# Chapter VII

## Integral extensions

Goal: define the correct analogue, for general rings, of algebraic extensions of fields, and of algebraic elements. One cannot simply say that (say) $x \in \mathbb{C}$ is "algebraic over $\mathbb{Z}$" if there is $P \neq 0$ in $\mathbb{Z}[X]$ s.t. $P(x) = 0$, because then there would be no difference with $x$ algebraic over $\mathbb{Q}$.

### 1 - Integral elements [ACL 4.1]

**Definition** - Let $s : R \longrightarrow A$ be an $R$-algebra. An element $a \in A$ is integral over $R$ if there exists a polynomial $P \in R[X]$ which is monic [or has leading term in $R^\times$] and satisfies $P(a) = 0$.

**Examples** - (1) If $L/K$ is a field extension, then $x \in L$ is integral over $K$ if and only if $x$ is algebraic over $K$.

(2) Let $R = \mathbb{Z} \subset A = \mathbb{Q}$. Then $a = \frac{1}{2} \in \mathbb{Q}$ is not integral over $\mathbb{Z}$ [although it is of course "algebraic" in the sense that $2 \cdot a - 1 = 0$].

Indeed, more generally:

**Proposition** - Let $R$ be a UFD with fraction field $K$. Any $a \in K$ that is integral over $R$ is in $R$.

**Proof** - Let $n \geq 1$ and $P = X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ in $R[X]$ be such that $P(a) = 0$. So

$$a^n + a_{n-1} a^{n-1} + \dots + a_1 a + a_0 = 0.$$

Write further $a = \frac{\alpha}{\beta}$ with $\alpha, \beta$ in $R$, $\beta \neq 0$ and $\alpha, \beta$ coprime [this uses the fact that $R$ is a UFD]. Then, multiplying by $\beta^n$,

we get

$$\alpha^n + a_{n-1}\alpha^{n-1}\beta + \dots + a_1\alpha\beta^{n-1} + a_0\beta^n = 0$$

Modulo $\beta$ we deduce $\beta \mid \alpha^n$, which implies that $\beta \in R^\times$ since $\beta$ is coprime to $\alpha^n$.

□

(3) For $n \geq 1$, $\zeta = e^{2i\pi/n}$ is integral over $\mathbb{Z}$ since $\zeta^n = 1$.

The element $\omega = \frac{1+i\sqrt{3}}{2} \in \mathbb{Z}$ is integral over $\mathbb{Z}$ since

$$\omega^2 = \frac{1}{4}(1 + 2i\sqrt{3} - 3) = \frac{-1+i\sqrt{3}}{2} = \omega - 1.$$

[ACL 4.1.5]

**Proposition** - Let $s : R \longrightarrow A$ be an $R$-algebra, and let $a \in A$ and $B = R[a] \subset A$ the subalgebra generated by $a$. ( $B$ is the image of the morphism $R[X] \xrightarrow{f} A$ s.t. $f(X) = a$ ]

Then: (i) $a$ integral over $R$

$\Leftrightarrow$ (ii) $R[a]$ is a finitely-generated $R$-module

$\Leftrightarrow$ (iii) There exists an $R[a]$-module $M$ with $\{ x \in R[a] \mid xM = 0 \} = \{0\}$ (*) such that $M$ is a finitely-generated $R$-module.

Proof - (i) $\Rightarrow$ (ii): let $P \in R[x]$ be a monic polynomial with $P(a) = 0$. Let $d = \deg(P)$. Then the subalgebra $R[a]$ is generated by $1, a, \dots, a^{d-1}$ as an $R$-module [since $P(a) = 0$ implies $a^d \in R + aR + \dots + a^{d-1}R$, and by induction $a^k \in R + \dots + a^{d-1}R$ for all $k \geq 0$.]

(ii) $\Rightarrow$ (iii): note simply that $M = R[a]$ has the desired properties, since $xM = 0$ implies in particular $x \cdot 1_R = x = 0$.

