Chapter 3

Commutative Rings

3.1 Introduction

The ordinary arithmetic of the integers and simple generalizations (such as the Gaussian Integers) as well as of analogues like the polynomial ring in one variable over a field gave rise to the study of number theory and then to the study of commutative rings. The assumption of commutativity in multiplication makes possible a much deeper theory with more satisfying applications. Nowadays, a thorough knowledge of this Chapter is essential in order to do Algebraic Geometry and Algebraic Number Theory (and their mixture: Arithmetic Algebraic Geometry); one also needs to know the material here for Algebraic Topology. Many of the results are direct consequences of prodding from geometry, physics and number theory. A modern problem is to use our physical knowledge (quantum theory), our knowledge of modules and representation theory, and the hints from the forefront of number theory to augment these results to a new and better theory of not necessarily commutative rings. This endeavor will probably be a big part of the twenty-first century in mathematics.

3.2 Classical Localization

All rings in this chapter are commutative with unity.

Definition 3.1 Let $A \in \mathrm{CR}$ and $S \subseteq A$ be a subset of A. We say that S *is a multiplicative subset in* A iff

(1) $1 \in S$

(2) If $x, y \in S$, then $xy \in S$

(3) $0 \notin S$.

Examples:

(1) $S = \mathbb{G}_m(A) =$ the units of A; the idea is to abstract this case.

(2) $S = \{\alpha \in A \mid \alpha \text{ is not a zero divisor in } A\}$.

(3) $S = \{x \in \mathbb{R} \mid x > 0\} \subseteq \mathbb{G}_m(\mathbb{R})$.

(3a) S has property (1) and (2) and is contained in $\mathbb{G}_m(A)$.

(4) Given $f \in A$, let $S = \{f^n \mid n \in \mathbb{Z},\ n \geq 0\}$ and assume that $f \notin \mathcal{N}(A)$ (i.e., $f^n \neq 0$ for all $n \geq 0$).

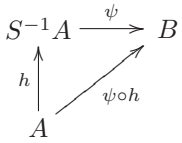
Fix a base ring, C, and look at C-algebras in CR (we get CR when $C = \mathbb{Z}$). Let A and B be C-algebras, where B varies, and let S be a multiplicative subset in A. Look at

$$\mathrm{Hom}_{C-\mathrm{alg}}(A, B; S) = \{\varphi \in \mathrm{Hom}_{C-\mathrm{alg}}(A, B) \mid \varphi(S) \subseteq \mathbb{G}_m(B)\}.$$

Check that $B \rightsquigarrow \mathrm{Hom}_{C-\mathrm{alg}}(A, B; S)$ is a functor from C-algebras to $\mathcal{S}$ets. Is it representable? This means, is there a C-algebra, $S^{-1}A$, and a map (of C-algebras), $h\colon A \to S^{-1}A$, so that

$$\theta_B\colon \mathrm{Hom}_{C-\mathrm{alg}}(S^{-1}A, B) \cong \mathrm{Hom}_{C-\mathrm{alg}}(A, B; S)$$

functorially, where $\theta_B(\psi) = \psi \circ h \in \mathrm{Hom}_{C-\mathrm{alg}}(A, B; S)$, as illustrated below:



Proposition 3.1 *The functor $B \rightsquigarrow \mathrm{Hom}_{C-\mathrm{alg}}(A, B; S)$ is representable. The representing object, $S^{-1}A$, is called the fraction ring of A w.r.t. S (or the localization of A w.r.t. S). The C-algebra map, $h\colon A \to S^{-1}A$, is the canonical map.*

Proof. Look at $A \times S$ (in $\mathcal{S}$ets) and form the equivalence relation, $\sim$, given by:

$$(a, s) \sim (b, t) \quad \text{iff} \quad (\exists u \in S)(u(at - sb) = 0 \quad \text{in } A).$$

Write $\dfrac{a}{s}$ for the equivalence class of (a, s). So,

$$\frac{a}{s} = \frac{b}{t} \quad \text{iff} \quad (\exists u \in S)(u(at - sb) = 0).$$

Define addition and multiplication by:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + sb}{st} \quad \text{and} \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Check that these operations are well defined and that $S^{-1}A$ is a C-algebra $\left(c \cdot \dfrac{a}{s} = \dfrac{f(c)a}{s}\right)$;[1] the C-algebra map, $h\colon A \to S^{-1}A$, is given by $h(a) = \dfrac{a}{1}$.

Functorial part. Given $\psi \in \mathrm{Hom}_{C-\mathrm{alg}}(S^{-1}A, B)$, form $\psi \circ h$ taking A to B. Now, elements of S become units in $S^{-1}A$, because

$$\frac{s}{1} \cdot \frac{1}{s} = \frac{1}{1}, \quad \text{the unit element of } S^{-1}A.$$

But, ψ maps units of $S^{-1}A$ to units of B, so $\psi \circ h \in \mathrm{Hom}_{C-\mathrm{alg}}(A, B; S)$. Next, given $\varphi \in \mathrm{Hom}_{C-\mathrm{alg}}(A, B; S)$, define

$$[\varphi]\left(\frac{a}{s}\right) = \varphi(s)^{-1}\varphi(a) \in B.$$

Check

(a) The homomorphism $[\varphi]\colon S^{-1}A \to B$ is well defined.

(b) θ_B and $\varphi \mapsto [\varphi]$ are inverse maps. $\square$

[1] Here, $f\colon C \to A$ is the ring homomorphism making A into a C-algebra.

We can do the same thing with modules. Let M be an A-module and S a multiplicative set in A. Make $(M \times S)/\sim$, where $\sim$ is given by

$$(m,s) \sim (n,t) \quad \text{iff} \quad (\exists u \in S)(u(tm - sn) = 0 \quad \text{in } M).$$

Write $\dfrac{m}{s}$ for the equivalence class of (m,s). Define addition and the action of A by

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'} \quad \text{and} \quad a \cdot \frac{m}{s} = \frac{am}{s}.$$

This gives the A-module, $S^{-1}M$. We have the canonical map, $h\colon M \to S^{-1}M$, given by $h(m) = m/1$.

To discuss what this means, look at the general case of a ring homomorphism, $\psi\colon A \to B$. We have two functors: $\psi^\bullet\colon \mathcal{M}\mathrm{od}(B) \rightsquigarrow \mathcal{M}\mathrm{od}(A)$ (*the backward image functor*) and $\psi_\bullet\colon \mathcal{M}\mathrm{od}(A) \rightsquigarrow \mathcal{M}\mathrm{od}(B)$ (*the forward image functor*). Here, $\psi^\bullet(M) = M$ as an A-module *via* ψ; that means $a \cdot m = \psi(a) \cdot m$. The functor $\psi^\bullet$ is an exact functor. Also, the functor $\psi_\bullet$ is given by: $\psi_\bullet(M) = B \otimes_A M$. The forward image functor is only right-exact, in general. These functors form a pair of adjoint functors:

$$\mathrm{Hom}_B(\psi_\bullet(M), N) \cong \mathrm{Hom}_A(M, \psi^\bullet(N)).$$

Proposition 3.2 *The module $S^{-1}M$ is, in a natural way, an $S^{-1}A$-module. The map $M \rightsquigarrow S^{-1}M$ is a functor from $\mathcal{M}\mathrm{od}(A)$ to $\mathcal{M}\mathrm{od}(S^{-1}A)$ and is left-adjoint to $h^\bullet$. That is,*

$$\mathrm{Hom}_{S^{-1}A}(S^{-1}M, N) \cong \mathrm{Hom}_A(M, h^\bullet(N)).$$

Consequently,

$$S^{-1}M \cong S^{-1}A \otimes_A M \cong M \otimes_A S^{-1}A = h_\bullet(M).$$

Proof. Let $\dfrac{a}{t} \cdot \dfrac{m}{s} = \dfrac{am}{ts}$, this is well-defined and makes $S^{-1}M$ into an $S^{-1}A$-module. If $\varphi\colon M \to \widetilde{M}$ in $\mathcal{M}\mathrm{od}(A)$, the assignment $\dfrac{m}{s} \mapsto \dfrac{\varphi(m)}{s}$ yields $S^{-1}\varphi\colon S^{-1}M \to S^{-1}\widetilde{M}$. Check this makes $M \rightsquigarrow S^{-1}M$ a functor.

Say $\theta \in \mathrm{Hom}_{S^{-1}A}(S^{-1}M, N)$, set

$$\Theta(m) = \theta\left(\frac{m}{1}\right) \in h^\bullet(N).$$

Now,

$$\Theta(am) = \theta\left(\frac{am}{1}\right) = \theta\left(\frac{a}{1}\frac{m}{1}\right) = \frac{a}{1} \cdot \theta\left(\frac{m}{1}\right) = \left(a \cdot \theta\left(\frac{m}{1}\right) \text{ in } h^\bullet(N)\right) = a \cdot \Theta(m).$$

So, we have a map from $\mathrm{Hom}_{S^{-1}A}(S^{-1}M, N)$ to $\mathrm{Hom}_A(M, h^\bullet(N))$ given by $\theta \mapsto \Theta$. Now, say $\varphi \in \mathrm{Hom}_A(M, h^\bullet(N))$; then, $S^{-1}\varphi \in \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}h^\bullet(N))$. But, if $N \in \mathcal{M}\mathrm{od}(S^{-1}A)$, then $S^{-1}h^\bullet(N) = N$, and we get the map in the opposite direction, $\varphi \mapsto S^{-1}\varphi$. These maps are mutually inverse. Each of $S^{-1}-$; $S^{-1}A \otimes_A -$; $- \otimes_A S^{-1}A$, are left adjoint to $h^\bullet$; so, they are all isomorphic. □

Proposition 3.3 *The functor $M \rightsquigarrow S^{-1}M$ is exact, hence, $S^{-1}A$ is a flat A-algebra.*

Proof. Given any exact sequence $M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3$, we will show that $S^{-1}M_1 \xrightarrow{S^{-1}\varphi} S^{-1}M_2 \xrightarrow{S^{-1}\psi} S^{-1}M_3$ is again exact. Clearly, as $M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3$ is exact, we have $\psi \circ \varphi = 0$; and so, $(S^{-1}\psi) \circ (S^{-1}\varphi) = 0$. This shows that $\mathrm{Im}\,(S^{-1}\varphi) \subseteq \mathrm{Ker}\,(S^{-1}\psi)$. Say $\xi \in S^{-1}M_2$ and $S^{-1}\psi(\xi) = 0$. As $\xi = m/s$, for some $m \in M_2$ and some $s \in S$, and as $S^{-1}\psi(\xi) = \psi(m)/s = 0$ in $S^{-1}M_3$, there is some $u \in S$ with $u\psi(m) = 0$, i.e., $\psi(um) = 0$. By exactness, there is some $m' \in M_1$ so that $um = \varphi(m')$. Consider the element $m'/(su)$; we have

$$S^{-1}\varphi\left(\frac{m'}{su}\right) = \frac{\varphi(m')}{su} = \frac{um}{su} = \frac{m}{s} = \xi.$$

Therefore, $\xi \in \mathrm{Im}\,(S^{-1}\varphi)$, as required. □

Examples:

(1) $S = \mathrm{G}_m(A)$ or more generally, $S \subseteq \mathrm{G}_m(A)$. Then, $S^{-1}A = A$.

(2) $S =$ all nonzero divisors of A. Here, $S^{-1}A$ is a bigger ring if we are not in case (1). The ring $S^{-1}A$ is called the *total fraction ring of* A and it is denoted $\mathrm{Frac}(A)$. If A is a domain, then $\mathrm{Frac}(A)$ is a field, the *fraction field of* A. For example, $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$. The field, $\mathrm{Frac}(k[X_1, \ldots, X_n])$, denoted $k(X_1, \ldots, X_n)$, is the *rational function field* in n variables (where k is a field). If A is the ring of entire (holomorphic) functions, then $\mathrm{Frac}(A)$ is the field of meromorphic functions on $\mathbb{C}$. If $A = \mathrm{Hol}(U)$, the ring of holomorphic functions on an open, $U \subseteq \mathbb{C}$, then $\mathrm{Frac}(A) = \mathcal{M}\mathrm{er}(U) =$ the field of meromorphic functions on U.

(3) $S = \{f^n \mid f \in A\,(f \text{ fixed}); f \notin \mathcal{N}(A)\}$. The ring $S^{-1}A$ has the special notation A_f. Observe that

$$A_f = \left\{ \frac{\alpha}{f^n} \;\middle|\; \alpha \in A, n \geq 0 \right\},$$

while, in general,

$$\mathrm{Ker}\,(h\colon A \longrightarrow S^{-1}A) = \left\{\alpha \in A \;\middle|\; \frac{\alpha}{1} = 0\right\} = \{\alpha \in A \mid (\exists u \in S)(u\alpha = 0)\}.$$

In cases (1) and (2), the map, h, is injective. In case (3), Ker $h = \{\alpha \in A \mid (\exists n \geq 0)(f^n\alpha = 0)\}$. Consider the map $A[X] \longrightarrow A_f$, *via* $X \mapsto 1/f$ ($a \mapsto h(a)$, for $a \in A$). Since $aX^n \mapsto a/f^n$, our map is surjective. What is its kernel?

Consider the diagram

$$\begin{array}{ccc} A_f[X] & \xrightarrow{X \mapsto 1/f} & A_f \\ {\scriptstyle h}\uparrow & & \| \\ A[X] & \xrightarrow{X \mapsto 1/f} & A_f. \end{array}$$

The kernel of the top arrow is: $(X - 1/f)$. The answer to our question is now easily seen to be

$$\{P(X) \in A[X] \mid (\exists r \geq 0)(f^r P(X) \in (Xf - 1)\} = (Xf - 1)^{ec}.$$

Here, $(Xf - 1)^{ec}$ is, for the moment, just a notation for the left hand side. So,

$$A[X]/(Xf - 1)^{ec} \cong A_f.$$

Generalities on extension (e) and contraction (c).

Let $\psi\colon A \to B$ be a map of rings. Say $\mathfrak{A}$ is an ideal in A. Let $\mathfrak{A}^e =$ (*the extended ideal*) be the ideal of B generated by $\psi(\mathfrak{A})$. If $\mathfrak{B}$ is an ideal in B, then let $\mathfrak{B}^c =$ (*the contracted ideal*) be the ideal of A given by

$$\mathfrak{B}^c = \psi^{-1}(\mathfrak{B}) = \{x \in A \mid \psi(x) \in \mathfrak{B}\}.$$

Take $B = S^{-1}A$. If $\mathfrak{A} \subseteq A$, what is $\mathfrak{A}^e$?

Claim: $\mathfrak{A}^e = \left\{ \alpha/s \mid \alpha \in \mathfrak{A},\, s \in S \right\}$. Indeed, we have

$$\mathfrak{A}^e = \left\{ \sum_{i=1}^{n} \frac{b_i}{s_i}\frac{a_i}{1} \;\middle|\; a_i \in \mathfrak{A},\, b_i \in A,\, s_i \in S \right\}.$$

Such a sum is of the form $\dfrac{1}{\sigma}\sum_{i=1}^{n} c_i a_i$, where $\sigma = s_1 \cdots s_n$; $c_i \in A$ and $a_i \in \mathfrak{A}$. Since $\mathfrak{A}$ is an ideal, this sum is of the form α/σ, where $\alpha \in \mathfrak{A}$. We have proved part of

Proposition 3.4 *For any commutative ring, A, and any multiplicative subset, S, of A we have:*

(1) $\mathbb{G}_m(S^{-1}A) = \{\alpha/s \mid (\exists b \in A)(b\alpha \in S)\}$.

(2) If $\mathfrak{A} \subseteq A$ *then* $\mathfrak{A}^e = \{\alpha/s \mid \alpha \in \mathfrak{A},\ s \in S\}$.

(3) $\mathfrak{A}^e = (1) = S^{-1}A$ *iff* $\mathfrak{A} \cap S \neq \emptyset$.

Proof. (1) We have $\alpha/s \in \mathbb{G}_m(S^{-1}A)$ iff there is some β/t with $\dfrac{\beta\alpha}{ts} = 1 = \dfrac{1}{1}$ iff $(\exists u \in S)((u\beta)\alpha = ust)$. But, $ust \in S$; so, if we set $b = u\beta$, we get $b\alpha \in S$. The converse is clear.

(2) Already done.

(3) We have $\mathfrak{A}^e = (1)$ iff some element of $\mathfrak{A}^e$ is a unit iff α/s is a unit for some $\alpha \in \mathfrak{A}$ iff there is some $b \in A$ with $b\alpha \in S$. But, $\alpha \in \mathfrak{A}$, so $b\alpha \in \mathfrak{A}$, yet $b\alpha \in S$; so, $\mathfrak{A} \cap S \neq \emptyset$. Conversely, if $\mathfrak{A} \cap S \neq \emptyset$, then $\{s/1 \mid s \in S\} \cap \mathfrak{A}^e \neq \emptyset$. Consequently, $\mathfrak{A}^e$ has a unit in it, and so, $\mathfrak{A}^e = (1)$. □

Say $\mathfrak{A} \subseteq A$, when is $\mathfrak{A}$ contracted? First an easier question: What is $\mathfrak{A}^{ec}$?

Note: for all $v \in A$, we have $\mathfrak{A} \subseteq (v \longrightarrow \mathfrak{A})$ (this only uses the fact that $\mathfrak{A}$ is a two-sided ideal).

Claim: $(v \longrightarrow \mathfrak{A}) = \mathfrak{A}$ iff v is not a zero divisor mod $\mathfrak{A}$, i.e., $\overline{v} \in A/\mathfrak{A}$ is not a zero divisor. (Terminology: v is *regular* w.r.t, $\mathfrak{A}$).

We have $(v \longrightarrow \mathfrak{A}) = \mathfrak{A}$ iff $(v \longrightarrow \mathfrak{A}) \subseteq \mathfrak{A}$ iff for every $\xi \in A$, when $\xi v \in \mathfrak{A}$, then $\xi \in \mathfrak{A}$. Reading this mod $\mathfrak{A}$, we find the above statement is equivalent to

$$(\forall \overline{\xi} \in A/\mathfrak{A})(\overline{\xi}\overline{v} = 0 \implies \overline{\xi} = 0),$$

which holds iff $\overline{v}$ is not a zero divisor in $A/\mathfrak{A}$.

Going back to the question: What is $\mathfrak{A}^{ec}$?, we have $\xi \in \mathfrak{A}^{ec}$ iff $h(\xi) \in \mathfrak{A}^e$ iff $h(\xi) = \alpha/s$, for some $\alpha \in \mathfrak{A}$ and some $s \in S$, iff $\xi/1 = \alpha/s$ iff there is some $u \in S$ so that $u(\xi s - \alpha) = 0$, i.e. $u\xi s = u\alpha \in \mathfrak{A}$. As $us \in S$, this implies that there is some $v \in S$ with $v\xi \in \mathfrak{A}$. Conversely, if $v\xi \in \mathfrak{A}$ for some $v \in S$, then

$$\frac{v}{1}\frac{\xi}{1} \in \mathfrak{A}^e \implies \frac{1}{v}\frac{v}{1}\frac{\xi}{1} \in \mathfrak{A}^e \implies \frac{\xi}{1} \in \mathfrak{A}^e \implies h(\xi) \in \mathfrak{A}^e,$$

and so, $\xi \in \mathfrak{A}^{ec}$. Therefore,

$$\begin{aligned} \mathfrak{A}^{ec} &= \{\xi \mid (\exists v \in S)(v\xi \in \mathfrak{A})\} \\ &= \{\xi \mid (\exists v \in S)(\xi \in (v \longrightarrow \mathfrak{A}))\} \\ &= \bigcup_{v \in S} (v \longrightarrow \mathfrak{A}). \end{aligned}$$

Now, $\mathfrak{A} = (1 \longrightarrow \mathfrak{A}) \subseteq \bigcup_{s \in S}(s \longrightarrow \mathfrak{A}) = \mathfrak{A}^{ec}$.

When is $\mathfrak{A}$ contracted, i.e., when is it of the form $\mathfrak{A} = \mathfrak{B}^c$, for some $\mathfrak{B} \subseteq S^{-1}A$?

Of course, if $\mathfrak{A} = \mathfrak{A}^{ec}$, then $\mathfrak{B} = \mathfrak{A}^e$ will do. In fact, we shall prove that $\mathfrak{A} = \mathfrak{B}^c$ for some $\mathfrak{B} \subseteq S^{-1}A$ iff $\mathfrak{A} = \mathfrak{A}^{ec}$. First, we claim that $\mathfrak{B} = \mathfrak{B}^{ce}$ for *every* $\mathfrak{B} \subseteq S^{-1}A$; that is, every ideal, $\mathfrak{B}$, of $S^{-1}A$ is an extended ideal. For, any ξ in $\mathfrak{B}$ is of the form $\xi = \alpha/s$, for some $\alpha \in A$ and some $s \in S$. But, $s\xi \in \mathfrak{B}$, too, and so, $\alpha/1 \in \mathfrak{B}$, which implies that $\alpha \in \mathfrak{B}^c$. Consequently, $\xi = \alpha/s \in \mathfrak{B}^{ce}$. Conversely, if $\xi \in \mathfrak{B}^{ce}$, then $\xi = \beta/t$, with $\beta \in \mathfrak{B}^c$; it follows that $\xi = (1/t)(\beta/1) \in \mathfrak{B}$, and so, $\mathfrak{B} = \mathfrak{B}^{ce}$.

But now, $\mathfrak{A} = \mathfrak{B}^c$ implies that $\mathfrak{A}^e = \mathfrak{B}^{ce} = \mathfrak{B}$; so, $\mathfrak{A}^{ec} = \mathfrak{B}^c = \mathfrak{A}$. These remarks prove most of the

Proposition 3.5 *If* $A \in$ CR *and S is a multiplicative system in A, then*

(1) An ideal, $\mathfrak{A}$, of A is contracted iff $\mathfrak{A} = \mathfrak{A}^{ec}$ iff every element of S is regular for $\mathfrak{A}$.

(2) Every ideal, $\mathfrak{B} \subseteq S^{-1}A$, is extended.

(3) The map, $\mathfrak{A} \mapsto \mathfrak{A}^e$, is a one-to-one inclusion-preserving correspondence between all the contracted ideals of A and **all** *ideals of $S^{-1}A$.*

(4) If A is noetherian, then $S^{-1}A$ is noetherian.

Proof. (1) We proved earlier that $\mathfrak{A}^{ec} = \bigcup_{v \in S}(v \longrightarrow \mathfrak{A})$ and we know that $(v \longrightarrow \mathfrak{A}) = \mathfrak{A}$ iff v is regular for $\mathfrak{A}$. So, (1) is now clear.

(2) This has already been proved.

(3) Assume that $\mathfrak{A}$ and $\widetilde{\mathfrak{A}}$ have the same extension and both are contracted. Then, by (1) $\mathfrak{A} = \mathfrak{A}^{ec}$ and $\widetilde{\mathfrak{A}} = \widetilde{\mathfrak{A}}^{ec}$, and since, by hypothesis $\mathfrak{A}^e = \widetilde{\mathfrak{A}}^e$, we get $\mathfrak{A} = \widetilde{\mathfrak{A}}$. It is also clear that if $\mathfrak{A} \subseteq \widetilde{\mathfrak{A}}$, then $\mathfrak{A}^e \subseteq \widetilde{\mathfrak{A}}^e$.

(4) (DX) from (1), (2), (3). □

The same argument shows the corresponding proposition for modules.

Proposition 3.6 *If $A \in$ CR and S is a multiplicative system in A, for any module, $M \in \mathcal{M}\mathrm{od}(A)$,*

(1) A submodule, N, of M is contracted iff it is equal to its S-saturation. The S-saturation of N is the submodule given by

$$\{\xi \in M \mid (\exists v \in S)(v\xi \in N)\} = \bigcup_{v \in S}(v \longrightarrow N),$$

where $(v \longrightarrow N) = \{\xi \in M \mid v\xi \in N\}$.

(2) Every submodule of $S^{-1}M$ is extended, i.e., has the form $S^{-1}N$, for some submodule, N, of M.

(3) The map, $N \mapsto S^{-1}N$, is a one-to-one inclusion-preserving correspondence between all the S-saturated submodules of M and **all** *submodules of $S^{-1}M$.*

(4) If M is a noetherian module, then $S^{-1}M$ is a noetherian module.

Proposition 3.7 *Say $A \in$ CR and S is a multiplicative system in A. For any ideal, $\mathfrak{A} \subseteq A$, we have*

(a) The image, $\overline{S}$, of S in $A/\mathfrak{A}$, is a multiplicative subset provided that $S \cap \mathfrak{A} = \emptyset$.

(b) $S^{-1}A/\mathfrak{A}^e \xrightarrow{\sim} \overline{S}^{-1}(A/\mathfrak{A})$.

Proof. (a) This is trivial.

(b) We have $A \longrightarrow A/\mathfrak{A} \longrightarrow \overline{S}^{-1}(A/\mathfrak{A})$. The elements of S become units in $\overline{S}^{-1}(A/\mathfrak{A})$. By the universal mapping property, we have the map $S^{-1}A \longrightarrow \overline{S}^{-1}(A/\mathfrak{A})$. This map is $a/s \mapsto \overline{a}/\overline{s}$; so, it is surjective. We have $\overline{a}/\overline{s} = 0$ in $\overline{S}^{-1}(A/\mathfrak{A})$ iff there is some $\overline{u} \in \overline{S}$ so that $\overline{u}\,\overline{a} = \overline{0}$ iff $a/1 \in \mathfrak{A}^e$ iff $a/s \in \mathfrak{A}^e$. Therefore, the kernel of our map is $\mathfrak{A}^e$, and so, $S^{-1}A/\mathfrak{A}^e \xrightarrow{\sim} \overline{S}^{-1}(A/\mathfrak{A})$. □

3.3 Prime and Maximal Ideals

Recall that an ideal, $\mathfrak{p}$, of $A \in \mathrm{CR}$ is a *prime ideal* iff $\mathfrak{p} \neq (1)$ and for all $a, b \in A$, if $ab \in \mathfrak{p}$, then one of $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ holds.

Proposition 3.8 *Given a commutative ring, A, for any ideal, $\mathfrak{A} \subseteq A$, the following are equivalent:*

(1) The ideal, $\mathfrak{A}$, is a prime ideal.

(2) The ring $A/\mathfrak{A}$ is an integral domain.

(3) The set $S = A - \mathfrak{A} =$ the complement of $\mathfrak{A}$ is a multiplicative subset of A.

(4) If $\mathfrak{B}$ and $\widetilde{\mathfrak{B}}$ are two ideals of A and if $\mathfrak{B}\widetilde{\mathfrak{B}} \subseteq \mathfrak{A}$, then one of $\mathfrak{B} \subseteq \mathfrak{A}$ or $\widetilde{\mathfrak{B}} \subseteq \mathfrak{A}$ holds.

(5) There is a ring, B, a homomorphism, $\varphi\colon A \to B$ and a maximal ideal, $\mathfrak{m}$, of B, so that $\varphi^{-1}(\mathfrak{m}) = \mathfrak{A}$.

(6) There is a multiplicative set, $S \subseteq A$, so that

(i) $\mathfrak{A} \cap S = \emptyset$ and

(ii) $\mathfrak{A}$ is maximal among the ideals having (i).

Proof. Equivalence of (1)–(4) is known and clear. Now, the inverse image of a prime ideal is *always* a prime ideal (DX). Every maximal ideal is prime, so it follows that (5) $\Rightarrow$ (1). Moreover, (1) implies (6) because take $S = A - \mathfrak{p}$. This is a multiplicative set by (3) and (6) follows tautologically.

(1) $\Rightarrow$ (5). Given a prime, $\mathfrak{A}$, let $S = A - \mathfrak{A}$, a multiplicative set by (3) and let $B = S^{-1}A$ and $\varphi = h$. We claim that $\mathfrak{A}^e$ is a maximal ideal of $S^{-1}A$. This is because $S^{-1}A/\mathfrak{A}^e \xrightarrow{\sim} \overline{S}^{-1}(A/\mathfrak{A})$, but $A/\mathfrak{A}$ is an integral domain and $\overline{S} =$ nonzero elements of $A/\mathfrak{A}$. Consequently, $\overline{S}^{-1}(A/\mathfrak{A}) = \mathrm{Frac}(A/\mathfrak{A})$ is a field; so, $\mathfrak{A}^e$ is a maximal ideal. Now, $h^{-1}(\mathfrak{A}^e) = \mathfrak{A}^{ec} = \bigcup_{v \in S}(v \longrightarrow \mathfrak{A})$. Now, $\xi \in (v \longrightarrow \mathfrak{A})$ iff $v\xi \in \mathfrak{A}$, where $v \notin \mathfrak{A}$. But, $\mathfrak{A}$ is prime, so $\xi \in \mathfrak{A}$. Therefore, $(v \longrightarrow \mathfrak{A}) = \mathfrak{A}$, for all $v \in S$; and so, $\mathfrak{A}^{ec} = h^{-1}(\mathfrak{A}^e) = \mathfrak{A}$ and (5) follows.

(6) $\Rightarrow$ (1). Given any $a, b \notin \mathfrak{A}$, we must show that $ab \notin \mathfrak{A}$. The hypotheses imply that $\mathfrak{A} + (a) > \mathfrak{A}$ and $\mathfrak{A} + (b) > \mathfrak{A}$, and by (6) (i) and (ii), we have $(\mathfrak{A} + (a)) \cap S \neq \emptyset$ and $(\mathfrak{A} + (b)) \cap S \neq \emptyset$. So, there are some $s, t \in S$, where $s = \alpha + \rho a$, $t = \beta + \sigma b$, with $\alpha, \beta \in \mathfrak{A}$, $\rho, \sigma \in A$. Since $st \in S$, it follows that

$$\alpha\beta + \rho a\beta + \sigma b\alpha + \rho\sigma(ab) \in S.$$

If $ab \in \mathfrak{A}$, then $st \in \mathfrak{A} \cap S$, a contradiction. Therefore, $ab \notin \mathfrak{A}$. □

Corollary 3.9 *Given any multiplicative set, S, in A, there exists a prime ideal, $\mathfrak{p}$, so that $\mathfrak{p} \cap S = \emptyset$.*

Proof. Look at $\mathcal{S} = \{\mathfrak{A} \mid \mathfrak{A} \text{ an ideal and } \mathfrak{A} \cap S = \emptyset\}$. We have $(0) \in \mathcal{S}$, partially order $\mathcal{S}$ by inclusion and check that $\mathcal{S}$ is inductive. By Zorn's lemma, $\mathcal{S}$ has some maximal element, $\mathfrak{p}$. By (6), the ideal $\mathfrak{p}$ is prime. □

Notation: If $S = A - \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal, write $A_{\mathfrak{p}}$ instead of $S^{-1}A$; the ring $A_{\mathfrak{p}}$ is called the *localization of A at $\mathfrak{p}$*. Recall that a *local ring* is a ring that has a unique maximal ideal.

Corollary 3.10 *For any prime ideal, $\mathfrak{p}$, in A, the ring $A_{\mathfrak{p}}$ is always a local ring and its maximal ideal is just $\mathfrak{p}^e$.*

Proof. Say $\mathfrak{A}$ is an ideal of A. Ideals of $A_{\mathfrak{p}} = S^{-1}A$ are extended ideals, i.e., they are of the form $\mathfrak{A}^e$. We have $\mathfrak{A}^e = (1)$ iff $\mathfrak{A} \cap S \neq \emptyset$ iff $\mathfrak{A} \not\subseteq \mathfrak{p}$. Thus, $\mathfrak{A}^e$ is a proper ideal iff $\mathfrak{A} \subseteq \mathfrak{p}$; the latter implies that $\mathfrak{A}^e \subseteq \mathfrak{p}^e$. So, $\mathfrak{p}^e$ is *the* maximal ideal of $A_{\mathfrak{p}}$, as contended. □

Remark: We have $\mathfrak{p}^{ec} = \mathfrak{p}$. We saw this above in the proof that (1) $\Rightarrow$ (5).

Proposition 3.11 *Let $A \in \mathrm{CR}$ be a commutative ring, S be a multiplicative set in A and let $\mathfrak{P}$ be a prime ideal of A. Then,*

(1) The ideal $\mathfrak{P}^e$ is a prime ideal of $S^{-1}A$ iff $\mathfrak{P}^e \neq (1)$ iff $\mathfrak{P} \cap S = \emptyset$.

(2) Every prime ideal of $S^{-1}A$ has the form $\mathfrak{P}^e$, for some prime ideal, $\mathfrak{P}$, of A.

(3) There is a one-to-one, inclusion-preserving, correspondence between the prime ideals of $S^{-1}A$ and the prime ideals, $\mathfrak{P}$, of A for which $\mathfrak{P} \cap S = \emptyset$.

When $S = A - \mathfrak{p}$ for some prime, $\mathfrak{p}$, of A, we have

(1′) The ideal $\mathfrak{P}^e$ is a prime of $A_\mathfrak{p}$ iff $\mathfrak{P}$ is a prime in A and $\mathfrak{P} \subseteq \mathfrak{p}$.

(2′) Every prime ideal of $A_\mathfrak{p}$ is $\mathfrak{P}^e$, for some prime, $\mathfrak{P}$, of A with $\mathfrak{P} \subseteq \mathfrak{p}$.

(3′) There is a one-to-one, inclusion-preserving, correspondence between all primes of $A_\mathfrak{p}$ and the primes of A contained in $\mathfrak{p}$.

Proof. (1) We know that $\mathfrak{P}^e \neq (1)$ iff $\mathfrak{P} \cap S = \emptyset$. By definition, a prime ideal is never equal to (1), so, all we must show is: If $\mathfrak{P}$ is prime in A, then $\mathfrak{P}^e$ is prime in $S^{-1}A$ (of course, $\mathfrak{P}^e \neq (1)$). Say $(\alpha/s)(\beta/t) \in \mathfrak{P}^e$. Then, $(\alpha\beta)/1 \in \mathfrak{P}^e$, and so, $\alpha\beta \in \mathfrak{P}^{ec}$. But, $\mathfrak{P}^{ec} = \bigcup_{v \in S}(v \longrightarrow \mathfrak{P})$ and $\xi \in (v \longrightarrow \mathfrak{P})$ iff $v\xi \in \mathfrak{P}$; moreover, $v \notin \mathfrak{P}$ since $\mathfrak{P} \cap S = \emptyset$, so, $\xi \in \mathfrak{P}$. Therefore, $\mathfrak{P}^{ec} = \mathfrak{P}$, and so, $\alpha\beta \in \mathfrak{P}$. Since $\mathfrak{P}$ is prime, either $\alpha \in \mathfrak{P}$ or $\beta \in \mathfrak{P}$; it follows that either $\alpha/s \in \mathfrak{P}^e$ or $\beta/t \in \mathfrak{P}^e$.

