# Estensioni intere

## 1 Estensioni Intere

Il comportamento delle estensioni e delle contrazioni di ideali tramite omomorfismi di anelli è piuttosto caotico ed è difficile poter avere risultati a priori. Dei risultati si possono però ottenere considerando estensioni intere:

**Definizione 1.1.** Siano $A \subseteq B$ anelli. Un elemento $x \in B$ si dice *intero* su $A$ se $x$ è radice di un polinomio *monico* $p \in A[x]$.

Il parallelo è con la nozione di algebricità vista per estensioni di campi; lavorando con anelli è importante che il polinomio sia monico. Per esempio, se consideriamo $\mathbb{Z} \subseteq \mathbb{Q}$ gli $x$ interi su $\mathbb{Z}$ sono tutti e soli gli elementi di $\mathbb{Z}$.

Mostriamo ora delle definizioni equivalenti di elemento intero:

**Teorema 1.2.** Sono equivalenti:

1. $b \in B$ è intero su $A$
2. $A[b]$ è un $A$-modulo finitamente generato
3. $A[b] \subseteq C$, dove $C \subseteq B$ è un sottoanello che è un $A$-modulo finitamente generato
4. Esiste un $A[b]$-modulo *fedele*[1] $M$ che è finitamente generato come $A$-modulo.

*Dimostrazione.*

($1 \Rightarrow 2$) La relazione $p(b) = 0$ permette di limitare il grado dei polinomi, e ci bastano monomi di grado limitato per generare tutto.

($2 \Rightarrow 3$) Basta prendere $C = A[b]$.

($3 \Rightarrow 4$) Basta prendere $M = C$. Questo è fedele perché contiene 1, e se non fosse fedele dovrebbe essere $p(b) \cdot 1 = 0$, e quindi $p = 0$.

[1] Cioè $\mathrm{Ann}(M) = 0$.

($4 \Rightarrow 1$) Ricordiamo che se $M$ è un $A$-modulo finitamente generato, e $\varphi = x\cdot$ è un omomorfismo di $A$-moduli, per Cayley-Hamilton $\varphi^n + \sum a_i \varphi^i = 0$, con $a_i \in A$. Se l'operatore $(x^n + \sum a_i x^i = 0)\cdot$ è nullo, dato che $M$ è fedele deve essere $b^n + \sum a_i b^i = 0$.

□

I seguenti Corollari sono analoghi ai risultati che si hanno per le estensioni algebriche.

**Corollario 1.3.** Siano $x_1, \ldots, x_n \in B$ interi su $A$. Allora $A[x_1, \ldots, x_n]$ è un $A$-modulo finitamente generato.

**Corollario 1.4.** L'insieme $C \subseteq B$ degli elementi interi su $A$ è un sottoanello di $B$.

*Dimostrazione.* Siano $x, y \in C$. Per vedere che $x + y \in C$ consideriamo $A[x + y] \subseteq A[x, y]$. Il secondo è finitamente generato, e basta porlo come $C$ nel punto 3 del Teorema 1.2. Allo stesso modo, si mostra che $xy \in C$. □

**Definizione 1.5.** $C$ come sopra si dice *chiusura integrale di $A$ in $B$*. Se $C = A$ si dice che $A$ è *integralmente chiuso* in $B$. Se $C = B$ si dice che $B$ è intero su $A$.

**Proposizione 1.6.** Siano $A \subseteq B \subseteq C$ anelli e supponiamo che $B$ sia intero su $A$ e che $C$ sia intero su $B$. Allora $C$ è intero su $A$.

*Dimostrazione.* Sia $x \in C$, che in quanto intero su $B$ soddisfa un'equazione del tipo $x^n + \sum b_i x^i = 0$. Considerando l'anello $B' = A[b_0, \ldots, b_{n-1}]$ abbiamo che $x$ è intero su $B'$, e allora $B'[x]$, che è sicuramente finitamente generato come $B'$-modulo, è $A[b_0, \ldots, b_{n-1}][x]$, ed è quindi anche un $A$-modulo finitamente generato. Inoltre $A[x] \subseteq B'[x]$ e basta utilizzare il Teorema. □

Una conseguenza di questo fatto è che se $A \subseteq C \subseteq B$, dove $C$ è la chiusura integrale di $A$ in $B$, la chiusura integrale di $C$ in $B$ è sempre $C$, cioè l'idempotenza della chiusura integrale. La chiusura integrale si comporta bene anche rispetto a operazioni fra anelli:

**Proposizione 1.7.** Sia $A \subseteq B$, $B$ intero su $A$, $\mathfrak{q}$ un ideale di $B$ e $\mathfrak{p} = \mathfrak{q} \cap A$ la sua contrazione. Allora $B/\mathfrak{q}$ è intero su $A/\mathfrak{p}$.