(iii) $\Rightarrow$ (i): let $M$ be given by (iii); define $u: M \longrightarrow M$ by $u(m) = am$. This is an $R$-linear map, and since $M$ is finitely-generated, there exists $f \in R[X]$ monic

with $f(u) = 0$. Then for all $m \in M$, we get

$$f(u)(m) = f(a)\, m = 0, \quad \text{so} \quad f(a) = 0$$

by the assumption (*). [Why does $f$ exist? if $M$ is free, one can take $f = \det(X - u)$ by the Cayley-Hamilton Theorem; in general, fixing a generating set $(x_1, \ldots, x_r)$ of $M$ as $R$-module, we get a commutative diagram

$$\begin{array}{ccc} R^r & \xrightarrow{v} & R^r \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha} \\ M & \xrightarrow{u} & M \end{array}$$

with $\alpha(a_1, \ldots, a_r) = \sum a_i x_i$ and $v$ determined by $v(e_i) = (u_{i1}, \ldots, u_{ir})$ where $u(x_i) = \sum_j u_{ij} x_j$. Then taking $f = \det(T - v)$, one gets $f(v) = 0$, and it follows that $f(u) = 0$ also because $\alpha$ is surjective and $f(u \circ \alpha) = \alpha \circ f(v) = 0$.]

□

Note - The condition (*) is necessary : for example, take $R = \mathbb{Z}$, $A = \mathbb{Q}$ and $a = \frac{1}{2}$, which is not integral over $\mathbb{Z}$. Then $M = \mathbb{Z}/3\mathbb{Z}$ is a finitely-generated $\mathbb{Z}[\frac{1}{2}]$-module [because $2 = -1$ has an inverse in $\mathbb{Z}/3\mathbb{Z}$].

## 2. Integral extensions

**Definition** - An $R$-algebra $A$ [with structure morphism $s: R \longrightarrow A$] is **integral over $R$** if all elements of $A$ are integral over $R$.

**Proposition / definition** - Let $A$ be an $R$-algebra. The set $B \subset A$ of all $a \in A$ which are integral over $R$ is a subalgebra of $A$, which is integral over $R$; it is called the **integral closure** of $R$ in $A$.

**Proof** - One needs to show that if $a_1, a_2$ in $A$ are $R$-integral, then so are $a_1 a_2$ and

$a_1 + a_2$. But $a_1 a_2$ and $a_1 + a_2$ are in $R[a_1, a_2]$ $= R[a_1][a_2]$ and this is finitely-generated as an $R$-module [because $a_1, a_2$ are integral over $R$ so $a_2$ is integral over $R[a_1]$; if $(x_i)$ generate $R[a_1]$ as $R$-module and $(y_j)$ generate $R[a_1][a_2]$ as $R[a_1]$-module, then $(x_i y_j)$ generate $R[a_1][a_2]$ as $R$-module].

Moreover, $x\, R[a_1, a_2] = \{0\} \Rightarrow x \cdot 1 = 0$ so the previous criterion shows that $a_1, a_2$ and $a_1 + a_2$ are indeed integral over $R$.

□

**Definition** - Let $R \subset A$ be rings. Then $R$ is **integrally closed in $A$** if its integral closure in $A$ is $R$ itself. [It always contains $R$].

If $R$ is an **integral domain**, it is said to

be integrally-closed if it is so in its fraction field.

Example - (1) We have seen that if $R$ is a UFD, then it is integrally closed.

More generally:

Lemma - If $R$ is integrally-closed and $S$ is a multiplicative set with $0 \notin S$, then $S^{-1}R$ is integrally closed. [in particular, an integral domain]

Proof - The fraction field of $S^{-1}R$ is the same as the fraction field $K$ of $R$.

Let $x = \frac{a}{b}$ be an element of $K$, integral over $S^{-1}R$; suppose

$$x^n + \frac{a_{n-1}}{s_{n-1}} x^{n-1} + \cdots + \frac{a_0}{s_0} = 0$$

with $s_i \in S$. Then multiplying this equation by $(s_0 \cdots s_{n-1})^n$, we get an equation

$$(sx)^n + b_{n-1}(sx)^{n-1} + \cdots + b_0 = 0$$

in $R$, where $s = s_0 \cdots s_{n-1}$ and $b_i \in R$.

So $sx$ is integral over $R$, which means that $sx \in R$ since $R$ is integrally closed, so $x \in S^{-1}R$.

□

(2) Let $R$ be a ring and $f \in R[X]$ a monic polynomial. Then $A = R[X]/(f)$ is an integral $R$-algebra. (For instance, $\mathbb{Z}[i]$ or $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ are integral over $\mathbb{Z}$.)

