

(iii) $\Rightarrow$ (i) Per il Teorema 13.7, basta far vedere che A ha dimensione uno. Questo segue dalla Proposizione 12.5(1). Infatti, sia $M \in \mathrm{Max}(A)$. Siccome A_M è un dominio di valutazione essenziale per A, deve essere $A_M = A_P$, per qualche primo P di altezza uno. Dunque $M = P$.

(ii) $\Leftrightarrow$ (iv) segue dal Teorema 14.1. □

Poiché gli ideali primi di un dominio di valutazione sono linearmente ordinati per inclusione, lo spettro primo di un dominio di Prüfer è *un albero*, cioè un ideale primo di un dominio di Prüfer non può contenere due ideali primi incomparabili per inclusione.

Per la corrispondenza tra gli ideali primari di un dominio e quelli di una sua localizzazione, gli ideali primari di un dominio di Prüfer hanno proprietà analoghe a quelle dei domini di valutazione (Paragrafo 4). In particolare i primi ramificati di un dominio di Prüfer possono essere caratterizzati localmente come nella Proposizione 4.7.

Vogliamo ora caratterizzare i domini di Prüfer attraverso alcune proprietà dei loro sopra-anelli.

Proposizione 14.5 *Sia A un dominio di Prüfer e sia B un suo sopra-anello. Allora:*

(1) *Se $Q \in \mathrm{Spec}(B)$ e $P = Q \cap A$, allora $B_Q = A_P$ e $Q = PA_P \cap B$. Quindi ogni sopra-anello di valutazione di A è essenziale.*

(2) *Se $P \in \mathrm{Spec}(A)$ è non nullo, $PB \neq B$ se e soltanto se $B \subseteq A_P$.*

(3) *Per ogni ideale $J \subseteq B$, risulta $J = (J \cap A)B$.*

Dimostrazione. (1) Si ha $B_Q \supseteq B_{A \setminus P} \supseteq A_P$. Poiché A_P è di valutazione, B_Q è di valutazione ed è una localizzazione di A_P (Proposizione 2.4). Allora B_Q è una localizzazione di A in un ideale primo M, con $M = QB_Q \cap A = (QB_Q \cap B) \cap A = Q \cap A = P$. In conclusione $B_Q = A_P$ e $Q = QB_Q \cap B = PA_P \cap B$.

(2) Se $B \subseteq A_P$, allora $PB \subseteq PA_P \subsetneq A_P$. Quindi $PB \neq B$.

Viceversa, sia $PB \neq B$ e sia $M \in \operatorname{Max}(B)$ tale che $PB \subseteq M$. Allora $P \subseteq M \cap A$ e $A_{M\cap A} \subseteq A_P$. Ma, per (1), $A_{M\cap A} = B_M$. Dunque $B \subseteq B_M \subseteq A_P$.

(3) Basta far vedere che $J \subseteq (J \cap A)B$; verifichiamolo localmente. Sia $M \in \operatorname{Max}(B)$ e $P = M \cap A$. Allora $B_M = A_P$ e $JB_M = JA_P$. Se $x \in JB_M = JA_P$, possiamo scrivere $x = b/s$, con $b \in J$ e $s \in A \setminus P$. Ma poiché $B \subseteq B_M = A_P$, possiamo anche scrivere $b = a/t$, con $a \in A$ e $t \in A \setminus P$. Dunque $x = b/s = a/(st)$ con $a = tb \in J \cap A$. Ne segue che $x \in (J \cap A)A_P = (J \cap A)B_M$. In conclusione $JB_M \subseteq (J \cap A)B_M$ per ogni $M \in \operatorname{Max}(B)$ e dunque $J \subseteq (J \cap A)B$. □

Proposizione 14.6 *Sia A un dominio di Prüfer e sia B un suo sopra-anello. Sia $\Delta \subseteq \operatorname{Spec}(A)$ l'insieme degli ideali primi di A tali che $PB \neq B$. Allora:*

(1) *B è di Prüfer.*

(2) *$B = \cap\{A_P; P \in \Delta\}$.*

(3) *$\operatorname{Spec}(B) = \{PB, P \in \Delta\}$.*

(4) *Se A ha dimensione finita, $\dim(A) \leq \dim(B)$.*

Dimostrazione. Applichiamo la Proposizione 14.5.

(1) Se $Q \in \operatorname{Spec}(B)$ si ha che $B_Q = A_{Q\cap A}$ è di valutazione. Quindi B è di Prüfer.

(2) $P \in \Delta$ se e soltanto se $B \subseteq A_P$. Quindi $B \subseteq \cap\{A_P; P \in \Delta\}$. Viceversa, per ogni $M \in \operatorname{Max}(B)$ si ha $M = (M \cap A)B$ e $B_M = A_{M\cap A}$. Siccome $M \cap A \in \Delta$, risulta

$$\cap\{A_P; P \in \Delta\} \subseteq \cap\{A_{M\cap A};\ M \in \operatorname{Max}(B)\} = \cap\{B_M;\ M \in \operatorname{Max}(B)\} = B.$$

(3) Se $Q \in \operatorname{Spec}(B)$, allora $Q = (Q \cap A)B$ con $Q \cap A \in \Delta$.

Viceversa, se $P \in \Delta$, si ha $B \subseteq A_P$ e posto $Q := PA_P \cap B$ risulta $Q = [(PA_P \cap B) \cap A]B = PB \in \operatorname{Spec}(B)$.