*Dimostrazione.* Sia $x + \mathfrak{q} \in B/\mathfrak{q}$. Allora $x \in B$ è intero su $A$ e dunque risolve un'equazione

$$x^n + \sum_{i=0}^{n-1} a_i x^i = 0$$

Di conseguenza, riducendo modulo $\mathfrak{q}$,

$$(x+\mathfrak{q})^n + \sum_{i=0}^{n-1}(a_i+\mathfrak{p})(x+\mathfrak{q})^i = 0$$

dove abbiamo sfruttato che $\mathfrak{p} = A \cap \mathfrak{q}$. □

**Proposizione 1.8.** Siano $A \subseteq B$ anelli, $C$ la chiusura integrale di $A$ in $B$, $S$ una parte moltiplicativa di $A$. Allora $S^{-1}C$ è la chiusura integrale di $S^{-1}A$ in $S^{-1}B$.

*Dimostrazione.* Sia $x/s \in S^{-1}C$, con $x^n + \sum a_i x^i = 0$, dove $a_i \in A$. Allora

$$\left(\frac{x}{s}\right)^n + \sum \frac{a_i}{s^{n-i}}\left(\frac{x}{s}\right)^i = 0$$

e quindi $\frac{x}{s}$ è intero su $S^{-1}A$. Se viceversa $b/s \in S^{-1}B$ è intero su $S^{-1}A$ soddisfa un equazione del tipo

$$\left(\frac{b}{s}\right)^n + \sum \frac{a_i}{s_i}\left(\frac{b}{s}\right)^i = 0$$

e basta porre $t = \prod s_i$ e moltiplicare per $(st)^n$. Notiamo subito che $(bt)$ è intero su $A$ e quindi appartiene a $C$. Ma allora $b/s = (bt)/(st) \in S^{-1}C$. □

Le estensioni si comportano bene anche passando all'anello dei polinomi in una variabile.

**Teorema 1.9.** Siano $A \subseteq B$ anelli, $C$ la chiusura integrale di $A$ in $B$. Allora $C[t]$ è la chiusura integrale di $A[t] \subseteq B[t]$.

Ci sarà utile questo risultato:

**Lemma 1.10.** Siano $A \subseteq B$ anelli, $C$ la chiusura integrale di $A$ in $B$ e siano $f, g \in B[t]$ due polinomi monici tali che $fg \in C[t]$. Allora $f, g \in C[t]$.

*Dimostrazione.* Supponiamo dapprima che $A$ e $B$ siano due domini. Allora $A \subseteq B \subseteq K \coloneqq k(B)$ e fissiamo $\bar{K}$ un chiusura algebrica. Allora esistono $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_k$ tali che $f(t) = \prod(t-\alpha_j)$ e $g(t) = \prod(t-\beta_j)$. Quindi $f(t)g(t) = \prod(t-\alpha_j)(t-\beta_j) \in C[t]$ da una relazione di interezza per gli $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_k$ su $C$, per la Proposizione 1.6. I coefficienti di $f$ e $g$ sono combinazioni algebriche delle radici, allora sono elementi interi su $A$ e perciò stanno in $C$.
In generale se $A \subseteq B$ mostriamo che esiste un anello $D \supseteq B$ tale che $f(t) = \prod(t-\delta_j)$ con $\delta_j \in D$. Infatti se esiste $b \in B$ tale che $f(b) = 0$ poniamo $\delta_1$ $D_1 = B$ e $\delta_1 = b$; altrimenti se non esiste poniamo $D_1 = {}^{B[x]}\!/_{f(x)}$ e $\delta_1 = \bar{x}$. Chiaramente $f(\delta_1) = 0$, poi

$$\begin{array}{rccc} i\colon & B & \longrightarrow & D_1 \\ & b & \longmapsto & b \end{array}$$

è iniettiva perché il polinomio $f$ è monico e non si può "dividere"per alcuna costante. Iterando questo procedimento a partire da $f(t)/(t-\delta_1)$ otteniamo un catena ascendente di anelli e l'ultimo è il $D$ che cercavamo. A questo punto possiamo ripetere esattamente il ragionamento fatto per il caso dei domini.