Indeed, $A$ is generated as an $R$-algebra by the class $x \in A$ of the variable $X$, and we have $f(x) = 0$ in $A$, so $x$ is integral over $R$, hence the integral closure of $R$ in $A$ contains (so must be equal to) $A$.

The following proposition summarizes a few useful properties of integral extensions.

as algebra!

**Proposition** - (1) Let $A$ be a finitely-generated $R$-algebra. Then $A$ is integral over $R$ $\iff$ $A$ is finitely-generated as an $R$-module.

(2) Let $B$ be integral over $A$ and $A$ integral over $R$. Then $B$ is integral over $R$.

(3) If $A$ is integral over $R$ and $S \subset R$ is multiplicative, then $S^{-1}A$ is integral over $S^{-1}R$.

$S^{-1}A = f(S)^{-1}A$, $f: R \to A$

(4) If $s: R \longrightarrow A$ is integral and $I \subset R$ is an ideal and $J \subset A$ satisfies $s(I) \subset J$ then $R/I \longrightarrow A/J$ is integral.

**Proof.** We only give basic hints. For (1) and (2), we have statements that are very similar to known facts for algebraic field extensions, and the proofs are the same. (For instance, for $\Rightarrow$ in (1): if $A = R[a_1, \dots, a_m]$ is

integral over $R$, then $R[a_1]$ is a f.g. $R$-module, then $R[a_1, a_2] = R[a_1][a_2]$ also, etc...)

(3) Let $x = \frac{a}{s} \in S^{-1}A$; then there is an equation

$$a^n + r_{n-1}a^{n-1} + \dots + r_1 a + r_0 = 0$$

with $r_i \in R$; then

$$\left(\frac{a}{s}\right)^n + \frac{r_{n-1}}{s}\left(\frac{a}{s}\right)^{n-1} + \dots + \frac{r_1}{s^{n-1}}\frac{a}{s} + \frac{r_0}{s^n} = 0$$

$\frac{r_0}{s^n}$ → in $S^{-1}R$

so $x$ is integral over $S^{-1}R$.

(4) Let $y \in A/J$ be the class of $x \in A$;

let $x^n + r_{n-1}x^{n-1} + \dots + r_1 x + r_0 = 0$;

then $y^n + r_{n-1}y^{n-1} + \dots + r_1 y + r_0 = 0$

and $y^n + s_{n-1}y^{n-1} + \dots + s_1 y + s_0 = 0$

where $s_i$ is the class of $r_i$ in $A/I$.

□

## 3- Integrality and dimension

**Theorem-** Let $R \subset A$, $A$ integral over $R$.

Then $\dim(A) = \dim(R)$.

In fact, more precisely, we have:

[ACL 9.3.9; 9.3.10 "going up" theorem of Cohen-Seidenberg]

For any prime chain $q_0 \subsetneq \dots \subsetneq q_m$ in $A$, we have $q_0 \cap R \subsetneq \dots \subsetneq q_m \cap R$.

For any prime chain $p_0 \subsetneq \dots \subsetneq p_m$ in $R$, there is a prime chain $q_0 \subsetneq \dots \subsetneq q_m$ in $A$ with $p_i = q_i \cap R$.

(In particular, $q \subset A$ is maximal $\iff q \cap R$ is maximal.)

The proof will require a few steps. First, note that the "More precisely" does show that $\dim(A) = \dim(R)$, since prime chains in $A$ of length $m$ lead to prime chains in $R$ of length $m$, and conversely. (Note: we are not saying that $q \longmapsto q \cap R$ is a bijection!)

**Example.** This theorem gives us immediately many new examples of known dimension. For instance, $A = \mathbb{Z}[x]/(x^n - 1)$ is integral over $\mathbb{Z}$, contains $\mathbb{Z}$, so $\dim A = \dim \mathbb{Z} = 1$. Similarly, $\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2 - 5)$ has dimension 1.

We now prove the theorem in steps.

**Step 1.** If $A$ is an integral domain, then

$\dim(A) = 0 \iff \dim(R) = 0$. (I.e. $A$ is a field $\iff R$ is a field)

**Proof.** Suppose $A$ is a field. Let $x \neq 0$ be an element of $R$, and $x^{-1} \in A$ its inverse. Let

$$(x^{-1})^n + r_{n-1}(x^{-1})^{n-1} + \cdots + r_1 x^{-1} + r_0 = 0$$

be an equation satisfied by $x^{-1}$. Then

$$1 + r_{n-1}x + \cdots + r_1 x^{n-1} + r_0 x^n = 0$$

so

$$x \cdot \underbrace{\left(-r_{n-1} - \cdots - r_1 x^{n-2} - r_0 x^{n-1}\right)}_{\in R} = 1$$

which shows that $x^{-1} \in R$.