(4) Se $M \in \operatorname{Max}(B)$, B_M è una localizzazione di A, quindi ha dimensione al più uguale alla dimensione di A. □

Lemma 14.7 *Sia A un dominio integralmente chiuso, con campo dei quozienti K e sia $M \in \operatorname{Max}(A)$. Se $\xi \in K^*$ è radice di un polinomio $f(X) \in A[X] \setminus M[X]$, allora $\xi \in A_M$ oppure $\xi^{-1} \in A_M$.*

Dimostrazione. Se $f(X) \in A[X] \setminus M[X]$, allora $f(X) \in A_M[X] \setminus MA_M[X]$. Quindi possiamo supporre che A sia locale, con ideale massimale M.

Sia ξ radice del polinomio $f(X) := \sum_{i=1}^{m} a_i X^i \in A[X] \setminus M[X]$.

(a) Se $a_m \notin M$, allora a_m è invertibile in A e ξ è radice del polinomio monico $a_m^{-1}f(X) \in A[X]$. Quindi $\xi \in A$.

(b) Se $a_0 \notin M$, allora a_0 è invertibile in A e ξ^{-1} è radice del polinomio monico $a_0^{-1}X^n f(X^{-1}) \in A[X]$. Quindi $\xi^{-1} \in A$.

(c) Supponiamo che $a_0, a_m \in M$. Siccome $f(X) \notin M[X]$ esiste un coefficiente $a_i \notin M$, $0 < i < m$. Allora

$$-(a_0 + a_1\xi + \cdots + a_i\xi^i) = a_{i+1}\xi^{i+1} + a_{i+2}\xi^{i+2} + \cdots + a_m\xi^m,$$

da cui, moltiplicando per ξ^{-i},

$$\alpha := -(a_0\xi^{-i} + a_1\xi^{-(i-1)} + \cdots + a_i) = a_{i+1}\xi + a_{i+2}\xi^2 + \cdots + a_m\xi^{m-i}.$$

Questo implica che α è intero su A, e quindi $\alpha \in A$. Infatti, consideriamo l'ideale frazionario I di A generato da $1, \xi, \dots, \xi^{m-1}$ e mostriamo che $\alpha \in (I : I)$. Per questo, notiamo che risulta $\alpha\xi^j = a_{i+1}\xi^{j+1} + \cdots + a_m x^{j+m-i} \in I$ per $j = 1, \dots, i-1$ e $\alpha\xi^j = -(a_0\xi^{j-i} + \cdots + a_i x^j) \in I$ per $j = i, \dots, m-1$.

Ora, se $\alpha \in M$, si ha $\alpha + a_i \notin M$ e $(\alpha + a_i)\xi^i + a_{i-1}\xi^{i-1} \cdots + a_0 = 0$. Dunque, come in (a), $\xi \in A$.

Se invece $\alpha \notin M$, si ha $a_m\xi^{m-i} + \cdots + a_{i+1}\xi - \alpha = 0$. Dunque, come in (b), $\xi^{-1} \in A$. □

Teorema 14.8 *Le seguenti proprietà sono equivalenti per un dominio A integralmente chiuso:*

(i) *A è un dominio di Prüfer;*

(ii) *Ogni sopra-anello di A è di Prüfer;*

(iii) *Ogni sopra-anello di A è intersezione di localizzazioni di A;*

(iv) *Ogni sopra-anello di A è integralmente chiuso.*

Dimostrazione. (i) $\Rightarrow$ (ii), (iii) per la Proposizione 14.6 e (ii) $\Rightarrow$ (i) è ovvio.

(iii) $\Rightarrow$ (iv) perché ogni localizzazione di A è un dominio di valutazione.

(iv) $\Rightarrow$ (i) Facciamo vedere che $B := A_M$ è un dominio di valutazione, per ogni $M \in \mathrm{Max}(A)$.

Dato $\xi \in K^*$, mostriamo che $\xi \in B$ o $\xi^{-1} \in B$. Siccome ogni sopra-anello di B è integralmente chiuso, $B[\xi^2]$ è integralmente chiuso. Poiché ξ è intero su $B[\xi^2]$ (è radice di $X^2 - \xi^2$), allora $\xi \in B[\xi^2]$. Scrivendo $\xi = a_0 + a_1\xi^2 + \cdots + a_n\xi^{2n}$, vediamo che ξ è radice del polinomio

$$f(X) := a_0 - X + a_1X^2 + \cdots + a_nX^{2n} \in B[X] \setminus MB[X].$$

Dunque, per il Lemma 14.7, $\xi \in B$ oppure $\xi^{-1} \in B$. □

Esempio 14.9 (1) Se $(V_1, M_1), \dots, (V_n, M_n)$ sono anelli di valutazione del campo K inconfrontabili per inclusione, allora $A := V_1 \cap \dots \cap V_n$ è un dominio di Prüfer (anzi di Bezout) semilocale, con ideali massimali $P_i := M_i \cap A$. Infatti $A_{P_i} = V_i$ (Proposizione 12.2). Inoltre, A è noetheriano, equivalentemente un dominio a ideali principali, se e soltanto se ogni V_i è un DVR.

(2) Nel caso noetheriano, i domini di Prüfer coincidono con i domini di Dedekind (Teorema 14.4) e i domini di Bezout coincidono con i domini a ideali principali. Poiché esistono domini di Dedekind che non sono principali, non tutti i domini di Prüfer sono di Bezout. Un dominio di Dedekind non a ideali principali è ad esempio $\mathbb{Z}[i\sqrt{5}]$.

(3) Una intersezione di localizzazioni di A non è necessariamente un anello di frazioni. Se ogni sopra-anello di A è un anello di frazioni, A si chiama un *QR-dominio*. Per il Teorema 14.8, ogni QR-dominio integralmente chiuso è di Prüfer, ma il viceversa non è vero. Ad esempio è noto che se A è di Dedekind, A è un QR-dominio se e soltanto se ogni ideale di A ha una potenza principale.