(2) If $\mathfrak{q}$ is a prime in $S^{-1}A$, then $\mathfrak{q} = \mathfrak{q}^{ce}$ and $\mathfrak{q}^c$ is a prime, as $\mathfrak{q}^c = h^{-1}(\mathfrak{q})$. Take $\mathfrak{P} = \mathfrak{q}^c$ to satisfy (2). Conversely, $\mathfrak{P}^e$ is prime iff $\mathfrak{P} \cap S = \emptyset$.

(3) follows from (1) and (2) and previous work.

Finally, (1′), (2′) and (3′) are special cases of (1), (2) and (3), respectively. □

Definition 3.2 If $\mathfrak{p}$ is a prime ideal of $A \in \mathrm{CR}$, look at chains of prime ideals

$$\mathfrak{p} = \mathfrak{p}_0 > \mathfrak{p}_1 > \cdots > \mathfrak{p}_n,$$

where each $\mathfrak{p}_j$ is prime ideal of A. Call n the *length* of this chain and define the *height of* $\mathfrak{p}$ by

$$\mathrm{ht}(\mathfrak{p}) = \sup\{\text{length of all chains } \mathfrak{p} = \mathfrak{p}_0 > \mathfrak{p}_1 > \cdots > \mathfrak{p}_n\}.$$

Observe that $\mathrm{ht}(\mathfrak{p})$ might be infinite. Since there is a one-to-one inclusion-preserving correspondence between the set of all primes, $\mathfrak{P}$, contained in $\mathfrak{p}$ and the set of all prime ideals of $A_\mathfrak{p}$, we get

$$\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\text{maximal ideal of } A_\mathfrak{p}).$$

Definition 3.3 The *Krull dimension* of a commutative ring, A, denoted $\dim(A)$, is the supremum of the set $\{\mathrm{ht}(\mathfrak{m}) \mid \mathfrak{m} \text{ is a maximal ideal of } A\}$.

Hence, we see that $\mathrm{ht}(\mathfrak{p}) = \dim(A_\mathfrak{p})$, and

$$\dim(A) = \sup\{\dim(A_\mathfrak{m}) \mid \mathfrak{m} \text{ is a maximal ideal of } A\}.$$

Examples.

(1) Say $\dim(A) = 0$. This holds iff every prime ideal is maximal iff every maximal ideal is a minimal prime ideal. An example is a field, or $\mathbb{Z}/n\mathbb{Z}$.

(2) $\dim(A) = 1$. Here, A = a P.I.D. will do. For example, $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}[T]$, more generally, $k[T]$, for any field, k. Also, $\mathbb{Z}[\sqrt{-5}]$, a non-P.I.D., has dimension 1.

(3) $\mathbb{C}[T_1, \ldots, T_n]$ has dimension n (this is not obvious, try it!) Given a commutative ring, A, for applications to algebraic geometry and number theory, it is useful to introduce two important sets, $\operatorname{Spec} A$ and $\operatorname{Max} A$, and to make these sets into topological spaces. Let

$$\begin{aligned} \operatorname{Spec} A &= \{\mathfrak{p} \mid \mathfrak{p} \text{ is a prime ideal of } A\} \\ \operatorname{Max} A &= \{\mathfrak{m} \mid \mathfrak{m} \text{ is a maximal ideal of } A\}. \end{aligned}$$

The set, $X = \operatorname{Spec} A$, is given a topology (the *Zariski topology* or *spectral topology*) for which a basis of open sets consists of the sets

$$X_f = \{\mathfrak{p} \in \operatorname{Spec} A \mid f \notin \mathfrak{p}\} \quad (f \in A),$$

and $\operatorname{Max} A \subseteq \operatorname{Spec} A$ is given the relative topology.

Remarks:

(1) $X_{f^n} = X_f$, for all $n \geq 1$. This is because $f^n \notin \mathfrak{p}$ iff $f \notin \mathfrak{p}$, as $\mathfrak{p}$ is prime.

(2) $X_{fg} = X_f \cap X_g$. This is because $\mathfrak{p} \in X_{fg}$ iff $fg \notin \mathfrak{p}$ iff $(f \notin \mathfrak{p})$ and $(g \notin \mathfrak{p})$.

(3) $X_f = \operatorname{Spec} A = X$ iff $f \notin \mathfrak{p}$, for every prime $\mathfrak{p}$ iff $f \in \mathbb{G}_m(A)$ iff $X_f = X_1$.

(4) $X_f = \emptyset$ iff $f \in \mathfrak{p}$, for all primes, $\mathfrak{p}$.

The open sets in $X = \operatorname{Spec} A$ are just the sets of the form $\bigcup_{f \in T} X_f$, for any subset, T, of A. So, a set, C, is closed in X iff it is of the form $C = \bigcap_T X_f^{\mathrm{c}}$, where

$$X_f^{\mathrm{c}} = \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \notin X_f\} = \{\mathfrak{p} \in \operatorname{Spec} A \mid f \in \mathfrak{p}\} = \{\mathfrak{p} \in \operatorname{Spec} A \mid (f) \subseteq \mathfrak{p}\}.$$

Thus, $\mathfrak{p} \in C$ iff the ideal generated by the set T is contained in $\mathfrak{p}$. This suggests the following definition: For any ideal, $\mathfrak{A}$, in A, let

$$V(\mathfrak{A}) = \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \supseteq \mathfrak{A}\}$$

be the *variety defined by* $\mathfrak{A}$. Then, we have

$$V(\mathfrak{A}) = \bigcap_{f \in \mathfrak{A}} X_f^{\mathrm{c}} = \bigcap \{X_f^{\mathrm{c}} \mid f \text{ is part of a generating set for } \mathfrak{A}\}.$$

The dual properties to (1)–(4) are:

(1′) $V(\mathfrak{A} \cap \mathfrak{B}) = V(\mathfrak{A}\mathfrak{B}) = V(\mathfrak{A}) \cup V(\mathfrak{B})$

(2′) $V(\sum_\alpha \mathfrak{A}_\alpha) = \bigcap_\alpha V(\mathfrak{A}_\alpha)$ $\quad$ ($\sum_\alpha \mathfrak{A}_\alpha$ = the ideal generated by the $\mathfrak{A}_\alpha$'s).

(3′) $V(\mathfrak{A}) = \emptyset$ iff $\mathfrak{A} = (1)$.

(4′) $V(\mathfrak{A}) = X = \operatorname{Spec} A$ iff $(\forall \mathfrak{p} \in \operatorname{Spec} A)(\mathfrak{A} \subseteq \mathfrak{p})$.

From now on, when we refer to $\operatorname{Spec} A$ and $\operatorname{Max} A$, we mean these as *topological spaces*.

To give a more informative criterion for (4) and (4′), we need to study $\mathcal{N}(A)$ = the *nilradical of* A, defined by

$$\mathcal{N}(A) = \{x \in A \mid x^n = 0, \text{ for some integer } n > 0\}.$$

This is an ideal of A. Indeed, if $x \in \mathcal{N}(A)$ and $y \in A$, since A is commutative, we have $(yx)^n = y^n x^n = 0$. Also, if $x, y \in \mathcal{N}(A)$, then there is some integer $n \geq 0$ so that $x^n = y^n = 0$, and by the binomial formula,

$$(x \pm y)^{2n} = \sum_{j=0}^{2n} \binom{2n}{j} x^j (\pm 1)^{2n-j} y^{2n-j} = 0,$$

since $y^{2n-j} = 0$ if $j \leq n$ and $x^j = 0$ if $j \geq n$. Therefore, $x \pm y \in \mathcal{N}(A)$ and $\mathcal{N}(A)$ is an ideal.

More generally, if $\mathfrak{A}$ is an ideal, the *radical* of $\mathfrak{A}$, denoted $\sqrt{\mathfrak{A}}$, is

$$\sqrt{\mathfrak{A}} = \{x \in A \mid (\exists n \geq 0)(x^n \in \mathfrak{A})\}.$$

It is easy to check that $\sqrt{\mathfrak{A}}$ is an ideal and that $\mathfrak{A} \subseteq \sqrt{\mathfrak{A}}$. Note: $\sqrt{(0)} = \mathcal{N}(A)$.

That $\sqrt{\mathfrak{A}}$ is an ideal can also be seen as follows: Consider the projection map, $A \xrightarrow{\text{bar}} A/\mathfrak{A}$, and look at $\mathcal{N}(A/\mathfrak{A})$. Then, $\sqrt{\mathfrak{A}}$ is the inverse image of $\mathcal{N}(A/\mathfrak{A})$ under bar, and so, $\sqrt{\mathfrak{A}}$ is an ideal. Furthermore, by the first homomorphism theorem,

$$A/\sqrt{\mathfrak{A}} \cong (A/\mathfrak{A})/\mathcal{N}(A/\mathfrak{A}).$$

Observe that $A/\mathcal{N}(A)$ is a ring without nonzero nilpotent elements. Such a ring is called a *reduced ring* and $A/\mathcal{N}(A)$ is reduced. We write A_{red} for $A/\mathcal{N}(A)$. Note: $(A/\mathfrak{A})_{\text{red}} = A/\sqrt{\mathfrak{A}}$. For example, $(\mathbb{Z}/p^n\mathbb{Z})_{\text{red}} = \mathbb{Z}/p\mathbb{Z}$, for any prime p.

The following facts are easy to prove (DX):

(a) $\sqrt{\sqrt{\mathfrak{A}}} = \sqrt{\mathfrak{A}}$.

(b) $\sqrt{\mathfrak{A} \cap \mathfrak{B}} = \sqrt{\mathfrak{A}} \cap \sqrt{\mathfrak{B}}$.

(c) If $\mathfrak{A}^k \subseteq \mathfrak{B}$, for some $k \geq 1$, then $\sqrt{\mathfrak{A}} \subseteq \sqrt{\mathfrak{B}}$.

There is another radical, the *Jacobson radical*, $\mathcal{J}(A)$, given by

$$\mathcal{J}(A) = \bigcap_{\mathfrak{m} \in \text{Max}(A)} \mathfrak{m}.$$

Proposition 3.12 *For any ring, $A \in$ CR, we have*

(1) $x \notin \mathbb{G}_m(A)$ iff there is some maximal ideal, $\mathfrak{m}$, so that $x \in \mathfrak{m}$.

(2) If $x \in \mathcal{J}(A)$, then $1 + x \in \mathbb{G}_m(A)$.

(3) $\mathcal{N}(A) = \bigcap_{\mathfrak{p} \in \text{Spec } A} \mathfrak{p}$; hence $\mathcal{N}(A) \subseteq \mathcal{J}(A)$.

Proof. (1) is clear (use Zorn's lemma).

(2) Assume $(1 + x) \notin \mathbb{G}_m(A)$. By (1), there is some $\mathfrak{m} \in \text{Max}\, A$, so that $1 + x \in \mathfrak{m}$. So, $x \notin \mathfrak{m}$ (else, $1 \in \mathfrak{m}$, a contradiction). As $\mathcal{J}(A)$ is contained in every maximal ideal, we get $x \notin \mathcal{J}(A)$.

(3) Suppose $x \in \mathcal{N}(A)$; then, $x^n = 0$, for some $n \geq 0$. Consequently, $x^n \in \mathfrak{p}$, for every prime $\mathfrak{p}$; so, $x \in \mathfrak{p}$, as $\mathfrak{p}$ is prime. Conversely, assume $x \in \bigcap_{\mathfrak{p} \in \text{Spec}(A)} \mathfrak{p}$. Look at the set $S = \{x^n \mid n \geq 0\}$. Were S a multiplicative set, then there would be some prime ideal, $\mathfrak{p}$, with $\mathfrak{p} \cap S = \emptyset$. As $x \in \mathfrak{p}$, this is impossible. Therefore, S is not a multiplicative set, which happens iff x is nilpotent. □

Now, we can give the criteria for (4) and (4′).

(4) $X_f = \emptyset$ iff $f \in \mathcal{N}(A)$.

(4′) $V(\mathfrak{A}) = X = \operatorname{Spec} A$ iff $\mathfrak{A} \subseteq \mathcal{N}(A)$.

Corollary 3.13 *Given any ideal, $\mathfrak{A}$,*

$$\sqrt{\mathfrak{A}} = \bigcap\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \supseteq \mathfrak{A}\} = \bigcap\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \in V(\mathfrak{A})\}.$$

Proof. There is a one-to-one correspondence between the set of prime ideals, $\mathfrak{p}$, containing $\mathfrak{A}$ and the set of prime ideals, $\overline{\mathfrak{p}}$, in $A/\mathfrak{A}$. So, $\bigcap\{\mathfrak{p} \mid \mathfrak{p} \supseteq \mathfrak{A}\}$ is the inverse image of $\mathcal{N}(A/\mathfrak{A})$, but this inverse image is $\sqrt{\mathfrak{A}}$. □

The minimal elements among primes, $\mathfrak{p}$, such that $\mathfrak{p} \supseteq \mathfrak{A}$ are called the *isolated primes* of $\mathfrak{A}$. Therefore,

$$\sqrt{\mathfrak{A}} = \bigcap\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \text{ is an isolated prime of } \mathfrak{A}\}.$$

Proposition 3.14 *The space $X = \operatorname{Spec} A$ is always quasi-compact (i.e., compact but not necessarily Hausdorff).*

Proof. Say $\bigcup_\alpha U_\alpha = X$ is an open cover of X. Each open U_α has the form $U_\alpha = \bigcup_\beta X_{f_\beta^{(\alpha)}}$. Therefore, we get an open cover $\bigcup_{\alpha,\beta} X_{f_\beta^{(\alpha)}} = X$. If we prove that this cover has a finite subcover, we are done (DX). The hypothesis implies that $\bigcap_{\alpha,\beta} X^{\mathrm{c}}_{f_\beta^{(\alpha)}} = \emptyset$. However the left hand side is $V((f_\beta^{(\alpha)}))$ and so $(f_\beta^{(\alpha)}) = (1)$, by previous work. We find

$$1 = c_{\alpha_1,\beta_1} f_{\beta_1}^{(\alpha_1)} + \cdots + c_{\alpha_s,\beta_s} f_{\beta_s}^{(\alpha_s)}, \quad \text{for some } c_{\alpha_j,\beta_j} \in A.$$

Thus, already, $(f_{\beta_j}^{(\alpha_j)})_{j=1}^s = (1)$, and so, $\bigcap_{j=1}^s X^{\mathrm{c}}_{f_{\beta_j}^{(\alpha_j)}} = \emptyset$. Thus, $\bigcup_{j=1}^s X_{f_{\beta_j}^{(\alpha_j)}} = X$, a finite cover. □

Remark: The space, $\operatorname{Spec} A$, is almost never Hausdorff. For example,
$\operatorname{Spec}(\mathbb{Z}) = \{(0), (2), (3), (5), (7), (11), \ldots\}$, and $\{(0)\}$ is dense in $\operatorname{Spec}(\mathbb{Z})$, i.e., every open set contains (0).

Another geometric example of $\operatorname{Spec} A$ and $\operatorname{Max} A$ is this:

Proposition 3.15 *Let X be a compact, Hausdorff space and write $A = \mathcal{C}(X)$ (the ring of real-valued (or complex-valued) continuous functions on X). For each $x \in X$, write $\mathfrak{m}_x = \{f \in A \mid f(x) = 0\}$. Then*

(1) Each $\mathfrak{m}_x$ is a maximal ideal of A and

(2) The map $x \mapsto \mathfrak{m}_x$ is a bijection of X with $\operatorname{Max} A$. (In fact, $x \mapsto \mathfrak{m}_x$ is a homeomorphism).

Proof. Note that the map $f \mapsto f(x)$ is a homomorphism of $\mathcal{C}(X)$ *onto* $\mathbb{R}$ (resp. $\mathbb{C}$). Its kernel is $\mathfrak{m}_x$, and so, $\mathfrak{m}_x$ is maximal. By Urysohn's lemma, if $x \neq y$, there is some continuous function, $f \in A$, so that $f(x) = 0$ and $f(y) = 1$. Thus, $f \in \mathfrak{m}_x$ and $f \notin \mathfrak{m}_y$; it follows that $\mathfrak{m}_x \neq \mathfrak{m}_y$; so, our map is an injection (of sets). Take any $\mathfrak{m}$ in $\operatorname{Max} A$. Say, $\mathfrak{m} \neq \mathfrak{m}_x$ for all $x \in X$. Given $x \in X$, since $\mathfrak{m} \neq \mathfrak{m}_x$, there is some $f_x \in \mathfrak{m}$ and $f_x \notin \mathfrak{m}_x$, Therefore, $f_x(x) \neq 0$. Since f is continuous, there is some open subset, U_x, with $x \in U_x$, and $f \restriction U_x \neq 0$. Then, the family $\{U_x\}$ is an open cover of X, and by compactness, it contains a finite subcover, say $\{U_{x_j}\}_{j=1}^t$. We have a function, $f_{x_j} \in \mathfrak{m}$, for each $j = 1, \ldots, t$. Let

$$F = \sum_{j=1}^t f_{x_j}^2 \quad \Big(F = \sum_{j=1}^t |f_{x_j}|^2, \quad \text{in the complex case}\Big).$$

Clearly, $F \geq 0$. Pick any $\xi \in X$. Then, there is some j, with $1 \leq j \leq t$, so that $\xi \in U_{x_j}$, and so, $f_{x_j}(\xi) \neq 0$. It follows that $F(\xi) > 0$. Thus, F is *never* zero on X; consequently, $1/F \in A$. But now, F is a unit and yet, $F \in \mathfrak{m}$, a contradiction. Therefore, the map $x \mapsto \mathfrak{m}_x$ is surjective. We leave the fact that it is a homeomorphism as a (DX). □

Here are some useful lemmas on primes.

Lemma 3.16 *If $\mathfrak{p}$ is a prime of A and $\mathfrak{A}_1, \ldots, \mathfrak{A}_t$ are some given ideals, then $\mathfrak{p} \supseteq \bigcap_{j=1}^t \mathfrak{A}_j$ iff $\mathfrak{p} \supseteq \mathfrak{A}_j$, for some j.*

Proof. ($\Leftarrow$). This is a tautology.

($\Rightarrow$). Observe that $\mathfrak{p} \supseteq \bigcap_{j=1}^t \mathfrak{A}_j \supseteq \prod_{j=1}^t \mathfrak{A}_j$, and since $\mathfrak{p}$ is prime, we must have $\mathfrak{p} \supseteq \mathfrak{A}_j$, for some j. □

Lemma 3.17 *(Prime avoidance lemma) Let $\mathfrak{A}$ be an ideal and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be some prime ideals. If $\mathfrak{A} \subseteq \bigcup_{j=1}^t \mathfrak{p}_j$, then $\mathfrak{A} \subseteq \mathfrak{p}_j$, for some j. (The lemma says that if $\mathfrak{A}$ avoids all the $\mathfrak{p}_j$, in the sense that $\mathfrak{A} \not\subseteq \mathfrak{p}_j$, then it avoids $\bigcup_{j=1}^t \mathfrak{p}_j$).*

Proof. We proceed by induction on t. The case $t = 1$ is obvious. Assume the induction hypothesis for $t < n$. Given n prime ideals, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, by the induction hypothesis, we may assume that $\mathfrak{A} \not\subseteq \bigcup_{j \neq i} \mathfrak{p}_j$, for $i = 1, \ldots, n$. Since, by hypothesis, $\mathfrak{A} \subseteq \bigcup_{j=1}^n \mathfrak{p}_j$, for every $i = 1, \ldots, n$, there is some $x_i \in \mathfrak{A}$ with

$$x_i \in \mathfrak{p}_i \quad \text{and} \quad x_i \notin \mathfrak{p}_j, \quad \text{for all } j \neq i. \tag{$\dagger$}$$

Let k be given and form

$$y_k = x_1 \cdots x_{k-1} \widehat{x_k} x_{k+1} \cdots x_n,$$

where, as usual, the hat over x_k means that x_k is omitted. Then, $y_k \in \mathfrak{p}_i$, for all $i \neq k$. We claim that $y_k \notin \mathfrak{p}_k$. Indeed, were it not the case, then we would have $y_k = x_1 \cdots \widehat{x_k} \cdots x_n \in \mathfrak{p}_k$; since $\mathfrak{p}_k$ is prime, there would be some $x_j \in \mathfrak{p}_k$ for some $j \neq k$, a contradiction of ($\dagger$).

Of course, $y_k \in \mathfrak{A}$, for all k. Now, take $a = y_1 + \cdots + y_n$.

Claim. $a \notin \bigcup_{j=1}^n \mathfrak{p}_j$.

Suppose that $a \in \mathfrak{p}_k$, for some k. We can write

$$a = y_k + \sum_{j \neq k} y_j \in \mathfrak{p}_k, \tag{$*$}$$

and since we proved that $y_j \in \mathfrak{p}_k$ for all $j \neq k$, the fact that $a \in \mathfrak{p}_k$ implies that $y_k \in \mathfrak{p}_k$, a contradiction. □

Lemma 3.18 *Say $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are prime ideals in A, then $S = A - \bigcup_{j=1}^n \mathfrak{p}_j$ is a multiplicative subset of A.*

Proof. We have $0 \notin S$ and $1 \in S$. Suppose that $s, t \in S$ and $st \notin S$. Then, $st \in \bigcup_{j=1}^n \mathfrak{p}_j$, and so, $st \in \mathfrak{p}_j$ for some j; as $\mathfrak{p}_j$ is prime, either $s \in \mathfrak{p}_j$ or $t \in \mathfrak{p}_j$, a contradiction. □

Now, I.S. Cohen (1950) showed that noetherian-ness of a ring is controlled by its prime ideals.

Lemma 3.19 *(Cohen, 1950) If $\mathfrak{A}$ is an ideal in a commutative ring, A, and if b is an element of A for which $\mathfrak{A} + (b)$ is f.g. and $(b \longrightarrow \mathfrak{A})$ is also f.g., then $\mathfrak{A}$ is f.g.*

Proof. Say $\mathfrak{A} + (b)$ is generated by $\beta_1, \ldots, \beta_t$. Each β_j is of the form $a_j + \rho_j b$, for some $a_j \in \mathfrak{A}$ and some $\rho_j \in A$. So, the elements $a_1, \ldots, a_t$ and b generate $\mathfrak{A} + (b)$. Let $c_1, \ldots, c_s$ generate $(b \longrightarrow \mathfrak{A})$. Then, $c_j b \in \mathfrak{A}$, for $j = 1, \ldots, s$.

We claim that the elements $a_1, \ldots, a_t, c_1 b, \ldots, c_s b$ generate $\mathfrak{A}$.

Pick $\alpha \in \mathfrak{A}$, then $\alpha \in \mathfrak{A} + (b)$, and so, $\alpha = \sum_{j=1}^t v_j a_j + \rho b$, with a_j as above, for $j = 1, \ldots, t$. But,

$$\rho b = \alpha - \sum_{j=1}^t v_j a_j \in \mathfrak{A},$$

and so, $\rho \in (b \longrightarrow \mathfrak{A})$. Consequently, we can write $\rho = \sum_{j=1}^s u_j c_j$, as the c_j's generate $(b \longrightarrow \mathfrak{A})$. It follows that

$$\alpha = \sum_{j=1}^t v_j a_j + \sum_{j=1}^s u_j (c_j b),$$

as contended. □

Proposition 3.20 *Let A be a commutative ring, then the following are equivalent:*

(1) A is noetherian (A has the ACC).

(2) Every ideal of A is f.g.

(3) A has the maximal condition on ideals.

(4) A has the ACC on f.g. ideals.

(5) (I.S. Cohen, 1950) Every prime ideal of A is f.g.

Proof. We already proved the equivalence (1)–(3) (c.f. Proposition 2.9). Obviously, (1) implies (4) and (2) implies (5).

(4) $\Rightarrow$ (1). Suppose

$$\mathfrak{A}_1 < \mathfrak{A}_2 < \mathfrak{A}_3 < \cdots$$

is a strictly ascending chain of ideals of A. By the axiom of choice, we can find a tuple, $(a_j)_{j=1}^{\infty}$, of elements in A so that $a_j \in \mathfrak{A}_j$ and $a_j \notin \mathfrak{A}_{j-1}$. Look at the ascending chain

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \cdots \subseteq (a_1, \ldots, a_n) \subseteq \cdots .$$

This is a strictly ascending sequence, by the choice of the a_j's, a contradiction.

(5) $\Rightarrow$ (2). Take $\mathcal{F} = \{\mathfrak{A} \text{ an ideal of } A \mid \mathfrak{A} \text{ is not f.g.}\}$ and partially order $\mathcal{F}$ by inclusion. If $\mathcal{F}$ is not empty, it is inductive (DX). By Zorn's lemma, $\mathcal{F}$ has a some maximal element, $\mathfrak{A}$. Since $\mathfrak{A} \in \mathcal{F}$, it is not f.g. and by (5), the ideal $\mathfrak{A}$ is not prime. So, there exist $a, b \in A$ with $a, b \notin \mathfrak{A}$ and yet, $ab \in \mathfrak{A}$. Since $b \notin \mathfrak{A}$, we have $\mathfrak{A} + (b) > \mathfrak{A}$. Now, $a \in (b \longrightarrow \mathfrak{A})$ (since $ab \in \mathfrak{A}$), yet, $a \notin \mathfrak{A}$, and so, $(b \longrightarrow \mathfrak{A}) > \mathfrak{A}$. As $\mathfrak{A}$ is maximal in $\mathcal{F}$, it follows that both $\mathfrak{A} + (b)$ and $(b \longrightarrow \mathfrak{A})$ are f.g. By Cohen's lemma, the ideal $\mathfrak{A}$ is f.g., a contradiction. Therefore, $\mathcal{F} = \emptyset$, and (2) holds. □

We now move back to modules. Given an A-module, M, we make the definition

Definition 3.4 The *support* of an A-module, M, denoted $\mathrm{Supp}(M)$ is that subset of $\mathrm{Spec}\, A$ given by

$$\mathrm{Supp}(M) = \{\mathfrak{p} \in \mathrm{Spec}\, A \mid M_{\mathfrak{p}} \neq (0)\}.$$

Proposition 3.21 *If M is an A-module, then*

$$\mathrm{Supp}(M) \subseteq V((M \longrightarrow (0))) = V(\mathrm{Ann}(M)).$$

If M is f.g., then

$$\mathrm{Supp}(M) = V((M \longrightarrow (0))).$$

So, the support of a f.g. module is **closed** *in* $\mathrm{Spec}\, A$.

Proof. Pick $\mathfrak{p}$ in $\mathrm{Supp}(M)$, i.e., $M_{\mathfrak{p}} \neq (0)$. We need to show that $\mathfrak{p} \in V((M \longrightarrow (0)))$, i.e., $\mathfrak{p} \supseteq (M \longrightarrow (0))$. We will show that if $\mathfrak{p} \not\supseteq (M \longrightarrow (0))$ then $M_{\mathfrak{p}} = (0)$. But, $\mathfrak{p} \not\supseteq (M \longrightarrow (0))$ implies that there is some $s \notin \mathfrak{p}$ with $s \in (M \longrightarrow (0))$. In $M_{\mathfrak{p}}$,

$$\frac{s}{1}\frac{m}{t} = \frac{sm}{t} = 0, \quad \text{as } s \text{ kills } M$$

But, $s/1$ is a unit in $A_{\mathfrak{p}}$, and so, $m/t = 0$ already, and $M_{\mathfrak{p}} = (0)$.

Now, say M is f.g. with $m_1, \ldots, m_t$ as generators. Pick $\mathfrak{p} \in V((M \longrightarrow (0)))$, we need to show that $\mathfrak{p} \in \mathrm{Supp}(M)$. This means, if $\mathfrak{p} \supseteq \mathrm{Ann}(M)$, then $M_{\mathfrak{p}} \neq (0)$. We will prove that if $M_{\mathfrak{p}} = (0)$, then $\mathfrak{p} \not\supseteq \mathrm{Ann}(M)$.

If $M_{\mathfrak{p}} = (0)$, then $m/1 = 0$. So, there is some $s = s(m) \in S$ with $sm = 0$ in M. If we repeat this process for each of the $m_1, \ldots, m_t$ that generate M, we get $s_1, \ldots, s_t \in S$ such that $s_j m_j = 0$, for $j = 1, \ldots, t$. Write $\sigma = s_1 \cdots s_t \in S$. We get $\sigma m_j = 0$ for all $j = 1, \ldots, t$; so, $\sigma \in \mathrm{Ann}(M)$. But, $\sigma \in S$ implies that $\sigma \notin \mathfrak{p}$; consequently, $\mathfrak{p} \not\supseteq \mathrm{Ann}(M)$. □

Proposition 3.22 *Say M is an A-module (where $A \in \mathrm{CR}$). Then, the following are equivalent:*

(1) $M = (0)$.

(2) $\mathrm{Supp}(M) = \emptyset$.

(2a) $M_{\mathfrak{p}} = (0)$, *for all* $\mathfrak{p} \in \mathrm{Spec}\, A$.

(3) $\mathrm{Supp}(M) \cap \mathrm{Max}\, A = \emptyset$.

(3a) $M_{\mathfrak{m}} = (0)$, *for all* $\mathfrak{m} \in \mathrm{Max}\, A$.

Proof. The implications (2) $\Leftrightarrow$ (2a) and (3) $\Leftrightarrow$ (3a) are obvious. Similarly, (1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (3) are trivial. So, we need to show (3) $\Rightarrow$ (1). Let us first assume that M is f.g., Then, we know that $\mathrm{Supp}(M) = V((M \longrightarrow (0)))$. The hypothesis (3) implies that $\mathfrak{m} \supseteq (M \longrightarrow (0))$ for **no** maximal ideal, $\mathfrak{m}$. This implies that $(M \longrightarrow (0)) = (1)$, the unit ideal. Consequently, $1 \in (M \longrightarrow (0))$, and so, $M = (0)$.

Let us now consider the case where M is not f.g. We can write $M = \varinjlim_{\alpha} M_\alpha$, where the M_α's range over the f.g. submodules of M. Now, $M_\alpha \subseteq M$ and localization being exact, $(M_\alpha)_{\mathfrak{m}} \subseteq M_{\mathfrak{m}}$; so, $(M_\alpha)_{\mathfrak{m}} = (0)$ for all $\mathfrak{m} \in \mathrm{Max}\, A$. By the f.g. case, we get $M_\alpha = (0)$ for all α, and thus, $M = (0)$. $\square$

Remark: The implication (3) $\Rightarrow$ (1) can also be proved without using right limits. Here is the proof. Assume $M \neq (0)$. Then, there is some $m \in M$ with $m \neq 0$, and let $\mathrm{Ann}(m) = \{a \in A \mid am = 0\}$; we have $\mathrm{Ann}(m) \neq (1)$; so, $\mathrm{Ann}(m) \subseteq \mathfrak{m}$, for some maximal ideal, $\mathfrak{m}$. Consider $m/1 \in M_{\mathfrak{m}}$. Since $M_{\mathfrak{m}} = (0)$, we have $\lambda m = 0$, for some $\lambda \in A - \mathfrak{m}$; thus, $\lambda \in \mathrm{Ann}(m)$, and yet $\lambda \notin \mathfrak{m} \supseteq \mathrm{Ann}(m)$, a contradiction. Therefore, $M = (0)$. $\square$

Corollary 3.23 *If $M' \xrightarrow{\varphi} M \xrightarrow{\psi} M''$ is a given sequence of modules and maps, then it is exact iff for all $\mathfrak{p} \in \mathrm{Spec}\, A$, the sequence $M'_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \longrightarrow M''_{\mathfrak{p}}$ is exact iff for all $\mathfrak{m} \in \mathrm{Max}\, A$, the sequence $M'_{\mathfrak{m}} \longrightarrow M_{\mathfrak{m}} \longrightarrow M''_{\mathfrak{m}}$ is exact.*

Proof. ($\Rightarrow$). This direction is trivial as localization is an exact functor.

Observe that we need only assume that the sequence $M'_{\mathfrak{m}} \longrightarrow M_{\mathfrak{m}} \longrightarrow M''_{\mathfrak{m}}$ is exact for all $\mathfrak{m} \in \mathrm{Max}\, A$. Then, $(\psi \circ \varphi)_{\mathfrak{m}} = \psi_{\mathfrak{m}} \circ \varphi_{\mathfrak{m}} = 0$; so if N is the image of the map $\psi \circ \varphi$, we find $N_{\mathfrak{m}} = (0)$, for all $\mathfrak{m} \in \mathrm{Max}\, A$. By Proposition 3.22, we get $N = (0)$, and thus $\psi \circ \varphi = 0$.

Let $H = \mathrm{Ker}\ \psi / \mathrm{Im}\ \varphi$. The same argument (using exactness of localization) shows that $H_{\mathfrak{m}} \cong (\mathrm{Ker}\ \psi)_{\mathfrak{m}} / (\mathrm{Im}\ \varphi)_{\mathfrak{m}} = (0)$. Again, Proposition 3.22 implies that $H = (0)$ and $\mathrm{Ker}\ \psi = \mathrm{Im}\ \varphi$, as contended. $\square$

The statement is not that a whole family of local morphisms comes from a global morphism, rather we must have the global morphisms and then exactness is a local property.

Local Terminology: If P is property of A-modules (or morphisms), then a module (or morphism) is *locally P* iff for every $\mathfrak{p} \in \mathrm{Spec}\, A$, the module $M_{\mathfrak{p}}$ has P as $A_{\mathfrak{p}}$-module.[2]

Examples: Locally f.g., locally f.p., locally flat, locally exact, locally free, locally zero. etc.

Sometimes, you get a global result from an everywhere local result.

Proposition 3.24 *(Local flatness criterion) Say M is an A-module (where $A \in \mathrm{CR}$). Then, the following are equivalent:*

(1) M is flat over A.

[2]In reality, this ought to be called "pointwise P".

(2) M is locally flat.

(2a) For every $\mathfrak{p} \in \operatorname{Spec} A$, the module $M_{\mathfrak{p}}$ is flat over A.

(3) For every $\mathfrak{m} \in \operatorname{Max} A$, the module $M_{\mathfrak{m}}$ is flat over $A_{\mathfrak{m}}$.

(3a) For every $\mathfrak{m} \in \operatorname{Max} A$, the module $M_{\mathfrak{m}}$ is flat over A.