Suppose now that $R$ is a field. Let $a \in A$ be non-zero, and let

$$a^n + r_{n-1} a^{n-1} + \cdots + r_1 a + r_0 = 0$$

be an equation satisfied by $a$. Since $a \neq 0$, we can assume that $r_0 \neq 0$ (otherwise, since $A$ is an integral domain, we can cancel $a$ to get a lower-degree equation, and repeat).

So $a\left(-r_0^{-1}\left(a^{n-1} + r_{n-1} a^{n-2} + \cdots + r_1\right)\right) = 1$, with $-r_0^{-1}\left(a^{n-1} + r_{n-1} a^{n-2} + \cdots + r_1\right) \in A$,

which gives $a \in A^\times$.

□

Step 2. $q \subset A$ is maximal if and only if $q \cap R \subset R$ is maximal.

Proof. Indeed, observe that we have an injective integral morphism $R/_{q \cap R} \longrightarrow A/_q$, with $A/_q$ an integral domain, so the result follows

from Step 1.

□

(Note: in particular, it follows that $\dim(A) = 0$ if $\dim(R) = 0$, since this means that $A \neq \{0\}$ and all prime ideals are maximal.)

Step 3. The map $q \xrightarrow{f} q \cap R$ from prime ideals in $A$ to prime ideals in $R$ is "injective on chains": if $q_1 \subset q_2$ then

$$f(q_1) = f(q_2) \iff q_1 = q_2.$$

(It is not injective in general: for instance in $\mathbb{Z}[i]$, we have $(1+2i) \cap \mathbb{Z} = (1-2i) \cap \mathbb{Z} = 5\mathbb{Z}$)

Proof. We start with $q \subset A$ prime and define $p = q \cap R$.

Claim. The ideal $qA_p \subset A_p$ is maximal, where $A_p = \underbrace{(R-p)^{-1}}_{\text{multiplicative in } A} A$.

Assume this: Then we have, for $p = q_1 \cap R = q_2 \cap R$ with $q_1 \subset q_2$ that

$$q_1 A_p \subset q_2 A_p$$

and both are maximal, so $q_1 A_p = q_2 A_p$. But $q \longmapsto q A_p$ is bijective from prime ideals of $A$ not intersecting $R - p$ to prime ideals in $A_p$, so we conclude $q_1 = q_2$.

To prove the Claim, observe that

$$q A_p \cap R_p \supset p R_p$$

which is maximal, and $q A_p \subset q A_q$ so $1 \notin q A_p \cap R_p$, hence $q A_p \cap R_p = p R_p$ is maximal. But note the integral morphism

$$R_p \longrightarrow A_p$$

so by Step 2, $q A_p \cap R_p$ maximal implies that $q A_p$ is also maximal.

□

Step 4 - Any prime chain $q_0 \subsetneq \dots \subsetneq q_m$ in $A$ gives a prime chain $q_0 \cap R \subsetneq \dots \subsetneq q_m \cap R$ in $R$.

This follows immediately from Step 3.

Step 5 - The map $q \longmapsto q \cap R$ is surjective from prime ideals in $A$ to those of $R$.

Proof - Let $p \subset R$ be prime. Now consider again the morphism $R_p \longrightarrow A_p = (R-p)^{-1}A$. It is integral, and injective. So $A_p \neq \{0\}$ and we can find a maximal ideal $m \subset A_p$. Let $q = m \cap A$. Then $q$ is prime and $q \cap (R-p) = \emptyset$ so $f(q) = q \cap R \subset p$. But, on the other hand, $m \cap R_p$ is maximal according to Step 2, so $m \cap R_p = pR_p$, so

$$p \subset pR_p = m \cap R_p \subset m$$

and so $p \subset m \cap R = (m \cap A) \cap R = q \cap R$.

□

Step 6 - For any prime chain

$$p_0 \subsetneq \cdots \subsetneq p_m \subset R$$

there is a prime chain $q_0 \subsetneq \cdots \subsetneq q_m \subset A$ such that $q_i \cap R = p_i$ for all $i$.