(4) Si può dimostrare che l'anello dei polinomi $A[X]$ su un dominio (di Prüfer) A non è mai un dominio di Prüfer, a meno che A non sia un campo. Tuttavia, se A è di Prüfer, alcune localizzazioni di $A[X]$ sono ancora di valutazione. Le proprietà di A che sopravvivono in $A[X]$ hanno portato alla definizione della classe più generale dei *domini di Prüfer v-moltiplicativi*, o PVMD.

(5) La *dimensione valutativa* di un dominio A, denotata con $\dim_v(A)$ è definita nel seguente modo. Diciamo che $\dim_v(A) = n$ se esiste un sopra-anello di valutazione di A di rango n e ogni altro sopra-anello di valutazione di A ha rango al più uguale ad n. Altrimenti poniamo $\dim_v(A) = \infty$.

Poiché ogni dominio locale è dominato da un anello di valutazione (Proposizione 2.8), si vede facilmente (procedendo per induzione sulla dimensione), che se A ha dimensione finita, allora $\dim(A) \leq \dim_v(A)$. D'altra parte, se A è di Prüfer, ogni sopra-anello di valutazione di A è una localizzazione di A (Proposizione 14.5) e quindi $\dim_v(A) \leq \dim(A)$. Ne segue che, per i domini di Püfer, la dimensione e la dimensione valutativa coincidono.

I domini di dimensione finita per i quali $\dim(A) = \dim_v(A)$ si chiamano *domini di Jaffard*. Come appena visto i domini di Prüfer sono di Jaffard.

I domini di Jaffard sono precisamente i domini per i quali gli anelli di polinomi hanno dimensione minima. È infatti noto che $\dim(A) = n = \dim_v(A)$ se e soltanto se $\dim(A[X_1, \dots, X_m]) = n + m$, per ogni $m \geq 1$. Questo implica che anche i domini noetheriani sono di Jaffard.

Ricordiamo che, se $\dim(A) = n$, risulta $n + 1 \leq \dim(A[X]) \leq 2n + 1$ e che, per ogni m tale che $n + 1 \leq m \leq 2n + 1$ esiste un dominio (locale integralmente chiuso) A di dimensione n tale che $A[X]$ abbia dimensione m. Per $m > n + 1$, tutti questi domini non sono di Jaffard.

Per approfondire questi argomenti, si veda il Capitolo V del libro di Gilmer e la bibliografia relativa.

15 Restrizione ed Estensione di Valutazioni

In questo paragrafo manterremo le seguenti notazioni: $K \subseteq L$ è un ampliamento di campi, W è l'anello di una valutazione su L e $V := W \cap K$.

Proposizione 15.1 *Con le notazioni precedenti, V è l'anello di una valutazione su K, con ideale massimale uguale al centro di W.*

Dimostrazione. Sia w una valutazione su L con anello associato $W := (W, N)$ e sia $w_{|K}$ la restrizione di w a K. Allora $w_{|K}$ è una valutazione su K e chiaramente $w_{|K}(x) \geq 0$ (resp. $w_{|K}(x) > 0$) se e soltanto se $x \in W \cap K$ (resp. $x \in N \cap K = N \cap V$). $\square$

Date una valutazione w su L, con anello W, e una valutazione v su K, con anello V, diciamo che w *estende* v (oppure che W *estende* V) se $W \cap K = V$. Chiaramente w estende la sua restrizione $w_{|K}$ a K, ma estende anche tutte le valutazioni equivalenti a $w_{|K}$. Inoltre se w estende v anche ogni valutazione equivalente a w estende v. Per evitare queste ambiguità si considerano sempre estensioni tra loro non equivalenti. Inoltre si può supporre che se w estende v allora $v = w_{|K}$, ad esempio decidendo di prendere sempre come gruppo dei valori di una valutazione il gruppo di divisibilità del suo anello (Pragrafo 8).

Per il Teorema di Krull (Teorema 2.9), esistono sempre valutazioni su L che estendono una valutazione v su K. Le proprietà di queste estensioni di v dipendono da quelle dell'ampliamento $K \subseteq L$ e il loro studio è in generale molto complesso. Di seguito diamo qualche primo risultato nel caso algebrico.

Lemma 15.2 *Con le notazioni precedenti, se l'ampliamento $K \subseteq L$ è algebrico e $y \in W$, esiste un polinomio $g(X) \in V[X] \setminus M[X]$ tale che $g(y) = 0$.*

Dimostrazione. Sia $f(X) := \sum_{i=1}^{n} a_i X^i \in K[X]$ un polinomio non nullo tale che $f(y) = 0$. Moltiplicando per un denominatore comune dei coefficienti, possiamo supporre che $f(X) \in V[X]$. Poiché V è di valutazione, gli ideali principali $\langle a_i \rangle$ di V sono linearmente ordinati. Quindi esiste un coefficiente $a_j \neq 0$ che divide tutti gli altri coefficienti e possiamo scrivere $f(X) = ag(X)$, con $a := a_j \in V^*$ e $g(X) \in V[X] \setminus P[X]$. Chiaramente $g(y) = 0$. $\square$

Proposizione 15.3 *Con le notazioni precedenti:*

(1) *Per ogni ideale $I \subseteq V$, si ha $I = IW \cap V$.*

(2) $\mathrm{Spec}(V) = \{Q \cap K;\ Q \in \mathrm{Spec}(W)\}$.