Proof. The implications (1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (3) hold, the first by base extension and the second because it is a tautology. We shall prove that (3) $\Rightarrow$ (1) (and along the way, (3) $\Longleftrightarrow$ (3a) and hence, (2) $\Longleftrightarrow$ (2a)). Assume $0 \longrightarrow N' \longrightarrow N$ is exact. Tensoring with M, we get $N' \otimes_A M \longrightarrow N \otimes_A M$. Consider the exact sequence

$$0 \longrightarrow K \longrightarrow N' \otimes_A M \longrightarrow N \otimes_A M,$$

where $K = \operatorname{Ker}(N' \otimes_A M \longrightarrow N \otimes_A M)$. By localizing at $\mathfrak{m}$, we get the exact sequence

$$0 \longrightarrow K \otimes_A A_{\mathfrak{m}} \longrightarrow (N' \otimes_A M) \otimes_A A_{\mathfrak{m}} \longrightarrow (N \otimes_A M) \otimes_A A_{\mathfrak{m}}. \tag{$*$}$$

It follows that the sequence

$$0 \longrightarrow K_{\mathfrak{m}} \longrightarrow N' \otimes_A M_{\mathfrak{m}} \longrightarrow N \otimes_A M_{\mathfrak{m}} \quad \text{is exact.} \tag{$**$}$$

Now, for any module, L,

$$(L \otimes_A M) \otimes_A A_{\mathfrak{m}} \cong (L \otimes_A A_{\mathfrak{m}}) \otimes_{A_{\mathfrak{m}}} (M \otimes A_{\mathfrak{m}}) \cong L_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}},$$

and so, the sequence

$$0 \longrightarrow K_{\mathfrak{m}} \longrightarrow N'_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \quad \text{is also exact.} \tag{$\dagger$}$$

Since, the sequence $0 \longrightarrow N'_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}}$ is exact and

(a) $M_{\mathfrak{m}}$ is $A_{\mathfrak{m}}$-flat; we find $K_{\mathfrak{m}} = (0)$.

(b) $M_{\mathfrak{m}}$ is A-flat; we find $K_{\mathfrak{m}} = (0)$, again.

But, the above holds for all $\mathfrak{m} \in \operatorname{Max} A$, and thus, $K = (0)$, as required. □

This method amounts to studying modules over the $A_{\mathfrak{p}}$'s and the latter are local rings, where matters are usually easier. The basic fact is Nakayama's lemma.

Lemma 3.25 *(Nakayama's lemma) Say A is a commutative ring and $\mathcal{J}(A)$ is its Jacobson radical. Suppose that M is a f.g. A-module and that $\mathcal{J}(A)M = M$. Then, $M = (0)$. That is, if $M \otimes_A (A/\mathcal{J}(A)) = (0)$, then $M = (0)$ (recall that $M \otimes_A (A/\mathcal{J}(A)) \cong M/(\mathcal{J}(A)M)$).*

Proof. Pick a generating set for M of least cardinality. If $M \neq (0)$, this set is nonempty. Write $m_1, \ldots, m_t$ for these generators. As $M = \mathcal{J}(A)M$, we can express $m_t \in M$ as $m_t = \sum_{j=1}^{t} \alpha_j m_j$, where $\alpha_j \in \mathcal{J}(A)$. Consequently,

$$(1 - \alpha_t)m_t = \sum_{j=1}^{t-1} \alpha_j m_j.$$

Now, $1 - \alpha_t \in \mathbb{G}_m(A)$, since $\alpha_t \in \mathcal{J}(A)$. Therefore, $m_t = \sum_{j=1}^{t-1} \alpha_j (1-\alpha_t)^{-1} m_j$, contradicting the minimality of t. □

Corollary 3.26 *(Classical Nakayama) Say A is a local ring and $\mathfrak{m}_A$ is its maximal ideal. Suppose that M is a f.g. A-module and that $\mathfrak{m}_A M = M$. Then, $M = (0)$.*

Corollary 3.27 *On the category of f.g. modules, $A/\mathcal{J}(A)$ is a faithful module. This means if $M \otimes_A (A/\mathcal{J}(A)) = (0)$, then $M = (0)$. (In the local ring case, if $M \otimes_A \kappa(A) = (0)$, then $M = (0)$, with $\kappa(A) = A/\mathfrak{m}_A$.)*

Corollary 3.28 *Let M be an f.g. A-module and say $m_1, \ldots, m_t \in M$ have residues $\overline{m_1}, \ldots, \overline{m_t}$ in $\overline{M} = M \otimes_A (A/\mathcal{J}(A)) \cong M/(\mathcal{J}(A)M)$ which generate $\overline{M}$. Then, $m_1, \ldots, m_t$ generate M.*

Proof. Let N be the submodule of M generated by $m_1, \ldots, m_t$. Look at $\overline{M}/\overline{N} = \overline{M/N}$. Since M is f.g., M/N is f.g. and $\overline{M/N} = \overline{M}/\overline{N} = (0)$. By Corollary 3.27, we get $M/N = (0)$, i.e., $M = N$. □

Corollary 3.29 *Let M be an f.g. A-module and let N be a submodule for which $N + \mathcal{J}(A)M = M$. Then, $N = M$.*

Proof. The hypothesis means $\overline{M} = \overline{N}$; so, $\overline{M/N} = (0)$. We conclude using Corollary 3.27, again. □

Corollary 3.30 *Let A be a local ring and M be a f.g. A-module. Write t for the minimal cardinality of a set of generators for M. Then*

(1) A set of elements $m_1, \ldots, m_r$ generate M iff $\overline{m_1}, \ldots, \overline{m_r}$ span the vector space $M \otimes_A \kappa(A)$.

(2) Every set of generators of M contains a subset generating M with exactly t elements.

The integer t is equal to $\dim_{\kappa(A)}(M \otimes_A \kappa(A))$.

Proof. (1) The implication ($\Rightarrow$) is clear and the implication ($\Leftarrow$) follows from Corollary 3.28.

(2) For vector spaces, each spanning set contains a basis; this implies that each generating set of M contains elements which pass to a basis. So, $t \geq d = \dim_{\kappa(A)}(M \otimes_A \kappa(A))$. As any basis of a vector space spans the vector space, Corollary 3.28 shows that M has a generating set of d elements, and so, $t \leq d$. Therefore, $t = d$. □

Proposition 3.31 *Let A be a local ring and M be an A-module. Assume one of*

(a) A is noetherian and M is f.g.

(b) M is f.p.

Then, the following are equivalent:

(1) M is free over A.

(2) M is projective over A.

(3) M is faithfully flat over A.

(4) M is flat over A.

Proof. The implications (1) $\Rightarrow$ (2), (2) $\Rightarrow$ (4) and (1) $\Rightarrow$ (3), are already known (c.f. Remark (1) after Definition 2.4 for (1) $\Rightarrow$ (2) and c.f. Proposition 2.53 and Proposition 2.66 for (2) $\Rightarrow$ (4) and (1) $\Rightarrow$ (3)). We need only prove (4) $\Rightarrow$ (1). Hypothesis (b) follows from hypothesis (a), so, we assume that M is f.p. and flat. Pick a minimal set of generators for M, having say, having t generators. We have the exact sequence

$$0 \longrightarrow K \longrightarrow A^t \longrightarrow M \longrightarrow 0.$$

As M is f.p. and A^t is f.g., by Proposition 2.41 (or Proposition 2.17), we know that K is also f.g. Since M is flat, when we tensor with $\kappa(A)$, the sequence

$$0 \longrightarrow \overline{K} \longrightarrow \kappa(A)^t \xrightarrow{\Theta} \overline{M} \longrightarrow 0$$

remains exact (a Homework problem, but c.f. below). Since the vector spaces $\overline{M}$ and $\kappa(A)^t$ have the same dimension, Θ is an isomorphism. So, $\overline{K} = (0)$. Since K is f.g., by Nakayama's lemma, $K = (0)$. Therefore, $M \cong A^t$ and M is free over A. $\square$

Remark: For the sake of completeness, here is a proof of the fact referred to during the proof of the previous proposition.

Proposition 3.32 *Let Λ be a ring and consider the exact sequence of Λ-modules*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0. \qquad (*)$$

If M'' is flat, then for any Λ^{op}-module, N, the sequence

$$0 \longrightarrow N \otimes_\Lambda M' \longrightarrow N \otimes_\Lambda M \longrightarrow N \otimes_\Lambda M'' \longrightarrow 0 \quad \textit{is still exact.}$$

Proof. We can write N as a factor of some free Λ^{op}-module, F:

$$0 \longrightarrow K \longrightarrow F \longrightarrow N \longrightarrow 0. \qquad (**)$$

Then, by tensoring $(*)$ with K, F and N and by tensoring $(**)$ with M', M and M'' we obtain the following commutative diagram:

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & K\otimes_\Lambda M' & \longrightarrow & K\otimes_\Lambda M & \longrightarrow & K\otimes_\Lambda M'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \delta_1} & & \downarrow{\scriptstyle \delta_2} & & \downarrow{\scriptstyle \delta_3} & & \\
0 & \longrightarrow & F\otimes_\Lambda M' & \longrightarrow & F\otimes_\Lambda M & \longrightarrow & F\otimes_\Lambda M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & N\otimes_\Lambda M' & \xrightarrow{\theta} & N\otimes_\Lambda M & \longrightarrow & N\otimes_\Lambda M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

The second row is exact because F is free, and thus flat; the third column is exact because M'' is flat, and the other rows and columns are exact because tensor is right-exact. We need to prove that $\theta\colon N \otimes_\Lambda M' \to N \otimes_\Lambda M$ is injective. However, this follows from the snake lemma applied to the first two rows. $\square$

Theorem 3.33 *Let A be a commutative ring and M be an A-module. Assume one of*

(a) A is noetherian and M is f.g.

(b) M is f.p.

Then, the following are equivalent:

(1) M is projective over A.

(2) M is flat over A.

(3) M is locally free over A.

Proof. The implication (1) $\Rightarrow$ (2) is known (c.f. Proposition 2.53 and Proposition 2.66) and (2) $\Rightarrow$ (3) follows from Proposition 3.31. We need to prove (3) $\Rightarrow$ (1). Consider the functor $T\colon N \rightsquigarrow \mathrm{Hom}_A(M, N)$; we must show it is exact. Say

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0 \quad \text{is exact}$$

and apply T. We get

$$0 \longrightarrow \mathrm{Hom}_A(M, N') \longrightarrow \mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_A(M, N'') \longrightarrow C \longrightarrow 0, \qquad (\dagger)$$

where C is the cokernel of the map $\mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_A(M, N'')$. We have the lemma (proved in the Problems):

Lemma 3.34 *If B is a flat A-algebra and M is a f.p. A-module, then the canonical map*

$$\mathrm{Hom}_A(M, N) \otimes_A B \longrightarrow \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B)$$

is an isomorphism.

Let $B = A_{\mathfrak{p}}$, for any $\mathfrak{p} \in \operatorname{Spec} A$. If we localize $(\dagger)$ at $\mathfrak{p}$, we get

$$0 \longrightarrow \mathrm{Hom}_A(M, N')_{\mathfrak{p}} \longrightarrow \mathrm{Hom}_A(M, N)_{\mathfrak{p}} \longrightarrow \mathrm{Hom}_A(M, N'')_{\mathfrak{p}} \longrightarrow C_{\mathfrak{p}} \longrightarrow 0,$$

and Lemma 3.34 implies, this is

$$0 \longrightarrow \mathrm{Hom}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}, N'_{\mathfrak{p}}) \longrightarrow \mathrm{Hom}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}}) \longrightarrow \mathrm{Hom}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}, N''_{\mathfrak{p}}) \longrightarrow C_{\mathfrak{p}} \longrightarrow 0.$$

Yet, by (3), M is locally free, i.e., $M_{\mathfrak{p}}$ is free over $A_{\mathfrak{p}}$. So, $C_{\mathfrak{p}} = (0)$ (since $\mathrm{Hom}(F, -)$ is exact for F free). As $\mathfrak{p}$ is arbitrary, $C = (0)$. □

Proof of Lemma 3.34. Define the map $\theta\colon \mathrm{Hom}_A(M, N) \times B \longrightarrow \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B)$ by

$$\theta(f, b) = b(f \otimes \mathrm{id}_B), \quad \text{for all } f \in \mathrm{Hom}_A(M, N) \text{ and all } b \in B.$$

The map θ is clearly bilinear, so, it induces a canonical linear map

$$\Theta\colon \mathrm{Hom}_A(M, N) \otimes_A B \longrightarrow \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B).$$

Since M is an f.p. A-module, there is an exact sequence

$$\coprod_q A \longrightarrow \coprod_p A \longrightarrow M \longrightarrow 0,$$

for some integers $p, q \geq 0$. Since $\mathrm{Hom}_A(-, N)$ is a left-exact cofunctor, we get

$$0 \longrightarrow \mathrm{Hom}_A(M, N) \longrightarrow \prod_p \mathrm{Hom}_A(A, N) \longrightarrow \prod_q \mathrm{Hom}_A(A, N) \quad \text{is exact.}$$

Tensoring with B, since B is a flat A-algebra, we get

$$0 \longrightarrow \mathrm{Hom}_A(M, N) \otimes_A B \longrightarrow \prod_p \mathrm{Hom}_A(A, N) \otimes_A B \longrightarrow \prod_q \mathrm{Hom}_A(A, N) \otimes_A B \quad \text{is exact.}$$

Similarly, the sequence

$$\Big(\coprod_q A\Big) \otimes_A B \longrightarrow \Big(\coprod_p A\Big) \otimes_A B \longrightarrow M \otimes_A B \longrightarrow 0 \quad \text{is exact,}$$

i.e., the sequence

$$\coprod_q B \longrightarrow \coprod_p B \longrightarrow M \otimes_A B \longrightarrow 0 \quad \text{is exact,}$$

and since $\mathrm{Hom}_B(-, N \otimes_A B)$ is a left-exact cofunctor, we get

$$0 \longrightarrow \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B) \longrightarrow \prod_p \mathrm{Hom}_B(B, N \otimes_A B) \longrightarrow \prod_q \mathrm{Hom}_B(B, N \otimes_A B) \quad \text{is exact.}$$

Thus, we have the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_A(M, N) \otimes_A B & \longrightarrow & \prod_p \mathrm{Hom}_A(A, N) \otimes_A B & \longrightarrow & \prod_q \mathrm{Hom}_A(A, N) \otimes_A B \\
 & & \downarrow \Theta & & \downarrow \Theta_p & & \downarrow \Theta_q \\
0 & \longrightarrow & \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B) & \longrightarrow & \prod_p \mathrm{Hom}_B(B, N \otimes_A B) & \longrightarrow & \prod_q \mathrm{Hom}_B(B, N \otimes_A B).
\end{array}$$

But, clearly Θ_p and Θ_q are isomorphisms; so, the five lemma shows that Θ is an isomorphism. □

These results are wrong if M has no finiteness properties.

Take $A = \mathbb{Z}_{(p)} = \left\{ \frac{r}{s} \;\middle|\; (s,p) = 1 \right\}$ $(= \widehat{\mathbb{Z}_{(p)}} \cap \mathbb{Q})$; this is a local ring, in fact, a local P.I.D. Take $M = \mathbb{Q}$ as $\mathbb{Z}_{(p)}$-module. What is $\kappa(p) = \mathbb{Z}_{(p)}/\mathfrak{m}_p$, where $\mathfrak{m}_p = (p)^e = \left\{ \frac{r}{s} \;\middle|\; r \equiv 0 \,(\mathrm{mod}\, p),\ (s,p) = 1 \right\}$? We have $\mathbb{Z}_{(p)}/\mathfrak{m}_p$ is equal to the localization of $\mathbb{Z}/p\mathbb{Z}$, i.e., $\kappa(p) = \mathbb{Z}/p\mathbb{Z}$. How about $\mathbb{Q} \otimes_{\mathbb{Z}_{(p)}} \kappa(p)$? We have a surjection $\mathbb{Q} \otimes_{\mathbb{Z}} \kappa(p) \longrightarrow \mathbb{Q} \otimes_{\mathbb{Z}_{(p)}} \kappa(p)$. But, $\mathbb{Q} \otimes_{\mathbb{Z}} \kappa(p) = (0)$, so $\mathbb{Q} \otimes_{\mathbb{Z}_{(p)}} \kappa(p) = (0)$. Therefore, $\kappa(p)$ is **not** faithful on $\mathbb{Q}$. Now, were $\mathbb{Q}$ free, then $\mathbb{Q} \otimes_{\mathbb{Z}_{(p)}} \kappa(p)$ would be a vector space of rank equal to $\mathrm{rk}(\mathbb{Q})$ over $\kappa(p)$. So, $\mathbb{Q}$ is not free over $\mathbb{Z}_{(p)}$. But $\mathbb{Q}$ is flat over $\mathbb{Z}_{(p)}$ as $\mathbb{Q}$ is $(\mathbb{Z}_{(p)})_{(0)}$ (the localization of $\mathbb{Z}_{(p)}$ at (0)). Note: $\mathbb{Q} = \varinjlim_n \mathbb{Z}_{(p)} \left[\frac{1}{p^n} \right]$.

Remarks on $M_\mathfrak{p}$, for any A module, M.

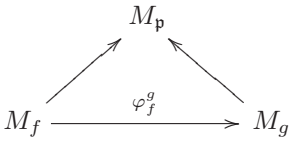
Let $S = A - \mathfrak{p}$, for a given $\mathfrak{p} \in \mathrm{Spec}\, A$. We can partially order S:

$$f \leq g \quad \text{iff} \quad f \mid g^n \quad \text{for some } n > 0,$$

i.e. iff there is some $\xi \in A$ with $f\xi = g^n$. (Note, $\xi \in S$, automatically). Check: This partial order has the Moore–Smith property. So, we can form $\varinjlim_{f \notin \mathfrak{p}} M_f$.

Claim: $\varinjlim_{f \notin \mathfrak{p}} M_f = M_\mathfrak{p}$.

We have maps $M_f \longrightarrow M_\mathfrak{p}$, for all f, and the commutative diagram



for all $f \leq g$. (Since $f \leq g$ iff $f\xi = g^n$ for some $\xi \in S$ and some $n > 0$, the map φ_f^g is given by $\varphi_f^g \left(\frac{m}{f^r} \right) = \frac{m\xi^r}{g^{nr}}$.) Check that φ_f^g is well-defined (DX). Hence, there exists a map $\varinjlim_{f \notin \mathfrak{p}} M_f \longrightarrow M_\mathfrak{p}$. To go backwards, pick $\xi \in M_\mathfrak{p}$. The element ξ is the class of some m/s, with $s \notin \mathfrak{p}$. Now, $m/s \in M_s$; hence, $\mathrm{can}_s(m/s) \in \varinjlim_{f \notin \mathfrak{p}} M_f$. Check that

(1) $\xi \mapsto \mathrm{can}_s(m/s)$ is well defined. It maps $M_\mathfrak{p} \longrightarrow \varinjlim_{f \notin \mathfrak{p}} M_f$.

(2) The map (1) and $\varinjlim_{f \notin \mathfrak{p}} M_f \longrightarrow M_\mathfrak{p}$ from above are mutually inverse.

Geometric Interpretation: We claim that $f \leq g$ iff $X_g \subseteq X_f$.

Indeed, $X_g \subseteq X_f$ iff $V((f)) \subseteq V((g))$ iff $\mathfrak{p} \supseteq (f)$ implies $\mathfrak{p} \supseteq (g)$ iff $\bigcap_{\mathfrak{p} \supseteq (f)} \mathfrak{p} \supseteq (g)$ iff $\sqrt{(f)} \supseteq (g)$ iff $\sqrt{(f)} \supseteq \sqrt{(g)}$. Now, $\sqrt{(f)} \supseteq \sqrt{(g)}$ iff $g \in \sqrt{(f)}$ iff $g^n \in (f)$ for some $n > 0$ iff $f \mid g^n$ iff $f \leq g$. This shows that $\varinjlim_{X_f \ni \mathfrak{p}} M_f = M_\mathfrak{p}$ and so, $M_\mathfrak{p}$ represents germs of some kind. We will come back and elucidate this point later. However, we want to note that for ideals, $\mathfrak{A}$ and $\mathfrak{B}$, the reasoning above shows that

$$V(\mathfrak{A}) \subseteq V(\mathfrak{B}) \quad \text{iff} \quad \sqrt{\mathfrak{A}} \supseteq \sqrt{\mathfrak{B}}.$$

Remark: The following proposition involving comaximal ideals will be needed in the next Chapter and is often handy.

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a ring A are *comaximal* iff $\mathfrak{a}+\mathfrak{b}=A$. The following simple fact holds (DX): If $\mathfrak{a},\mathfrak{b}_1,\ldots,\mathfrak{b}_n$ are ideals so that $\mathfrak{a}$ and $\mathfrak{b}_i$ are comaximal for $i=1,\ldots,n$, then $\mathfrak{a}$ and $\mathfrak{b}_1\cdots\mathfrak{b}_n$ are comaximal.

Proposition 3.35 *(Chinese Remainder Theorem) Let $\mathfrak{a}_1,\ldots,\mathfrak{a}_n$ be ideals of a ring A. If for all $i\neq j$, the ideals $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are comaximal, then*

(1) The canonical map $\varphi\colon A\to\prod_{i=1}^n A/\mathfrak{a}_i$ is surjective.

(2) $\operatorname{Ker}\varphi=\bigcap_{i=1}^n\mathfrak{a}_i=\prod_{i=1}^n\mathfrak{a}_i$.

Consequently, we have a canonical isomorphism

$$\psi\colon A\Big/\Big(\prod_{i=1}^n\mathfrak{a}_i\Big)\to\prod_{i=1}^n(A/\mathfrak{a}_i).$$

Moreover, the converse of (1) holds: If the canonical map $\varphi\colon A\to\prod_{i=1}^n A/\mathfrak{a}_i$ is surjective, then for all $i\neq j$, the ideals $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are comaximal.

Proof. We prove (1) and (2) together by induction on n. If $n=2$, there exist $e_1\in\mathfrak{a}_1$ and $e_2\in\mathfrak{a}_2$ with $e_1+e_2=1$. For any element $(\overline{a}_1,\overline{a}_2)\in A/\mathfrak{a}_1\prod A/\mathfrak{a}_2$, let $a=e_2a_1+e_1a_2$. Then,

$$\pi_i(a)=\pi_i(e_2a_1)+\pi_i(e_1a_2)=\overline{a}_i,\quad i=1,2$$

(where $\pi_i\colon A\to A/\mathfrak{a}_i$ is the canonical projection onto $A/\mathfrak{a}_i$). Thus, φ is surjective.

Since $\mathfrak{a}_1\mathfrak{a}_2\subseteq\mathfrak{a}_1\cap\mathfrak{a}_2$, it is enough to prove that $\mathfrak{a}_1\cap\mathfrak{a}_2\subseteq\mathfrak{a}_1\mathfrak{a}_2$. Now, as $1=e_1+e_2$, for every $a\in\mathfrak{a}_1\cap\mathfrak{a}_2$, we have $a=ae_1+ae_2$; however, $ae_1\in\mathfrak{a}_1\mathfrak{a}_2$ and $ae_2\in\mathfrak{a}_1\mathfrak{a}_2$, so $a\in\mathfrak{a}_1\mathfrak{a}_2$. As $\operatorname{Ker}\varphi=\mathfrak{a}_1\cap\mathfrak{a}_2$, we find $\operatorname{Ker}\varphi=\mathfrak{a}_1\mathfrak{a}_2$.

For the induction step, observe that (by the fact stated just before Proposition 3.35), $\mathfrak{b}=\mathfrak{a}_1\cdots\mathfrak{a}_{n-1}$ and $\mathfrak{a}_n$ are comaximal. Then, by the case $n=2$, we have $\mathfrak{b}\cap\mathfrak{a}_n=\mathfrak{b}\mathfrak{a}_n$; moreover, by the induction hypothesis, $\mathfrak{b}=\bigcap_{i=1}^{n-1}\mathfrak{a}_i=\prod_{i=1}^{n-1}\mathfrak{a}_i$, so we have $\bigcap_{i=1}^n\mathfrak{a}_i=\prod_{i=1}^n\mathfrak{a}_i$.

By the case $n=2$, we have an isomorphism

$$A/\mathfrak{b}\mathfrak{a}_n\cong(A/\mathfrak{b})\prod(A/\mathfrak{a}_n)$$

and by the induction hypothesis, we have an isomorphism

$$A/\mathfrak{b}\cong\prod_{i=1}^{n-1}(A/\mathfrak{a}_i).$$

Therefore, we get an isomorphism

$$A\Big/\Big(\prod_{i=1}^n\mathfrak{a}_i\Big)\cong\prod_{i=1}^n A/\mathfrak{a}_i.$$

Finally, assume that the canonical map $\varphi\colon A\to\prod_{i=1}^n A/\mathfrak{a}_i$ is surjective. Pick i,j with $i\neq j$. By surjectivity, there is some $a\in A$ so that $\pi_i(a)=0$ and $\pi_j(a)=1$, i.e., $\pi_j(1-a)=0$. Therefore, $a\in\mathfrak{a}_i$ and $b=1-a\in\mathfrak{a}_j$ with $a+b=1$, which proves $\mathfrak{a}_i+\mathfrak{a}_j=A$. □

The classical version of the Chinese Remainder Theorem is the case where $A=\mathbb{Z}$ and $\mathfrak{a}_i=m_i\mathbb{Z}$, where the $m_1,\ldots,m_n$ are pairwise relatively prime natural numbers. The theorem says that given any natural numbers $k_1,\ldots,k_n$, there is some natural number, q, so that

$$q\equiv k_i\,(\operatorname{mod} m_i),\quad i=1,\ldots,n,$$

and the solution, q, is unique modulo $m_1m_2\cdots m_n$.

Proposition 3.35 can be promoted to modules.

Proposition 3.36 *Let $M_1, \ldots, M_n$ be submodules of the A-module, M. Suppose the M_i are pairwise comaximal ($M_i + M_j = M$), then the natural map*

$$M \Big/ \Big(\bigcap_{i=1}^{n} M_i \Big) \longrightarrow \prod_{i=1}^{n} (M/M_i)$$

is an isomorphism. (Observe that, $M_i = \mathfrak{a}_i M$ with the $\mathfrak{a}_i$ comaximal ideals, is a special case.)

3.4 First Applications of Fraction Rings

A) **Rings with the DCC**

In this subsection, every ring is a commutative ring with unity.

Lemma 3.37 *If the ring A has the DCC, then* $\mathrm{Max}(A) = \mathrm{Spec}(A)$ *and* $\#(\mathrm{Max}(A))$ *is finite. Thus,* $\dim(A) = 0$.

Proof. Note, $\mathrm{Max}(A) = \mathrm{Spec}(A)$ iff $\dim(A) = 0$, in any commutative ring A. Pick $\mathfrak{p} \in \mathrm{Spec}(A)$ and look at $A/\mathfrak{p}$; the ring $A/\mathfrak{p}$ is a domain and it has the DCC. But, every integral domain with the DCC is a field and conversely. This is proved as follows: Say D is a domain with the DCC, and pick $x \neq 0$ in D. Look at the decreasing chain

$$(x) \supseteq (x^2) \supseteq (x^3) \supseteq \cdots \supseteq (x^n) \supseteq \cdots .$$

By the DCC, there is some n so that $(x^n) = (x^{n+1})$. Thus, $x^n \in (x^{n+1})$, and so, there is some $u \in D$ with $x^n = ux^{n+1}$. It follows that $x^n(1 - ux) = 0$; as $x \neq 0$ and D is a domain, we get $1 - ux = 0$, so, $x^{-1} = u$ and D is a field. Therefore, $\mathfrak{p}$ is maximal since $A/\mathfrak{p}$ is a field.

Let $\mathcal{S}$ be the set of finite intersections of distinct maximal ideals of A. Of course, $\mathcal{S} \neq \emptyset$, so, by the DCC, $\mathcal{S}$ has a minimal element, say $\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n$. We claim that $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_n$ are *all* the maximal ideals of A.

Take another maximal ideal, $\mathfrak{m}$, and look at $\mathfrak{m} \cap \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n$. This ideal is in $\mathcal{S}$ and

$$\mathfrak{m} \cap \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n \subseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n.$$

By minimality, we have

$$\mathfrak{m} \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n \supseteq \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_n.$$

As $\mathfrak{m}$ is prime, $\mathfrak{m} \supseteq \mathfrak{m}_j$, for some j; but both $\mathfrak{m}$ and $\mathfrak{m}_j$ are maximal, so $\mathfrak{m} = \mathfrak{m}_j$. □

Lemma 3.38 *If A is a noetherian ring, then every ideal, $\mathfrak{A}$, contains a product of prime ideals. In particular,* (0) *is a product of prime ideals.*

Proof. (Noetherian induction) Say the conclusion of the lemma is false and let $\mathcal{S}$ denote the collection of all ideals *not* containing a finite product of prime ideals. By assumption, $\mathcal{S} \neq \emptyset$. Since A is noetherian, $\mathcal{S}$ has a maximal element, $\mathfrak{A}$. The ideal $\mathfrak{A}$ can't be prime; so, there exist $a, b \notin \mathfrak{A}$ and yet, $ab \in \mathfrak{A}$. As $\mathfrak{A} + (a) > \mathfrak{A}$, we have $\mathfrak{A} + (a) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$, for some primes $\mathfrak{p}_i$. Similarly, $\mathfrak{A} + (b) \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_s$, for some primes $\mathfrak{q}_j$. Now, we have $\mathfrak{A} = \mathfrak{A} + (ab)$, since $ab \in \mathfrak{A}$; consequently, we get

$$\mathfrak{A} = \mathfrak{A} + (ab) \supseteq (\mathfrak{A} + (a))(\mathfrak{A} + (b)) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

a contradiction. Therefore, $\mathcal{S} = \emptyset$ and the lemma holds. □

Proposition 3.39 *(Akizuki, 1935) Say A is a local ring with the DCC. Then, the maximal ideal, $\mathfrak{m}$, of A is nilpotent (i.e., $\mathfrak{m}^n = (0)$ for some $n \geq 1$) and A is noetherian. The converse is also true.*

Proof. (Nagata) Consider the chain

$$\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \mathfrak{m}^3 \supseteq \cdots \supseteq \mathfrak{m}^n \supseteq \cdots ,$$

it must stop, by the DCC. Thus, there is some $n > 0$ so that $\mathfrak{m}^n = \mathfrak{m}^{n+1}$. Were $\mathfrak{m}^n \neq (0)$, the set $\mathcal{S} = \{\mathfrak{A} \mid \mathfrak{A}\mathfrak{m}^n \neq (0)\}$ would not be empty as $\mathfrak{m} \in \mathcal{S}$. By the DCC, the set $\mathcal{S}$ has a minimal element, call it $\mathfrak{A}$. Let $\mathfrak{p} = \mathrm{Ann}(\mathfrak{A}\mathfrak{m}^n)$. We claim that $\mathfrak{p}$ is a prime ideal. Pick $a, b \notin \mathfrak{p}$. Then, by definition of $\mathfrak{p}$, we have $a\mathfrak{A}\mathfrak{m}^n \neq (0)$ and $b\mathfrak{A}\mathfrak{m}^n \neq (0)$. Yet, $a\mathfrak{A} \subseteq \mathfrak{A}$ and $b\mathfrak{A} \subseteq \mathfrak{A}$ and $\mathfrak{A}$ is minimal in $\mathcal{S}$. Therefore,

$$a\mathfrak{A} = b\mathfrak{A} = \mathfrak{A}.$$

Now,

$$ab\mathfrak{A}\mathfrak{m}^n = a(b\mathfrak{A})\mathfrak{m}^n = (a\mathfrak{A})\mathfrak{m}^n = \mathfrak{A}\mathfrak{m}^n \neq (0),$$

and so, $ab \notin \mathfrak{p}$. Consequently, $\mathfrak{p}$ is indeed prime. By Lemma 3.37, the prime ideal, $\mathfrak{p}$, is maximal; as A is a local ring, we get $\mathfrak{m} = \mathfrak{p}$. As $\mathfrak{m} = \mathfrak{p} = \mathrm{Ann}(\mathfrak{A}\mathfrak{m}^n)$, we have $\mathfrak{m}\mathfrak{A}\mathfrak{m}^n = (0)$, so, $\mathfrak{A}\mathfrak{m}^{n+1} = (0)$, i.e., $\mathfrak{A}\mathfrak{m}^n = (0)$ (remember, $\mathfrak{m}^n = \mathfrak{m}^{n+1}$), a contradiction. Therefore, the maximal ideal, $\mathfrak{m}$, of A is nilpotent.

To prove A has the ACC, argue by induction on the least n so that $\mathfrak{m}^n = (0)$. When $n = 1$, we have $\mathfrak{m} = (0)$ and $A = \kappa(A)$ is a field. Since every field has the ACC, we are done. Assume that the induction hypothesis holds for all $r < n$. Consider the exact sequence

$$0 \longrightarrow \mathfrak{m}^{n-1}/\mathfrak{m}^n \,(= \mathfrak{m}^{n-1}) \longrightarrow A/\mathfrak{m}^n \,(= A) \longrightarrow A/\mathfrak{m}^{n-1} \longrightarrow 0.$$

The left hand term has the DCC and is a module over $A/\mathfrak{m} = \kappa(A)$; so, it is vector space over $\kappa(A)$ and it is finite dimensional. Consequently, it has the ACC, The righthand term has the ACC, by the induction hypothesis. It follows that the middle term, A, has the ACC.

Now, for the converse, assume that A is noetherian, local and that $\mathfrak{m}^n = (0)$ for some $n \geq 1$. We prove that A has the DCC by induction on the index of nilpotence of $\mathfrak{m}$. When $n = 1$, the ring $A = A/\mathfrak{m}$ is a field and so, it has the DCC. Assume that the induction hypothesis holds for all $r < n$. Say $\mathfrak{m}^n = (0)$. Then, we have the exact sequence

$$0 \longrightarrow \mathfrak{m}^{n-1}/\mathfrak{m}^n \,(= \mathfrak{m}^{n-1}) \longrightarrow A/\mathfrak{m}^n \,(= A) \longrightarrow A/\mathfrak{m}^{n-1} \longrightarrow 0,$$

where the righthand side has the DCC by the induction hypothesis. But, the left hand side is a module over $A/\mathfrak{m} = \kappa(A)$; so, it is vector space over $\kappa(A)$ and it has the ACC because A does. Thus, $\mathfrak{m}^{n-1}$ is a finite dimensional vector space, and so, it has the DCC. Therefore, A is caught between two DCC modules, and A is artinian. □

Theorem 3.40 *(Akizuki's structure theorem, 1935) If A is a commutative ring with unity, then A has the DCC iff A has the ACC and* $\mathrm{Max}(A) = \mathrm{Spec}(A)$ *(i.e.,* $\dim(A) = 0$*). When A has the DCC, the map*

$$\theta\colon A \to \prod_{\mathfrak{p}\in \mathrm{Spec}(A)} A_{\mathfrak{p}} \qquad (*)$$

is an isomorphism and each $A_{\mathfrak{p}}$ is an Artin local ring. Moreover, each map $h_{\mathfrak{p}}\colon A \to A_{\mathfrak{p}}$ is a surjection.

Proof. ($\Rightarrow$) By Lemma 3.37, we have $\mathrm{Max}(A) = \mathrm{Spec}(A)$ and $\mathrm{Max}(A)$ only has finitely many elements. Therefore, the product in $(*)$ is a finite product. Each $A_{\mathfrak{p}}$ is local with the DCC, so, it has the ACC (and its maximal ideal is nilpotent), by Proposition 3.39. If θ is an isomorphism, we are done with this part.