(The last step of the proof!)

Proof - By induction on $m$: the case $m = 0$ is given by Step 5, and it is clear that if then is enough to handle the case $m = 1$: given

$$\left.\begin{array}{l} q_0 \\ p_0 \subsetneq p_1 \end{array}\right) \quad q_0 \cap R = p_0$$

we need to find $q_1$ with $q_1 \cap R = p_1$ and $q_0 \subset q_1$. We do this by considering the integral morphism $R/p_0 \longrightarrow A/q_0$; there is a prime ideal $\tilde{q}_1 \subset A/q_0$ s.t. $\tilde{q}_1 \cap (R/p_0) = p_1/p_0$, and $\tilde{q}_1 = q_1/q_0$ where $q_1 \subset A$ is prime with $q_1 \cap R = p_1$

and with $q_0 \subset q_1$.

□

## 4. Heights of ideals

Parallel to the dimension property, integral extensions also have very good properties with respect to heights.

**Theorem.** Let $R \subset A$ be integral domains, with

(i) $A$ integral over $R$

(ii) $R$ integrally closed

Then we have $ht(q \cap R) = ht(q)$ for all prime ideals $q \subset A$.

In fact, more precisely:

["going down theorem"; ACL 9.5.2]

For any prime chain $p_0 \subsetneq \dots \subsetneq p_m$ in $R$ and any $q_m \subset A$ prime such that $q_m \cap R = p_m$, there exists $q_0 \subsetneq \dots \subsetneq q_m \subset A$ (primes) such

that $p_i = q_i \cap R$ for all $i$.

Note first here also that the more precise statement implies the first statement: for any prime chain $p_0 \subsetneq \cdots \subsetneq p_m = q \cap R$, we can find $q_0 \subsetneq \cdots \subsetneq q_{m-1} \subsetneq q$ in $A$, so that $ht(q) \geq ht(q \cap R)$; conversely, the previous theorem (esp. Step 3) shows that any prime chain $q_0 \subsetneq \cdots \subsetneq q_m = q$ in $A$ gives a prime chain $q_0 \cap R \subsetneq \cdots \subsetneq q \cap R$ in $R$ of the same length, so $ht(q \cap R) \geq ht(q)$.

The proof of this theorem relies on a result of independent interest.

Proposition - [ACL 9.5.1]

Let $R$ be integrally closed with fraction field $K$. Let $L/K$ be a normal field extension (not necessarily Galois: it may not be

separable) and let $A \subset L$ be the integral closure of $R$ in $L$.

Let $p \subset R$ be prime. The automorphism group $\mathrm{Aut}(L/K)$ acts on prime ideals $q \subset A$ such that $q \cap R = p$ by $\sigma \cdot q = \sigma(q) \subset A$; this action is transitive (i.e., for any $q_1, q_2$ s.t. $q_i \cap R = p_i$, we can find $\sigma \in \mathrm{Aut}(L/K)$ with $\sigma(q_1) = q_2$).

$$\begin{array}{ccc} A & \subset & L \\ | & & | \\ R & \subset & K \end{array}$$

Proof - We prove this only if $L/K$ is separable (so is a Galois extension; this is true for instance if $K$ has characteristic zero) and $[L:K]$ is finite. (The statement is true in general but needs infinite Galois theory.)

Step 1. For $\sigma \in \mathrm{Aut}(L/K)$, we have $\sigma(A) = A$ and for $I \subset A$ ideal, $\sigma(I) \cap R = I \cap R$, and $\sigma$ induces an isomorphism $A/I \longrightarrow A/\sigma(I)$.

(In particular, the action in the statement is well-defined).

Indeed, if $x \in A$ then from an equation

$$x^n + r_{n-1} x^{n-1} + \cdots + r_1 x + r_0 = 0$$

with $r_i \in R \subset K$, we obtain

$$\sigma(x)^n + \cdots + r_1 \sigma(x) + r_0 = 0$$

(since $\sigma \in \mathrm{Aut}(L/K)$, so $\sigma$ is the identity on $R$)

hence $\sigma(x)$ is integral over $R$, which means $\sigma(x) \in A$. So $\sigma(A) \subset A$, and applying $\sigma^{-1}$ we get equality.

Finally, $\sigma(I) \cap R = \sigma(I \cap R) = I \cap R$, and $\sigma$ gives $A \xrightarrow{\sigma}_{\sim} A \longrightarrow A/\sigma(I)$ with kernel $I$.