(3) *Se l'ampliamento $K \subseteq L$ è algebrico, W/Q è algebrico su $V/(Q \cap V)$, per ogni $Q \in \mathrm{Spec}(W)$.*

(4) *Se l'ampliamento $K \subseteq L$ è algebrico, ideali primi distinti di W si contraggono su ideali primi distinti di V. Quindi W e V hanno lo stesso rango.*

(5) *Se W è un anello di valutazione discreta, anche V lo è.*

(6) *Se l'ampliamento $K \subseteq L$ è finito e V è un anello di valutazione discreta, anche W lo è.*

Dimostrazione. (1) Chiaramente $I \subseteq IW \cap V$. Per l'inclusione inversa, sia $x \in IW \cap V$. Allora possiamo scrivere $x = \sum_{i=1}^{n} a_i x_i$, con $a_i \in I$ e $x_i \in W$. Se $a_1V + \cdots + a_nV = aV$ (Proposizione 2.2), allora $a \in I$ e $x \in aW$. Ne segue che $xa^{-1} \in W \cap K = V$ e $x \in aV \subseteq I$.

(2) Per ogni $Q \in \mathrm{Spec}(W)$ risulta $Q \cap K \in \mathrm{Spec}(V)$. Viceversa, sia $P \in \mathrm{Spec}(V)$. Per il punto (2), si ha $P = I \cap V$ per qualche ideale I di W. Mostriamo che esiste $Q \in \mathrm{Spec}(W)$ tale che $P = Q \cap V$ è primo.

Questo dipende solo dal fatto che P è primo ed è vero per ogni estensione di anelli commutativi unitari. Infatti, sia $S := V \setminus P$. Poiché S è una parte moltiplicativa di W e $I \cap S = \emptyset$, esiste un ideale primo $Q \in \mathrm{Spec}(W)$ contenente I tale che $Q \cap S = \emptyset$. Allora $Q \cap V \subseteq P$ e poiché $I \subseteq Q$ si ha $P = I \cap V \subseteq Q \cap V \subseteq P$. Da cui $P = Q \cap V$.

(3) Siano $Q \in \mathrm{Spec}(W)$ e $P := Q \cap W$. Se $y \in W$, esiste un polinomio $\underline{g(X)} \in V[X] \setminus P[X]$ tale che $g(y) = 0$ (Lemma 15.2). Allora il polinomio $\overline{g(X)}$ in $V[X]/P[X] = (V/P)[X]$ è non nullo ed è annullato da $\overline{y} \in W/Q$.

(4) Siano Q_1 e Q_2 due ideali primi di W e supponiamo che $Q_1 \subsetneq Q_2$. Allora Q_2/Q_1 è un ideale primo non nullo di W/Q_1. Mostriamo che Q_2/Q_1 non si contrae sullo zero di $V/(Q_1 \cap V)$. Questo dipende dal fatto che, per il punto (4), W/Q_1 è algebrico su $V/(Q_1 \cap V)$.

Infatti, sia $A \subseteq B$ un' estensione algebrica di anelli commutativi unitari e sia $I \subseteq B$ un ideale non nullo. Mostriamo che $I \cap A \neq (0)$. Sia $y \in I$ e sia $f(X) = \sum_{i=1}^{n} a_i X^i \in A[X]$ un polinomio di grado minimo annullato da y. Allora $a_0 \neq 0$ e $a_0 = -(a_1 y + \cdots + a_n y^n) \in I \cap A$.

(5) Dobbiamo far vedere che ogni primo ramificato di V non è idempotente.

Sia $P \in \mathrm{Spec}(V)$ ramificato e sia $Q \neq P$ un ideale P-primario. Sia $M := \sqrt{PW} \subseteq W$. Siccome $M \cap V = P = PW \cap V$ e $QW \cap V = Q$ (punto (2)), allora $QW \subsetneq PW \subseteq M$ e dunque M è ramificato. Poiché W è discreto, si ha $M^2 \neq M$, da cui $P^2 \neq P$.

(6) Sia $[L:K]=n$. Facciamo vedere che, se $M \in \operatorname{Spec}(W)$ è ramificato, allora $M \neq M^2$. Sia $\{Q_\lambda\}$ l'insieme degli ideali M primari di W. Allora $M' := \cap_\lambda Q_\lambda$ è un ideale primo di W e $M' \subsetneq M$ (Corollario 4.9). Se $P := M \cap V$, gli ideali $Q_\lambda \cap V$ sono P-primari. Per il punto (5), $P = M \cap V \neq M' \cap V = \cap_\lambda \{Q_\lambda \cap V\}$. Dunque esiste un ideale P-primario di V diverso da P e quindi P è ramificato. Poiché V è discreto, risulta $P \neq P^2$. Ora $P = PW \cap P \supsetneq P^2W \cap P = P^2$; quindi $PW \neq P^2W$. Se mostriamo che $M^n \subseteq PW$, otterremo che $M^{2n} \subseteq P^2W \subsetneq M$, da cui $M \neq M^2$.

Sia $y \in M$ non nullo e sia $f(X) := \sum_{i=1}^{r} a_i X^i \in V[X]$ un polinomio di grado $r \leq n$ annullato da y. Sia w una valutazione su L di anello W. Poiché $\sum_{i=1}^{r} a_i y^i = 0$, esistono due indici $0 \leq i < j \leq n$ tali che $a_i, a_j \neq 0$ e $w(a_i y^i) = w(a_j y^j)$ (Proposizione 7.3). Siccome $j - i > 0$, allora $w(y^{j-i}) = w(a_i/a_j) > 0$. Ne segue che $a_i/a_j \in M \cap K = P$. Inoltre $w(y^{j-i} a_j/a_i) = 0$ e $y^{j-i} a_j/a_i$ è invertibile. Dunque $(y^{j-i} a_j/a_i) = W$ e $y^{j-i} \in (a_i/a_j)W \subseteq PW$. Poiché $j - i < r \leq n$, $y^n \in PW$. Questo basta a concludere che $M^n \in PW$. Infatti M^n è generato da tutti i prodotti $x_1 \dots x_n$ di elementi di M. Allora, se y genera l'ideale $\langle x_1, \dots, x_n \rangle$, si ha $x_1 \dots x_n \in y^n W \subseteq PW$. □