(1) The map θ is injective (this is true in general). Pick $a \in A$ and look at the principal ideal $(a) = Aa$. If $\theta(a) = 0$, then $(Aa)_{\mathfrak{p}} = (0)$ for every prime, $\mathfrak{p} \in \mathrm{Spec}(A)$. Therefore, $Aa = (0)$, so, $a = 0$.

(2) The map θ is surjective. The ideal $\mathfrak{p}^e$ in $A_{\mathfrak{p}}$ is nilpotent. So, $(\mathfrak{p}^e)^n = (0)$ in $A_{\mathfrak{p}}$, yet $(\mathfrak{p}^e)^n = (\mathfrak{p}^n)^e$, and thus,

$$A_{\mathfrak{p}} = A_{\mathfrak{p}}/(\mathfrak{p}^e)^n = A_{\mathfrak{p}}/(\mathfrak{p}^n)^e = (A/\mathfrak{p}^n)_{\overline{\mathfrak{p}}},$$

where $\overline{\mathfrak{p}}$ is the image of $\mathfrak{p}$ in $A/\mathfrak{p}^n$. Now, $\mathfrak{p}$ is the unique prime ideal of A which contains $\mathfrak{p}^n$ (since $\mathrm{Spec}(A) = \mathrm{Max}(A)$). Therefore, $A/\mathfrak{p}^n$ is a local ring and $\overline{\mathfrak{p}}$ is its maximal ideal. It follows that $(A/\mathfrak{p}^n)_{\overline{\mathfrak{p}}} = A/\mathfrak{p}^n$, and so $A_{\mathfrak{p}} \cong A/\mathfrak{p}^n$. Each $h_{\mathfrak{p}}$ is thereby a surjection. Since $\mathfrak{p}^{n_{\mathfrak{p}}}$ and $\mathfrak{q}^{n_{\mathfrak{q}}}$ are pairwise comaximal, which means that $(1) = \mathfrak{p}^{n_{\mathfrak{p}}} + \mathfrak{q}^{n_{\mathfrak{q}}}$ (because $\mathrm{Spec}(A) = \mathrm{Max}(A)$), the Chinese Remainder Theorem implies that θ is surjective.

($\Leftarrow$) This time, A has the ACC and $\mathrm{Max}(A) = \mathrm{Spec}(A)$. By Lemma 3.38, the ideal (0) is a product of maximal ideals, say $(0) = \prod_{j=1}^{t} \mathfrak{m}_j$. Let $\mathfrak{m}$ be any maximal ideal. Now $0 \in \mathfrak{m}$ implies that $\mathfrak{m} \supseteq \mathfrak{m}_j$, for some

j. Since both $\mathfrak{m}$ and $\mathfrak{m}_j$ are maximal, $\mathfrak{m} = \mathfrak{m}_j$. Thus, $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ are all the maximal ideals of A. Consider the descending chain

$$A \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \cdots \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_t = (0).$$

In this chain, we have $\mathfrak{m}_1 \cdots \mathfrak{m}_{s-1} \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_s$. The module $\mathfrak{m}_1 \cdots \mathfrak{m}_{s-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_s$ is an $A/\mathfrak{m}_s$-module, hence, a vector space, since $A/\mathfrak{m}_s$ is a field. By hypothesis, this vector space has the ACC. Thus, it is finite-dimensional and it has the DCC. But then, $\mathfrak{m}_1 \cdots \mathfrak{m}_{s-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_s$ has a composition series. If we do this for each s, we obtain a composition series for A. Consequently, A has finite length as A-module, so, it has the DCC. □

Remark: This is false for noncommutative rings. Take the ring R of $n \times n$ lower triangular matrices over $\mathbb{C}$. The "primes of R" are n in number and the localization at the j-th one, M_j, is the full ring of $j \times j$ matrices over $\mathbb{C}$. But, $\theta\colon R \to \prod_{j=1}^{n} M_j(\mathbb{C})$ is only injective, *not surjective*.

B) **Locally Free f.g. A-Modules**.

We begin by restating and reproving that $\mathrm{Supp}(M)$ is closed when M is f.g.

Lemma 3.41 *If M is a f.g. A-module and if $M_\mathfrak{p} = (0)$ for some $\mathfrak{p} \in \operatorname{Spec} A$, then there exists some $\sigma \notin \mathfrak{p}$ so that $\sigma M = (0)$ and $M_\sigma = (0)$.*

Proof. Write $m_1, \ldots . m_t$ for generators of M. Then, $m_j/1 = 0$ in $M_\mathfrak{p} = (0)$. So, there is some $s_j \notin \mathfrak{p}$ with $s_j m_j = 0$ for $j = 1, \ldots, t$. Let $\sigma = s_1 \cdots s_t$, then $\sigma m_j = 0$ for $j = 1, \ldots, t$. Consequently, $\sigma M = (0)$ and $m_j/1 = 0$ in M_σ for $j = 1, \ldots, t$, so, $M_\sigma = (0)$. □

Geometric Interpretation. If $\varphi\colon A \to B$ is a ring map we get a map, $\varphi^{\mathrm{a}}\colon \operatorname{Spec} B \to \operatorname{Spec} A$, namely, $\mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})$. This is a continuous map (because $(\varphi^{\mathrm{a}})^{-1}(V(\mathfrak{A})) = V(B \cdot \varphi(\mathfrak{A}))$, for every ideal $\mathfrak{A} \subseteq A$). Since there is a map $A \longrightarrow A_s$, we get a map $\operatorname{Spec}(A_s) \longrightarrow \operatorname{Spec}(A)$. For this map we have

Proposition 3.42 *The map* $\operatorname{Spec}(A_s) \longrightarrow \operatorname{Spec}(A)$ *takes* $\operatorname{Spec}(A_s)$ *homeomorphically onto the open set, X_s, of* $\operatorname{Spec} A$.

Proof. We make a map $X_s \longrightarrow \operatorname{Spec}(A_s)$. For this, observe that $\mathfrak{p} \in X_s$ iff $s \notin \mathfrak{p}$ iff $\mathfrak{p}^e \in \operatorname{Spec}(A_s)$. Thus, the desired map is $\mathfrak{p} \mapsto \mathfrak{p}^e$. Now, $\mathfrak{q} = \mathfrak{p}^e$ iff $\mathfrak{p} = \mathfrak{q}^c$ = inverse image of $\mathfrak{q}$; therefore, our maps are inverse to one-another and the image of the contraction is X_s (an open set in $\operatorname{Spec} A$). We must now show that the map $X_s \longrightarrow \operatorname{Spec}(A_s)$ *via* $\mathfrak{p} \mapsto \mathfrak{p}^e$ is continuous. The open X_s has as basis of opens the $X_s \cap X_t = X_{st}$, where $t \in A$. The topology in $\operatorname{Spec}(A_s)$ has as basis the opens Y_τ, where $\tau \in A_s$ and $\mathfrak{q} \in Y_\tau$ iff $\tau \notin \mathfrak{q}$. We have $\tau = t/s^n$, for some t and some n. Moreover, $\mathfrak{q} = \mathfrak{p}^e$; so $\tau \notin \mathfrak{q}$ iff $t \notin \mathfrak{p}$ and it follows that $X_s \cap X_t$ corresponds to Y_τ. □

To continue with the 'geometric interpretation, let M be an A-module. We make a presheaf over $\operatorname{Spec} A$ from M, denote it by $\widetilde{M}$. For every open subset, U, in $X = \operatorname{Spec} A$,

$$\widetilde{M}(U) = \left\{ f\colon U \longrightarrow \bigcup_{\mathfrak{p} \in U} M_\mathfrak{p} \;\middle|\; \begin{array}{l} (1)\ f(\mathfrak{p}) \in M_\mathfrak{p} \\ (2)\ (\forall \mathfrak{p} \in U)(\exists m \in M, \exists s \in A)(s \notin \mathfrak{p}, \text{ i.e., } \mathfrak{p} \in X_s) \\ (3)\ (\forall \mathfrak{q} \in X_s \cap U)\left(f(\mathfrak{q}) = \text{image}\left(\tfrac{m}{s}\right) \text{ in } M_\mathfrak{q}\right). \end{array} \right\}$$

The intuition is that $\widetilde{M}(U)$ consists of kinds of functions ("sections") such that for every "point" $\mathfrak{p} \in U$, each function is locally defined in a consistent manner on a neighborhood $(X_s \cap U)$ of $\mathfrak{p}$ (in terms of some element $m \in M$).

The reader should prove that the presheaf, $\widetilde{M}$, is in fact a sheaf on $\operatorname{Spec} A$ (where $\operatorname{Spec} A$ has the Zariski topology) (DX).

Here are two important properties of the sheaf $\widetilde{M}$ (DX):

(1) $\widetilde{M}$ is an exact functor of M. This means, if

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is an exact sequence of A-modules, then

$$0 \longrightarrow \widetilde{M'} \longrightarrow \widetilde{M} \longrightarrow \widetilde{M''} \longrightarrow 0$$

is an exact sequence *of sheaves*. (Recall that if $\mathcal{F} \longrightarrow \mathcal{G}$ is a morphism of sheaves, it is surjective iff for every open, U, and every $\xi \in \mathcal{G}(U)$, there is a covering $\{U_\alpha \longrightarrow U\}_\alpha$ so that $\xi_\alpha = \rho_U^{U_\alpha}(\xi) \in \mathcal{G}(U_\alpha)$ comes from some $\eta_\alpha \in \mathcal{F}(U_\alpha)$ for all α.)

(2) The functor $M \rightsquigarrow \widetilde{M}$ commutes with arbitrary coproducts, i.e., if $M = \coprod_\alpha M_\alpha$, then $\widetilde{M} = \coprod_\alpha \widetilde{M}_\alpha$.

The easiest way to see (1) and (2) is *via* the following ideas: Say $\mathcal{F}$ is a presheaf on some space X. If $x \in X$ is a point, let $\mathcal{F}_x = \varinjlim_{U \ni x} \mathcal{F}(U)$. We call $\mathcal{F}_x$ the *stalk of the presheaf*, $\mathcal{F}$, at x.

Remark: The module, $M_\mathfrak{p}$, is the stalk of $\widetilde{M}$ at $\mathfrak{p}$. This is immediate from the definition (DX).

Proposition 3.43 *Say $\theta\colon \mathcal{F} \to \mathcal{G}$ is a map of sheaves (with values in a category based on sets, e.g., sets, groups, rings, ...) and suppose for all $x \in X$, the map $\theta_x\colon \mathcal{F}_x \to \mathcal{G}_x$ is injective (resp. surjective, bijective). Then θ is injective (resp. surjective, bijective). If $\mathcal{F}_x = (0)$ for all $x \in X$, then $\mathcal{F} = (0)$. (Here, $\mathcal{F}$ has values in groups or modules.)*

Proof. One checks that $\mathcal{F} \rightsquigarrow \mathcal{F}_x$ is an exact functor of $\mathcal{F}$ (for each $x \in X$). Then the last statement implies all the others. For example,

$$0 \longrightarrow \text{Ker } \theta \longrightarrow \mathcal{F} \xrightarrow{\theta} \mathcal{G} \longrightarrow \text{Coker } \theta \longrightarrow 0 \quad \text{is exact;}$$

so, take stalks at x. We get

$$0 \longrightarrow (\text{Ker } \theta)_x \longrightarrow \mathcal{F}_x \xrightarrow{\theta_x} \mathcal{G}_x \longrightarrow (\text{Coker } \theta)_x \longrightarrow 0 \quad \text{is exact.}$$

If θ_x is injective, then $(\text{Ker } \theta)_x = (0)$. By the last statement of the proposition, Ker $\theta = 0$, etc. So, we need to prove that $\mathcal{F}_x = (0)$ for all $x \in X$ implies that $\mathcal{F} = (0)$.

Pick an open, U, of X and pick any $x \in U$. We have $\mathcal{F}_x = \varinjlim_{V \ni x} \mathcal{F}(V)$ (with $V \subseteq U$). If $\xi \in \mathcal{F}(U)$, then ξ_x = image of ξ in $\mathcal{F}_x = 0$. This means that there is some open subset, $V = V_x$, with $\rho_U^V(\xi) = 0$ in $\mathcal{F}(V)$. Then, as x ranges over U, we have a cover, $\{V_x \longrightarrow U\}$, of U and $\rho_U^{V_x}(\xi) = 0$, for all V_x in the cover. By the uniqueness sheaf axiom, we must have $\xi = 0$. Since ξ is arbitrary in $\mathcal{F}(U)$, we get $\mathcal{F}(U) = (0)$. □

It is clear that the remark and this proposition imply (1) and (2) above.

As a special case of the tilde construction, if we view A has a module over itself, we can make the sheaf $\widetilde{A}$ on X, usually denoted $\mathcal{O}_X$. More explicitly, for every open subset, U, in $X = \text{Spec } A$,

$$\mathcal{O}_X(U) = \left\{ f\colon U \longrightarrow \bigcup_{\mathfrak{p} \in U} A_\mathfrak{p} \;\middle|\; \begin{array}{l} (1)\ f(\mathfrak{p}) \in A_\mathfrak{p} \\ (2)\ (\forall \mathfrak{p} \in U)(\exists a, g \in A)(g \notin \mathfrak{p}, \text{ i.e., } \mathfrak{p} \in X_g) \\ (3)\ (\forall \mathfrak{q} \in X_g \cap U)\left(f(\mathfrak{q}) = \text{image}\left(\frac{a}{g}\right) \text{ in } A_\mathfrak{q}\right). \end{array} \right\}$$

Observe that $\mathcal{O}_X$ is a sheaf of local rings, which means that $\mathcal{O}_X(U)$ is a ring for all U and $\mathcal{O}_{X,\mathfrak{p}}$ $(= A_\mathfrak{p})$ is a local ring, for every $\mathfrak{p}$. The sheaf $\widetilde{M}$ is a sheaf of modules over $\mathcal{O}_X$.

Given a module M and an element $s \in A$, we have the sheaves $\widetilde{M} \restriction X_s$ and $\widetilde{M_s}$. Note that $\widetilde{M_s}$ is a sheaf on Spec(A_s) and $\widetilde{M} \restriction X_s$ is a sheaf on X_s, but the map Spec$(A_s) \longrightarrow$ Spec A gives a homeomorphism of Spec$(A_s) \xrightarrow{\sim} X_s$.

Proposition 3.44 *Under the homeomorphism,* $\varphi\colon \operatorname{Spec}(A_s) \widetilde{\longrightarrow} X_s$*, the sheaves* $\widetilde{M}_s$ *and* $\widetilde{M} \restriction X_s$ *correspond.*

Proof. Say $\varphi\colon X \to Y$ is a continuous map of spaces and $\mathcal{F}$ is a sheaf on X. We can make $\varphi_*\mathcal{F}$, a new sheaf on Y, called the *direct image of* $\mathcal{F}$. For any open, V, in Y, set

$$\varphi_*\mathcal{F}(V) = \mathcal{F}(\varphi^{-1}(V)).$$

The sense of our proposition is that $\varphi_*(\widetilde{M}_s)$ and $\widetilde{M} \restriction X_s$ are isomorphic as sheaves on X_s. Now, $\varphi_*(\widetilde{M}_s)(U)$ is just $\widetilde{M}_s(\varphi^{-1}(U))$, where U is an open in $X_s \subseteq \operatorname{Spec} A$. The map $\varphi\colon Y = \operatorname{Spec} A_s \to X_s$ is just $\mathfrak{q} \in \operatorname{Spec}(A_s) \mapsto \mathfrak{q}^c \in \operatorname{Spec} A$. We have

$$\widetilde{M}_s(\varphi^{-1}(U)) = \left\{ f\colon \varphi^{-1}(U) \longrightarrow \bigcup_{\mathfrak{p}\in\varphi^{-1}(U)} (M_s)_{\mathfrak{p}} \;\middle|\; \begin{array}{l} (1)\ f(\mathfrak{p}) \in (M_s)_{\mathfrak{p}} \\ (2)\ (\forall \mathfrak{p} \in \varphi^{-1}(U))(\exists \mu \in M_s, \exists \tau \in A_s)(\mathfrak{p} \in Y_\tau) \\ (3)\ (\forall \mathfrak{q} \in Y_\tau \cap \varphi^{-1}(U))\left(f(\mathfrak{q}) = \text{image}\left(\tfrac{\mu}{\tau}\right) \text{ in } (M_s)_{\mathfrak{q}}\right). \end{array} \right\}$$

Now, $\mathfrak{q} \in \varphi^{-1}(U)$ iff $\mathfrak{q} = \mathfrak{p}^e$ and $\mathfrak{p} \in U \subseteq X_s$. We also have $\mu = m/s^n$, for some $m \in M$; $\tau = t/s^n$, for some $t \in A$, and so, $\mu/\tau = m/t$. It follows that there exists a natural map, $\widetilde{M} \restriction X_s(U) \longrightarrow \varphi_*(\widetilde{M}_s)(U)$, *via* f [given by m/t] $\mapsto f$ [given by $(m/s^n)/(t/s^n)$] $= \mu/\tau$.

This gives a map of sheaves, $\widetilde{M} \restriction X_s \longrightarrow \varphi_*(\widetilde{M}_s)$. We check that on stalks the map is an isomorphism: $(\widetilde{M} \restriction X_s)_{\mathfrak{p}} = M_{\mathfrak{p}}$ and $\varphi_*(\widetilde{M}_s)_{\mathfrak{q}} = (M_s)_{\mathfrak{q}} = (M_s)_{\mathfrak{p}^e} = M_{\mathfrak{p}}$. Therefore, our global map, being a stalkwise isomorphism, is an isomorphism. □

Recall that the stalk $(\widetilde{M})_{\mathfrak{p}}$ is just $M_{\mathfrak{p}}$. So,

$$M_{\mathfrak{p}} = \varinjlim_{f\notin\mathfrak{p}} M_f = \varinjlim_{\mathfrak{p}\in X_f} M_f = \varinjlim_{\mathfrak{p}\in X_f} \widetilde{M}(X_f).$$

Consequently, $M_{\mathfrak{p}}$ consists indeed of "germs"; these are the germs of "sections" of the sheaf $\widetilde{M}$. Thus, $A_{\mathfrak{p}} =$ germs of functions in $\mathcal{O}_X(U)$, for any $\mathfrak{p} \in U$.

Say X is an open ball in $\mathbb{R}^n$ or $\mathbb{C}^n$. Equip X with the sheaf of germs of C^k-functions on it, where $0 \le k \le \infty$ or $k = \omega$:

$$\mathcal{O}_X(U) = \left\{ f\colon U \longrightarrow \bigcup_{u\in U} \mathcal{O}_{X,u} \;\middle|\; \begin{array}{l} (1)\ f(u) \in \mathcal{O}_{X,u} \text{ (germs of } C^k\text{-functions at } u) \\ (2)\ (\forall u \in U)(\exists \text{ small open } X_\epsilon \subseteq U)(\exists\, C^k\text{-function, } g, \text{ on } X_\epsilon) \\ (3)\ (\forall u \in X_\epsilon)\,(f(u) = \text{image}(g) \text{ in } \mathcal{O}_{X,u}). \end{array} \right\}$$

For $\mathbb{C}^n$ and $k = \omega$, we can take g to be a power series converging on X_ϵ. Observe that $\mathcal{O}_X$ is a sheaf of local rings (i.e., $\mathcal{O}_{X,u}$(= germs at u) is a local ring).

The concept of a sheaf help us give a reasonable answer to the question, "what is geometry?"

A *local ringed space* (LRS) is a pair, $(X, \mathcal{O}_X)$, so that

(1) X is a topological space.

(2) $\mathcal{O}_X$ is a sheaf of local rings on X.

Examples.

(1) Open balls in $\mathbb{R}^n$ or $\mathbb{C}^n$, with the sheaf of germs of C^k functions, for a given k, are local ringed spaces.

(2) $(\operatorname{Spec} A, \widetilde{A})$ is an LRS.

The LRS's form a category, $\mathcal{LRS}$. A map $(X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ is a pair of maps, (φ, Φ), such that:

(a) $\varphi\colon X \to Y$ is a continuous map.

(b) $\Phi\colon \mathcal{O}_Y \to \varphi_*\mathcal{O}_X$ is a homomorphism of sheaves of rings.

Now, *geometry is the study of local ringed spaces that are locally standard*, i.e., each point $x \in X$ has a neighborhood, U, and the LRS $(U, \mathcal{O}_X \restriction U)$ is isomorphic to a standard model.

Some standard models:

(a) C^k, *real geometry (C^k-manifolds)*: The standards are open balls, U, in $\mathbb{R}^n$ and $\mathcal{O}_X(U)$ is the sheaf of germs of real C^k-functions on U. (Here, $1 \leq k \leq \infty$, and $k = \omega$ is also allowed).

(b) *Holomorphic geometry*: $k = \omega$. The standards are open balls, U, in $\mathbb{C}^n$ and $\mathcal{O}_X(U)$ is the sheaf of germs of complex C^ω-functions on U (complex holomorphic manifolds).

(c) *Algebraic geometry*: The standard model is $(\operatorname{Spec} A, \widetilde{A})$.

Notice that we can "glue together" standard models to make the geometric objects that are locally standard. Namely, given a family $\{(U_\alpha, \mathcal{O}_{U_\alpha})\}$, of standard models of fixed kind, suppose for all α, β, there exist some opens $U_\alpha^\beta \subseteq U_\alpha$ and $U_\beta^\alpha \subseteq U_\beta$ and isomorphisms $\varphi_\alpha^\beta\colon (U_\alpha^\beta, \mathcal{O}_{U_\alpha} \restriction U_\alpha^\beta) \to (U_\beta^\alpha, \mathcal{O}_{U_\beta} \restriction U_\beta^\alpha)$, and suppose we also have the gluing conditions: $\varphi_\alpha^\beta = (\varphi_\beta^\alpha)^{-1}$ and $\varphi_\alpha^\gamma = \varphi_\beta^\gamma \circ \varphi_\alpha^\beta$ on $U_\alpha \cap U_\beta$, then we can glue all the $(U_\alpha, \mathcal{O}_{U_\alpha})$ together. That is, there is an LRS, $(X, \mathcal{O}_X)$, and it is locally isomorphic to each $(U_\alpha, \mathcal{O}_{U_\alpha})$.

What about a geometric interpretation of some of our previous results?

Consider Lemma 3.41: Given a f.p. module, M, if $M_\mathfrak{p} = (0)$ for some $\mathfrak{p} \in \operatorname{Spec} A$, then there is some $s \notin \mathfrak{p}$ so that $M_s = (0)$ and $sM = (0)$.

Observe that $M_\mathfrak{p} = (0)$ iff $(\widetilde{M})_\mathfrak{p} = (0)$ iff the stalk of $\widetilde{M}$ at $\mathfrak{p}$ is (0). Moreover, $M_s = (0)$ iff $\widetilde{M}_s = (0)$ iff $\widetilde{M} \restriction X_s$ vanishes. So, Lemma 3.41 says that if the stalk of $\widetilde{M}$ vanishes punctually at $\mathfrak{p} \in \operatorname{Spec} A$, then $\widetilde{M}$ vanishes on some open subset, containing $\mathfrak{p}$, of $\operatorname{Spec} A$.

Proposition 3.45 *If A is a commutative ring and M is a f.g. A-module, assume one of*

(i) M is projective, or

(ii) A is noetherian and $M_\mathfrak{p}$ is free over $A_\mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Spec} A$.

Then

(a) There exist $\sigma_1, \ldots, \sigma_t \in A$ so that M_{σ_j} is free over A_{σ_j} and $X = \operatorname{Spec} A = \bigcup_{j=1}^t X_{\sigma_j}$, or

(b) There is some $\sigma \in A$ with $\mathfrak{p} \in X_\sigma$ so that M_σ is free over A_σ.

Proof. We can write

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0,$$

for any f.g. module, M, with F f.g. and free. If M is projective, then the sequence splits. Therefore, K (being an image of F) is f.g., and so, M is f.p.

In (ii), the ring A is noetherian and M is f.g, which implies that M is f.p., here, too. Thus, we will assume that M is f.p. If we prove the (b) statement, then as a f.p. projective is locally free everywhere, the (b) conclusion holds everywhere on $\operatorname{Spec} A$. As $X = \operatorname{Spec} A$ is quasi-compact, we only need finitely many opens to cover X. Therefore, we only need prove (b).

There exists a free module and a map, $\theta\colon F \to M$, so that *at* $\mathfrak{p}$, we have $F_\mathfrak{p} \cong M_\mathfrak{p}$. The sequence

$$0 \longrightarrow \operatorname{Ker}\theta \longrightarrow F \longrightarrow M \longrightarrow \operatorname{Coker}\theta \longrightarrow 0 \quad \text{is exact.}$$

Now, Coker θ is f.g. and $(\text{Coker }\theta)_{\mathfrak{p}} = (0)$. So, there is some $s \in A$ with $(\text{Coker }\theta)_s = (0)$. If we restrict to $X_s \cong \text{Spec } A_s$, we get

$$0 \longrightarrow \text{Ker } \theta \longrightarrow F \longrightarrow M \longrightarrow \text{Coker } \theta \longrightarrow 0 \quad \text{is exact on } X_s.$$

By Proposition 2.41, as M is f.p. and F is f.g., we see that Ker θ is f.g. But, $(\text{Ker }\theta)_{\mathfrak{p}} = (0)$, and by the lemma, again, $(\text{Ker }\theta)_t = (0)$, for some $t \in A$. If we let $\sigma = st$, then $X_\sigma = X_s \cap X_t$, and on X_σ, we have an isomorphism $F_\sigma \xrightarrow{\sim} M_\sigma$. $\square$

Given an A-module, M, we can make the $\mathcal{O}_X$-module, $\widetilde{M}$. This is a sheaf of $\mathcal{O}_X$-modules. There exist index sets, I and J, so that

$$A^{(J)} \longrightarrow A^{(I)} \longrightarrow M \longrightarrow 0, \quad \text{is exact.}$$

(Here, $A^{(I)}$ is an abbreviation for the coproduct $\coprod_I A$.) So, we get

$$\mathcal{O}_X^{(J)} \longrightarrow \mathcal{O}_X^{(I)} \longrightarrow \widetilde{M} \longrightarrow 0,$$

an exact sequence of sheaves. Now, M is free iff $\widetilde{M} \cong \mathcal{O}_X^{(I)}$, for some I. We say that an $\mathcal{O}_X$-module, $\mathcal{F}$, is *locally-free* iff for every $\mathfrak{p} \in \text{Spec } A$, the module $\mathcal{F}_{\mathfrak{p}}$ is a free $\mathcal{O}_{X,\mathfrak{p}}$-module. Our proposition says: If $\mathcal{F} = \widetilde{M}$ and $\mathcal{F}$ is f.p. then $\mathcal{F}$ is projective[3] iff $\mathcal{F}$ is locally-free. One can characterize the $\mathcal{O}_X$-modules, $\mathcal{F}$, that are of the form $\widetilde{M}$ for some module, M; these are called *quasi-coherent $\mathcal{O}_X$-modules*.

We proved that if $\mathcal{F}_{\mathfrak{p}}$ is a free module of finite rank and if A is noetherian and $\mathcal{F}$ is quasi-coherent, then there is some open set, X_σ, with $\mathfrak{p} \in X_\sigma$, so that $\mathcal{F} \restriction X_\sigma = \mathcal{O}_X^n \restriction X_\sigma$. Actually, we only used f.p., so the statement also holds if $\mathcal{F}$ is projective (A not necessarily noetherian) and then it holds *everywhere* on *small* opens, U, so that

$$\mathcal{F} \restriction U = \mathcal{O}_X^{n(U)} \restriction U.$$

Let's assume that M is projective and f.g. over A. Define $\text{rk}(\widetilde{M}) = \text{rk}(\mathcal{F})$, a function from Spec A to $\mathbb{Z}$, by

$$(\text{rk}\,\mathcal{F})(\mathfrak{p}) = \text{rk}(\mathcal{F}_{\mathfrak{p}}).$$

We showed that this function is locally constant on Spec A, i.e., $\text{rk}\,\mathcal{F}$ is a continuous function from Spec A to $\mathbb{Z}$, where $\mathbb{Z}$ has the discrete topology. Hence, if Spec A is connected, then the rank is a constant.

Proposition 3.46 *Suppose M is a f.g. projective A-module (so, M is f.p.), and let $\mathcal{F} = \widetilde{M}$ on $X = \text{Spec } A$. Then, the function* rk$(\mathcal{F})$ *takes on only finitely many values, $n_1, \ldots, n_t$ (in $\mathbb{Z}$) and there exist ideals $\mathfrak{A}_1, \ldots, \mathfrak{A}_t$ of A, each a commutative ring with unity, so that*

(a) $A = \prod_{j=1}^t \mathfrak{A}_j$; so $1 = e_1 + \cdots + e_t$, with the e_j's being orthogonal idempotents (which means that $e_i^2 = e_i$ and $e_i e_j = 0$ for $i \neq j$) and $\mathfrak{A}_j = Ae_j$.

(b) If X_{e_j} is the usual open corresponding to the element e_j, then $X = \bigcup_{j=1}^t X_{e_j}$.

(c) If $M_j = \mathfrak{A}_j M$, then $M = \coprod_{j=1}^t M_j$ and each M_j is A and $\mathfrak{A}_j$-projective.

(d) Supp $M_j = X_{e_j}$, *and* rk(M_j) *on X_{e_j} is the constant n_j.*

The following lemma is needed:

Lemma 3.47 *If $X = \text{Spec } A$ and $X = X_1 \bigcup X_2$ is a disconnection, then there exist $e_1, e_2 \in A$ so that $X_j = X_{e_j}$ and $1 = e_1 + e_2$; $e_1^2 = e_1$; $e_2^2 = e_2$; $e_1 e_2 = 0$.*

[3] In the full subcategory of the $\mathcal{O}_X$-modules consisting of those of the form $\widetilde{M}$.

Proof. (DX)

Proof of Proposition 3.46. Let $X_n = \mathrm{rk}(\mathcal{F})^{-1}(\{n\})$ for every $n \geq 0$. Each X_n is an open and closed subset of X, by continuity. The X_n cover X and by quasi-compactness only finitely many are necessary. Yet, they are mutually disjoint. It follows that $\mathrm{rk}(\mathcal{F}) = n_1, \ldots, n_t$ and $\mathrm{rk}(\mathcal{F}) \restriction X_j = n_j$. (Here, $X_j = X_{n_j}$.) By Lemma 3.47, there exist $e_1, \ldots, e_t$, orthogonal idempotents with sum 1 and $X_j = X_{e_j}$, for $j = 1, \ldots, t$. Let $\mathfrak{A}_j = Ae_j$, this is an ideal, a ring and $e_j \in \mathfrak{A}_j$ is its unit element. Thus, parts (a) and (b) are proved.

Write $M_j = \mathfrak{A}_j M$; then, $M = \coprod_{j=1}^{t} M_j$, each M_j is a cofactor of M and, as M is A-projective, each M_j is A-projective. The ring A acts on M *via* $\mathfrak{A}_j$; therefore, M_j is $\mathfrak{A}_j$-projective.

Pick any $\mathfrak{q} \in \operatorname{Spec} \mathfrak{A}_j$ and write $\mathfrak{p} = \mathfrak{q} \coprod_{i \neq j} \mathfrak{A}_i$. This ideal, $\mathfrak{p}$, is a prime ideal of A. Note, e_i with $i \neq j$ lies in $\mathfrak{p}$, but $e_j \notin \mathfrak{p}$, so $\mathfrak{p} \in X_j$. Since $e_i e_j = 0$, we also have $e_i e_j = 0$ in $A_\mathfrak{p}$. Yet, $e_j \notin \mathfrak{p}$, so e_j is a unit in $A_\mathfrak{p}$; it follows that $e_i = 0$ in $A_\mathfrak{p}$ for all $i \neq j$. Then, we have

$$M_\mathfrak{p} = \coprod_i (M_i)_\mathfrak{p} = \coprod_i (\mathfrak{A}_i M)_\mathfrak{p} = \coprod_i (Ae_i M)_\mathfrak{p} = (M_j)_\mathfrak{p}.$$

The reader should check that $(M_j)_\mathfrak{p} = (M_j)_\mathfrak{q}$. Since $\mathfrak{p} \in X_j$, we deduce that $(\mathrm{rk}\, M_j)(\mathfrak{q}) = (\mathrm{rk}\, M)(\mathfrak{p}) = n_j$, so, $(\mathrm{rk}\, M_j)(\mathfrak{q}) = n_j$. As $e_i = 0$ iff $i \neq j$ in $A_\mathfrak{p}$, we get $\mathrm{Supp}(M_j) = X_{e_j} = X_j$. □

The simplest case, therefore, is: the A-module M is f.g., projective and $\mathrm{rk}\, M \equiv 1$ on $X = \operatorname{Spec} A$. We say that M is an *invertible module* or a *line bundle* if we wish to view it geometrically.

Note: If M and M' are invertible, then $M \otimes_A M'$ is again a rank 1 projective A-module because $(M \otimes_A M')_\mathfrak{p} = M_\mathfrak{p} \otimes_{A_\mathfrak{p}} M'_\mathfrak{p}$. Thus, these modules form a semigroup under $\otimes_A$ and A (the free module) is the unit element. Do they form a group?

Proposition 3.48 *If A is a commutative ring and M is a f.g. A-module, then M is rank* 1 *projective iff there is another module, M', so that $M \otimes_A M' \cong A$. When the latter condition holds, we can take $M' = M^D = \mathrm{Hom}_A(M, A)$.*

Proof. ($\Longrightarrow$) The module M is rank 1 projective and as it is projective, it is f.p. Look at $M \otimes_A M^D$. There exists a module map,

$$M \otimes_A M^D \longrightarrow A,$$

namely, the linear map induced by the bilinear map $(m, f) \mapsto f(m)$. Localize at each $\mathfrak{p}$. We get

$$M_\mathfrak{p} \otimes_{A_\mathfrak{p}} M^D_\mathfrak{p} \longrightarrow A_\mathfrak{p},$$

and $M^D_\mathfrak{p} = \mathrm{Hom}_A(M, A)_\mathfrak{p} \xrightarrow{\sim} \mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, A_\mathfrak{p})$, as M is f.p. and $A_\mathfrak{p}$ is flat over A. But, $M_\mathfrak{p} \cong A_\mathfrak{p}$, by hypothesis and the reader should check that $M_\mathfrak{p} \otimes_{A_\mathfrak{p}} M^D_\mathfrak{p} \longrightarrow A_\mathfrak{p}$ is an isomorphism. As this holds for every $\mathfrak{p} \in \operatorname{Spec} A$, the map $M \otimes_A M^D \longrightarrow A$ is an isomorphism.