□

Passiamo alla dimostrazione del Teorema:

*Dimostrazione.* $C[t]$ è contenuto nella chiusura integrale di $\bar{A[t]}$ dato che chiaramente $C \in \bar{A[t]}$ e inoltre $t$ è radice di $x - t \in A[t][x]$, quindi è intero su $A[t]$.
Viceversa, sia $f(t)$ intero su $A[t]$, dobbiamo mostrare che ha coefficienti in $C$. Sappiamo che esistono $\alpha_1(t), \dots, \alpha_n(t) \in A[t]$ tali che

$$f^n + \sum_1^n \alpha_j f^{n-j}$$

allora

$$f(f^{n-1} + \sum_1^{n-1} \alpha_j f^{n-j-1}) = -\alpha_n \in A[t] \subseteq C[t]$$

e indichiamo con $g(t) = f^{n-1} + \sum_1^{n-1} \alpha_j f^{n-j-1}$.
Se $g$ è monico per il Lemma precedente abbiamo la tesi. Altrimenti, poniamo $h = f + t^N$ con $N > \deg f$ e $N > \deg \alpha_j$ per ogni $j$ il quale, visto che la chiusura integrale è un anello, è intero su $A[t]$. Allora

$$(g - t^N)^n + \sum_1^n \alpha_j (g - t^N)^{n-j} = 0.$$

Svolgendo le potenze otteniamo che il grado degli addendi è al più $n \cdot N$. Allora, detto $b_n(t) = (t^N)^n - \sum_1^n \alpha_j (-t^N)^{n-j}$, abbiamo[2]

$$g(g^{n-1} + \dots) = b_n(t) \in A[t] \subseteq C[t]$$

ma in questo caso abbiamo che i fattori sono entrambi monici. Per il lemma allora $g \in C[t]$ e quindi $f = g - t^N \in C[t]$. □

## 2 I Teoremi di Cohen-Seidenberg

Studiamo ora gli ideali primi delle estensioni intere: ci chiediamo se riusciamo a trovare un ideale tale che $\mathfrak{q}^c = \mathfrak{p}$.

[2] $1 - \binom{m}{1} + \binom{m}{2} \cdots + (-1)^m \binom{m}{m-1} = (1-1)^m - (-1)^m$

$$\begin{array}{cc} B & \mathfrak{q}? \\ \cup| & \cup| \\ A & \mathfrak{p} \end{array}$$

**Proposizione 2.1.** Siano $A \subseteq B$ domini e $B$ intero su $A$. Allora $B$ è un campo se e solo se $A$ lo è.

*Dimostrazione.* Se $B$ è un campo prendiamo $0 \neq x \in A$. Sicuramente $x^{-1} \in B$, e siccome l'estensione è intera possiamo scrivere $(x^{-1})^m + \sum a_i (x^{-1})^i = 0$, con gli $a_i \in A$. Allora basta moltiplicare tutto per $x^{m-1}$ per ottenere $x^{-1} = \sum a_i x^{m-1-i}$.

Viceversa siano $A$ un campo e $y \neq 0$ un elemento intero su $A$. Sia $y^n + \sum a_i y^i = 0$ un'equazione di grado minimo per $y$. $A$ è un dominio, dunque $a_0 \neq 0$ perché altrimenti potremmo raccogliere $y$ nell'equazione e ridurre il grado della relazione. Portando a secondo membro $a_0$ e dividendo per esso, ricordando che $a_0$ è invertibile perché elemento non nullo di $A$, otteniamo

$$y \left( a_0^{-1} \sum_{i=1}^{n} a_i y^{i-1} \right) = 1$$

e dunque abbiamo trovato un inverso di $y$.

□

**Corollario 2.2.** Sia $A \subseteq B$ un'estensione intera, $\mathfrak{q} \in \mathrm{Spec}(B)$ e $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{q}^c$. Allora $\mathfrak{q}$ è massimale se e solo se lo è $\mathfrak{p}$.

*Dimostrazione.* $B/\mathfrak{q}$ è intero su $A/\mathfrak{p}$; basta allora applicare la Proposizione precedente, dato che il quoziente per un ideale massimale è un campo. □

**Corollario 2.3.** Se $A \subseteq B$ è un'estensione intera e $\mathfrak{q}_0 \subseteq \mathfrak{q}_1$ sono ideali primi di $B$ tali che $\mathfrak{q}_0^c = \mathfrak{q}_1^c = \mathfrak{p}$, allora $\mathfrak{q}_0 = \mathfrak{q}_1$.