Corollario 15.4 *Con le notazioni della proposizione precedente:*

(1) *Se W è un DVR, anche V è un DVR.*

(2) *Se V è un DVR e $[L:K] < \infty$, anche W è un DVR.*

Dimostrazione. Segue dalla Proposizione 15.3(4), (5), (6). □

Proposizione 15.5 *Sia $K \subseteq L$ un ampliamento algebrico e sia $V := (V, M)$ l'anello di una valutazione su K. Se V' è la chiusura integrale di V in L, le estensioni di V a L sono precisamente le localizzazioni V'_N, al variare di N in $\operatorname{Max}(V')$. In particolare V' è un dominio di Prüfer e $\dim V = \dim V'$.*

Dimostrazione. Mostriamo prima che V'_N è un dominio di valutazione di L, al variare di N in $\operatorname{Max}(V')$. Sia $x \in L$ non nullo. Siccome x è algebrico su V, esiste un polinomio $g(X) \in V[X] \setminus M[X]$ tale che $g(y) = 0$ (Lemma 15.2). Poiché $N \cap V = M$, si ha anche $f(X) \in V'[X] \setminus N[X]$. Allora , poiché V' è integralmente chiuso, $x \in V'_N$ oppure $x^{-1} \in V'_N$ (Lemma 14.7). Dunque V'_N è un dominio di valutazione.

Viceversa, sia $W := (W, P)$ un'estensione di V a L. Allora $V \subseteq V' \subseteq W$ e, posto $N := V' \cap P$ si ha $M = V \cap P = V \cap N$. Allora $N \in \operatorname{Max}(V')$ e $V'_N \subseteq W$. Siccome V'_N è di valutazione, W è una localizzazione di V'_N e possiamo scrivere $W = V'_Q$ con $Q \subseteq N$. Dunque $P = QV'_Q$ e $M = P \cap V = (QV'_Q \cap V'_N) \cap V = QV'_N \cap V = NV'_N \cap V$. Allora $P = QV'_N = NV'_N$ (Proposizione 15.1(5)) e $W = V'_N$. □

Proposizione 15.6 *Sia A un dominio di Prüfer con campo dei quozienti K. Se $K \subseteq L$ è un ampliamento algebrico, la chiusura integrale di A in L è un dominio di Prüfer.*

Dimostrazione. Sia A' la chiusura integrale di A in L e sia $N \in \mathrm{Max}(A')$. Se $M := N \cap A$ e $S := A \setminus M$, allora $A'_S = (A_M)'$ è la chiusura integrale di A_M in L. Poiché A è di Prüfer, A_M è di valutazione e dunque $A'_S = (A_M)'$ è di Prüfer (Proposizione 15.5). Siccome $N \cap S = \emptyset$, NA'_S è un ideale massimale e allora $(A'_S)_{NA'_S} = A'_N$ è di valutazione. Concludiamo che A' è di Prüfer. □

Un dominio di Prüfer tale che A_M sia un DVR, per ogni ideale massimale M, si chiama un dominio *almost Dedekind*. Un dominio di Dedekind è precisamente un dominio almost Dedekind con il carattere di finitezza (Teorema 13.7).

Proposizione 15.7 *Sia A un dominio almost Dedekind con campo dei quozienti K. Se $K \subseteq L$ è un ampliamento finito, la chiusura integrale di A in L è un dominio almost Dedekind.*

Dimostrazione. Sia $N \in \mathrm{Max}(A')$ e $M = N \cap A \in \mathrm{Max}(A)$. Procedendo come nella dimostrazione della Proposizione 15.6, osserviamo che A'_N è un dominio di valutazione di L che estende A_M. Poiché A_M è un DVR e $[L : K] = n$, anche A'_N è un DVR (Corollario 15.4). □

Esempio 15.8 (1) Si può dimostrare che anche la chiusura integrale di un dominio di Dedekind in un ampliamento finito del campo dei quozienti è di Dedekind. Il carattere di finitezza segue dal fatto che, se $[L : K] = n$, il numero delle valutazioni non equivalenti di L che estendono una valutazione su K è finito (al più uguale al grado di separabilità). Per questo si può vedere il Paragrafo 20 del Gilmer o il Capitolo 6 del Bourbaki.

Ad esempio, tutti gli anelli di interi algebrici in un ampliamento finito di $\mathbb{Q}$ sono domini di Dedekind.

(2) Sia $\Delta(A)$ il gruppo di divisibilità di un dominio di valutazione A. Con le solite notazioni, se W estende V, allora risulta $\Delta(V) \subseteq \Delta(W)$. L'indice di $\Delta(V)$ in $\Delta(W)$ si chiama l'*indice di ramificazione* di w rispetto a v e si denota con $e(w, v) := [\Delta(V) : \Delta(W)]$.

Poiché poi W domina V, si ha anche un'immersione dei campi residui $k(V) \subseteq k(W)$. Il grado di questo ampliamento di campi si chiama il *grado residuo* di w rispetto a v e si indica con $f(w, v) := [k(W) : k(V)]$. Notiamo che se $K \subseteq L$ è algebrico, anche l'ampliamento $k(V) \subseteq k(W)$ è algebrico (Proposizione 15.3(3)).

Se $[L : K] = n$, ci sono soltanto un numero finito $w_1, \dots, w_r$ di valutazioni non equivalenti di L che estendono v e risulta $e(w_1, v)f(w_1, v) + \cdots + e(w_r, v)f(w_r, v) \le n$, in particolare, se l'ampliamento $K \subseteq L$ è finito, indici di ramificazione e gradi residui sono finiti. L'uguaglianza è raggiunta ad esempio se v è discreta e l'ampliamento $K \subseteq L$ è separabile, come nel caso degli anelli di interi algebrici (Bourbaki, Capitolo 6, Paragrafo 8).