Step 2. Let $p \subset R$ be prime and let $q_1, q_2$ in $A$ be prime with $q_i \cap R = p$. We have

$$q_2 \subset \bigcup_{\sigma \in \mathrm{Aut}(L/K)} \sigma(q_1).$$

Indeed, let $x \in q_2$ be given. We define

$$y = \prod_{\sigma \in \mathrm{Aut}(L/K)} \sigma(x)$$

finite group

By Galois theory, from the relation $\sigma(y) = y$ for all $\sigma \in \mathrm{Aut}(L/K)$, we deduce $y \in K$. But moreover $y$ is integral over $R$, since $\sigma(x) \in A$ for all $\sigma$, so $y \in R$ since $R$ is integrally closed in $K$ by assumption. Finally, $y \in q_2$ (from the factor $x \in q_2$) so

$$y \in q_2 \cap R = q_1 \cap R \subset q_1.$$

Since $q_1$ is prime, this means that some $\sigma(x)$ belongs to $q_1$, finishing this step.

Step 3. We conclude that $q_2 \subset \sigma(q_1)$ for some $\sigma \in \mathrm{Aut}(L/K)$ using the useful lemma below; from $q_2 \cap R = \sigma(q_1) \cap R = p$, Step 3 of the previous theorem implies equality

$$q_2 = \sigma(q_1).$$

**Lemma.** [ACL 2.2.12] Let $R$ be a ring and $I \subset R$ an ideal, $p_1, \dots, p_m \subset R$ prime ideals. If $I \subset \bigcup p_i$, then there is an $i$ such that $I \subset p_i$.

**Proof.** We use induction on $m \geq 1$. The case $m = 1$ is tautological; assume $m \geq 2$ and the result for $m - 1$. If the conclusion fails, then induction implies $I \not\subset \bigcup_{j \neq i} p_j$ for all $i$; pick $x_i \in I$ s.t. $x_i \notin p_j$ for $j \neq i$. Then $x_i$ must be in $p_i$ since $I \subset \bigcup_i p_i$.

Define $$x = x_1 + x_2 \cdots x_m \in I.$$

But $x \equiv x_2 \cdots x_m \not\equiv 0 \mod p_1$, and

$x \equiv x_1 \not\equiv 0 \mod p_i$ for $i \geq 2$, so

$$x \notin \bigcup p_i,$$

a contradiction. □

We can now prove the "going down" theorem.

Step 1. We assume that the extension $L = \mathrm{Frac}(A)$ of $K = \mathrm{Frac}(R)$ is normal.

Then by going up we first get a chain

$$\tilde{q}_0 \subsetneq \dots \subsetneq \tilde{q}_m \subset A$$

with $\tilde{q}_i \cap R = p_i$. Then we find $\sigma \in \mathrm{Aut}(L/K)$ by the Proposition so that $\sigma(\tilde{q}_m) = q_m$; then

$$\sigma(\tilde{q}_0) \subsetneq \dots \subsetneq \sigma(\tilde{q}_m) = q_m$$

satisfies $\sigma(\tilde{q}_i) \cap R = \tilde{q}_i \cap R = p_i$.

Step 2. We consider the general case.

Let again $L = \mathrm{Frac}(A)$, $R = \mathrm{Frac}(K)$. We can find an extension $\tilde{L}/L$ such that $\tilde{L}/K$ is normal. Let $\tilde{A} \subset \tilde{L}$ be the integral closure of $R$ in $\tilde{L}$, so $R \subset A \subset \tilde{A}$.

Since $\tilde{A}$ is integral over $A$, we can find $\tilde{q}_m \subset \tilde{A}$ prime with $\tilde{q}_m \cap A = q_m$. Then by Step 1 applied to $R \subset \tilde{A}$, we

find $\tilde{q}_0 \subsetneq \dots \subsetneq \tilde{q}_m \subset \tilde{A}$ with $\tilde{q}_i \cap R = p_i$. But then let $q_i = \tilde{q}_i \cap A$ (which is consistent for $i = m$); we get

$$q_0 \subsetneq \dots \subsetneq q_m$$

and $q_i \cap R = (\tilde{q}_i \cap A) \cap R = \tilde{q}_i \cap R = p_i$.

This concludes the proof.