*Dimostrazione.* Sia $S = A \setminus \mathfrak{p}$. Allora $A_\mathfrak{p} = S^{-1}A \subseteq S^{-1}B$ è intera e abbiamo

$$S^{-1}\mathfrak{p} \subseteq S^{-1}A \subseteq S^{-1}B$$

Notiamo che $S^{-1}\mathfrak{q}_0$ e $S^{-1}\mathfrak{q}_1$ sono propri e si contraggono entrambi a $S^{-1}\mathfrak{p}$ e sono dunque massimali per il corollario precedente. Abbiamo allora $S^{-1}\mathfrak{q}_0 = S^{-1}\mathfrak{q}_1$, poiché $S^{-1}\mathfrak{q}_0 \subseteq S^{-1}\mathfrak{q}_1$ e sono entrambi massimali. Per concludere basta ricordare che $S^{-1}$ mette in bigezione gli ideali nell'anello di frazioni con gli ideali nell'anello che non intersecano $S$. Dunque $\mathfrak{q}_0 = \mathfrak{q}_1$. □

**Esempio 2.4.**

- Considerando $\mathbb{Z}[i] \subseteq \mathbb{Q}[i]$ c'è una corrispondenza massimali e primi $\mathbb{Z}[i]$ $\mathfrak{q} \cap \mathbb{Z} = \mathfrak{p}$. In un certo senso ci stiamo chiedendo quando il generatore di $\mathfrak{q}$ divide quello di $\mathfrak{p}$.

- Consideriamo la cubica $h(x,y) = y^2 - x^3 - 1 = 0$ e definiamo

$$B \coloneqq {}^{\mathbb{C}[x,y]}\!\diagup_{(y^2 - x^3 - 1)}$$

Dalla mappa

$$\begin{array}{rccc} f\colon & \mathbb{C}[x] & \longrightarrow & B \\ & x & \longmapsto & x \end{array}$$

otteniamo una mappa tra gli spettri massimali

$$\begin{array}{rccc} f^*\colon & \mathrm{SpecMax}(B) & \longrightarrow & \mathrm{SpecMax}(\mathbb{C}[x]) \\ & (x,y) & \longmapsto & x \end{array}$$

che è proprio la proiezione. Siamo nel caso $A\mathbb{C}[x] =\subseteq B$ dove $B = A[y]$ con $y$ intero su $A$, infatti è $y^2 - x^3 - 1 = 0$ e $x^3 + 1 \in A$.

**Teorema 2.5** (Lying Over)**.** Siano $A \subseteq B$ un'estensione intera e $\mathfrak{p} \in \mathrm{Spec}(A)$. Allora esiste $\mathfrak{q} \in \mathrm{Spec}(B)$ tale che $\mathfrak{q}^c = \mathfrak{p}$.

*Dimostrazione.* Consideriamo il diagramma

$$\begin{array}{ccc} A & \xrightarrow{\ i\ } & B \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ S^{-1}A & \xrightarrow[\ i\ ]{} & S^{-1}B \end{array}$$

e prendiamo $\mathfrak{m} \in \mathrm{SpecMax}(S^{-1}B)$. Per quanto visto la sua contrazione in $S^{-1}A = A_{\mathfrak{p}}$ è massimale, e quindi è $S^{-1}\mathfrak{p}$ e questo viene contratto a $\mathfrak{p}$. D'altra parte $\mathfrak{m}$ si contrae in $B$ a un $\mathfrak{q} \in \mathrm{Spec}(B)$, e per la commutatività del diagramma $\mathfrak{q}^c = \mathfrak{p}$. □

Questo appena dimostrato non è altro che il passo base della dimostrazione del seguente teorema:

**Teorema 2.6** (Going Up)**.** Sia $A \subseteq B$ un'estensione intera. Sia

$$\mathfrak{p}_0 \subseteq \ldots \subseteq \mathfrak{p}_n$$

una catena di ideali primi in $A$ e supponiamo di avere una catena più corta $(m \leq n)$

$$\mathfrak{q}_0 \subseteq \ldots \subseteq \mathfrak{q}_m$$

di primi in $B$ tali che $\mathfrak{q}_i^c = \mathfrak{p}_i$. Esistono allora ideali primi $\mathfrak{q}_{m+1}, \ldots, \mathfrak{q}_n$ che estendono la catena

$$\mathfrak{q}_0 \subseteq \ldots \subseteq \mathfrak{q}_m \subseteq \ldots \mathfrak{q}_n$$

preservando la proprietà $\mathfrak{q}_i^c = \mathfrak{p}_i$.