(3) Se l'ampliamento $K \subseteq L$ non è finito, non è detto che l'estensione in L di un DVR di K sia ancora un DVR, come mostra il seguente esempio: La chiusura integrale di $\mathbb{Z}$ nel campo $\mathbb{A}$ dei numeri algebrici è un dominio di Prüfer di dimensione uno in cui tutti gli ideali radicali sono idempotenti.

Quest'ultima proprietà discende dal fatto che $\mathbb{A}$ è un campo algebricamente chiuso. Infatti, sia A un dominio integralmente chiuso il cui campo dei quozienti K sia algebricamente chiuso. Facciamo vedere che se $Q = \sqrt{Q}$ è un ideale radicale si ha $Q = Q^2$. Sia $a \in Q$. Poiché K è algebricamente chiuso, esiste $x \in K$ tale che $x^2 = a$. Ma siccome x è intero su A, allora $x \in A$. Dunque $x \in Q$ e $a = x^2 \in Q^2$.

(4) Se $K(X)$ è un ampliamento semplice trascendente, le estensioni di una valutazione v su K ad una valutazione su $K(X)$ possono essere costruite dando un opportuno valore a X (in un gruppo totalmente ordinato contenente il gruppo dei valori Δ di v). Questo si può fare in infiniti modi.

Una valutazione su $K(X)$ che ha lo stesso gruppo dei valori Δ di v è quella indotta dall'applicazione $w : K[X]^* \longrightarrow \Delta$ definita da $w(a_0 + a_1X + \cdots + a_nX^n) = \min\{v(a_i)\}$ (w è tale che $w(X) = 0$).

Questa valutazione è stata già usata nella dimostrazione della Proposizione 13.5(2). Per approfondimenti si può vedere il Capitolo 6, Paragrafo 10, del Bourbaki.

16 APPENDICE: Ideali frazionari e ideali invertibili

Se A è un dominio con campo dei quozienti K, un *ideale frazionario* di A è un A-sottomodulo I di K tale che $dI \subseteq A$, per qualche elemento non nullo $d \in A$. Quindi I è un ideale frazionario di A se e soltanto se $I = d^{-1}J$, dove $0 \neq d \in A$ e $J \subseteq A$ è un ideale. Segue dalla definizione che ogni A-sottomodulo di un ideale frazionario è ancora un ideale frazionario.

Le proprietà elencate nelle seguenti due proposizioni sono di facile verifica.

Proposizione 16.1 *Siano I, J ideali frazionari di A. Allora:*

(a) $IJ := \{\sum_{i=1}^n x_iy_i\,;\ x_i \in I\,, y_i \in J\,, n \geq 1\}$*;*

(b) $I \cap J$*;*

(c) $I + J := \{x + y\,;\ x \in I\,, y \in J\}$

sono ideali frazionari. □

Dati due A-sottomoduli I, J di K, poniamo

$$(I : J) := (I :_K J) := \{x \in K\,;\, xJ \subseteq I\}\,;$$

$$(I :_A J) := (I :_K J) \cap A = \{x \in A\,;\, xJ \subseteq I\}.$$

Con questa notazione, un A-sottomodulo I di K è un ideale frazionario di A se e soltanto se $(A : I) \neq (0)$.

Proposizione 16.2 *Siano I, J, H ideali frazionari di A. Allora:*

(a) $(I : J)$ *è un ideale frazionario di A e $(I :_A J)$ è un ideale di A;*

(b) $(I : JH) = ((I : J) : H)$*;*

(c) $(xI : J) = x(I : J)$ *e* $(I : xJ) = x^{-1}(I : J)$*, per ogni elemento non nullo $x \in K$.*

Inoltre, per ogni famiglia di ideali frazionari $\{H_i\}$:

(d) $(\cap H_i : J) = \cap(H_i : J)$*;*

(e) $(I : \sum H_i) = \cap(I : H_i)$. □

Proposizione 16.3 *Siano I e J due ideali frazionari non nulli di A. Allora I e J sono isomorfi come A-moduli se e soltanto se $I = xJ$, con $x \in K \setminus \{0\}$.*

Dunque l'ideale frazionario $(I : J)$ è A-linearmente isomorfo al modulo $Hom_A(J, I)$ degli A-omomorfismi di J in I. Inoltre, $(I : I)$ è isomorfo all'anello degli A-endomorfismi di I.

Dimostrazione. Per ogni $x \in (I : J)$, la moltiplicazione per x

$$\mu_x : J \longrightarrow I\,; \quad a \mapsto ax$$

è un A-omomorfismo ed è iniettivo se $x \neq 0$.

Allora, se $x \in K \setminus \{0\}$ e $I = xJ$, si ha che $x \in (I : J)$ e $I = \mu_x(J)$ è isomorfo a J. Viceversa, sia $\varphi \in Hom_A(J, I)$ non nullo. Mostriamo che, per ogni $a, b \in J \setminus \{0\}$, $a^{-1}\varphi(a) = b^{-1}\varphi(b)$. Allora, posto $z := a^{-1}\varphi(a)$, per ogni $b \in J$ potremo scrivere $\varphi(b) = zb = \mu_z(b)$, da cui $\varphi = \mu_z$ è la moltiplicazione per z e $\varphi(J) = zJ$.