($\Longleftarrow$) Now, we have some A-module, M', and $M \otimes_A M' \cong A$. We can write

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0,$$

for some f.g. free module, F. Look at the last three terms in this sequence, and write $F = \coprod_{\text{finite}} A$:

$$\coprod_{\text{finite}} A \longrightarrow M \longrightarrow 0.$$

If we tensor with M', we get

$$\coprod_{\text{finite}} M' \longrightarrow M \otimes_A M' \cong A \longrightarrow 0.$$

But A is free, so the sequence splits and there is a map $A \longrightarrow \coprod_{\text{finite}} M'$. Now, tensor with M. We get

$$\coprod_{\text{finite}} A \longrightarrow M \longrightarrow 0,$$

and there is a splitting map $M \longrightarrow \coprod_{\text{finite}} A$. Thus, M is a cofactor of a free and f.g. module, so, M is f.g. and projective, and hence, f.p. Now look at

$$M \otimes_A M' \cong A$$

and localize at $\mathfrak{p}$. We get

$$M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} M'_{\mathfrak{p}} \cong A_{\mathfrak{p}},$$

and if we reduce mod $\mathfrak{p}^e$, we get

$$M_{\mathfrak{p}}/\mathfrak{p}^e M_{\mathfrak{p}} \otimes_{\kappa(A_{\mathfrak{p}})} M'_{\mathfrak{p}}/\mathfrak{p}^e M'_{\mathfrak{p}} \cong \kappa(A_{\mathfrak{p}}). \tag{$\dagger$}$$

All the modules in ($\dagger$) are vector spaces and, by counting dimensions, we get

$$\dim_{\kappa(A_{\mathfrak{p}})} M_{\mathfrak{p}}/\mathfrak{p}^e M_{\mathfrak{p}} = 1.$$

Since $M_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module, by Nakayama, we get $\mathrm{rk}(M_{\mathfrak{p}}) = 1$. Lastly,

$$M' \cong A \otimes_A M' \cong (M^D \otimes_A M) \otimes_A M' \cong M^D \otimes_A (M \otimes_A M') \cong M^D \otimes_A A \cong M^D.$$

Therefore, $M' \cong M^D$. $\square$

The group of (isomorphism classes) of the rank 1 projectives, M, is called the *Picard group* of A, denoted $\mathrm{Pic}(A)$.

Corollary 3.49 *If k is a field or a PID, then* $\mathrm{Pic}(A) = (0)$.

The group $\mathrm{Pic}(A)$ is a subtle invariant of a ring (generally hard to compute).

3.5 Integral Dependence

The notion of integral dependence first arose in number theory; later, thanks to Zariski, it found application in algebraic geometry. Throughout this section as throughout this chapter, all rings are commutative with unity.

Definition 3.5 Suppose $\varphi\colon A \to B$ is a ring homomorphism and $b \in B$. The element, b, is *integral over* A iff there is a non-trivial **monic** polynomial, $f(X) \in A[X]$, so that $f(b) = 0$. (Here, $f(b)$ is $b^n + \varphi(a_1)b^{n-1} + \cdots + \varphi(a_{n-1})b + \varphi(a_n)$ if $f(X)$ is $X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$.) The A-algebra B is *integral over* A iff all its elements are integral over A and, in this case, φ is an *integral morphism*.

Clearly, each ring surjection is an integral morphism, but this is not what is really intended. Each homomorphism, φ, as above factors into a surjection whose image, $\widetilde{A}$, is a subring of B followed by the inclusion $\widetilde{A} \hookrightarrow B$. It is for inclusions that integrality is a real question and is decisive for certain situations. As usual, there are a number of equivalent ways to say integrality and their equivalence is quite useful technically.

Proposition 3.50 *Suppose $\varphi\colon A \to B$ is a ring homomorphism and $b \in B$. Then the following are equivalent conditions:*

(1) b is integral over A

(2) The A-algebra $A[b]$ (a sub-A-algebra of B) is finitely generated as A-module.

(3) There exists a sub-A-algebra, $\widetilde{B}$, of B which is a finitely generated A-module and $b \in \widetilde{B}$.

(4) There exists a finitely generated sub-A-module, $\widetilde{B}$, of B so that α) $b\widetilde{B} \subseteq \widetilde{B}$ and β) $\widetilde{A}[b] \cap \mathrm{Ann}(\widetilde{B}) = (0)$.

Proof. (1) $\Longrightarrow$ (2). We have the equation of integral dependence

$$b^n + a_1b^{n-1} + \cdots + a_{n-1}b + a_n = 0$$

(here, we drop $\varphi(a_j)$ and just denote it by a_j). Hence, $b^n \in A$-module generated by $1, b, \ldots, b^{n-1}$. But then, b^{n+1} is also in this A-module, etc. Thus, $A[b]$ is the finitely generated A-module given by generators $1, b, \ldots, b^{n-1}$.

(2) $\Longrightarrow$ (3). We take $\widetilde{B} = A[b]$.

(3) $\Longrightarrow$ (4). We use our subalgebra, $\widetilde{B}$, of (3) for the module of (4). Of course, α) holds as $\widetilde{B}$ is a ring by (3) and β) is clear as $a \in \widetilde{B}$.

(4) $\Longrightarrow$ (1). Let $\xi_1, \ldots, \xi_t$ be generators for $\widetilde{B}$ as A-module. Since $b\widetilde{B} \subseteq \widetilde{B}$, we see that for each i, the element $b\xi_i$ is an A-linear combination of the ξ's:

$$b\xi_i = \sum_{j=1}^{t} z_{ij}\xi_j.$$

That is,

$$\sum_{j=1}^{t} (\delta_{ij}b - z_{ij})\xi_j = 0, \quad \text{for } i = 1, 2, \ldots, t. \tag{$*$}$$

Write Δ for $\det(\delta_{ij}b - z_{ij})$, then by linear algebra we get $\Delta\xi_j = 0$ for all j, i.e., $\Delta \in \mathrm{Ann}(\widetilde{B})$. Upon expanding Δ by minors, we find that $\Delta \in \widetilde{A}[b]$; so, β) implies $\Delta = 0$. But the expansion by minors shows Δ has the form $b^t +$ lower powers of b and this gives (1). $\square$

There are many corollaries, but first notice that *if A is noetherian, we may replace (3) by the weaker condition*

($3'$) There is a finitely generated sub-A-**module**, $\widetilde{B}$, of B and $A[b] \subseteq \widetilde{B}$.

Let's write

$$\mathrm{Int}_A(B) = \{b \in B \mid b \text{ is integral over } A\}$$

and refer to $\mathrm{Int}_A(B)$ as the *integral closure of A in B* (we assume φ is given *a priori*).

Corollary 3.51 *Say A and B are given as above and $b_1, \ldots, b_t$ are elements of B. Then, $b_1, \ldots b_t \in \mathrm{Int}_A(B)$ iff the A-algebra $A[b_1, \ldots, b_t]$ is a finitely generated A-module. In particular, $\mathrm{Int}_A(B)$ is a A-algebra.*

Proof. ($\Longleftarrow$). Here, $A[b_j] \subseteq A[b_1, \ldots, b_t]$ and we apply (3) of Proposition 3.50 to get $b_j \in \mathrm{Int}_A(B)$.

($\Longrightarrow$). We have the chain of A-algebras

$$A[b_1, \ldots, b_t] \supseteq \cdots \supseteq A[b_1] \supseteq \widetilde{A}$$

each a finite module over its predecessor by (2) of Proposition 3.50. Then, it is clear that $A[b_1, \ldots, b_t]$ is a finite A-module. Lastly, if $x, y \in \mathrm{Int}_A(B)$, we see that $x \pm y$ and xy lie in $A[x, y]$. By the above, the latter is a finite A-module and (3) of Proposition 3.50 completes the proof. □

Corollary 3.52 *(Transitivity of Integral Dependence) Suppose that B is an A-algebra and C is a B-algebra. Then,*

$$\mathrm{Int}_{\mathrm{Int}_A(B)}(C) = \mathrm{Int}_A(C).$$

In particular, if C is integral over B and B is integral over A, then C is integral over A.

Proof. If $\xi \in C$ and ξ is integral over A, then ξ is *a fortiori* integral over the "bigger' ring $\mathrm{Int}_A(B)$, and so

$$\mathrm{Int}_A(C) \subseteq \mathrm{Int}_{\mathrm{Int}_A(B)}(C).$$

Now, if ξ is integral over $\mathrm{Int}_A(B)$, then ξ is integral over $A[b_1, \ldots, b_t]$ where the b_i are coefficients in the polynomial of integral dependence for ξ. Each b_i is in $\mathrm{Int}_A(B)$, so Corollary 3.51 shows $A[b_1, \ldots, b_t]$ is a finite A-module. Yet $A[b_1, \ldots, b_t][\xi]$ is a finite $A[b_1, \ldots, b_t]$-module by integrality of ξ. Therefore ξ is in the finitely generated A-module $A[b_1, \ldots, b_t, \xi]$ which is an A-algebra and we apply (3) of Proposition 3.50. The element ξ is then in $\mathrm{Int}_A(C)$, as required.

When C is integral over B and B is integral over A, we get $C = \mathrm{Int}_B(C)$ and $B = \mathrm{Int}_A(B)$; so $C = \mathrm{Int}_A(C)$ by the above. □

When $\mathrm{Int}_A(B)$ is $\widetilde{A}$ (image of A in B) itself, we say A *is integrally closed in B*. (Usually, for this terminology, one assume φ is an inclusion $A \hookrightarrow B$.) If S is the set of non-zero divisors of A, then S is a multiplicative set and $S^{-1}A$ is the *total fraction ring of A*. We denote it by $\mathrm{Frac}(A)$. When A in integrally closed in $\mathrm{Frac}(A)$, we call A a *normal ring* or an *integrally closed ring*. For example

Proposition 3.53 *Every unique factorization domain is a normal ring.*

Proof. We suppose A is a UFD, write $K = \mathrm{Frac}(A)$ (in this case K is a field as A is a domain). Let $\xi = \alpha/\beta$ be integral over A, and put α/β in lowest terms. Then,

$$\xi^n + a_1\xi^{n-1} + \cdots + a_{n-1}\xi + a_n = 0, \quad \text{the } a_j \in A.$$

Insert the value of ξ ($= \alpha/\beta$) and clear denominators. We get

$$\alpha^n + a_1\alpha^{n-1}\beta + \cdots + a_{n-1}\alpha\beta^{n-1} + a_n\beta^n = 0.$$

If p is a prime element of A and p divides β, our equation shows $p \mid \alpha^n$; i.e., $p \mid \alpha$. This is a contradiction on lowest terms and so no p divides β. This means β is a unit; so, $\xi \in A$. □

Proposition 3.54 *If A is a normal domain and S is any multiplicative subset of A, then $S^{-1}A$ is also a normal domain.*

Proof. We know $\mathrm{Frac}(A) = \mathrm{Frac}(S^{-1}A)$. So, choose $\xi \in \mathrm{Frac}(A)$ integral over $S^{-1}A$. Then,

$$\xi^n + \frac{a_1}{s_1}\xi^{n-1} + \cdots + \frac{a_{n-1}}{s_{n-1}}\xi + \frac{a_n}{s_n} = 0.$$

We can write this with common denominator $s = \prod s_j$, then

$$\xi^n + \frac{a_1}{s}\xi^{n-1} + \cdots + \frac{a_{n-1}}{s}\xi + \frac{a_n}{s} = 0.$$

Upon multiplication by s^n, we find $(s\xi)$ is integral over A. By hypothesis, $s\xi \in A$; so, $\xi \in S^{-1}A$. □

Two easy facts are useful to know. Their proof are easy and will be left to the reader (DX):

Fact A. If B is integral over A and $\mathfrak{I}$ is any ideal of B, then $B/\mathfrak{I}$ is integral over $A/\varphi^{-1}(\mathfrak{I})$.

Fact B. If B is integral over A and S is a multiplicative set in A with $S \cap \mathrm{Ker}\ \varphi = \emptyset$, then $S^{-1}B$ is integral over $S^{-1}A$.

However, observe that *if A is a normal ring and $\mathfrak{A}$ is one of its ideals, then $A/\mathfrak{A}$ need* **not** *be normal.* A standard example is a "singular curve".

Here, we take $\mathbb{C}[X,Y]$ which is a normal ring as it is a UFD. Let $\mathfrak{A} = (Y^2 - X^3)$, then $\mathbb{C}[X,Y]/\mathfrak{A}$ is **not** normal (though it is a domain (DX)). For, the element $\overline{Y}/\overline{X}$ (in Frac$A/\mathfrak{A}$) is integral over $A/\mathfrak{A}$ as its square is $\overline{X}$, yet it is not itself in $A/\mathfrak{A}$ (DX). The interpretation is this: $Y^2 - X^3 = 0$ describes a curve in the plane over $\mathbb{C}$ and Y/X defines by restriction a function holomorphic on the curve except at $(0,0)$. But, $\overline{Y}/\overline{X}$ is bounded near $(0,0)$ *on the curve*, so it ought to be extendable to a holomorphic (and algebraic) function. Yet, the set of such (near $(0,0)$) is just $(A\mathfrak{A})_{\mathfrak{p}}$, where $\mathfrak{p} = \{f \in A/\mathfrak{A} \mid f(0,0) = 0\}$. Of course, $\overline{Y}/\overline{X} \notin (A\mathfrak{A})_{\mathfrak{p}}$. The trouble is that $Y^2 = X^3$ has a "singular point" at $(0,0)$, it is **not** a complex manifold there (but it is everywhere else). This shows up in the fact that $(A\mathfrak{A})_{\mathfrak{p}}$ is not normal.

When A is a noetherian ring, we can be more precise, but we need some of the material (on primary decomposition from Sections 3.6 and 3.7. The two main things necessary are the statement

If V is a submodule of the A-module, M, then $V = (0)$ iff $V_{\mathfrak{p}} = (0)$ for all $\mathfrak{p} \in \mathrm{Ass}(M)$ (see Section 3.6, Corollary 3.102 of Theorem 3.99); and Krull's Principal Ideal Theorem (Section 3.7, Theorem 3.120).

You should skip the proof of Lemma 3.55, Theorem 3.56 and Corollary 3.57 until you read this later material; pick up the thread in Theorem 3.58, below.

Write, for a ring A,

$$\mathrm{Pass}(A) = \{\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}(A/(a)), \text{ for some } \textit{non-zero divisor}, a, \text{ of } A\}.$$

Lemma 3.55 *If A is a reduced Noetherian ring, then an element $\xi \in \mathrm{Frac}(A)$ is actually in A if and only if for every, $\mathfrak{p} \in \mathrm{Pass}(A)$, the image of $\xi \in \mathrm{Frac}(A)_{\mathfrak{p}}$ is in $A_{\mathfrak{p}}$.*

Proof. If $\xi \in A$, then of course its image in $\mathrm{Frac}(A)_{\mathfrak{p}}$ lies in $A_{\mathfrak{p}}$ for all $\mathfrak{p}$. So, assume

$$\xi \in \bigcap \{A_{\mathfrak{p}} \mid \mathfrak{p} \in \mathrm{Pass}(A)\}$$

(here, of course, we mean the images of ξ in $\mathrm{Frac}(A)$ are in $A_{\mathfrak{p}}$). We write $\xi = \alpha/\beta$, where β is a non-zero divisor and suppose that $\xi \notin A$. Then, α is not in (β), so $V = A\overline{\alpha} \subseteq A/(\beta)$ is non-zero. By the statement italicized above, there is a $\mathfrak{p} \in \mathrm{Ass}(A/(\beta))$ with $(A\overline{\alpha})_{\mathfrak{p}} \neq (0)$. This means $\alpha/1 \notin (\beta)_{\mathfrak{p}}$; that is, $\xi = \alpha/\beta \notin A_{\mathfrak{p}}$. Yet, $\mathfrak{p} \in \mathrm{Pass}(A)$, a contradiction. □

Here is a characterization of normality for Noetherian domains:

Theorem 3.56 *Suppose that A is a noetherian domain, then the following conditions are equivalent:*

(1) A is normal

(2) For every $\mathfrak{p} \in \mathrm{Pass}(A)$, the ideal $\mathfrak{p}^e$ is a principal ideal of $A_{\mathfrak{p}}$

(3) (a) Every $\mathfrak{p} \in \mathrm{Pass}(A)$ has height 1 and

(b) For all height one primes, $\mathfrak{p}$, of A, the ring $A_{\mathfrak{p}}$ is a PID.

Proof. We first prove (2) $\Longleftrightarrow$ (3). Suppose $\mathfrak{p}$ is any prime ideal of A. If $\mathfrak{p}$ is a principal ideal of $A_{\mathfrak{p}}$. it is an isolated prime of itself and Krull's Principal Ideal Theorem shows that $\mathrm{ht}(\mathfrak{p}) = 1$. So by (2),

$$\mathrm{Pass}(A) \subseteq \{\mathfrak{p} \mid \mathrm{ht}(\mathfrak{p}) = 1\}.$$

But, $\mathrm{ht}(\mathfrak{p}) = 1$ implies $\mathfrak{p}$ is an isolated prime ideal of any of its non-zero elements and, since A is a domain, this shows $\mathfrak{p} \in \mathrm{Pass}(A)$. We've proved that (2) implies that

$$\mathrm{Pass}(A) = \{\mathfrak{p} \mid \mathrm{ht}(\mathfrak{p}) = 1\}. \tag{$*$}$$

This shows that (2) implies (3a) and for all height one primes, $\mathfrak{p}$, the maximal ideal, $\mathfrak{p}$, of $A_{\mathfrak{p}}$ is principal. We'll now show that $A_{\mathfrak{p}}$ is a PID. Pick an ideal, $\mathfrak{A}$, of $A_{\mathfrak{p}}$ and write $\mathfrak{m} = \mathfrak{p}^e$. As $\mathfrak{m}$ is the maximal ideal of $A_{\mathfrak{p}}$, we have $\mathfrak{A} \subseteq \mathfrak{m}$, and as $\mathfrak{m}$ is principal we may assume $(0) < \mathfrak{A} < \mathfrak{m}$. Now $\mathfrak{m}^n$ is principal for all $n \geq 0$ with generator π^n, where π generates $\mathfrak{m}$; we'll show $\mathfrak{A} = \mathfrak{m}^n$ for some n. Now, were $\mathfrak{A} \subseteq \mathfrak{m}^n$ for all n, the Krull Intersection Theorem (Theorem 3.113) would show $\mathfrak{A} = (0)$, contrary to assumption. So, pick n minimal so that $\mathfrak{A} \subseteq \mathfrak{m}^n$. Then, every $\xi \in \mathfrak{A}$ has the form $a\pi^n$, and for at least one ξ, the element a is a unit (else $a \in \mathfrak{m}$ implies $a = b\pi$ and all ξ have shape $b\pi^{n+1}$). But then,

$$\mathfrak{A} \supseteq (\xi) = (\pi^n) = \mathfrak{m}^n \supseteq \mathfrak{A}$$

and $\mathfrak{A}$ is indeed principal. Therefore, (2) implies (3a) and (3b). It is clear that (3a) and (3b) imply (3).

We come then to the main point of our theorem, that (1) is equivalent to both parts of (3). Observe that the argument in the very early part of the proof shows that we always have

$$\{\mathfrak{p} \mid \mathrm{ht}(\mathfrak{p}) = 1\} \subseteq \mathrm{Pass}(A).$$

(3) $\Longrightarrow$ (1). By (3a), $\mathrm{Pass}(A) = \{\mathfrak{p} \mid \mathrm{ht}(\mathfrak{p}) = 1\}$; so

$$\bigcap\{A_{\mathfrak{p}} \mid \mathrm{ht}(\mathfrak{p}) = 1\} = \bigcap\{A_{\mathfrak{p}} \mid \mathfrak{p} \in \mathrm{Pass}(A)\} \tag{$**$}$$

By Lemma 3.55, the right hand side of ($**$) is A and by (3b) each $A_{\mathfrak{p}}$ is a normal domain (Proposition 3.53). Hence, A, as an intersection of noremal domains in $\mathrm{Frac}(A)$, is itself normal.

(1) $\Longrightarrow$ (3). Here, we will actually show (1) $\Longleftrightarrow$ (2), then we will be done. Pick $\mathfrak{p} \in \mathrm{Pass}(A)$, say $\mathfrak{p} \in \mathrm{Ass}(A/(a))$. Then, there exists an element $\xi \in A$ so that $\mathfrak{p}$ is the annihilator of $\xi \pmod{(a)}$. We need to prove $\mathfrak{p}^e$ is principal, so we may replace A by $A_{\mathfrak{p}}$ and $\mathfrak{p}$ by $\mathfrak{p}^e$. Thus, our situation is that A is local and $\mathfrak{p}$ is its maximal ideal. Write

$$\mathfrak{A} = \{\eta \in \mathrm{Frac}(A) \mid \eta\mathfrak{p} \subseteq A\} = (\mathfrak{p} \longrightarrow A) \quad (\text{in } \mathrm{Frac}(A)).$$

Of course, $\mathfrak{A}\mathfrak{p}$ is an ideal of A and $A \subseteq \mathfrak{A}$ shows that $\mathfrak{p} = A\mathfrak{p} \subseteq \mathfrak{A}\mathfrak{p}$. Hence, there are only two possibilities: $\mathfrak{A}\mathfrak{p} = \mathfrak{p}$ or $\mathfrak{A}\mathfrak{p} = A$. I claim that the first cannot hold. If it did, condition (4) of Proposition 3.50 applied to each η of $\mathfrak{A}$ (with $\widetilde{B} = \mathfrak{p}$ and $B = \mathrm{Frac}(A)$) would show that all these η are integral over A. By (1), the η lies in A; so $\mathfrak{A} = A$. Now $\mathfrak{p}$ annihilates the element $\xi \pmod{(a)}$ and $\xi \notin (a)$; that is, $\xi\mathfrak{p} = \mathfrak{p}\xi \subseteq (a)$; so

$(\xi/a)\mathfrak{p} \subseteq A$. But then $\xi/a \in \mathfrak{A}$, i.e., $\xi/a \in A$. The last assertion is that $\xi \in (a)$, contrary to the choice of ξ. We deduce, therefore, that $\mathfrak{A}\mathfrak{p} = A$. Now, the map

$$\mathfrak{A} \otimes_A \mathfrak{p} \longrightarrow \mathfrak{A}\mathfrak{p}$$

is an isomorphism because if $\sum_i q_i \otimes p_i$ goes to zero in A, then using a common denominator, say d, for the q_i, we find $(1/d)\sum_i \alpha_i \otimes p_i$ is 0, too. Clearly, $\mathfrak{A} \otimes_A \mathfrak{p} \longrightarrow \mathfrak{A}\mathfrak{p}$ is surjective. Proposition 3.48 now shows $\mathfrak{p}$ is a free rank one A-module (remember A is local), i.e., a principal ideal. □

Corollary 3.57 *If A is a Noetherian normal domain, then*

$$A = \bigcap \{A_{\mathfrak{p}} \mid \mathrm{ht}(\mathfrak{p}) = 1\}.$$

Proof. Theorem 3.56, condition (3a) shows

$$\mathrm{Pass}(A) = \{\mathfrak{p} \mid \mathrm{ht}(\mathfrak{p}) = 1\}$$

and we then apply Lemma 3.55. □

There are relations between the prime ideals of A and B when B is integral over A. These are expressed in the three Cohen-Seidenberg Theorems. Here is the first of them:

Theorem 3.58 *(Lying over Theorem; Cohen-Seidenberg, I) If B is integral over A and $\mathfrak{p}$ is any prime ideal of A, then there is a prime ideal, $\mathfrak{Q}$, of B lying over $\mathfrak{p}$ (that is, $\varphi^{-1}(\mathfrak{Q}) = \mathfrak{p}$, where $\varphi\colon A \to B$).*

Proof. Of course, we may and do assume $A \subseteq B$. Let $\mathcal{S}$ be the collection of all ideals, $\mathfrak{B}$, of B with $\mathfrak{B} \cap A \subseteq \mathfrak{p}$; partially order $\mathcal{S}$ by inclusion. As $\mathcal{S} \neq \emptyset$ ($(0) \in \mathcal{S}$) and clealry inductive, Zorn's Lemma furnishes a maximal element, say $\mathfrak{Q}$, in $\mathcal{S}$. We must show both $\mathfrak{Q} \cap A = \mathfrak{p}$ and $\mathfrak{Q}$ is a prime ideal.

Were $\mathfrak{Q} \cap A < \mathfrak{p}$, we could find $\xi \in \mathfrak{p}$ with $\xi \notin \mathfrak{Q} \cap A$. Write $\widetilde{\mathfrak{Q}}$ for the ideal $\mathfrak{Q} + B\xi$; as $\xi \notin \mathfrak{Q}$, we get $\widetilde{\mathfrak{Q}} > \mathfrak{Q}$. So, $\widetilde{\mathfrak{Q}} \notin \mathcal{S}$ and thus $\widetilde{\mathfrak{Q}} \cap A \not\subseteq \mathfrak{p}$. Therefore, there is some $\eta \in \widetilde{\mathfrak{Q}} \cap A$ (thus $\eta \in A$) yet $\eta \notin \mathfrak{p}$. Now η is in $\widetilde{\mathfrak{Q}}$, so looks like $q + b\xi$, for some $b \in B$. Note that $\eta - b\xi = q \in \mathfrak{Q}$.

The element b is integral over A:

$$b^n + a_1 b^{n-1} + \cdots + a_{n-1}b + a_n = 0, \quad \text{all } a_j \in A.$$

If we multiply by ξ^n, we find

$$(b\xi)^n + a_1\xi(b\xi)^{n-1} + \cdots + a_{n-1}\xi^{n-1}(b\xi) + a_n\xi^n = 0. \tag{$*$}$$

View $(*)$ in $B/\mathfrak{Q}$; there $\overline{\eta} = \overline{b\xi}$, and so,

$$(\overline{\eta})^n + \overline{a_1\xi}(\overline{\eta})^{n-1} + \cdots + \overline{a_{n-1}\xi^{n-1}}\overline{\eta} + \overline{a_n\xi^n} = 0 \quad \text{in } A/\mathfrak{Q}. \tag{$**$}$$

But now, all elements on the left hand side of $(**)$ when read in B actually lie in A; so the left hand side of $(**)$ is in $\mathfrak{Q} \cap A$. We get

$$\eta^n + a_1\xi\eta^{n-1} + \cdots + a_{n-1}\xi^{n-1}\eta + a_n\xi^n \in \mathfrak{p}.$$

Remembering that $\xi \in \mathfrak{p}$, we find $\eta \in \mathfrak{p}$, a contradiction. This shows $\mathfrak{Q} \cap A = \mathfrak{p}$.

To show $\mathfrak{Q}$ is a prime ideal, write S for the multiplicatice set $A - \mathfrak{p}$; S is a multiplicative subset of B. Of course, $\mathfrak{Q} \cap S = \emptyset$. Suppose $\mathfrak{Q}$ were not maximal among ideals of B whose intersection with S is empty. We'd find $\widetilde{\mathfrak{Q}} > \mathfrak{Q}$ and $\mathfrak{Q} \cap S = \emptyset$. But then $\mathfrak{Q} \cap A = \mathfrak{p}$ and so $\widetilde{\mathfrak{Q}}$ lies in $\mathcal{S}$ where $\mathfrak{Q}$ is maximal contradicting $\widetilde{\mathfrak{Q}} > \mathfrak{Q}$. Therefore, $\mathfrak{Q}$ is maximal among ideals of B with $\mathfrak{Q} \cap S = \emptyset$. Now, Proposition 3.8 (the implication (6) $\Longrightarrow$ (1)) shows $\mathfrak{Q}$ is prime. □

Theorem 3.59 *(Going-up Theorem; Cohen-Seidenberg, II) Suppose B is integral over A and $\mathfrak{p} \subseteq \mathfrak{q}$ are two prime ideals of A. If $\mathfrak{P}$ is a prime ideal of B lying over $\mathfrak{p}$, there exists a prime ideal, $\mathfrak{Q}$, of B lying over $\mathfrak{q}$ with $\mathfrak{P} \subseteq \mathfrak{Q}$.*

Proof. This is just a corollary of the lying over theorem. For once again, we may assume $A \subseteq B$ and we consider $A/\mathfrak{p}$ and $B/\mathfrak{P}$. As $\mathfrak{P} \cap A = \mathfrak{p}$ and B is integral over A, we find $B/\mathfrak{P}$ is integral over $A/\mathfrak{p}$ and apply Cohen-Seidenberg I to $A/\mathfrak{p}$ and $B/\mathfrak{P}$, using $\overline{\mathfrak{q}}$ as our ideal of $A/\mathfrak{p}$. There *is* $\overline{\mathfrak{Q}}$, a prime of $B/\mathfrak{P}$, over $\overline{\mathfrak{q}}$ and the pull-back of $\overline{\mathfrak{Q}}$ in B is what we want. □

Corollary 3.60 *If A and B are integral domains and B is integral over A, then A is a field iff B is a field.*

Proof. Suppose A is a field and $\xi \neq 0$ is in B. The element ξ is integral over A; so

$$\xi^n + a_1\xi^{n-1} + \cdots + a_{n-1}\xi + a_n = 0$$

for some $a_1, \ldots, a_n \in A$. Of course, we may assume that $a_n \neq 0$. Then

$$\xi(\xi^{n-1} + a_1\xi^{n-2} + \cdots + a_{n-1}) = -a_n;$$

and, as A is field, the element

$$-\frac{1}{a_n}(\xi^{n-1} + a_1\xi^{n-2} + \cdots + a_{n-1})$$

lies in B and is the inverse of ξ.

If B is a field and A is not, there are prime ideals $(0) < \mathfrak{q}$ of A. The going-up theorem gives us prime ideals (0) and $\mathfrak{Q}$ of B lying over (0) and $\mathfrak{A}$—but, B is a field; contradiction.

(We may also argue directly as in the first implication of the proof: Given $\xi \in A$, the element ξ is in B and B is a field. So, $1/\xi \in$B; thus $1/\xi$ is integral over A. We have

$$\left(\frac{1}{\xi}\right)^n + a_1\left(\frac{1}{\xi}\right)^{n-1} + \cdots + a_{n-1}\left(\frac{1}{\xi}\right) + a_n = 0.$$

Multiply through by ξ^n; we find

$$1 = -\xi(a_1 + \cdots + a_{n-1}\xi^{n-2} + a_n\xi^{n-1});$$

so ξ has an inverse in A.) □

Corollary 3.61 *If B is integral over A and $\mathfrak{P} \in \operatorname{Spec} B$ lies over $\mathfrak{p} \in \operatorname{Spec} A$, then $\mathfrak{p}$ is maximal iff $\mathfrak{P}$ is maximal.*

This is merely a restatement of Corollary 3.60. A more important remark is the *incomparability* of two primes lying over a fixed prime:

Proposition 3.62 *Say B is integral over A and $\mathfrak{P}$, $\mathfrak{Q}$ are two primes of B lying over the same prime, $\mathfrak{p}$, of A. Then $\mathfrak{P}$ and $\mathfrak{Q}$ are incomparable; that is we cannot have either $\mathfrak{P} \subseteq \mathfrak{Q}$ or $\mathfrak{Q} \subseteq \mathfrak{P}$ without $\mathfrak{P} = \mathfrak{Q}$.*

Proof. Assume $\mathfrak{P} < \mathfrak{Q}$ and reduce A mod $\mathfrak{p}$ and B mod $\mathfrak{P}$. Then we may assume A and B are domains and we have to prove no non-zero prime contracts to the zero ideal of A. In fact, we prove: *If A, B are domains with B integral over A and if $\mathfrak{B}$ is a non-zero ideal of B, then $\mathfrak{B}$ contracts to a non-zero ideal of A .*

Choose $b \in \mathfrak{B}$ with $b \neq 0$. Then we find

$$b^n + a_1b^{n-1} + \cdots + a_{n-1}b + a_n = 0.$$

and we may assume $a_n \neq 0$ (else we could divide out b and lower the degree, n; etc.) But then $a_n \in \mathfrak{B} \cap A$; so $\mathfrak{B} \cap A \neq (0)$, as required. □

Now we come to the circle of ideas around the third (and deepest) of the Cohen-Seidenberg Theorems, the so-called "Going–Down Theorem". This is a study of prime ideals in integral extensions where the bottom ring is a *normal* ring. For the proof of the theorem, we need some simple ideas from Galois theory) most of which are already familiar) which are covered in full in Chapter 4, sections one through four. Readers are urged to skip the proofs of Propositions 3.63 and 3.64 and Theorem 3.65, and come back to these after having read Sections 4.2–4.5 of Chapter 4. Once again, one can pick up the thread of our discussion in Proposition 3.66. Nonetherless the statements of all results below are clear.

Recall that if k is a field and B is a k-algebra, and element ξ, of B is algebraic over B iff it satisfies a (non-zero) polynomial $f(X) \in k[X]$. Of course, the set of all polynomials, $g(X)$, with $g(\xi) = 0$ is a principal ideal of $k[X]$ and the monic polynomial generating this ideal is the *minimal polynomial of* ξ *over* k. If B has zero divisors, the minimal polynomial of ξ over k will not, in general, be irreducible in $k[X]$. Even if no non-zero element of k becomes a zero divisor in B, still the minimal polynomial might be reducible.[4] But when B is at least a domain the minimal polyomial will be irreducible. We also want to consider in k an integral domain, A, with $k = \mathrm{Frac}(A)$.

So, let $\xi \in B$ be integral over A, assume B is a domain. Then we can factor the minimal polynomial $f(X)$, for ξ over $k = \mathrm{Frac}(A)$ in some big field over B (Section 4.4 of Chapter 4) and it will have exactly n roots where $n = \deg(f)$. Write these as $\xi = \xi_1, \xi_2, \ldots, \xi_n$. By Section 4.3, Chapter 4, each n_i is repated p^e times where $p = \mathrm{char}(k)$ and $e \geq 0$; p^e is the degree of inseparability of ξ over k. Moreover, there is an automorphism fixing the elements of k taking each ξ to ξ; so each ξ_i satisfies the equation of integral dependence which ξ satisfies (Section 4.4, Chapter 4 again). Now when we write $f(X)$ as a product of the linear factors $(X - \xi_i)$ we get

$$f(X) = \prod_{i=1}^{n}(X - \xi_i) = \sum_{j=0}^{n} \sigma_j(\xi_1, \ldots, \xi_n)(-1)^j X^{n-j},$$

here the σ_j are the *elementary symmetric functions* of the ξ_i, given as

$$\begin{aligned}
\sigma_0(\xi_1, \ldots, \xi_n) &= 1 \\
\sigma_1(\xi_1, \ldots, \xi_n) &= \xi_1 + \cdots + \xi_n \\
\sigma_2(\xi_1, \ldots, \xi_n) &= \sum_{i<j} \xi_i \xi_j \\
&\vdots \\
\sigma_r(\xi_1, \ldots, \xi_n) &= \sum_{i_1 < i_2 < \cdots < i_r} \xi_{i_1} \xi_{i_2} \cdots \xi_{i_r} \\
&\vdots \\
\sigma_n(\xi_1, \ldots, \xi_n) &= \xi_1 \xi_2 \cdots \xi_n.
\end{aligned}$$

Thus, when ξ is integral over A, so are all the ξ_i and all the elements $\sigma_j(\xi_1, \ldots, \xi_n)$, for $j = 1, 2, \ldots, n$. But each $\sigma_j(\xi_1, \ldots, \xi_n)$ is in k, therefore each σ_j is in $\mathrm{Aut}_k(A)$. The symmetric functions σ_1 and σ_n have special designation—they are the *trace* and *norm of* ξ *over* k, respectively. This argument gives the first two statements of

Proposition 3.63 *If A is a domain and $k = \mathrm{Frac}(A)$, write B for an overing of A and K for $\mathrm{Frac}(B)$. Then,*

[4] A standard example is the "ring of dual numbers over k", namely, $k[X]/(X^2)$. The minimal polynomial of $\overline{X}$ is X^2.