*Dimostrazione.* Per induzione, possiamo ridurci al caso $n = 2$ e $m = 1$.

$$\begin{array}{ccccc} \mathfrak{p}_1 & \subset & \mathfrak{p}_2 & \subset & A \\ \cap & & \cap & & \cap \\ \mathfrak{q}_1 & \subset & \boxed{\mathfrak{q}_2} & \subset & B \end{array}$$

Siano $\bar{A} = A/\mathfrak{p}_1$ e $\bar{B} = B/\mathfrak{q}_1$. Abbiamo che $\bar{B}$ è intero su $\bar{A}$, e per il teorema precedente troviamo $\bar{\mathfrak{q}}^c = \bar{\mathfrak{p}}_2$. Detta $\pi\colon B \to B/\mathfrak{q}_1$, basta porre $\mathfrak{q}_2 = \pi^{-1}(\bar{\mathfrak{q}})$ per ottenere la tesi. □

Siano ora $A$ un dominio, $K$ il suo campo dei quozienti e $L$ un'estensione di $K$. Ha senso chiedersi se la nozione di elemento algebrico su $K$ sia legata a quella di elemento intero su $A$. Infatti, se $x \in L$ è algebrico su $K$ sappiamo che esiste $f \in K[t]$ il suo polinomio minimo. Se $f(t) = t^n + \sum a_i t^i$ e tutti gli $a_i$ sono in $a$ allora $x$ è intero su $A$. Purtroppo il viceversa in generale è falso. Siano $A = \mathbb{Z}[\sqrt{5}]$ (e quindi $K = \mathbb{Q}(\sqrt{5})$) e $x = (1 + \sqrt{5})/2 \in K$. Il polinomio minimo di $x$ su $K$ è $t - x$, che non è a coefficienti in $A$, ma $x$ è comunque intero su $A$. Infatti

$$\left(t - \frac{1+\sqrt{5}}{2}\right)\left(t - \frac{1-\sqrt{5}}{2}\right) = t^2 - t - 1$$

La proprietà è vera se si aggiunge la seguente ipotesi:

**Definizione 2.7.** Un dominio $A$ si dice *integralmente chiuso* o *normale* se è integralmente chiuso nel suo campo dei quozienti $K$, ossia se ogni $x \in K$ intero su $A$ appartiene ad $A$.

Vediamo una classe di domini normale:

**Proposizione 2.8.** Sia $A$ un UFD. Allora è normale.

*Dimostrazione.* Sia $x = p/q$, con $(p, q) = 1$. Da una relazione di dipendenza,

$$\left(\frac{p}{q}\right)^n + \sum_{i=0}^{n-1} a_i \left(\frac{p}{q}\right)^i = 0$$

si ottiene, moltiplicando per $q^n$,

$$p^n + \sum_{i=0}^{n-1} a_i p^i q^{n-i} = 0$$

da cui

$$p^n = -q\left(\sum_{i=0}^{n-1} a_i p^i q^{n-i-1}\right)$$

Di conseguenza, $q \mid p^n$; poiché siamo in un UFD e $(q, p) = 1$, si ha $q \mid p$ da cui $q = 1$.

□

Non è vero il viceversa, per mostrarlo usiamo il seguente Lemma:

**Lemma 2.9.** Sia $A$ un dominio e $K$ il suo campo dei quozienti, se $L/K$ è un'estensione di campi e $B$ la chiusura intera di $A$ in $L$, allora $B$ è integralmente chiuso.

*Dimostrazione.* $B$ è un sottoanello di $L$ e quindi è un dominio, ha senso considerare perciòil suo campo dei quozienti $E \subseteq L$. Se $b \in E$ è intero su $B$ allora è intero anche su $A$ e quindi deve stare in $B$. □

**Esempio 2.10.**

$$\begin{array}{ccc} \mathbb{Z} & \subset & \mathbb{Q} \\ \cap & & \cap \\ \mathbb{Z}[\sqrt{-5}] & \subset & \mathbb{Q}(\sqrt{-5}) \end{array}$$

**Proposizione 2.11.** Sia $A$ un dominio normale e sia $K$ il suo campo dei quozienti. Se $L/K$ è un'estensione algebrica di campi, allora $x \in L$ è intero su $A$ se e solo se $\mu_x$ il polinomio minimo di $x$ su $K$ appartiene a $A[t]$.