Sia $d \in A$ non nullo tale che $dJ \subseteq R$ e siano $a_1 := da$, $b_1 := db \in A$. Allora per A-linearità,

$$\varphi(a) = \varphi(\frac{a_1}{d}) = a_1\varphi(\frac{1}{d}) = \frac{a_1}{b_1}\varphi(\frac{b_1}{d}) = \frac{a_1}{b_1}\varphi(b)$$

da cui,

$$a^{-1}\varphi(a) = a^{-1}\frac{a_1}{b_1}\varphi(b) = \frac{d}{b_1}\varphi(b) = b^{-1}\varphi(b).$$

Per quanto appena visto, l'applicazione

$$\Psi : (I : J) \longrightarrow Hom_A(J, I)\,;\; x \mapsto \mu_x.$$

è A-lineare e biiettiva. Infine, $(I : I)$ e $End_A(I) := Hom_A(I; I)$ sono anelli e $\Psi : (I : I) \longrightarrow End_A(I)$ è anche un isomorfismo di anelli. □

Remark 16.4 Poiché, come appena visto, l'ideale frazionario $(A : I)$ è A-isomorfo a $Hom_A(I, A)$, esso si chiama anche il *duale* di I.

Se I è un ideale frazionario di A, I è isomorfo ad un ideale intero J e gli anelli degli endomorfismi di I e J coincidono. Infatti risulta $I = d^{-1}J$, con $0 \neq d \in A$ e $J \subseteq A$ ed inoltre $(I : I) = (J : J)$.

È evidente che gli A-sottomoduli ciclici di K (cioè quelli del tipo xA, con $x \in K$) sono ideali frazionari. Più generalmente, abbiamo il seguente risultato.

Proposizione 16.5 *Sia A un dominio con campo dei quozienti K. Ogni A-sottomodulo di K finitamente generato è un ideale frazionario di A.*

Dimostrazione. Sia $I := x_1A + \cdots + x_nA$, con $x_i := \frac{a_i}{b_i} \in K$. Allora posto $d := b_1 \dots b_n$ si ha $dI \subseteq A$. $\square$

Proposizione 16.6 *Siano I, J ideali frazionari di A e $S \subsetneq A^*$ una parte moltiplicativa. Allora $(I : J)A_S \subseteq (IA_S : JA_S)$. Se inoltre J è finitamente generato, $(I : J)A_S = (IA_S : JA_S)$.*

Dimostrazione. È evidente che $(I : J)A_S \subseteq (IA_S : JA_S)$. Inoltre, sia $J := \sum x_iA$ finitamente generato. Allora $(IA_S : JA_S) = (IA_S : \sum x_iA_S) = \cap(IA_S : x_iA_S) = \cap x_i^{-1}IA_S = \cap(I : x_iA)A_S = (I : \sum x_iA)A_S = (I : J)A_S$. $\square$

Proposizione 16.7 *Se A è un dominio, allora per ogni ideale frazionario I di A risulta $I = \cap\{IA_M \,;\ M \in \mathrm{Max}(A)\}$; in particolare $A = \cap\{A_M \,;\ M \in \mathrm{Max}(A)\}$. Dunque $I = J$ se e soltanto se $IA_M = JA_M$ per ogni ideale massimale M.*

Dimostrazione. Chiaramente $I \subseteq \cap\{IA_M \,;\ M \in \mathrm{Max}(A)\}$. Viceversa, fissato M, sia $x := \frac{a}{s} \in IA_M$, con $a \in I$ e $s \in A \setminus M$. Allora $s \in (I :_A x) \setminus M$, da cui $(I :_A x) \nsubseteq M$. Perciò, se $x \in \cap\{IA_M \,;\ M \in \mathrm{Max}(A)\}$, si ha $(I :_A x) \nsubseteq M$, per ogni $M \in \mathrm{Max}(A)$. Da cui $(I :_A x) = A \ni 1$ e $x = 1x \in A$. $\square$

Remark 16.8 Anche se $(I : J)A_M \subsetneq (IA_M : JA_M)$ per qualche $M \in \mathrm{Max}(A)$, si ha comunque $(I : J) = \cap(I : J)A_M = \cap(IA_M : JA_M)$. Infatti $I = \cap IA_M$ e $(I : J) = (\cap IA_M : J) = \cap(IA_M : J) = \cap(IA_M : JA_M)$.

Nel seguito indicheremo con $\mathcal{F}(A)$ l'insieme degli ideali frazionari non nulli del dominio A. Poiché $\mathcal{F}(A)$ è chiuso rispetto alla moltiplicazione di ideali, $\mathcal{F}(A)$ è un semigruppo moltiplicativo commutativo, con unità A.

Un ideale frazionario non nullo I di A si dice *invertibile* se è invertibile nel semigruppo $\mathcal{F}(A)$, cioè se esiste un (unico) ideale frazionario J tale che $IJ = A$.

Notiamo che un ideale invertibile I è *cancellabile*, ovvero, dati $H_1, H_2 \in \mathcal{F}(A)$, si ha $IH_1 \subseteq IH_2$ se e soltanto se $H_1 \subseteq H_2$.

Proposizione 16.9 *Se $I \in \mathcal{F}(A)$ è un ideale invertibile, allora il suo inverso è $(A : I)$. Dunque I è invertibile se e soltanto se $I(A : I) = A$.*

Dimostrazione. Sia $A = IJ$. Allora $J \subseteq (A : I)$ e $A = IJ \subseteq I(A : I) \subseteq A$, da cui $A = I(A : I)$. Per l'unicità dell'inverso, $J = (A : I)$. □

Proposizione 16.10 *Sia $A \subseteq B$ un'estensione di domini. Se $I \in \mathcal{F}(A)$ è invertibile, allora $IB \in \mathcal{F}(B)$ è invertibile.*

Dimostrazione. Sia $A = IJ$. Allora $B = IJB = (IB)(JB)$. □

Dalla proposizione precedente otteniamo che, se $I \in \mathcal{F}(A)$ è invertibile, per ogni estensione $A \subseteq B$, si ha $(A : I)B = (B : IB)$.