(1) When K is a field and $\xi \in K$ is integral over A, all the coefficients of the minimal polynomial for ξ over k are integral over A (so the norm and trace of ξ are integral over A).

(2) If A is a normal domain and K is a field, the minimal k-polynomial for an element $\xi \in K$ which is integral over A already lies in $A[X]$ and is an equation of integral dependence for ξ.

(3) If A is a normal domain and $f(X), g(X)$ are two monic polynomials in $k[X]$ so that $f(X)g(X)$ is in $A[X]$, then each of $f(X)$ and $g(X)$ is already in $A[X]$.

(4) If A is a normal domain and B is an overring of $\mathrm{Frac}(A)$*, and if $\xi \in B$ is integral over A, then the minimal k-polynomial of ξ is already in $A[X]$ and is an integral dependence relation for ξ. That is, (2) holds even K is not a field (B is an integral domain),* **provided** *$K \subseteq k$.*

(5) If A is a normal domain and B is an overring of A, with $\xi \in B$ integral over A, and if **non non-zero element of A becomes a zero divisor in** *B, then again the minimal k-polynomial for ξ is already in $A[X]$ and is an integral dependence.*

Proof. (1) and (2) are already proved; consider (3). Write $f(X) = \prod_i (X - \xi)$ and $g(X) = \prod_j (X - \eta_j)$ in some big overfield. Now $f(X)g(X)$ is a monic polynomial in $A[X]$ all xi_i and η_j satisfy it. But such a monic polynomial is an integral dependence relation; so, all ξ_i are integral over A and all the η_j are integral over A. By the argument for (1) each of the $\sigma_i(\xi_1, \ldots, \xi_t)$ and $\sigma_j(\eta_1, \ldots, \eta_r)$ are integral over A; hence they are in A by the normality of A. But, these are (up to sign) the coefficients of $f(X)$ and $g(X)$ and (3) is proved.

(4) B is a k-algebra, so ξ has a minimal polynomial, $f(X) \in k[X]$. Now ξ is also integral over A, therefore there is a monic polynomial, $h(X) \in A[X]$, with $h(\xi) = 0$. As f generates the principal $k[X]$ ideal of polynomials vanishing at ξ, there is a $g(X) \in k[X]$ with $f(X)g(X) = h(X)$ and clearly $g(X)$ is monic. Then, (3) shows $f(X) \in A[X]$ and is an equation of integral dependence.

(5) Here, if S is the multiplicative set of nonzero elements of A, then each $s \in S$ is a non-zero divisor of B and so $k = \mathrm{Frac}(A) \subseteq S^{-1}B \subseteq \mathrm{Frac}(B)$. We can then apply (4) to $S^{-1}B$ and conclude (5). □

Remark: Notice that the statement of (3) contains the essential ideal of Gauss' classical proof that if A is a UFD so is $A[X]$.

The hypothesis of (5) follows from a perhaps more easily checked condition:

Proposition 3.64 *If B is an A-algebra and B is flat over A, then no non-zero divisor of A becomes a non-trivial zero divisor in B.*

Proof. To say ξ is a non-zero divisor is to say

$$0 \longrightarrow A \xrightarrow{\xi} A \longrightarrow A/A\xi \longrightarrow 0$$

is exact. Now, tensor this exact sequence with B over A and use flatness to get

$$0 \longrightarrow B \xrightarrow{\xi} B \longrightarrow B/B\xi \longrightarrow 0$$

is exact. □

Theorem 3.65 *(Going-down Theorem; Cohen-Seidenberg, III) Suppose A is a normal domain and B is an overring of A. Assume either*

(1) B is integral over A and

(2) No non-zero element of A becomes a zero divisor of B

or

(1′) B is integral over A and

(2′) B is flat over A.

Then, given prime ideals $\mathfrak{p} \subseteq \mathfrak{q}$ of A and a prime ideal $\mathfrak{Q}$ of B over $\mathfrak{q}$, there is a prime ideal, $\mathfrak{P}$, of B, over $\mathfrak{p}$ so that $\mathfrak{P} \subseteq \mathfrak{Q}$.

Proof. If $\widetilde{A}$ is the image of A in B and (2′) holds, then B is flat over $\widetilde{A}$ and so, by Proposition 3.64, (2) holds. Therefore, we will assume (1) and (2).

The key to the proof is to find an apt multiplicative set, S, of B and to consider $S^{-1}B$. Take S to be the collection of products, $a\alpha$, where $a \in A - \mathfrak{p}$ and $\alpha \in B - \mathfrak{Q}$. Of course, S is closed under multiplication and $1 \in S$; further $0 \notin S$ else a, an element of A, would be a zero divisor of B contrary to (2). Observe, by taking $a = 1$ or $\alpha = 1$, we find $A - \mathfrak{p} \subseteq S$ and $B - \mathfrak{Q} \subseteq S$.

I claim the extended ideal, $\mathfrak{p}^e$, of $\mathfrak{p}$ in $S^{-1}B$ is not the unit ideal. Suppose, for the momemt, the claim is proved; we finish the proof as follows: The ideal $\mathfrak{p}^e$ is contained in some maximal ideal, $\mathfrak{M}$, of $S^{-1}B$, and so $\mathfrak{M}^c$ is a prime ideal of B. (As each ideal of $S^{-1}B$ is extended, $\mathfrak{M}$ is $\mathfrak{A}^e$ and so $\mathfrak{M}^{ce} = \mathfrak{A}^{ece} = \mathfrak{A}^e = \mathfrak{M} \neq S^{-1}B$; therefore, $\mathfrak{M}^e \neq B$.) Since $\mathfrak{M} \neq S^{-1}B$, the ideal $\mathfrak{M}^c$ cannot intersect S and $B - \mathfrak{Q} \subseteq S$ shows that $\mathfrak{M}^c \subseteq \mathfrak{Q}$. Now consider $\mathfrak{M}^c \cap A$, it is a prime ideal of A and cannot intersect S. Again, $A - \mathfrak{p} \subseteq S$ implies $\mathfrak{M}^c \cap A \subseteq \mathfrak{p}$. Yet

$$\mathfrak{p} \subseteq \mathfrak{p}B \cap A \subseteq \mathfrak{p}^{ec} \cap A \subseteq \mathfrak{M}^c \cap A,$$

therefore $\mathfrak{M}^c \cap A = \mathfrak{p}$ and we can set $\mathfrak{P} = \mathfrak{M}^c$.

We are therefore down to proving our claim, that is that $\mathfrak{p}B \cap S = \emptyset$. Pick $\xi \in \mathfrak{p}B$, write $\xi = \sum b_i p_i$ with $p_i \in \mathfrak{p}$ and $b_i \in B$. Let $\widetilde{B} = A[b_1, \ldots, b_t]$; it is a f.g. A-module (as well as A-algebra) by the integrality of B over A. We have $\xi\widetilde{B} \subseteq \mathfrak{p}\widetilde{B}$ and if $\xi_1, \ldots, \xi_r$ form a set of A-module generators for $\widetilde{B}$, we find from $\xi\xi_j \in \mathfrak{p}\widetilde{B}$ the linear equations:

$$\xi\xi_j = \sum_{i=1}^{r} p_{ij}\xi_i, \qquad p_{ij} \in \mathfrak{p}.$$

Just as in the argument (4) $\iff$ (1) of Proposition 3.50, this leads to $\Delta\xi_i = 0$ for $i = 1, \ldots, r$, where $\Delta = \det(\delta_{ij}\xi - p_{ij})$. Thus, $\Delta\widetilde{B} = 0$, yet $1 \in \widetilde{B}$; so $\Delta = 0$. By the minor expansion of Δ, we deduce the integral dependence

$$h(\xi) = \xi^r + \pi_1\xi^{n-1} + \cdots + \pi_{r-1}\xi + \pi_r = 0$$

and *here all the $\pi_i \in \mathfrak{p}$*.

Say ξ is in S, then it has the form $a\alpha$, with $a \in A - \mathfrak{p}$ and $\alpha \in B - \mathfrak{Q}$. By part (5) of Proposition 3.63, the minimal polynomial, $f(X) \in k[X]$, for ξ is already in $A[X]$ and is an integral dependence for ξ. But, also $f(X)$ divides $h(X)$ in $k[X]$ as $h(\xi) = 0$; so

$$f(X)g(X) = h(X) \qquad \text{in } k[X]$$

and $g(X)$ is monic. Apply part (3) of Proposition 3.63 and get that $g(X) \in A[X]$, too. This means we can reduce the coefficients of f, g, h mod $\mathfrak{p}$. The polynomial $h(X)$ becomes $\overline{h}(X) = X^r$. But $A/\mathfrak{p}$ is a domain and $\overline{h} = \overline{f}\,\overline{g}$; so $\overline{f}(X) = X^p$, that is

$$f(X) = X^s + \delta_1 X^{s-1} + \cdots + \delta_{s-1}X + \delta_s,$$

and *all the δ_i lie in $\mathfrak{p}$*.

Now $\xi = a\alpha$ and by (5) of Proposition 3.63 once again, we see that the k-minimal polynomial for α is actually in $A[X]$ and is an integral dependence for α. Write this polynomial, $m(X)$, as

$$m(X) = X^v + u_1 X^{v-1} + \cdots + u_{v-1}X + u_v$$

with each $u_i \in A$. Now multiply $m(X)$ by a^v, we get

$$a^v m(X) = (aX)^v + au_1(aX)^{v-1} + \cdots + a^{v-1}u_{v-1}(aX) + a^v u_v.$$

So, for the polynomial

$$\widetilde{f}(X) = X^v + au_1X^{v-1} + \cdots + a^{v-1}u_{v-1}X + a^v u_v$$

we find $\widetilde{f}(\xi) = a^v m(\alpha) = 0$ and therefore $f(X)$ divides $\widetilde{f}(X)$ in $k[X]$: $\widetilde{f}(X) = z(X)f(X)$. By (3) of Proposition 3.63, we see $z(X)$ is monic and in $A[X]$, and $v = \deg(\widetilde{f}) \geq \deg(f) = s$. However, by the same token if we divide $f(X)$ by a^s, we get

$$\left(\frac{X}{a}\right)^s + \frac{\delta_1}{a}\left(\frac{X}{a}\right)^{s-1} + \cdots + \frac{\delta_{s-1}}{a^{s-1}}\left(\frac{X}{a}\right) + \frac{\delta_s}{a^s}$$

giving us the k-polynomial

$$F(X) = X^s + \frac{\delta_1}{a}X^{s-1} + \cdots + \frac{\delta_{s-1}}{a^{s-1}}X + \frac{\delta_s}{a^s}.$$

We have $F(\alpha) = (1/a^s)f(\xi) = 0$; so $m \mid F$ in $k[X]$. Therefore,

$$s = \deg(F) \geq \deg(m) = v;$$

coupled with the above this shows $s = v$ and $Z(X) = 1$. Therefore, $f(X) = \widetilde{f}(X)$ so that

$$\delta_j = a^j u_j, \qquad j = 1, 2, \ldots, s.$$

Now $\delta_j \in \mathfrak{p}$ and, by choice of S, $a \notin \mathfrak{p}$. Therefore, *all the* u_j *belong to* $\mathfrak{p}$.

Finally, $m(\alpha) = 0$; so,

$$\alpha^s + u_1\alpha^{s-1} + \cdots + u_{s-1}\alpha + u_s = 0.$$

This shows $\alpha^s \in \mathfrak{p}B \subseteq \mathfrak{q}B \subseteq \mathfrak{Q}$; whence $\alpha \in \mathfrak{Q}$—a contradiction. □

The Cohen-Seidenberg Theorems have geometric content. It turns out that for a commutative ring A (over the complex numbers), $\operatorname{Spec} A$ can be made into a (generalized) complex space (perhaps of infinite dimension); that is into a complex manifold with some singularities (perhaps). For us, the important point is that $\operatorname{Spec} A$ is a topological space (see Section 3.3) and we'll only draw topological content from the Cohen-Seidenberg Theorems.

So, first say B is integral over A. The ring map $\varphi\colon A \to B$ gives a continuous map $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$, namely: $\mathfrak{P} \mapsto \varphi^{-1}(\mathfrak{P})$. The lying over theorem can now be expressed as:

If B is integral over A, the continuous map $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ *is surjective.*

Remark: *We've used a Cohen-Seidenberg Theorem; so, we've assumed $A \longrightarrow B$ is an* **injection** *in the above.*

The question of $A \longrightarrow B$ being an injection and the "real" content of integrality can be teased apart as follows:

Proposition 3.66 *Say $A \longrightarrow B$ is an injection. Then the continuous map* $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ *has dense image. If $A \longrightarrow B$ is surjective, then the continuous map* $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ *is a homeomorphism onto a closed subset of* $\operatorname{Spec} A$.

Proof. Write φ for the homomorphism $A \longrightarrow B$ and $|\varphi|$ for the continuous map $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$. Pick any $\mathfrak{p} \in \operatorname{Spec} A$ and any $f \notin \mathfrak{p}$ (so that $\mathfrak{p} \in X_f$ in $\operatorname{Spec} A$). We must find $\mathfrak{q} \in \operatorname{Spec} B$ so that $|\varphi|(\mathfrak{q}) \in X_f$. Now f is not nilpotent; so, as φ is injective, neither is $\varphi(f)$. But then there is a prime ideal, $\mathfrak{q}$, of B, and $\varphi(f) \notin \mathfrak{q}$ (cf. either Proposition 3.8 #(6) or remark #(4) after Proposition 3.11); that is $f \notin |\varphi|(\mathfrak{q})$, which is what we needed.

Recall, from the discussion on the Zariski topology following Proposition 3.11, that the closed sets in $\operatorname{Spec} A$ are all of the form $V(\mathfrak{A})$ for some ideal $\mathfrak{A}$, of A. Now there is the usual one-to-one correspondence of ideals, $\mathfrak{B}$, of A which contain $\mathfrak{A}$ and all ideals of $A/\mathfrak{A}$. If we take for $\mathfrak{A}$ the kernel of φ, then the first consequence is that $\mathfrak{p} \mapsto |\varphi|(\mathfrak{p})$ is a continuous bijection of $\operatorname{Spec} B$ $(= \operatorname{Spec} A/\mathfrak{A})$ and the closed set, $V(\mathfrak{A})$, of $\operatorname{Spec} A$. But, this is also a closed map, because for $\mathfrak{B}$, an ideal of B, the map $|\varphi|$ takes $V(\mathfrak{B})$ onto $V(\varphi^{-1}(\mathfrak{B})) \subseteq \operatorname{Spec} A$. □

Proposition 3.67 *If B is integral over A, where $\varphi\colon A \to B$ need not be injective, then the map $|\varphi|$ from $\operatorname{Spec} B$ to $\operatorname{Spec} A$ is a closed map. In fact, it is universally closed; that is, the map $|\varphi_C|\colon \operatorname{Spec}(B \otimes_A C) \to \operatorname{Spec} C$ is a closed map for every A-algebra, C.*

Proof. Note that if B is integral over A, then $B \otimes_A C$ is integral over C. To see this, observe that a general element of $B \otimes_A C$ is a sum of terms $b \otimes c$ with $b \in B$ and $c \in C$. If $b \otimes c$ is integral over C so is any sum of such terms. But, $b \otimes c = (b \otimes 1)(1 \otimes c)$ and $1 \otimes c$ is in C $(= A \otimes_A C)$ so all we need check is that $b \otimes 1$ is integral over C. Write the integral dependence for b over A, then tensor with 1 (as in $b \otimes 1$) and get the integral dependence of $b \otimes 1$ over C.

This remark reduces us to proving the first statement. Now the map $A \longrightarrow B$ factors as

$$A \longrightarrow \widetilde{A} = A/\mathfrak{A} \hookrightarrow B,$$

so for the spaces $\operatorname{Spec} A$, etc., we get

$$\operatorname{Spec} B \longrightarrow \operatorname{Spec} \widetilde{A} \longrightarrow \operatorname{Spec} A.$$

By Proposition 3.66, the second of thesex maps is closed, therefore we are reduced to the case where $A \longrightarrow B$ is injective. A closed set of $\operatorname{Spec} B$ is $V(\mathfrak{B})$ and we know by Fact A following Proposition 3.54 that $B/\mathfrak{B}$ is integral over $A/(\mathfrak{B} \cap A)$. The interpretation of Cohen–Seidenberg II shows that
$\operatorname{Spec}(B/\mathfrak{B}) \longrightarrow \operatorname{Spec}(A/(\mathfrak{B} \cap A))$ is surjective. Coupled with the homeomorphisms

$$\operatorname{Spec}(B/\mathfrak{B}) \cong V(\mathfrak{B}); \quad \operatorname{Spec}(A/(\mathfrak{B} \cap A)) \cong V(\mathfrak{B} \cap A),$$

this finishes the proof. □

Let's continue with these topological considerations a bit further. Take $\mathfrak{p} \in \operatorname{Spec} A$, one wants to consider $\{\mathfrak{p}\}$ as Spec(?) for some A-algebra "?". At first $A_{\mathfrak{p}}$ seems reasonable, but $\operatorname{Spec} A_{\mathfrak{p}}$ consist of *all* the primes contained in $\mathfrak{p}$. We can get rid of all these extraneous primes by factoring out by $\mathfrak{p}^e$ and forming

$$\kappa(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}^e.$$

The A-algebra, $\kappa(\mathfrak{p})$, is a field; so, $\operatorname{Spec} \kappa(\mathfrak{p})$ is one-point—it corresponds to $\mathfrak{p}$. Indeed, in the map
$\kappa(\mathfrak{p}) \longrightarrow \operatorname{Spec} A$ coming from the ring map

$$A \longrightarrow A_{\mathfrak{p}} \longrightarrow A_{\mathfrak{p}}/\mathfrak{p}^e = \kappa(\mathfrak{p}),$$

the one point of $\operatorname{Spec} \kappa(\mathfrak{p})$ goes to $\mathfrak{p}$ in $\operatorname{Spec} A$. If B is an A-algebra, then $B \otimes_A \kappa(\mathfrak{p})$ is a $\kappa(\mathfrak{p})$-algebra isomorphic to $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$. The commutative diagram

$$\begin{array}{ccc} B & \longrightarrow & B \otimes_A \kappa(\mathfrak{p}) \\ \uparrow & & \uparrow \\ A & \longrightarrow & \kappa(\mathfrak{p}) \end{array}$$

shows that the elements of $\operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p}))$ all go to $\mathfrak{p}$ under the map $\operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p}) \longrightarrow \operatorname{Spec} A$. *Therefore,* $\operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p})$ *is the fibre of the map* $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ *over* $\{\mathfrak{p}\}$.

Proposition 3.68 *Suppose B is a finitely generated A-algebra and is also integral over A. Then, each fibre of the map* $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ *is finite.*

Proof. The algebra B has the form $A[b_1, \ldots, b_t]$ and each b_j is integral over A. Thus, B is a finitely-generated A-*module*. So, each $B \otimes_A \kappa(\mathfrak{p})$ is a finitely generated $\kappa(\mathfrak{p})$-vector space and therefore has the D.C.C. By Lemma 3.37, $\operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p}))$ is a finite set. □

We have more than stated: B is not only a finitely generated A-algebra it is a f.g. A-*module*. This is stronger than the condition that all the fibres of $|\varphi|\colon \operatorname{Spec} B \to \operatorname{Spec} A$ be finite. Indeed, consider the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$. The points of $\operatorname{Spec}\mathbb{Z}$ are $\{0\}$, $\{2\}$, $\{3\}, \ldots$, $\{p\}, \ldots$, and the fibres of $\operatorname{Spec}\mathbb{Q}$ over $\operatorname{Spec}\mathbb{Z}$ are respectively $\{0\}$, $\emptyset$, $\emptyset, \ldots, \emptyset, \ldots$. Of course, $\mathbb{Q}$ is not integral over $\mathbb{Z}$ nor is it finitely–generated as $\mathbb{Z}$-algebra.

A more germane example is $\mathbb{C}[X]$ as included in $\mathbb{C}[X, Y]/(XY - 1)$. The primes of $\mathbb{C}[X]$ are $\{0\}$ and the principal ideals $(X - \lambda)$, where λ ranges over $\mathbb{C}$. The fibre over $\{0\}$ is $\{0\}$, that over $(X - \lambda)$ for $\lambda \neq 0$, is the principal ideal which is the kernel of $X \mapsto \lambda$; $Y \mapsto 1/\lambda$. But, over (X), the fibre is $\emptyset$. So, all fibres are finite, $B = \mathbb{C}[X, Y]/(XY - 1)$ is a finitely generated $\mathbb{C}[X]$-algebra yet B is not a finitely generated $\mathbb{C}[X]$-module; hence B is not integral over $A = \mathbb{C}[X]$ under the standard inclusion. Observe also that $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ is not a closed map in this case—this turns out to be the key. For, we have the following fact due to Chevalley:

Fact. If B is a finitely-generated A-algebra under a map φ and if $|\varphi|$ is both universally closed and has finite fibres, then B is a finite A-module (in particular, B is integral over A).

The proof of this is very far from obvious and is not part of our purview. However, the discussion does suggest the following question: Say A is a domain and write k for $\operatorname{Frac} A$. if K/k is a finite degree field extension, is $\operatorname{Int}_A(K)$ a finitely generated A-algebra (hence, a f.g. A-module)? The answer is "no", which perhaps is to be expected. But, even if A is noetherian, the answer is still "no". This is somewhat surprising and suggests that the finite generation of $\operatorname{Int}_A(K)$ is a delicate and deep matter. If we are willing to assume a bit more about K/k we get a very satisfying answer. We'll need some material from Chapter 4, Section 4.2 and 4.3 for this.

Theorem 3.69 *Suppose A is a normal domain with fraction field k and say K/k is a finite* **separable** *extension. Then,* $\operatorname{Int}_A(K)$ *is contained in a f.g. A-module in K. In fact, a basis for K/k can be found which generates the latter A-module. If A is, in addition, noetherian, then* $\operatorname{Int}_A(K)$ *is itself a finite A-module; hence is noetherian.*

Proof. We use the trace from K to k (see Chapter 4, Section 4.7), this is a k-linear map, $\operatorname{tr}\colon K \to k$. We set for $x, y \in K$

$$\langle x, y\rangle = \operatorname{tr}_{K/k}(xy).$$

The fact we need is that the separability of K/k entails the non-degeneracy of the pairing $\langle x, y\rangle$. (Actually, this is not proved in Section 4.7 of Chapter 4 but is an easy consequence of Newton's Identities connecting sums of powers of elements $x_1, \ldots, x_t$ with elementary symmetric functions in $x_1, \ldots, x_t$.) This being said, we see that K is self-dual as vector space over k, via our pairing $\langle x, y\rangle$.

Let $B = \operatorname{Int}_A(K)$, then in fact $\operatorname{Frac}(B) = K$. To see this, choose $x \in K$, then x has a minimal k-polynomial $m(T) \in k[T]$, say

$$m(x) = x^r + \alpha_1 x^{r-1} + \cdots + \alpha_{r-1}x + \alpha_r = 0, \qquad \alpha_i \in k. \tag{$\dagger$}$$

As $k = \operatorname{Frac}(A)$, for each i, there is $s_i \in A$ with $s_i\alpha_i \in A$. We take $s = \prod s_i$, then $s\alpha_i \in A$ for all i; so multiply ($\dagger$) by s^r, we get

$$(sx)^r + s\alpha_1(sx)^{r-1} + \cdots + s^{r-1}\alpha_{r-1}(sx) + s^r\alpha_r = 0.$$

This shows that $xs \in \mathrm{Int}_A(K) = B$, so $x \in \mathrm{Frac}(B)$. (It shows more. Namely, $K = (A - \{0\})^{-1}B$.) It follows that we may choose a k-basis for K from B; say this is $b_1, \ldots, b_t$. By the non-degeneracy of $\langle x, y\rangle$, the dual basis consists of elements of K, say they are $c_1, \ldots, c_t$. Thus,

$$\langle b_i, c_j\rangle = \delta_{ij}.$$

Now, choose $x \in B$ and write x in terms of the basis $c_1, \ldots, c_t$. We have $x = \sum \gamma_i c_i$, with the $\gamma_i \in k$. As x and the b_i lie in B, we see that $xb_i \in B$ and statement (1) of Proposition 3.63 shows that $\langle x, b_i\rangle \in A$ because A was assumed normal. But

$$\langle x, b_i\rangle = \langle \sum_j \gamma_j c_j, b_i\rangle = \sum_j \gamma_j \delta_{ji} = \gamma_i$$

so all $\gamma_i \in A$. Therefore $B \subseteq Ac_1 + \cdots + Ac_t$, as required in the first two conclusions of our theorem. Of course, if A is noetherian, then B, as a sub-module of a f.g. A-module, is itself finitely generated. □

Remark: We cannot expect B to be generated by just t elements as its containing module $Ac_1 + \cdots + Ac_t$ is so generated. On the other hand, it can never be generated by fewer than t elements. For if it were, say $B = Ad_1 + \cdots + Ad_r$, with $r < t$, then

$$(A - \{0\})^{-1}B = k \otimes_A B = k\text{-span of } d_1, \ldots, d_r.$$

Yet the left hand side is just K and so

$$t = \dim K \leq r,$$

a contradiction. When B *is* generated by t elements, this shows they must be a basis for K/k. If A is a P.I.D., one knows from $B \leq Ac_1 \coprod \cdots \coprod Ac_t$ that B is generated by t or fewer elements, and so we've proved

Corollary 3.70 *If A is a P.I.D. and K is a finite separable extension of $k = \mathrm{Frac}\, A$, then there exist elements $\beta_1, \ldots, \beta_t$ of $B = \mathrm{Int}_A(K)$ so that*

(1) B is the free A-module on $\beta_1, \ldots, \beta_t$ and

(2) $\beta_1, \ldots, \beta_t$ are a k-basis for K.

A set of elements $\beta_1, \ldots, \beta_t$ having properties (1) and (2) above is called an *integral basis for K/k*. An integral basis might exist for a given normal, noetherian A and an extension K/k, but it is guaranteed if A is a P.I.D.

Theorem 3.69 shows that the difficulty of the finite generation of $\mathrm{Int}_A(K)$ resides in the possible inseparability of the layer K/k. It can happen that we must continue to add more and more elements without end in a tower

$$A \subseteq B_1 \subseteq B_2 \subseteq \cdots \subseteq B_n \subseteq \cdots \subseteq B = \mathrm{Int}_A(K)$$

and examples (due to Nagata) exist of just this phenomenon. Fortunately, for a big class of integral domains of interest in both number theory and algebraic geometry, this does not happen—they are well-behaved. These are the integral domains, A, that are finitely generated k-algebras, where k is a *field*. We'll refer to them as *finitely generated domains over k*. We will also need some material from Chapter 4 Section 4.11, namely the notion of transcendence basis. This is just a subset of our domain, algebraically independent over k (i.e. satisfying no non-trivial polynomial in finitely many variables over k) and maximal with respect to this property. Every set of generators contains a transcendence basis and all transcendence bases have the same cardinality—called the *transcendence degree of A over k*. You should skip the proofs of Theorem 3.71 and 3.72 and come back to read them after Chapter 4.

A main step in proving that the finitely generated domains over k are well-behaved is the following important theorem due to E. Noether:

Theorem 3.71 *(Noether Normalization Lemma.) If A is a finitely generated domain over the field k, say $A = k[t_1, \ldots, t_n]$, and if d is the transcendence degree of A over k, then there exists a change of coordinates*

$$y_j = f_j(t_1, \ldots, t_n),$$

in A so that

(1) $y_1, \ldots, y_d$ are a transcendence basis for A over k and

(2) the injection $k[y_1, \ldots, y_d] \hookrightarrow A = k[y_1, \ldots, y_n]$ makes A integral over $k[y_1, \ldots, y_d]$.

If k is infinite, then f_j may be taken to be linear. If Frac A *is separably generated over k, then the y_j may be chosen to be a separating transcendence basis for* Frac A *over k.*

Proof. (Nagata). We prove the theorem by induction on n; the cases $n = 0$ or $n = 1$ are trivial. So, assume the theorem holds up to $n - 1$. If $d = n$, the remarks about transcendence bases just before our proof show that A is already the polynomial ring in n variables; so, again, nothing need be proved. Therefore, we may assume $d < n$. We'll show there exists $y_2, \ldots, y_n$ so that $k[y_2, \ldots, y_n] \hookrightarrow k[t_1, \ldots, t_n] = A$ is an integral morphism (separable in the separating transcendence basis case). If so, then the induction hypothesis applies to $k[y_2, \ldots, y_n]$ and this, together with transitivity of integral dependence and separability, will complete the proof.

Now $d < n$, so relabel the $t_1, \ldots, t_n$ to make t_1 algebraically dependent on $t_2, \ldots, t_n$. We have a non-trivial polynomial relation

$$\sum_{(\alpha)} c_{(\alpha)} t^{(\alpha)} = 0,$$

where $(\alpha) = (\alpha_1, \ldots, \alpha_n)$ is a multi-index and $t^{(\alpha)} = t_1^{\alpha_1} \cdots t_n^{\alpha_n}$. Set

$$y_j = t_j - t_1^{m_j}, \qquad j = 2, \ldots, n,$$

where the m_j are as yet undetermined integers (≥ 0). Then $t_j = y_j + t_1^{m_j}$ and so

$$\sum_{(\alpha)} c_{(\alpha)} t_1^{\alpha_1} (y_2 + t_1^{m_2})^{\alpha_2} \cdots (y_n + t_1^{m_n})^{\alpha_n} = 0.$$

Expand the latter equation by the binomial theorem to obtain the relation

$$\sum_{(\alpha)} c_{(\alpha)} t_1^{(\alpha)\cdot(m)} + G(t_1, y_2, \ldots, y_n) = 0, \tag{$\dagger$}$$

where $(m) = (1, m_2, \ldots, m_n)$ and $(\alpha) \cdot (m)$ stands for the dot product $\alpha_1 + \alpha_2 m_2 + \cdots + \alpha_n m_n$. The polynomial G has degree in t_1 less than the maximum of the exponents $(\alpha) \cdot (m)$. If we can choose the integers $m_2, \ldots, m_n$ so that the products $(\alpha) \cdot (m)$ are all distinct, then ($\dagger$) is an integral dependence of t_1 over $k[y_2, \ldots, y_n]$ as k is a field. But each t_j is expressed as $y_j + t_1^{m_j}$ for $j = 2, \ldots, n$; so each t_j is integral over $k[y_2, \ldots, y_n]$ and therefore $k[t_1, \ldots, t_n]$ is integral over $k[y_2, \ldots, y_n]$. When $k[t_1, \ldots, t_n]$ is separably generated over k, Mac Lane's Theorem (Theorem 4.90) shows we may choose t_1 separable algebraic over $k[t_2, \ldots, t_n]$. Then the relation $\sum_{(\alpha)} c_{(\alpha)} t^{(\alpha)} = 0$ may be chosen to be a separable polynomial in t_1 and the way we will choose the m's (below) will show t_1 is separable over $k[y_2, \ldots, y_n]$. As $t_j = y_j + t_1^{m_j}$, we get the separability of $k[t_1, \ldots, t_n]$ over $k[y_2, \ldots, y_n]$.

Now we must choose the integers $m_2, \ldots, m_n$. For this, consider the differences

$$(\delta)_{\alpha\alpha'} = (\delta_1, \ldots, \delta_n)_{\alpha\alpha'} = (\alpha) - (\alpha')$$

for all possible choices of our distinct multi-indices (α), except that we do not include $(\alpha') - (\alpha)$ if we have included $(\alpha) - (\alpha')$. Say there are N such differences, label them $\delta_1, \ldots, \delta_N$. Form the polynomial

$$H(T_2, \ldots, T_n) = \prod_{j=1}^{N} (\delta_{1j} + \delta_{2j} T_2 + \cdots + \delta_{nj} T_n)$$

here, $\delta_j = (\delta_{1j}, \ldots, \delta_{nj})$ and $T_2, \ldots, T_n$ are indeterminates. None of the δ_j are zero, so H is a non-zero polynomial and it has integer coefficients. It is well-known that there are non-negative integers $m_2, \ldots, m_n$ so that $H(m_2, \ldots, m_n) \neq 0$. Indeed, if b is a non-negative integer larger than any component of any of our (α)'s, then $b, b^2, \ldots, b^{m-1}$ is such a choice. It is also a choice which gives separability. The fact that $H(m_2, \ldots, m_n) \neq 0$ means that the $(\alpha) \cdot (m)$ are distinct.

Finally, assume k is infinite. Just as before, arrange matters so that t_1 depends algebraically (and separably in the separably generated case) on $t_2, \ldots, t_n$. Write the minimal polynomial for t_1 over $k(t_2, \ldots, t_n)$ as

$$P(U, t_2, \ldots, t_n) = 0.$$

We may asume the coefficients of $P(U, t_2, \ldots, t_n)$ are in $k[t_2, \ldots, t_n]$ so that the polynomial $P(U, t_2, \ldots, t_n)$ is the result of substituting $U, t_2, \ldots, t_n$ for $T_1, \ldots, T_n$ in some non-zero polynomial, $P(T_1, \ldots, T_n)$, having coefficients in k. Now perform the linear change of variables

$$y_j = t_j - a_j t_1, \qquad j = 2, \ldots, n,$$

where $a_2, \ldots, a_n$ are elements of k to be determined later. As before, each t_j is $y_j + a_j t_1$; so it suffices to prove that t_1 is integral (and separable in the separably generated case) over $k[y_2, \ldots, y_n]$.