*Dimostrazione.* Se il polinomio minimo di $x$ su $K$ è a coefficienti in $A$ allora $x$ è intero su $A$.
Viceversa, sia $x$ intero su $A$ e sia

$$p(t) = t^n + \sum a_i t^i$$

una relazione di interezza di grado minimo. Sia $\mu_x$ il polinomio minimo di $x$ su $K$ e fissiamo una chiusura algebrica $\bar{L} \supseteq L \supseteq K \supseteq A$. Per definizione di polinomio minimo $\mu_x \mid p$ e dunque ogni radice di $\mu_x$ è anche radice di $p$. Di conseguenza $p$ è una relazione di interezza per ogni radice di $\mu_x$. Ogni radice in $\bar{L}$ del polinomio minimo $\mu_x$ perciò è intera su $A$, allora il polinomio minimo è a coefficienti in $A$. Ma i coefficienti sono combinazioni delle radici e dunque elementi interi su $A$ appartenenti a $K$; $A$ è integralmente chiuso in $K$ e dunque è proprio a coefficienti in $A$. □

Con queste ipotesi vale anche un teorema analogo al Going Up per le catene discendenti finite di ideali primi. In generale, infatti, una simile proprietà non vale. Consideriamo la cubica in $\mathbb{C}^3$ data da $f(x, y, z) = y^2 - x^3 - x^2$. L'omomorfismo

$$A = \mathbb{C}[x, y, z]/(y^2 + x^3 + x^2) \longrightarrow B = \mathbb{C}[t, z]$$

con $x \mapsto t^2 - 1$ e $y \mapsto t^3 - t^2$ e $z \mapsto z$ rende $B$ intero su $A$. Consideriamo gli ideali

$$\mathfrak{p}_1 = (x - z^2 + 1, y - z^3 + z) \subseteq \mathfrak{p}_2 = (x, y, z - 1)$$

Preso $\mathfrak{q}_2 = (t + 1, z - 1)$ si ha che $\mathfrak{p}_2 = \subseteq A\mathfrak{q}_2$, inoltre esiste un unico ideale $\mathfrak{q}_1$ tale che $\mathfrak{p}_1 = \subseteq A\mathfrak{q}_1$, ma $V(\mathfrak{q}_1) \not\supseteq V(\mathfrak{q}_2)$.

Mostriamo ora un'importante proprietà di questi anelli:

**Lemma 2.12.** Sia $A$ un dominio. Sono equivalenti:

1. $A$ è integralmente chiuso
2. se $\mathfrak{p} \in \mathrm{Spec}(A)$ allora $A_\mathfrak{p}$ è integralmente chiuso
3. se $\mathfrak{m} \in \mathrm{SpecMax}(A)$ allora $A_\mathfrak{m}$ è integralmente chiuso

*Dimostrazione.*

$(1 \Rightarrow 2)$ Consideriamo $A \subset A_\mathfrak{p} \subset K$. Sappiamo che $\overline{A}^K = A$, ma posto $S = A \setminus \mathfrak{p}$ per la Proposizione 1.8 si ha

$$\overline{A}_p = \overline{S^{-1}A} = S^{-1}\overline{A} = S^{-1}A = A_\mathfrak{p}$$

e dunque $A_p$ è integralmente chiuso.

$(2 \Rightarrow 3)$ Ovvio.

$(3 \Rightarrow 1)$ Se $x \in K$ è intero su $A$ in particolare è intero su $A_\mathfrak{m} \supset A$, quindi

$$x \in M = \bigcap_{\mathfrak{m} \in \mathrm{SpecMax}\, A} A_\mathfrak{m} \supseteq A$$

Basta mostrare che $M \subset A$ per concludere. Sia dunque per assurdo $x \in M \setminus A$ e consideriamo l'ideale

$$I = \{a \in A \mid ax \in A\}$$

che è proprio perché $x \notin A$. Esiste allora un ideale massimale $\mathfrak{m}$ tale che $I \subset \mathfrak{m}$. Dato che $x \in M \subset A_\mathfrak{m}$ possiamo scrivere $x = y/s$ con $y \in A$ e $s \notin \mathfrak{m}$, e a maggior ragione $s \notin I$. Ciò è assurdo perché $sx = y \in A$.