Proposizione 16.11 *Sia I un ideale frazionario invertibile. Allora, per ogni $J, H \in \mathcal{F}(A)$,*

$$(IJ : H) = I(J : H)\,; \quad (H : IJ) = (A : I)(H : J).$$

In particolare $(I : I) = A$.

Dimostrazione. Per la prima uguaglianza, $x \in (IJ : H) \Leftrightarrow xH \subseteq IJ \Leftrightarrow x(A : I)H \subseteq J \Leftrightarrow x(A : I) \subseteq (J : H) \Leftrightarrow x \in I(J : H)$. Da questa, per $H = I$ e $J = A$, otteniamo $(I : I) = A$.

La seconda uguaglianza si prova in modo analogo. □

Proposizione 16.12 *Se $M \in \mathrm{Max}(A)$, allora M è invertibile se e soltanto se $(M : M) = A$.*

Dimostrazione. Se M è invertibile, allora $(M : M) = A$ per la Proposizione 16.11. Viceversa, se M non è invertibile, poiché $M \subseteq M(A : M) \subseteq A$, si ha $M(A : M) = M$, da cui $(M : M) = (A : M)$ e $A \subsetneq (A : M) = (M : M)$. □

Proposizione 16.13 (1) *Se $I \in \mathcal{F}(A)$ è un ideale invertibile e $I = JH$, con $J, H \in \mathcal{F}(A)$, allora J, H sono ideali invertibili.*

(2) *Se $J \subseteq I \subseteq A$ sono ideali e I è invertibile, allora $J = IH$, per un ideale $H \subseteq A$.*

(3) *Se P, Q sono ideali primi invertibili e $P \subseteq Q$, allora $P = Q$.*

Dimostrazione. (1) $A = I(A : I) = J((A : I)H) = (J(A : I))H$.

(2) Se $J \subseteq I$, allora $H := J(A : I) \subseteq A$. Perciò se I è invertibile, $J = I(A : I)J = IH$.

(3) Se $P \subseteq Q$, per (2), $P = QH$, con $H := (A : Q)P \subseteq A$. Poiché $H \nsubseteq P$ (altrimenti cancellando P sarebbe $(A : Q) = A$) allora $Q \subseteq P$ e $P = Q$. □

Proposizione 16.14 *Se $P \subsetneq I \subseteq A$ sono ideali, P è primo e I è invertibile, allora $\overline{I} := I/P$ è un ideale invertibile di $\overline{A} := A/P$.*

Dimostrazione. Poiché I è invertibile, per $x \in I \setminus P$ si ha $xA = IH$ con $H \subseteq A$ (Proposizione 16.13(2)). Passando alle classi modulo P, otteniamo $\overline{xA} = \overline{IH}$. Dunque $\overline{I}$ è invertibile in $\overline{A}$ (Proposizione 16.13(1)). $\square$

Terminiamo con una caratterizzazione locale degli ideali invertibili.

Proposizione 16.15 *Un ideale frazionario invertibile è finitamente generato.*

Dimostrazione. Sia $I \in \mathcal{F}(A)$ invertibile e sia $J \in \mathcal{F}(A)$ tale che $IJ = A$. Poiché $1 \in IJ$, esistono $x_1, \dots, x_n \in I$ e $y_1, \dots, y_n \in J$ tali che $1 = x_1y_1 + \cdots + x_ny_n$. Allora, per ogni $a \in I$, risulta $a = a1 = x_1(ay_1) + \cdots + x_n(ay_n)$. Poiché $ay_i \in IJ = A$, ne segue che $x_1, \dots, x_n$ generano I. $\square$

Proposizione 16.16 *Se A ha un numero finito di ideali massimali, ogni ideale frazionario invertibile di A è principale.*

Dimostrazione. È sufficiente dimostrare l'asserto per gli ideali interi. Siano $M_1, \dots, M_n$ gli ideali massimali di A e sia $I \subseteq A$ un ideale invertibile.

Se $n = 1$, A è locale, con ideale massimale $M = M_1$. Poiché I è invertibile, $I \neq IM$. Allora, se $x \in I \setminus IM$, $x(A : I) \subseteq A$ è un ideale che non è contenuto in M. Ne segue che $x(A : I) = A$ e $I = xA$ è principale.

Sia ora $n \geq 2$. Poiché $M_i \not\supseteq \cap_{j\neq i}M_j$ ed I è invertibile, allora $IM_i \not\supseteq I(\cap_{j\neq i}M_j)$ per ogni $i = 1, \dots, n$. Sia $x_i \in I(\cap_{j\neq i}M_j) \setminus IM_i$ e $x := x_1 + \cdots + x_n$. Allora $x \in I$ e $x \notin IM_i$. Ne segue che $x(A : I) \subseteq A$ e $x(A : I) \not\subseteq M_i$ per ogni i e dunque $x(A : I) = A$ e $I = xA$. $\square$

Proposizione 16.17 *Sia I un ideale frazionario non nullo di A. Le seguenti condizioni sono equivalenti:*

(i) *I è un ideale invertibile;*

(ii) *I è finitamente generato e IA_M è principale, per ogni ideale massimale M di A.*

Dimostrazione. (i) $\Rightarrow$ (ii) I è finitamente generato per la Proposizione 16.15. Poiché IA_M è invertibile (Proposizione 16.10) allora esso è principale per la Proposizione 16.16.

(ii) $\Rightarrow$ (i) Poiché I è finitamente generato, per ogni ideale massimale M di A, si ha $(A : I)A_M = (A_M : IA_M)$. Inoltre $I(A : I)A_M = IA_M(A_M : IA_M) = A_M$. Quindi $I(A : I) = A$ (Proposizione 16.7). $\square$