We have

$$P(t_1, y_2 + a_2 t_1, \ldots, y_n + a_n t_1) = 0$$

which gives us

$$t_1^q f(1, a_2, \ldots, a_n) + Q(t_1, y_2, \ldots, y_n) = 0, \tag{$*$}$$

where $f(T_1, \ldots, T_n)$ is the highest degree form of $P(T_1, \ldots, T_n)$ and q is its degree The polynomial, Q, contains just terms of degree lower than q in t_1. If we produce elements a_j in k $(j = 2, 3, \ldots, n)$ so that $f(1, a_2, \ldots, a_n) \neq 0$, then $(*)$ is the required integral dependence of t_1 on the y's. In the separable case, we also need t_1 to be a simple root of its minimal polynomial, i.e.,

$$\frac{dP}{dt_1}(t_1, y_2, \ldots, y_n) \neq 0$$

(c.f. Theorem 4.5 of Chapter 4). By the chain rule, the latter condition is

$$\frac{dP}{dt_1}(t_1, y) = \frac{\partial P}{\partial t_1} + a_2 \frac{\partial P}{\partial t_2} + \cdots + a_n \frac{\partial P}{\partial t_n} \neq 0. \tag{$**$}$$

Now the middle term of $(**)$ is a linear form in $a_2, \ldots, a_n$ and it is not identically zero since on $a_2 = a_3 = \cdots = a_n = 0$ it takes the value $\partial P / \partial t_1$ and the latter is not zero because t_1 is separable over $k(t_2, \ldots, t_n)$ (Theorem 4.5, again). Thus, the vanishing of the middle term of $(**)$ defines a translate of a (linear) hyperplane in $n-1$ space over k, and on the complement of this hyperplane translate we have $dP/dt_1(t_1, y) \neq 0$. The latter complement is an infinite set because k is an infinite field. But from an infinite set we can always choose $a_2, \ldots, a_n$ so that $f(1, a_2, \ldots, a_n) \neq 0$; therefore both our conditions $dP/dt_1(t_1, y) \neq 0$ and $f(1, a_2, \ldots, a_n) \neq 0$ will hold, and the proof is finished. $\square$

The example discussed previously of $\mathbb{C}[X]$ embedded (in the standard way) in $\mathbb{C}[X,Y]/(XY-1)$ is an extremely simple instance of the normalization lemma. Namely, rotate the coordinates

$$X \mapsto X+Y; \quad Y \mapsto X-Y$$

and let $T = 1/2(X+Y)$; $W = 1/2(X-Y)$. Then our situation becomes $\mathbb{C}T$ embedded in $\mathbb{C}[T,W]/(T^2-W^2-1)$, an integral extension. See Figures 3.1 and 3.2 below:

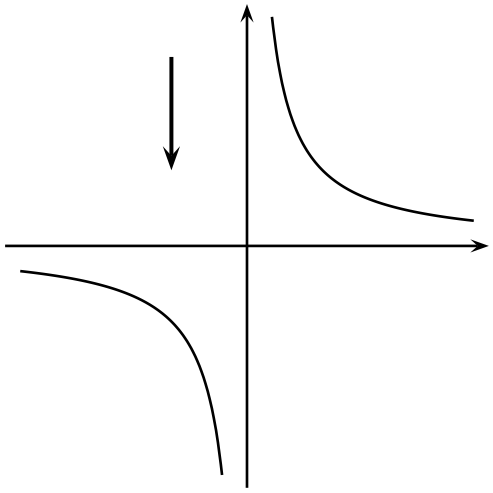


Figure 3.1: Before Normalization: A non-integral morphism

becomes after $\pi/4$ rotation

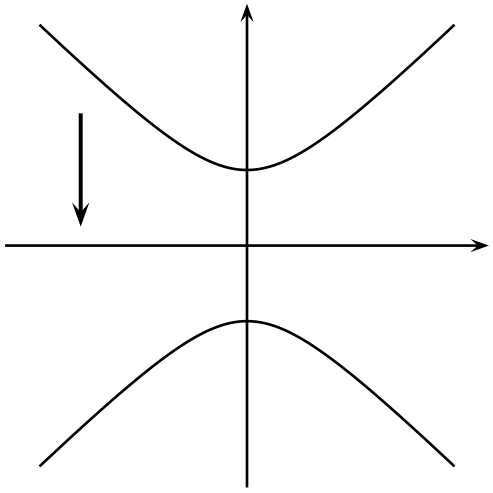


Figure 3.2: After Normalization: An integral morphism

Theorem 3.71 is not the sharpest form of the normalization lemma. Here's an improvement due to Eisenbud based on a previous improvement of Nagata's. We offer no proof as we won't use this sharper

version.

Theorem 3.72 *If $A = k[t_1, \ldots, t_n]$ is a finitely generated integral domain over a field k with $\mathrm{tr.d}_k\, A = d$ and if we are given a maximal length descending chain of prime ideals of A*

$$\mathfrak{p}_0 > \mathfrak{p}_1 > \cdots > \mathfrak{p}_{d-1} > (0),$$

then there exists a change of coordinates

$$y_j = f_j(t_1, \ldots, t_n)$$

so that

(1) $y_1, \ldots, y_d$ are a transcendence basis for A over k,

(2) the injection $k[y_1, \ldots, y_d] \hookrightarrow A$ makes A integral over $k[y_1, \ldots, y_d]$, and

(3) $\mathfrak{p}_j \cap k[y_1, \ldots, y_d] = (y_1, \ldots, y_{d-j})$.

Here is the promised application of Theorem 3.71 to the well behavedness of finitely generated integral domains over fields.

Theorem 3.73 *When A is a finitely generated integral domain over k and K is a finite extension field over $\mathrm{Frac}(A)$, then $\mathrm{Int}_A(K)$ is both a finitely generated integral domain over k and a finite A-module.*

Proof. We first make two reductions and then treat the main case:

(1) We may assume $K = \mathrm{Frac}\, A$. For if it is known that the integral closure of A in its own fraction field satisfies the conclusions of the theorem, then choose a basis $y_1, \ldots, y_s$ for$K$ over $\mathrm{Frac}\, A$ which basis consists of elements from $\mathrm{Int}_A(K)$. This can be done by the argument in the middle of the proof of Theorem 3.69, which argument made no use of any separability hypothesis. Of course, $A[y_1, \ldots, y_s]$is both a finite A-module and a finitely generated integral domain over k and its fraction field is K. So by our assumption $\mathrm{Int}_{A[y_1,\ldots,y_s]}(K)$ satisfies the conclusions of the theorem. But, clearly, $\mathrm{Int}_A(K) = \mathrm{Int}_{A[y_1,\ldots,y_s]}(K)$, which achieves our first reduction.

(2) We may assume both that k is infinite and that $\mathrm{Frac}\, A$ is separably generated over k. (Here, we are already using reduction (1) having replaced K by $\mathrm{Frac}\, A$.) To see this, write Ω for the algebraic closure of $\mathrm{Frac}\, A$ (see Theorem 4.77) and note that Ω contains $\overline{k}$, the algebraic closure of k. Now $\overline{k}$ is both infinite and perfect, so by Corollary 4.91, the field $\overline{k}(t_1, \ldots, t_n)$ is separably generated over $\overline{k}$; here, $A = k[t_1, \ldots, t_n]$. By our assumption, $\mathrm{Int}_{\overline{k}[t_1,\ldots,t_n]}(\overline{k}(t_1, \ldots, t_n))$ is a finite $\overline{k}[t_1, \ldots, t_n]$-module and a finitely generated $\overline{k}$-algebra, say $\overline{k}[w_1, \ldots, w_q]$.

Now by the normalization lemma (in the infinite, separable case) there are $z_1, \ldots, z_d$, algebraically independent, which are linear combinations

$$z_j = \sum_{i=1}^{n} \alpha_{ij} t_i$$

of the $t_1, \ldots, t_n$ so that $\overline{k}[t_1, \ldots, t_n]$ is integral and separable over $\overline{k}[z_1, \ldots, z_d]$. Each w_j satisfies a separable, integral dependence

$$g_j(w_j, z_1, \ldots, z_d) = 0, \qquad j = 1, 2, \ldots, q,$$

over the polynomial ring $\overline{k}[z_1, \ldots, z_d]$. Also,

$$\mathrm{Int}_{\overline{k}[z_1,\ldots,z_d]}(\overline{k}(t_1, \ldots, t_n)) = \overline{k}[w_1, \ldots, w_q].$$

Adjoin to k all the coefficients of these q polynomials and all the α_{ij} to get a field, $\widetilde{k}$, of finite degree over k. The entire situation involving $\overline{k}[z\text{'s}]$ and $\overline{k}[w\text{'s}]$ comes from the same situation involving $\widetilde{k}[z\text{'s}]$ and $\widetilde{k}[w\text{'s}]$; so, *by the algebraic independence of the z's*, we find

$$\mathrm{Int}_{\widetilde{k}[z_1,\ldots,z_d]}(\widetilde{k}(t_1,\ldots,t_n)) = \widetilde{k}[w_1,\ldots,w_q]$$

and we know

$$\mathrm{Int}_{\widetilde{k}[z_1,\ldots,z_d]}(\widetilde{k}(t_1,\ldots,t_n)) = \mathrm{Int}_{k[t_1,\ldots,t_n]}(\widetilde{k}(t_1,\ldots,t_n)).$$

Of course, $\widetilde{k}[w_1,\ldots,w_q]$ is a finite $\widetilde{k}[t_1,\ldots,t_n]$-module and $\widetilde{k}[t_1,\ldots,t_n]$ is a finite $k[t_1,\ldots,t_n] = A$-module as $\widetilde{k}$ has finite degree over k. Thus, $\widetilde{k}[w_1,\ldots,w_q]$ is a finite A-module as are all of its submodules, A being noetherian. But $\mathrm{Int}_A(\mathrm{Frac}\,A))$ is the submodule $\mathrm{Frac}(A) \cap \widetilde{k}[w_1,\ldots,w_q]$ and as A is a finitely generated k-algebra so is any A-algebra which is a finite A-module. This achieves reduction (2).

Finally we have the case $K = \mathrm{Frac}\,A$, k is infinite and $\mathrm{Frac}\,A$ is separably generated over k. By the normalization lemma, there are linear combinations

$$z_j = \sum_{i=1}^{n} \beta_{ij} t_i, \qquad j = 1,\ldots,d$$

so that $z_1,\ldots,z_d$ are algebraically independent and A is integral and separable over $k[z_1,\ldots,z_d]$. By Theorem 3.69, $\mathrm{Int}_{k[z_1,\ldots,z_d]}(\mathrm{Frac}\,A)$ is a finite $k[z_1,\ldots,z_d]$-module; hence, a finite A-module. Yet, by transitivity of integral dependence,

$$\mathrm{Int}_{k[z_1,\ldots,z_d]}(\mathrm{Frac}\,A) = \mathrm{Int}_A(\mathrm{Frac}\,A).$$

So, $\mathrm{Int}_A(\mathrm{Frac}\,A)$ is a finite A-module; thereby a finitely generated k-algebra, as required. □

The somewhat involved nature of the two finiteness Theorems (Theorems 3.69 and 3.73) indicates the delicate nature of the finiteness of $\mathrm{Int}_A(K)$ as A-module. If the Krull dimension of A is 3 or larger, it can even happen that $\mathrm{Int}_A(K)$ is not noetherian (even if A is so). The Japanese school around Nagata studied these questions and Grothendieck in his algebraic geometry treatise (EGA, IV, part 1, [21]) called attention to the class of domains having the finiteness property together with all their finitely generated algebra extensions. He used the terminology *universally Japanese rings*, but it seems that *Nagata rings* is the one used most often now. The formal definition is this

Definition 3.6 An integral domain, A, is a *Nagata ring* if and only if for every finitely generated A-algebra, B, which is a domain and any finite extension, K, of $\mathrm{Frac}\,B$, the ring $\mathrm{Int}_B(K)$ is a finite B-module.

As a corollary of Theorem 3.69, we see immediately the following

Proposition 3.74 *If A is the ring of integers in a number field (i.e., $A = \mathrm{In}_{\mathbb{Z}}(K)$, where K is a finite extension of $\mathbb{Q}$), then A is a Nagata ring as is $A[t_1,\ldots,t_n]$.*

A main theorem, proved by Nagata, concerning these matters is the following:

Theorem 3.75 *(Nagata) Say A is a complete, noetherian local domain, and K is a finite degree extension field of* $\mathrm{Frac}(A)$*, then* $\mathrm{Int}_A(K)$ *is a finitely generated A-algebra and a finite A-module.*

This theorem is not part of our purview, nor will we use it; so, its proof is omitted.

There is another finiteness result involving integrality which has many uses.

Proposition 3.76 *(E. Noether) If B is a finitely generated A-algebra, A being noetherian, and if C is a sub A-algebra of B so that B is integral over C, then C is a finitely generated A-algebra.*

Proof. Write $B = A[t_1, \ldots, t_n]$; each t_j satisfies an integral dependence over C

$$g_j(t_j) = 0, \qquad j = 1, \ldots, n.$$

If $\alpha_1, \ldots, \alpha_q$ are the coefficients ($\in C$) of all these equations, form $A[\alpha_1, \ldots, \alpha_q] \subseteq C$. The t_i are integral over $A[\alpha_1, \ldots, \alpha_q]$ and they generate B; so, B is a finite $A[\alpha_1, \ldots, \alpha_q]$-module. But C is a sub $A[\alpha_1, \ldots, \alpha_q]$-module of B and $A[\alpha_1, \ldots, \alpha_q]$ is noetherian. Therefore, C is a finitely generated $A[\alpha_1, \ldots, \alpha_q]$-module, say $C = A[\alpha_1, \ldots, \alpha_q][z_1, \ldots, z_s]$; we are done. □

What happens if $A \subseteq \mathrm{Frac}(A)$ is not a normal domain? Of course we'll form $\mathrm{Int}_A(\mathrm{Frac}(A)) = \widetilde{A}$, then we want to study the relations between A and $\widetilde{A}$. For example look at

$$A = \mathbb{Z}[ni], \quad n \in \mathbb{Z} \quad \text{and} \quad n > 0$$

and

$$\widetilde{A} = \mathrm{Int}_A(\mathbb{Q}(i)) = \mathbb{Z}[i].$$

The main invariant controlling the relations between A and $\widetilde{A}$ is the transporter $(\widetilde{A} \longrightarrow A)$ in A. That is, we examine

$$f = (\widetilde{A} \longrightarrow A) = \{\xi \in A \mid \xi\widetilde{A} \subseteq A\}.$$

The set f is, of course, an ideal of A; it is called the *conductor* of A in $\widetilde{A}$ or just the *conductor of the integral closure of* A. The symbol f comes from the German word for conductor: Führer. But, clearly, f is also an ideal of $\widetilde{A}$. In the example above,

$$f = \{\xi \in \mathbb{Z}[ni] \mid n | \Re(\xi)\}.$$

Remark: The domain, A, is normal if and only if f is the unit ideal. An ideal, $\mathfrak{A}$, of A which is also an ideal of $\widetilde{A}$ must necessarily be contained in the conductor, f. That is, f is the unique largest ideal of A which is simultaneously an ideal of $\widetilde{A}$.

The first of these statetements is obvious; for the second, we have $\mathfrak{A}\widetilde{A} \subseteq \mathfrak{A}$ as $\mathfrak{A}$ is an $\widetilde{A}$-ideal and $\mathfrak{A} \subseteq A$ as $\mathfrak{A}$ is an A-ideal. Thus,

$$\mathfrak{A}\widetilde{A} \subseteq \mathfrak{A} \subseteq A$$

and this says $\mathfrak{A} \subseteq (\widetilde{A} \longrightarrow A) = f$.

The connection between A and $\widetilde{A}$ *vis a vis* localization and prime ideals is this:

Proposition 3.77 *For a domain, A, its integral closure $\widetilde{A}$ and the conductor, f, of A in $\widetilde{A}$ we have*

(1) If S is a multiplicative set in A, then $S^{-1}\widetilde{A} = \mathrm{Int}_{S^{-1}A}(\mathrm{Frac}(A))$

(2) If $f \cap S \neq \emptyset$, then $S^{-1}A = S^{-1}\widetilde{A}$, that is $S^{-1}A$ is normal.

(3) If $\widetilde{A}$ is a finite A-module then the conductor of $S^{-1}A$ in $S^{-1}\widetilde{A}$ is $f \cdot S^{-1}A = f^e$.

(4) If $\widetilde{A}$ is a finite A-module, them $S^{-1}A$ is normal if and only if $f \cap S \neq \emptyset$.

(5) If $\widetilde{A}$ is a finite A-module, then

$$\{\mathfrak{p} \in \mathrm{Spec}\, A \mid A_{\mathfrak{p}} \quad \textit{is } \textbf{not } \textit{normal}\}$$

is closed in Spec A*; indeed it is $V(f)$. Hence, in this case, $A_{\mathfrak{p}}$ is a normal ring on an open dense set of* Spec A.

Proof. (1) This is clear from Proposition 3.54 and Fact B following it.

(2) Write $s \in f \cap S$ and choose $\alpha \in \widetilde{A}$. We know $s\alpha = a \in A$; so, $\alpha = a/s \in S^{-1}A$. We find $\widetilde{A} \subseteq S^{-1}A$, hence $S^{-1}\widetilde{A} \subseteq S^{-1}A$. The other inclusion is clear.

(3) Write $\alpha_1, \ldots, \alpha_t$ for a finite set of A-module generators for $\widetilde{A}$ in this part and in part (4). To check that an element $x \in S^{-1}A$ lies in $(S^{-1}\widetilde{A} \longrightarrow S^{-1}A)$, it suffices to see that it is in $(\widetilde{A} \longrightarrow S^{-1}A)$. For the latter, all we need is $x\alpha_j \in S^{-1}A$ for $j = 1, \ldots, t$. Conversely, if $x \in (S^{-1}\widetilde{A} \longrightarrow S^{-1}A)$, then certainly $x\alpha_j \in S^{-1}A$, all j.

Now $x\alpha_j \in S^{-1}A$ implies there is some $s_j \in S$ with $s_j x\alpha_j \in A$. If $s = s_1 \cdots s_t$, then $sx\alpha_j \in A$ therefore $sx \in f$, i.e., $x \in f^e$. The converse is clear.

(4) The "if" part of our conclusion is (2), so say $S^{-1}A$ is normal. Then the conductor $(S^{-1}\widetilde{A} \longrightarrow S^{-1}A)$ is the unit ideal; so, (3) shows $f^e =$ unit ideal. This implies $f \cap S \neq \emptyset$.

(5) Write $S(\mathfrak{p})$ for $A - \mathfrak{p}$, then $A_\mathfrak{p}$ is not normal iff $f \cap S(\mathfrak{p}) = \emptyset$ which holds iff $f \subseteq \mathfrak{p}$; that is iff $\mathfrak{p} \in V(f)$. To finish the proof we need only show that any non-empty open set of Spec A is dense when A is a domain. But, this will hold if we show $X_f \cap X_g \neq \emptyset$ (provided neither X_f nor X_g is empty) (DX). However, $X_f \cap X_g = X_{fg}$, and, as neither f nor g is zero, their product is non-zero (and not nilpotent). Now apply Proposition 3.12 part (3). □

Corollary 3.78 *For a domain A and its integral closure, $\widetilde{A}$, assume $\widetilde{A}$ is a finite A-module. Then, for a prime $\mathfrak{p}$ of* Spec A *not in $V(f)$, there exists one and only one prime ideal, $\widetilde{\mathfrak{p}}$, of $\widetilde{A}$ lying over A. This prime ideal is $\mathfrak{p}A_\mathfrak{p} \cap \widetilde{A}$.*

Proof. Existence is clear either by the Lying Over Theorem or by the fact that $\mathfrak{p}A_\mathfrak{p}$ is prime and $A_\mathfrak{p} \supseteq \widetilde{A}$. (The latter holds as $A_\mathfrak{p}$ is normal since $\mathfrak{p} \notin V(f)$.) To see uniqueness, observe as $\mathfrak{p} \not\supseteq f$ there is $\delta \in f$ with $\delta \notin \mathfrak{p}$. Then for any ideal, $\mathfrak{A}$, of $\widetilde{A}$

$$\delta\mathfrak{A} \subseteq \delta\widetilde{A} \subseteq A$$

and $\delta\mathfrak{A} \subseteq \mathfrak{A}$, too. Therefore $\delta\mathfrak{A} \subseteq \mathfrak{A} \cap A$; so if $\mathfrak{A}$ is an ideal contracting to $\mathfrak{p}$ we get $\delta\mathfrak{A} \subseteq \mathfrak{p}$. Now, $\delta \notin \mathfrak{p}$, therefore $\mathfrak{A} \subseteq \mathfrak{p}A_\mathfrak{p}$, so $\mathfrak{A} \subseteq \mathfrak{p}A_\mathfrak{p} \cap \widetilde{A} = \widetilde{\mathfrak{p}}$. Suppose, in fact, $\mathfrak{A}$ is prime yet $\mathfrak{A} < \widetilde{\mathfrak{p}}$, then we'd have a contradiction to non-comparability (Proposition 3.62). □

Note: Generally, $\mathfrak{p}\widetilde{A}$ is not a prime ideal of $\widetilde{A}$; but, of course, $\mathfrak{p}\widetilde{A}$ is always contained in $\widetilde{\mathfrak{p}}$.

3.6 Primary Decomposition

In $\mathbb{Z}$, we have unique factorization and we know this is not valid in an arbitrary (even Noetherian) commutative ring. Can one generalize so as to obtain a "decomposition" of ideals (or submodules) into special ideals (resp. modules) which resemble prime powers? Surprisingly, the answer is connected with a generalization of Fitting's lemma from linear algebra.

Lemma 3.79 *(Fitting's lemma) If V is a finite dimensional vector space over a field, k, and $\theta\colon V \to V$ is an endomorphism, then there exist subspaces W and Z of V so that*

(1) $V = W \coprod Z$.

(2) $\theta \restriction W$ *is an isomorphism.*

(3) $\theta \restriction Z$ *is nilpotent.*

Proof. See any introductory algebra text. □

Look at $\mathbb{Z}$. Pick n, then we have the ideal $\mathfrak{A} = n\mathbb{Z}$. Factor n as $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, where $p_1, \ldots, p_t$ are distinct prime numbers. We get $\mathfrak{A} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_t^{e_t}$, where $\mathfrak{P}_j$ is the prime ideal $p_j\mathbb{Z}$. Now, we also have $\mathfrak{A} = \bigcap_{j=1}^{t} \mathfrak{P}_j^{e_j}$, since the $\mathfrak{P}_j$ are pairwise comaximal.

This last equality is still wrong, say in $\mathbb{C}[X, Y]$, and the fault is the $\mathfrak{P}_i^{e_i}$. They are not general enough.

Let A be a commutative ring, M an A-module and $N \subseteq M$ a submodule. Set

$$\mathrm{Rad}_M(N) = \sqrt{(M \longrightarrow N)} = \sqrt{\{x \in A \mid xM \subseteq N\}} = \{x \in A \mid (\exists k > 0)(x^k M \subseteq N)\}.$$

This is the *relative radical of N in M*. The following properties are easily checked:

(1) $\mathrm{Rad}_{M/N}((0)) = \mathrm{Rad}_M(N)$.

(2) $\mathrm{Rad}_M((0)) = \sqrt{\mathrm{Ann}(M)}$.

(3) $\mathrm{Rad}_A(\mathfrak{q}) = \sqrt{\mathfrak{q}}$.

(3a) $\mathrm{Rad}_{A/\mathfrak{q}}((0)) = \sqrt{\mathfrak{q}}$.

(4) $\mathrm{Rad}_M(N \cap P) = \mathrm{Rad}_M(N) \cap \mathrm{Rad}_M(P)$.

(5) $\mathrm{Rad}_M(\mathfrak{A}N) \supseteq \sqrt{\mathfrak{A}} \cap \mathrm{Rad}_M(N)$.
Here, $\mathfrak{A}$ is an ideal of A; M is an A-module; N is a submodule of M.

Definition 3.7 A module, M, is *coprimary* iff for every $a \in A$, the map $\sigma_a\colon M \to M$ *via* $\sigma_a(m) = am$ is either injective or nilpotent. (The map σ_a is called a *homothety*.) An ideal, $\mathfrak{q}$, of A is a *primary ideal* iff the module, $A/\mathfrak{q}$, is coprimary.

Notice the clear connection of this idea with Fitting's lemma.

Proposition 3.80 *For any commutative ring, A, and any ideal, $\mathfrak{q}$, the following are equivalent:*

(α) For all $x, y \in A$ if $xy \in \mathfrak{q}$ but $y \notin \mathfrak{q}$, then $x^k \in \mathfrak{q}$, for some $k \geq 1$.

(β) For all $y \notin \mathfrak{q}$, we have $(y \longrightarrow \mathfrak{q}) \subseteq \sqrt{\mathfrak{q}}$.

(γ) $\bigcup_{y \notin \mathfrak{q}} (y \longrightarrow \mathfrak{q}) = \sqrt{\mathfrak{q}}$.

(δ) Every zero divisor of the ring $A/\mathfrak{q}$ is nilpotent.

(ϵ) The ideal $\mathfrak{q}$ *is primary.*

Proof. The equivalence $(\alpha) \Longleftrightarrow (\beta)$ is clear and the implication $(\gamma) \Longrightarrow (\beta)$ is a tautology. If (β), then pick $\xi \in \sqrt{\mathfrak{q}}$. If $\xi \in \mathfrak{q}$, then $\xi \in (y \longrightarrow \mathfrak{q})$ for all y. Thus, we may assume that $\xi \notin \mathfrak{q}$ and so, there is a minimum $k \geq 2$ so that $\xi^k \in \mathfrak{q}$. Let $y = \xi^{k-1} \notin \mathfrak{q}$. We have $\xi y = \xi^k \in \mathfrak{q}$, so, $\xi \in (\xi^{k-1} \longrightarrow \mathfrak{q})$ and (γ) holds.

$(\alpha) \Longrightarrow (\delta)$. Pick $\overline{x} \in A/\mathfrak{q}$, a zero divisor, which means that there is some $\overline{y} \neq 0$ with $\overline{x}\,\overline{y} = 0$. It follows that $y \notin \mathfrak{q}$ and $xy \in \mathfrak{q}$; by (α), we get $x^k \in \mathfrak{q}$, for some k, and so, $\overline{x}^k = 0$.

$(\delta) \Longrightarrow (\epsilon)$. Pick $a \in A$. We need to show that σ_a is injective or nilpotent in $A/\mathfrak{q}$. Say σ_a is not injective. Then, there is some $\overline{y} \neq 0$ in $A/\mathfrak{q}$ and $a\overline{y} = 0$ in $A/\mathfrak{q}$, i.e. $\overline{a}\,\overline{y} = 0$. But, $\overline{y} \neq 0$, so, by (δ), $\overline{a}$ is nilpotent. Consequently, $\overline{a}^k = 0$, and so, $(\sigma_a)^k = 0$ in $A/\mathfrak{q}$.

$(\epsilon) \Longrightarrow (\alpha)$. Pick x, y with $xy \in \mathfrak{q}$ and $y \notin \mathfrak{q}$. Look at σ_x on $A/\mathfrak{q}$. We have

$$\sigma_x(\overline{y}) = \overline{x}\,\overline{y} = \overline{xy} = 0, \quad \text{as } xy \in \mathfrak{q}.$$

As $\overline{y} \neq 0$, the map σ_x is not injective on $A/\mathfrak{q}$. By (ϵ), the map σ_x is nilpotent. This means that $(\sigma_x)^k = \sigma_{x^k} = 0$ in $A/\mathfrak{q}$. In particular, $\sigma_{x^k}(1) = \overline{x}^k 1 = 0$, i.e., $\overline{x^k} = 0$. Therefore, $x^k \in \mathfrak{q}$. □

Corollary 3.81 *If* $\sqrt{\mathfrak{q}}$ *is maximal, then* $\mathfrak{q}$ *is primary. In particular, if* $\mathfrak{m}$ *is a maximal ideal, then* $\mathfrak{m}^n$ *is primary for all* $n > 0$.

Proof. The image of $\sqrt{\mathfrak{q}}$ in $A/\mathfrak{q}$ is the nilradical of $A/\mathfrak{q}$. Since $\sqrt{\mathfrak{q}}$ is maximal in A, the ring $A/\mathfrak{q}$ has a unique maximal ideal. It follows that every element of $A/\mathfrak{q}$ is either a unit or nilpotent, so Proposition 3.80 (3) applies. The second part of the statement follows from the first since $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ for every prime ideal, $\mathfrak{p}$. □

There exist prime ideals, $\mathfrak{p}$, such that $\mathfrak{p}^n$ is not primary. There exist primary ideals, $\mathfrak{q}$, **not** of the form $\mathfrak{p}^n$, where $\mathfrak{p} \in \operatorname{Spec} A$.

Corollary 3.82 *Say* $\mathfrak{q}$ *is a primary ideal of* A*, then* $\sqrt{\mathfrak{q}}$ *is a prime ideal.*

Proof. Pick $x, y \in A$ with $xy \in \sqrt{\mathfrak{q}}$ and $y \notin \sqrt{\mathfrak{q}}$. Then, $x^k y^k = (xy)^k \in \mathfrak{q}$, for some $k > 0$. So, $\sigma_{x^k}(\overline{y}^k) = 0$ in $A/\mathfrak{q}$ and $\overline{y}^k \neq 0$ in $A/\mathfrak{q}$. Therefore, our homothety, σ_{x^k}, is nilpotent, so, σ_x is nilpotent, i.e., $(\sigma_x)^l \equiv 0$ on $A/\mathfrak{q}$. Then, $(\sigma_x)^l(1) = x^l \cdot 1 = x^l = 0$ in $A/\mathfrak{q}$, and so, $x^l \in \mathfrak{q}$, i.e., $x \in \sqrt{\mathfrak{q}}$. □

There exist *non-primary ideals*, $\mathfrak{A}$, yet $\sqrt{\mathfrak{A}}$ *is* prime.

Definition 3.8 A submodule, N, of a module, M, is *primary in* M iff M/N is co-primary. Then, $\operatorname{Rad}_M(N)$ is prime (same argument), say $\mathfrak{p}$. In this case, we say N is $\mathfrak{p}$-primary when M/N is $\mathfrak{p}$-coprimary, *i.e.*, M/N is coprimary and $\operatorname{Rad}_M(N) = \mathfrak{p}$.

Say M is an A-module, N is a submodule of M and S is a multiplicative set in A. Look at

$$N^{ec} = \{m \in M \mid (\exists s \in S)(sm \in N)\} = S(N),$$

and call it the *S-component* of N or *S-saturation* of N.

Further Properties:

(6) $S((0)) = \operatorname{Ker}(M \longrightarrow S^{-1}M)$.

(7) $S(\bigcap_{i=1}^t N_i) = \bigcap_{i=1}^t S(N_i)$.

(8) $S(V \longrightarrow N) = (V \longrightarrow S(N))$.

Proposition 3.83 *If A is a commutative ring, M is a f.g. A-module and N a submodule of M, then the following are equivalent:*

(1) N is primary in M.

(2) For all multiplicative sets, $S \subseteq A$, we have

$$S(N) = \begin{cases} N \\ \\ M. \end{cases} \quad or$$

(3) For all multiplicative sets, $S \subseteq A$, the map $M/N \longrightarrow S^{-1}(M/N)$ is either injective or zero.

Proof. Note that $S_{M/N}(0) = \overline{S(N)} = \text{Ker}\,(M/N \longrightarrow S^{-1}(M/N))$. Therefore, (2) and (3) are equivalent.

(1) $\Longrightarrow$ (2). Take any S and examine $\sqrt{(M \longrightarrow N)} = \text{Rad}_{M/N}((0))$. There are two cases:
(1) $S \cap \text{Rad}_{M/N}((0)) = \emptyset$ or (2) $S \cap \text{Rad}_{M/N}((0)) \neq \emptyset$.

Case 2. There is some $s \in S$ with $s \in \text{Rad}_{M/N}((0))$. So, $s^k \in (M \longrightarrow N)$ and then $s^k \in S$ implies that $M \subseteq S(N)$; thus, $M = S(N)$.

Case 1. Pick $s \in S$ and look at σ_s. If σ_s is nilpotent on M/N, then $(\sigma_s)^k = \sigma_{s^k} \equiv 0$ on M/N, which implies that $s^k M \subseteq N$. So, $s \in \sqrt{(M \longrightarrow N)} \cap S$, a contradiction. Therefore, σ_s must be injective on M/N, by (1). This means given any $m \in M$, we have $\sigma_s(\overline{m}) = s\overline{m} = 0$ in M/N iff $m \in N$, already, i.e., $sm \in N$ iff $m \in N$. As this holds for all $s \in S$, we have $S(N) = N$.

(2) $\Longrightarrow$ (1). Pick $s \in A$ and look at $S = \{s^k \mid k \geq 0\}$. If $s \in \mathcal{N}(A)$, then $(\sigma_s)^k = \sigma_{s^k} \equiv 0$ on *any* module. So, we may assume $s \notin \mathcal{N}(A)$ and then, S is a multiplicative set. Thus, (2) holds for S. We have to show that M/N is coprimary, i.e., σ_s is either nilpotent or injective. Say, σ_s is not injective on M/N, i.e., $S(N) \neq N$. By (2), we have $S(N) = M$. Pick generators, $m_1, \ldots, m_t$ for M. As $S(N) = M$, each $m_j \in S(N)$; so, there is some k_j with $s^{k_j} m_j \in N$, for $j = 1, \ldots, t$. Let $k = \max\{k_1, \ldots, k_t\}$, then $s^k m_j \in N$, for $j = 1, \ldots, t$. It follows that $s^k M \subseteq N$ and so, s^k kills M/N, i.e. σ_s is nilpotent on M/N. □

Proposition 3.84 *(E. Noether, 1921) If M is a noetherian module, then any non-primary submodule, N, of M is reducible, i.e., N is the intersection, $N = Q_1 \cap Q_2$, of proper submodules of M properly containing N.*

Proof. (Adapted from Fitting's lemma.) Since N is non-primary, M/N is not coprimary. So, there is some $a \in A$ so that σ_a is not injective and not nilpotent on M/N. Write $\overline{M_j} = \text{Ker}\,(\sigma_a)^j = \text{Ker}\,(\sigma_{a^j})$ on M/N. We have an ascending chain

$$\overline{M_1} \subseteq \overline{M_2} \subseteq \overline{M_3} \subseteq \cdots .$$

By the ACC, the chain stops, say at r. We have $\overline{M_r} = \overline{M_{r+1}} = \cdots = \overline{M_{2r}}$. Let $\varphi = \sigma_{a^r} \in \text{End}_A(M/N)$. We have $\text{Ker}\,\varphi \neq M/N$, else $(\sigma_a)^r \equiv 0$, contradicting the non-nilpotence of σ_a. So, $\text{Im}\,\varphi \neq (0)$. Also, $\text{Ker}\,\varphi \supseteq \text{Ker}\,\sigma_a \neq (0)$, as σ_a is not injective. I claim that $\text{Ker}\,\varphi \cap \text{Im}\,\varphi = (0)$.