□

L'interezza può essere trattata anche rispetto ad ideali:

**Definizione 2.13.** Sia $A \subset B$ e $I$ un ideale di $A$. Un elemento $x \in B$ è *intero su* $I$ se esiste $f(t) = t^n + \sum a_i t^i$ tale che $f(x) = 0$ e $\forall i\ a_i \in I$.

**Lemma 2.14.** Sia $I \subset A \subset B$ e $I$ un ideale di $A$. Allora detta $C$ la chiusura integrale di $A$ in $B$

$$\overline{I} \coloneqq \{x \in B \mid x \text{ è intero su } I\} = \sqrt[C]{(I)_C}$$

dove $(I)_C = IC$ è l'ideale generato da $I$ in $C$ e con $\sqrt[C]{\ }$ intendiamo il radicale in $C$.

*Dimostrazione.* Mostriamo l'inclusione $\overline{I} \subseteq \sqrt[C]{(I)_C}$. Se $x \in \overline{I}$, allora $x$ è intero su $A$ e dunque esiste una relazione $x^n = \sum a_i x^i \in (I)_C$. Quindi $x \in \sqrt[C]{(I)_C}$. Viceversa, supponiamo che $x \in \sqrt[C]{(I)_C}$. Allora $x^n = \sum c_i x_i \in (I)_C$ con gli $x_i \in I$ e gli $c_i \in C$. Consideriamo l'$A$-modulo $M = A[c_1, \ldots, c_n]$. $M$ è finitamente generato come $A$-modulo; definiamo l'omomorfismo di $A$-moduli

$$\begin{array}{rccc} \Phi\colon & M & \longrightarrow & M \\ & m & \longmapsto & x^n m \end{array}$$

Notiamo che $\varphi(M) \subset IM$: per il teorema di Hamilton-Cayley esistono $b_1, \ldots, b_z \in I$ tali che $\varphi^z + \sum b_i \varphi^i = 0$. Dunque $x^{nz} + \sum b_i x^{ni} = 0$ da cui la tesi. □

È vero un analogo della Proposizione 2.11:

**Lemma 2.15.** Sia $A$ integralmente chiuso, $K$ il suo campo dei quozienti, $K \subset L$ un'estensione algebrica di campi. $x \in L$ e $I$ un ideale di $A$. Allora $x$ è intero su $I$ se e solo se il polinomio minimo $\mu_x$ di $x$ su $K$ è della forma $t^n + \sum a_i t^i$, con gli $a_i \in \sqrt{I}$

*Dimostrazione.* Indichiamo con $B$ gli elementi in $L$ interi su $A$, il polinomio minimo $\mu_x$ di $x$ da una relazione di interezza su $A$, inoltre $x^n = -\sum a_i x^i \in IB$. Allora $x \in \sqrt{IB}$, che per il lemma precedente è equivalente alla tesi.
Viceversa, se $x$ è intero su $I$ con gli stessi ragionamenti della Proposizione 2.11 abbiamo che i coefficienti di $\mu_x$ sono interi su $I$. Allora per ogni $j$ $a_j \in \sqrt[\bar{A}]{(I)_{\bar{A}}} = \sqrt{I}$ visto che $A$ è integralmente chiuso. □

Per dimostrare il teorema del Going-Down, abbiamo bisogno del seguente lemma:

**Lemma 2.16.** Sia $\varphi\colon A \to B$ un omomorfismo di anelli e sia $\mathfrak{p}$ un primo di $A$. Allora $\mathfrak{p}$ è la contrazione di un ideale primo $\mathfrak{q}$ di $B$ se e solo se $\mathfrak{p}^{ec} = \mathfrak{p}$.

*Dimostrazione.*

- $\Rightarrow$ Dalla relazione $\mathfrak{q}^c = \mathfrak{p}$, ricaviamo $\mathfrak{p}^{ec} = (q^c)^{ec} = \mathfrak{q}^{cec} = \mathfrak{q}^c = p$, come voluto.
- $\Leftarrow$ Sia $S = A \setminus \mathfrak{p}$. Consideriamo il diagramma

$$\begin{array}{ccc} A & \longrightarrow & S^{-1}A \\ \downarrow & & \downarrow \\ B & \longrightarrow & S^{-1}B \end{array}$$

Dato che $\mathfrak{p}^{ec} = \mathfrak{p}$, $\mathfrak{p}^e$ non interseca $S$ e dunque in $S^{-1}B$ $\mathfrak{p}^e$ è un ideale proprio. Dunque è contenuto in un massimale $\mathfrak{q}$ di $S^{-1}B$. Per commutatività del diagramma, la contrazione di $\mathfrak{q}$ in $S^{-1}A$ deve essere un ideale primo di $S^{-1}A$ che contiene $\mathfrak{p}$ e dunque coincide con $\mathfrak{p}$. Dunque $\mathfrak{q}^c = \mathfrak{p}$.

□

**Teorema 2.17** (Going Down)**.** Siano $A \subset B$ domini con $A$ integralmente chiuso e $B$ intero su $A$. Siano $\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{Spec} A$ tali che $\mathfrak{p}_1 \subset \mathfrak{p}_2$ e sia $\mathfrak{q}_2 \in \operatorname{Spec} B$ tale che $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. Allora esiste $\mathfrak{q}_1 \in \operatorname{Spec} B$ tale che $\mathfrak{q}_1 \subset \mathfrak{q}_2$ e $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.

$$\begin{array}{ccccc} \mathfrak{p}_1 & \subset & \mathfrak{p}_2 & \subset & A \\ \cap & & \cap & & \cap \\ \boxed{\mathfrak{q}_1} & \subset & \mathfrak{q}_2 & \subset & B \end{array}$$

*Dimostrazione.* Sia $S = B \setminus \mathfrak{q}_2$. Per il Lemma 2.16, basta mostrare che $\mathfrak{p}_1^{ec} = (S^{-1}\mathfrak{p}_1 B) \cap A = \mathfrak{p}_1$: in tal caso infatti esisterebbe un primo $\mathfrak{q} \in S^{-1}B$ tale che $\mathfrak{q} \cap A = \mathfrak{p}_1$ e per corrispondenza avremmo che $\mathfrak{q}_2 = \mathfrak{q} \cap B$ sarebbe il primo cercato.

$$\begin{array}{ccccc} \mathfrak{p}_1 & \subset & \mathfrak{p}_2 & \subset & A \\ \cap & & \cap & & \cap \\ \boxed{\mathfrak{q}_1} & \subset & \mathfrak{q}_2 & \subset & B \\ \cap & & \cap & & \cap \\ \mathfrak{q} & \subset & {\mathfrak{q}_2}^e & \subset & B \end{array}$$

Mostriamo che $\mathfrak{p}_1$ soddisfa le ipotesi del Lemma 2.16. Ovviamente $\mathfrak{p}_1 \subseteq \mathfrak{p}_1^{ec}$. Sia ora $x \in \mathfrak{p}_1^{ec}$. Allora $x \in \mathfrak{p}_1^e \cap A \subseteq \mathfrak{p}_1^e$, per cui $x = y/s$ con $y \in \mathfrak{p}_1 B$ e $s \in B \setminus \mathfrak{q}_2 = S$. Poiché $y$ è intero su $A$, il suo polinomio minimo su $K$ $f(t) = t^n + \sum a_i t^i$ è a coefficienti $a_i \in A$, e dato che $y \in \mathfrak{p}_1 B \subset \sqrt{\mathfrak{p}_1 B}$ sappiamo anche che $y$ è intero su $\mathfrak{p}_1$. Calcoliamo il polinomio minimo di $s = y/x$ su $K$. Dalla relazione

$$y^n + \sum_{i=0}^{n-1} a_i y^i = 0$$

dividendo per $x^n$ troviamo

$$s^n + \sum_{i=0}^{n-1} \frac{a_i}{x^{n-i}} s^i = 0$$

Il polinomio $p(t) = t^n + \sum a_i t^i / x^{n-i} \in K[t]$ è il polinomio minimo di $s$ su $K$; se ce ne fosse uno di grado minore ne otterremmo uno di grado minore anche per $y$ moltiplicando per una potenza di $x$ opportuna[3]. Ricordando

[3] Ad esempio da $s^2 = 1$ otterremmo $y^2 = x^2$.

che $s \in B \setminus \mathfrak{q}_2 \subset B$, si ottiene che $s$ è intero su $A$, per cui $b_i = a_i/x^{n-i} \in A$ e $\mathfrak{p}_i \ni a_i = x^{n-i}b_i$. Se fosse $x \notin \mathfrak{p}_1$ allora $b_i \in \mathfrak{p}_1$, quindi $s$ sarebbe intero anche su $\mathfrak{p}_1$, per cui avremmo l'assurdo

$$s \in \sqrt{B\mathfrak{p}_1} \subset \sqrt{B\mathfrak{p}_2} \subset \sqrt{\mathfrak{q}_2} = \mathfrak{q}_2$$

□