Pick $\xi \in \text{Ker}\,\varphi \cap \text{Im}\,\varphi$. So, $\xi = \varphi(\eta) = a^r\eta$. As $\varphi(\xi) = 0$, we have $\varphi(a^r\eta) = 0$; thus $a^r\varphi(\eta) = 0$, and so, $a^{2r}\eta = 0$, i.e., $\eta \in \overline{M_{2r}} = \overline{M_r}$. Consequently, $a^r\eta = 0$, i.e., $\xi = 0$, as desired. But, now, $\text{Ker}\,\varphi \cap \text{Im}\,\varphi = (0)$ implies that

$$N = \pi^{-1}(\text{Ker}\,\varphi) \cap \pi^{-1}(\text{Im}\,\varphi),$$

where $\pi\colon M \to M/N$ is the natural projection. □

We need a restatement of a Proposition 3.83 for the reduction process:

Proposition 3.85 *Say N is a submodule of M, and $\mathfrak{p}$ is a given prime ideal.*

(a) N is $\mathfrak{p}$-primary in M iff for all multiplicative sets, S, of A, we have

$$S(N) = \begin{cases} N & \text{iff } \mathfrak{p} \cap N = \emptyset \\ M & \text{iff } \mathfrak{p} \cap N \neq \emptyset. \end{cases}$$

(b) If $N_1, \ldots, N_t$ are all $\mathfrak{p}$-primary, then $N_1 \cap \cdots \cap N_t$ is again $\mathfrak{p}$-primary.

(c) If V is any submodule of M, then when N is $\mathfrak{p}$-primary, we have

$$S(V \longrightarrow N) = \begin{cases} A & \text{iff } V \subseteq N \\ \mathfrak{p}\text{-primary ideal} & \text{iff } V \not\subseteq N. \end{cases}$$

Proof. (a) The module N is primary iff M/N is coprimary iff $S((0)) = (0)$ or $S((0)) = M/N$, for any multiplicative subset, S (where $(0) \subseteq M/N$) iff $S(N) = N$ or $S(N) = M$, for any such S. (Recall, $S((0)) = \overline{S(N)}$.) But, the dichotomy: $S(N) = N$ or M, depends on $S \cap \mathrm{Rad}_M(N) = S \cap \mathrm{Rad}_{M/N}((0)) = S \cap \sqrt{(M \longrightarrow N)}$. Namely, $S(N) = N$ iff $S \cap \mathrm{Rad}_M(N) = \emptyset$ and $S(N) = M$ iff $S \cap \mathrm{Rad}_M(N) \neq \emptyset$. But here, $\mathfrak{p} = \mathrm{Rad}_M(N)$, so (a) is proved.

(b) Now, $S(\bigcap_{i=1}^t N_i) = \bigcap_{i=1}^t S(N_i)$, so (a) implies (b).

(c) If $V \subseteq N$, then $(V \longrightarrow N) = A$, so, $S(V \longrightarrow N) = A$. So, we may assume $V \not\subseteq N$. Recall that $S(V \longrightarrow N) = (V \longrightarrow S(N))$. We will test $S(V \longrightarrow N)$ by part (a) (here, $M = A$). But,

$$S(N) = \begin{cases} M & \text{iff } S \cap \mathfrak{p} \neq \emptyset \\ N & \text{iff } S \cap \mathfrak{p} = \emptyset. \end{cases}$$

In the case $S \cap \mathfrak{p} \neq \emptyset$, we have $S(V \longrightarrow N) = (V \longrightarrow M) = A$. If $S \cap \mathfrak{p} = \emptyset$, then $S(V \longrightarrow N) = (V \longrightarrow N)$, and the test of (a) shows (c). □

Reduction Process for Primary Decomposition

Say $N = Q_1 \cap Q_2 \cap \cdots \cap Q_t$ is a decomposition of N as a finite intersection of $\mathfrak{p}_i$-primary modules, Q_i.

No assertion $\mathfrak{p}_i \neq \mathfrak{p}_j$ is made.

(1) Remove all Q_j from the intersection $\bigcap_{i=1}^t Q_i$, whose removal does not affect the intersection.

(2) Lump together as an intersection all the Q_i's for which the $\mathfrak{p}_i$'s agree. By (b), the "new" intersection satisfies:

(α) No $\widetilde{Q}_j$, still primary, can be removed without changing the intersection.

(β) All the $\mathfrak{p}_j$ $\left(= \sqrt{(M \longrightarrow \widetilde{Q}_j)}\right)$ are distinct.

Such a primary decomposition is called *reduced*.

Theorem 3.86 *(Lasker-Noether Decomposition Theorem, 1921) Every submodule, N, of a noetherian module, M, can be represented as a reduced primary decomposition:*

$$N = Q_1 \cap Q_2 \cap \cdots \cap Q_t.$$

Proof. (Noetherian induction—invented for this theorem.) Let

$$\mathcal{S} = \{N \subseteq M \mid N \text{ is not a finite intersection of primary submodules}\}.$$

If $\mathcal{S} \neq \emptyset$, by the ACC, the set $\mathcal{S}$ has maximal element. Call it N. Of course, N is not primary. By Noether's proposition (Proposition 3.84), there exist $Q_1, Q_2 > N$, so that $N = Q_1 \cap Q_2$. But N is maximal in $\mathcal{S}$, so

$Q_j \notin \mathcal{S}$ for $j = 1, 2$. Thus, we can write $Q_1 = \bigcap_{j=1}^{t_1} Q_j^{(1)}$ and $Q_2 = \bigcap_{k=1}^{t_2} Q_j^{(2)}$, where the $Q_j^{(i)}$ are primary ($i = 1, 2$, finitely many j's). Consequently, we get

$$N = Q_1^{(1)} \cap \cdots \cap Q_{t_1}^{(1)} \cap Q_1^{(2)} \cap \cdots \cap Q_{t_2}^{(2)},$$

contradicting $N \in \mathcal{S}$. Therefore, $\mathcal{S} = \emptyset$. Now apply the reduction process to a primary decomposition of N and we get the conclusion. □

Corollary 3.87 *(Lasker's Decomposition Theorem, original form, 1905) If $A = \mathbb{C}[X_1, \ldots, X_n]$, then every ideal, $\mathfrak{A}$, admits a reduced primary decomposition: $\mathfrak{A} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$.*

Corollary 3.88 *(Noether's statement) If A is any noetherian ring and $\mathfrak{A}$ is any ideal of A, then $\mathfrak{A}$ admits a reduced primary decomposition: $\mathfrak{A} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$.*

Now, what about uniqueness?

Proposition 3.89 *Say that N is an A-submodule of M, and $N = Q_1 \cap \cdots \cap Q_t$ is a reduced primary decomposition for N. Let $I = \{1, \ldots, t\}$ and given any multiplicative subset, S, of A, write*

$$S(I) = \{i \in I \mid S \cap \mathfrak{p}_i = \emptyset\}.$$

Here, $\mathfrak{p}_i = \mathrm{Rad}_M(Q_i)$ is the prime associated to Q_i. Then,

$$(a) \qquad S(N) = \bigcap_{j \in S(I)} Q_j.$$

$$(b) \qquad S^{-1}Q_i = \begin{cases} S^{-1}M & \text{if } i \notin S(I) \\ \mathfrak{p}_i^e\text{-primary submodule of } S^{-1}M & \text{if } i \in S(I). \end{cases}$$

$$(c) \qquad S^{-1}N = \bigcap_{j \in S(I)} S^{-1}Q_j,$$

and this is a reduced primary decomposition for $S^{-1}N$ as submodule of $S^{-1}M$.

Proof. (a) We know that $S(N) = \bigcap_{j=1}^{t} S(Q_j)$ and $S(Q_j) = M$ when $j \notin S(I)$ and $S(Q_j) = Q_j$ for $j \in S(I)$ (previous proposition). Thus, it is clear that (a) holds.

(b) Now, Q_i is $\mathfrak{p}_i$-primary, so $S(Q_i) = M$ if $\mathfrak{p}_i \cap S \neq \emptyset$ else $S(Q_i) = Q_i$ or equivalently, $S((0)) = M/Q_i$ if $i \notin S(I)$ else $S((0)) = (0)$ (where (0) is the zero ideal in M/Q_i). Say, $i \notin S(I)$, then $S(Q_i) = M$, and so, for every $m \in M$, there is some $s = s(m) \in S$ with $sm \in Q_i$. Hence, $m/1 \in S^{-1}Q_i$ and it follows that $S^{-1}M \subseteq S^{-1}Q_i$; yet, of course, $S^{-1}Q_i \subseteq S^{-1}M$, so $S^{-1}Q_i = S^{-1}M$, as required. Now, say $i \in S(I)$, so $\mathfrak{p}_i \cap S = \emptyset$. Observe, every multiplicative set, say T, of $S^{-1}A$, has the form $S^{-1}T_0$, for some multiplicative set, T_0, of A. But, M/Q_i is coprimary which means that $M/Q_i \longrightarrow T_0^{-1}(M/Q_i)$ is either injective (case: $T_0((0)) = (0)$) or zero (case: $T_0((0)) = M/Q_i$)). Therefore, as $S^{-1}A$ is flat over A, we get

$$S^{-1}(M/Q_i) \longrightarrow S^{-1}T_0^{-1}(M/Q_i) \quad \text{is injective or zero,} \qquad (*)$$

the first if $T_0 \cap \mathfrak{p}_i = \emptyset$, i.e., $T(= S^{-1}T_0) \cap \mathfrak{p}_i^e = \emptyset$, the second if $T_0 \cap \mathfrak{p}_i \neq \emptyset$, i.e., $T(= S^{-1}T_0) \cap \mathfrak{p}_i^e \neq \emptyset$. But, $S^{-1}T_0^{-1}(M/Q_i) = T^{-1}(S^{-1}M/S^{-1}Q_i)$ and $S^{-1}M/S^{-1}Q_i = S^{-1}(M/Q_i)$, so

$$S^{-1}M/S^{-1}Q_i \longrightarrow T^{-1}(S^{-1}M/S^{-1}Q_i) \quad \text{is injective or zero}$$

depending on $T \cap \mathfrak{p}_i^e$ being empty or not. Therefore, $S^{-1}Q_i$ satisfies our test for $\mathfrak{p}_i^e$-primariness.

(c) We know from (b) that $S^{-1}Q_j$ is $\mathfrak{p}_j^e$-primary and $\mathfrak{p}_i^e \neq \mathfrak{p}_j^e$ if $i \neq j$, as $i, j \in S(I)$ and there is a one-to-one correspondence between the $\mathfrak{p}$'s so that $\mathfrak{p} \cap S = \emptyset$ and the $\mathfrak{p}^e$ of $S^{-1}A$. The rest should be obvious (DX). □

Theorem 3.90 *(First Uniqueness Theorem) If N, an A-submodule of M, has a reduced primary decomposition $N = Q_1 \cap \cdots \cap Q_t$, then the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ ($\mathfrak{p}_i = \sqrt{(M \longrightarrow Q_i)}$) are uniquely determined by N and M, up to the order of their listing.*

Proof. Assume that $N = Q_1 \cap \cdots \cap Q_s = Q'_1 \cap \cdots \cap Q'_t$ are two reduced decompositions for N in M. We use induction on $s+t$. When $s+t=2$, we have $s=t=1$ and $Q_1 = Q'_1$ and uniqueness is obvious. Assume that uniqueness holds for all submodules, N, for which $s+t \leq r-1$. Consider N and two decompositions with $s+t=r$ and let

$$S = A - \bigcup_{i=1}^{s-1} \mathfrak{p}_i - \bigcup_{\mathfrak{p}'_j \neq \mathfrak{p}_s} \mathfrak{p}'_j.$$

Now, $S \cap \mathfrak{p}_i = \emptyset$ for $i = 1, \ldots, s-1$ and $S \cap \mathfrak{p}'_j = \emptyset$ for all j with $\mathfrak{p}'_j \neq \mathfrak{p}_s$. So,

$$S(N) = \bigcap_{i=1}^{s} S(Q_i) = \bigcap_{i=1}^{s-1} Q_i$$

as $S(Q_i) = Q_i$ whenever $S \cap \mathfrak{p}_i = \emptyset$. Also,

$$S(N) = \bigcap_{\mathfrak{p}'_j \neq \mathfrak{p}_s} S(Q'_j) = \bigcap_{\mathfrak{p}'_j \neq \mathfrak{p}_s} Q'_j.$$

For $S(N)$, the sum of the number of components is at most $s-1+t < r$; so, the induction hypothesis implies $S(N)$ has the uniqueness property. However, can it be that $\mathfrak{p}'_j \neq \mathfrak{p}_s$ for $j = 1, \ldots, t$? Were that true, the second intersection would give $S(N) = \bigcap_{j=1}^{t} Q'_j = N$. Thus, we would have

$$\bigcap_{i=1}^{s} Q_i = N = S(N) = \bigcap_{j=1}^{s-1} Q_j,$$

contradicting the fact that the first decomposition is reduced. Therefore, there is some j with $\mathfrak{p}'_j = \mathfrak{p}_s$, and now the induction hypothesis implies

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-1}\} = \{\mathfrak{p}'_j \mid \mathfrak{p}'_j \neq \mathfrak{p}_s\},$$

and the proof is complete. □

Definition 3.9 If N is a submodule of M and N has a primary decomposition, then the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ corresponding to the Q_j's which appear in the decomposition are called the *essential primes of N in M*. The set of such is denoted $\mathrm{Ess}_M(N)$. When $N = (0)$, the primes appearing are called *associated primes of M* and this set is denoted $\mathrm{Ass}(M)$. Of course, $\mathrm{Ass}(M/N) = \mathrm{Ess}_M(N)$. The minimal elements of $\mathrm{Ess}_M(N)$ or $\mathrm{Ass}(M)$ are called *isolated essential primes* of N in M (resp. *isolated associated primes* of M). The Q_i corresponding to isolated primes of either type are called *isolated primary components* of N in M or *isolated primary components* of M.

Theorem 3.91 *(Second Uniqueness Theorem) The isolated primary components of N in M are uniquely determined by M and N.*

Proof. Let Q be such an isolated component of N in M and let $\mathfrak{p}$ be the corresponding minimal prime. Look at $S = A - \mathfrak{p}$. If $\mathfrak{P} \in \mathrm{Ess}_M(N)$, then $\mathfrak{P} > \mathfrak{p}$ implies that $\mathfrak{P} \cap S \neq \emptyset$ and as $\mathfrak{p}$ is minimal, all other $\mathfrak{P}$ touch S. It follows from Proposition 3.89 that $S(N) = Q$. □

The Lasker-Noether theorem has an immediate application to number theory. This concerns factorization and it shows clearly how Lasker-Noether provides a generalization to Noetherian rings of unique factorization in UFD's.

Definition 3.10 A *Dedekind domain* is a noetherian, normal domain of Krull dimension 1.

Examples of Dedekind domains.

(1) Every P.I.D. is a Dedekind domain.

(2) If K is a finite extension of $\mathbb{Q}$ (that is, K is a *number field*) and $O_K = \mathrm{Int}_{\mathbb{Z}}(K)$ (the integral closure of $\mathbb{Z}$ in K), then O_K is a Dedekind domain. The ring O_K is called the *ring of integers in* K.

(3) Let X be a compact Riemann surface and $x \in X$, any point in X. Let

$$\mathcal{A} = \{f \in \mathcal{M}\mathrm{er}(X) \mid \text{ poles of } f \text{ are only at } x\}.$$

Then, $\mathcal{A}$ is a Dedekind domain.

(3a) Let X be an open Riemann surface of finite character, which means that $\overline{X} = X \cup$ finite set of points is a compact Riemann surface. Then, $\mathrm{Hol}(X)$(= the ring of all holomorphic functions on X) is a Dedekind domain.

Say A is a Dedekind domain. If $\mathfrak{p} \in \mathrm{Spec}\, A$ but $\mathfrak{p} \neq (0)$, then dimension 1 implies that $\mathfrak{p} \in \mathrm{Max}(A)$. From Theorem 3.56, $A_{\mathfrak{p}}$ is a PID. Take any non-zero ideal, $\mathfrak{A}$, then by Lasker-Noether, we can write $\mathfrak{A} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$, a reduced primary decomposition. Now,

$$\mathfrak{p}_j = \sqrt{\mathfrak{q}_j} \supseteq \mathfrak{A} > (0),$$

so each of the $\mathfrak{p}_j$'s is a maximal ideal. It follows that each $\mathfrak{p}_j$ is isolated and, by the second uniqueness theorem, the $\mathfrak{q}_j$'s are unique. Moreover, whenever $i \neq j$,

$$\sqrt{\mathfrak{q}_i + \mathfrak{q}_j} = \sqrt{\mathfrak{p}_i + \mathfrak{p}_j} = A,$$

so that $1 \in \mathfrak{q}_i + \mathfrak{q}_j$. We deduce that the $\mathfrak{q}_j$ are pairwise comaximal and the Chinese Remainder Theorem says

$$\mathfrak{A} = \bigcap_{i=1}^{t} \mathfrak{q}_i = \prod_{i=1}^{t} \mathfrak{q}_i.$$

The ring $A/\mathfrak{q}_i$ is noetherian and any $\mathfrak{p} \in \mathrm{Spec}(A/\mathfrak{q}_i)$ corresponds to a prime of A containing $\mathfrak{p}_i$; that is, $\mathfrak{p}$ must be $\mathfrak{p}_i$. Consequently, $A/\mathfrak{q}_i$ is a local ring with the DCC and by Nagata's Theorem $\overline{\mathfrak{p}_i}$ (= image $\mathfrak{p}_i$ in $A/\mathfrak{q}_i$) is nilpotent. Let e_i be its index of nilpotence so that

$$\mathfrak{p}_i^{e_i} \subseteq \mathfrak{q}_i < \mathfrak{p}_i^{e_i - 1}.$$

But, $A_{\mathfrak{p}_i}$ is a PID, and Proposition 3.5 shows that $\mathfrak{q}_i = \mathfrak{p}_i^{e_i}$. In summary, we get the following theorem of Dedekind:

Theorem 3.92 *(Dedekind, 1878) In a Dedekind domain, every nonzero ideal, $\mathfrak{A}$, is a unique product of powers of prime ideals: $\mathfrak{A} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_t^{e_t}$.*

Corollary 3.93 *(Kummer, 1833) In the ring of integers of a number field, every nonzero ideal is a unique product of powers of prime ideals.*

After this little excursion into number theory and the connection of primary decomposition to questions of factorization, we resume our study of primary decomposition for modules—especially its applications to the structure of modules.

Lemma 3.94 *Say M is a $\mathfrak{p}$-coprimary module and N ($\neq (0)$) is a submodule of M. Then, N is also $\mathfrak{p}$-coprimary.*

Proof. Pick $a \in A$ with σ_a not injective on N. Then, σ_a is not injective on M, so, σ_a is nilpotent on M (as M is coprimary). Therefore, $\sigma_a \restriction N$ is also nilpotent; so, N is coprimary. Let $\widetilde{\mathfrak{p}}$ be the prime associated with N while $\mathfrak{p}$ is the prime for M. We know that $\mathfrak{p} = \sqrt{\mathrm{Ann}(M)}$, while $\widetilde{\mathfrak{p}} = \sqrt{\mathrm{Ann}(N)}$. If $x \in \mathfrak{p}$, then $x^k \in \mathrm{Ann}(M)$; so, $x^k \in \mathrm{Ann}(N)$, i.e, $x \in \widetilde{\mathfrak{p}}$. Thus, $\mathfrak{p} \subseteq \widetilde{\mathfrak{p}}$.

Now, pick x with σ_x not injective on N. This implies that $(\sigma_x)^k \equiv 0$ on N, that is, $x^k \in \mathrm{Ann}(N)$, *i.e.*, $x \in \widetilde{\mathfrak{p}}$. Thus, $x \in \widetilde{\mathfrak{p}}$ implies σ_x is not injective on N, hence σ_x is not injective on M, and so $(\sigma_x)^k \equiv 0$ on M as M is coprimary which implies that $x \in \mathfrak{p}$. Therefore, we also have $\widetilde{\mathfrak{p}} \subseteq \mathfrak{p}$, and $\widetilde{\mathfrak{p}} = \mathfrak{p}$. □

Proposition 3.95 *A necessary and sufficient condition that M be $\mathfrak{p}$-coprimary is that* $\mathrm{Ass}(M) = \{\mathfrak{p}\}$. *Let $N \subseteq M$, for arbitrary M and N, then* $\mathrm{Ass}(N) \subseteq \mathrm{Ass}(M)$.

Proof. Assume M is $\mathfrak{p}$-coprimary. Then (0) is $\mathfrak{p}$-primary in M. By the first uniqueness theorem, $\mathrm{Ass}(M) = \{\mathfrak{p}\}$. Conversely, if $\mathrm{Ass}(M) = \{\mathfrak{p}\}$, then (0) has just one primary component, whose prime is $\mathfrak{p}$. So, (0) is $\mathfrak{p}$-primary and it follows that M is $\mathfrak{p}$-coprimary.

Assume $N \subseteq M$. Write $(0) = Q_1 \cap \cdots \cap Q_t$, a reduced primary decomposition of (0) in M. Then, $\mathrm{Ass}(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$. By intersecting $(0) = Q_1 \cap \cdots \cap Q_t$ with N, we get

$$(0) = (Q_1 \cap N) \cap \cdots \cap (Q_t \cap N).$$

Observe that we have the composite map

$$N \hookrightarrow M \longrightarrow M/Q_i$$

and its kernel is $N \cap Q_i$. Hence, $N/(N \cap Q_i) \hookrightarrow M/Q_i$. But, M/Q_i is $\mathfrak{p}_i$-coprimary; so, from the argument above, $N/(N \cap Q_i)$ is also $\mathfrak{p}_i$-coprimary, provided that $N/(N \cap Q_i) \neq (0)$. Now, we have $N/(N \cap Q_i) = (0)$ iff $Q_i \supseteq N$. Consequently, we have

$$(0) = (Q_{i_1} \cap N) \cap \cdots \cap (Q_{i_s} \cap N) \quad \text{in } N,$$

where $Q_{i_l} \not\supseteq N$, for each i_l, and $Q_{i_l} \cap N$ is $\mathfrak{p}_{i_l}$-primary in N. By the first uniqueness theorem, we deduce that

$$\mathrm{Ass}(N) = \{\mathfrak{p} \in \mathrm{Ass}(M) \mid Q \not\supseteq N, \text{ where } Q \text{ corresponds to } \mathfrak{p}\}.$$

□

Corollary 3.96 *(of the proof) If $N \subseteq M$, then*

$$\mathrm{Ass}(N) = \{\mathfrak{p} \in \mathrm{Ass}(M) \mid Q \not\supseteq N, \text{ where } Q \text{ corresponds to } \mathfrak{p}\}.$$

Proposition 3.97 *Say $(0) = \bigcap_{i=1}^{t} Q_i$ is a reduced primary decomposition of (0) in M and let N be a submodule of M. Then, N is $\mathfrak{p}_i$-coprimary if and only if $N \cap Q_i = (0)$. In particular, there exist $\mathfrak{p}_i$-coprimary submodules of M, namely, $\bigcap_{j \neq i} Q_j$. In fact, $\mathfrak{p} \in \mathrm{Ass}(M)$ iff M contains a submodule which is $\mathfrak{p}$-coprimary. Lastly, if $N \cap (Q_i + Q_j) = (0)$, then $N = (0)$. Therefore, M is an essential extension of $Q_i + Q_j$.*

Proof. Say $N \cap Q_i = (0)$, then

$$N = N/(N \cap Q_i) \hookrightarrow M/Q_i.$$

Therefore, N is a submodule of the $\mathfrak{p}_i$-coprimary module M/Q_i. But then, N is $\mathfrak{p}_i$-coprimary (as a submodule of a $\mathfrak{p}_i$-coprimary is $\mathfrak{p}_i$-coprimary). Conversely, since $(0) = \bigcap_i Q_i$, we get

$$(0) = \bigcap_i (Q_i \cap N), \tag{$*$}$$

and we know that $Q_i \cap N$ is $\mathfrak{p}_i$-primary if $Q_i \cap N \neq N$, and that $(*)$ is a reduced decomposition. Since N is $\mathfrak{p}_i$-coprimary, by the first uniqueness theorem, there can be only one term in $(*)$, i.e., $Q_j \supseteq N$ for all $j \neq i$; then $(0) = Q_i \cap N$. The second statement is now obvious. If $N \cap (Q_i + Q_j) = (0)$, then, of course, $N \cap Q_i = N \cap Q_j = (0)$. Then, $\mathfrak{p}_i$ and $\mathfrak{p}_j$ would be primes of N, yet, N is coprimary by the first statement. Consequently, $\mathfrak{p}_i = \mathfrak{p}_j$, a contradiction. So, $N = (0)$. □

To finish this chain of ideas, we need the "power lemma":

Lemma 3.98 *(Power lemma) Say A is a commutative ring with unity and M, F are A-module with $F \subseteq M$. Write $\mathfrak{A} = \sqrt{(M \longrightarrow F)}$ and assume $\mathfrak{A}$ is f.g. as ideal. Then, there is some $\rho >> 0$ so that $\mathfrak{A}^\rho M \subseteq F$.*

Proof. Let $\alpha_1, \ldots, \alpha_t$ be generators for $\mathfrak{A}$. For $l = 1, \ldots, t$, there is some $k_l > 0$ so that $\alpha_l^{k_l} M \subseteq F$. Let $\rho = k_1 + \cdots + k_t$. Every element of $\mathfrak{A}$ has the form $r_1\alpha_1 + \cdots + r_t\alpha_t$, where $r_i \in A$. Every element of $\mathfrak{A}^\rho$ is a sum of terms $s(a_1a_2 \cdots a_\rho)$; $s \in A$; $a_1, \ldots, a_\rho \in \mathfrak{A}$. Then, $a_1 \cdots a_\rho$ is a sum of monomials of the form $c\alpha_1^{i_1} \cdots \alpha_t^{i_t}$, where $c \in A$ and $i_1 + \cdots + i_t = \rho$. Now, at least one $i_l \geq k_l$ in the last sum, and then, $\alpha_1^{i_1} \cdots \alpha_t^{i_t} M \subseteq F$. Therefore, $\mathfrak{A}^\rho M \subseteq F$. □

Theorem 3.99 *If A is a noetherian ring and M is a f.g. A-module, then for all submodules, N, of M, all the prime ideals of $\mathrm{Ann}(N)$ are in $\mathrm{Ass}(M)$. A prime ideal, $\mathfrak{p}$, is in $\mathrm{Ass}(M)$ iff there is some $x \in M$ so that $\mathfrak{p} = \mathrm{Ann}(x)$ iff $A/\mathfrak{p}$ is isomorphic to a submodule of M.*

Proof. In M, we have $(0) = \bigcap_i Q_i$, a reduced primary decomposition, and we let $\mathfrak{p}_i$ correspond to Q_i. The first uniqueness theorem implies $\mathrm{Ass}(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$. Also,

$$\mathrm{Ann}(N) = (N \longrightarrow (0)) = \bigcap_i (N \longrightarrow Q_i).$$

But, we know that

$$(N \longrightarrow Q_i) = \begin{cases} A & \text{if } N \subseteq Q_i \\ \mathfrak{p}_i\text{-primary ideal} & \text{otherwise.} \end{cases}$$

We get a reduced primary decomposition of $\mathrm{Ann}(N)$:

$$\mathrm{Ann}(N) = \bigcap_{j | Q_j \not\supseteq N} (N \longrightarrow Q_j).$$

By the first uniqueness theorem, the primes of $\mathrm{Ann}(N)$ are the $\mathfrak{p}_j$'s for which $Q_j \not\supseteq N$, so, they are contained in $\mathrm{Ass}(M)$.

We have $\mathfrak{p} = \mathrm{Ann}(A/\mathfrak{p})$ and $A/\mathfrak{p} = A\xi$, for some ξ (where ξ is the image of 1 modulo $\mathfrak{p}$). Given x with $\mathrm{Ann}(x) = \mathfrak{p}$, the map $\xi \mapsto x$ gives $A/\mathfrak{p} \cong Ax \subseteq M$ and conversely. Say $\mathfrak{p}$ kills some x exactly, then, as $A/\mathfrak{p}$ is $\mathfrak{p}$-coprimary, $\mathrm{Ass}(Ax) = \{\mathfrak{p}\}$. Yet $Ax \subseteq M$, so, $\mathfrak{p} \in \mathrm{Ass}(M)$.

Conversely, say $\mathfrak{p} \in \mathrm{Ass}(M)$. We must find $x \in M$ with $\mathrm{Ann}(x) = \mathfrak{p}$.

By Proposition 3.97, if $\mathfrak{p} \in \mathrm{Ass}(M)$, then there is a submodule, P, so that P is $\mathfrak{p}$-coprimary. Thus, $\mathfrak{p} = \sqrt{\mathrm{Ann}(P)}$, i.e., $\mathfrak{p} = \sqrt{(P \longrightarrow (0))}$. In the power lemma, set $\mathfrak{p} = \mathfrak{A}$, $P = M$, $(0) = F$. As A is noetherian, $\mathfrak{p}$ is f.g. and by the power lemma, there is some $\rho >> 0$ with $\mathfrak{p}^\rho P = (0)$. If we choose ρ minimal with the above property, we have $\mathfrak{p}^\rho P = (0)$ and $\mathfrak{p}^{\rho-1} P \neq (0)$. Pick any $x \neq 0$ in $\mathfrak{p}^{\rho-1}P$. Then,

$$\mathfrak{p}x \subseteq \mathfrak{p}\mathfrak{p}^{\rho-1}P = \mathfrak{p}^\rho P = (0),$$

so, $\mathfrak{p} \subseteq \mathrm{Ann}(x)$. But $x \in P$ implies $Ax \subseteq P$ and P is $\mathfrak{p}$-coprimary; consequently, Ax is also $\mathfrak{p}$-coprimary. It follows that

$$\sqrt{\mathrm{Ann}(Ax)} = \sqrt{\mathrm{Ann}(x)} = \mathfrak{p}.$$

So, we get $\mathfrak{p} \subseteq \mathrm{Ann}(x) \subseteq \sqrt{\mathrm{Ann}(x)} = \mathfrak{p}$. □

In all of the following corollaries, A is a noetherian ring and M is a f.g. A-module. By taking $N = M$ in Theorem 3.99, we get:

Corollary 3.100 *The primes of* $\mathrm{Ann}(M)$ *are in* $\mathrm{Ass}(M)$.

Corollary 3.101 *Say* $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$ *is exact. Then,*

$$\mathrm{Ass}(M) \subseteq \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N).$$

Proof. Pick $\mathfrak{p} \in \mathrm{Ass}(M)$ and say $\mathfrak{p} \notin \mathrm{Ass}(N)$. By Theorem 3.99, there is some $x \in M$ so that $\mathfrak{p} = \mathrm{Ann}(x)$. Look at $(Ax) \cap N$. We claim that $(Ax) \cap N = (0)$. If not, $(Ax) \cap N \subseteq Ax$ and Ax is $\mathfrak{p}$-coprimary. Thus, $(Ax) \cap N$ is also $\mathfrak{p}$-coprimary and $\mathrm{Ass}((Ax) \cap N) = \{\mathfrak{p}\}$, But, $(Ax) \cap N \subseteq N$; so, $\mathrm{Ass}((Ax) \cap N) \subseteq \mathrm{Ass}(N)$. It follows that $\mathfrak{p} \in \mathrm{Ass}(N)$, a contradiction.

Therefore, $(Ax) \cap N = (0)$. Thus, we have

$$Ax \xrightarrow{\sim} Ax/((Ax) \cap N) \hookrightarrow M/N,$$

which means that Ax is a submodule of M/N. By Theorem 3.99, we have $\mathfrak{p} \in \mathrm{Ass}(M/N)$. □

Corollary 3.102 *We have* $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$.

Proof. If $\mathfrak{p} \in \mathrm{Ass}(M)$, then $\mathfrak{p} = \mathrm{Ass}(Ax)$, for some $x \in M$, i.e., we have the inclusion $A/\mathfrak{p} \longrightarrow M$. By localizing, we get $(A/\mathfrak{p})_{\mathfrak{p}} \subseteq M_{\mathfrak{p}}$, yet

$$(A/\mathfrak{p})_{\mathfrak{p}} = \mathrm{Frac}(A/\mathfrak{p}) \neq (0).$$

Thus, $M_{\mathfrak{p}} \neq (0)$, i.e., $\mathfrak{p} \in \mathrm{Supp}(M)$. □

Corollary 3.103 *Each of our* M*'s possesses a chain (of submodules)*

$$(0) = M_0 < M_1 < M_2 < \cdots < M_n = M \tag{$\dagger$}$$

for which $M_j/M_{j-1} \cong A/\mathfrak{p}_j$*, for some* $\mathfrak{p}_j \in \mathrm{Spec}\, A$*. Every* $\mathfrak{p} \in \mathrm{Ass}(M)$ *appears as at least one of these* $\mathfrak{p}_j$ *in each such chain.*

Proof. If $\mathfrak{p} \in \mathrm{Ass}(M)$, there is some $x \in M$ so that $A/\mathfrak{p} \cong Ax \subseteq M$. If we let $M_1 = Ax$, it follows that $M_1/M_0 \cong A/\mathfrak{p}$. Look at M/M_1. If $\widetilde{\mathfrak{p}} \in \mathrm{Ass}(M/M_1)$, repeat the argument to get $\overline{M_2} \subseteq M/M_1$ with $\overline{M_2} = A\overline{y}$, for some $\overline{y} \in M/M_1$, and $A/\widetilde{\mathfrak{p}} \cong A\overline{y}$. By the second homomorphism theorem, $\overline{M_2} = M_2/M_1$. Then, we have $(0) < M_1 < M_2$; $M_2/M_1 \cong A/\widetilde{\mathfrak{p}}$; $M_1/M_0 \cong A/\mathfrak{p}$. If we continue this process, we obtain an ascending chain of the desired type

$$(0) = M_0 < M_1 < M_2 < \cdots < M_n < \cdots .$$

As M is noetherian, this chain stops. This proves the first statement.

We prove the last statement by induction on the length of a given chain.

Hypothesis: If M has a chain, ($\dagger$), of length n, each $\mathfrak{p} \in \mathrm{Ass}(M)$ appears among the primes from ($\dagger$).

If $n = 1$, then $M \cong A/\widetilde{\mathfrak{p}}$. As $A/\widetilde{\mathfrak{p}}$ is $\widetilde{\mathfrak{p}}$-coprimary, we have $\mathrm{Ass}(M) = \{\widetilde{\mathfrak{p}}\}$; yet $\mathfrak{p} \in \mathrm{Ass}(M)$, so, $\mathfrak{p} = \widetilde{\mathfrak{p}}$.

Assume the induction hypothesis holds up to $n-1$. Given a chain, ($\dagger$), of length n and $\mathfrak{p} \in \mathrm{Ass}(M)$, we know there exists some $x \in M$ with $\mathfrak{p} = \mathrm{Ann}(x)$, i.e., we have an inclusion $A/\mathfrak{p} \hookrightarrow M$. There is some j such that $x \in M_j$ and $x \notin M_{j-1}$, where the M_j's are in ($\dagger$). If $j < n$, then apply the induction hypothesis to M_{n-1} to conclude that $\mathfrak{p}$ is among $\mathfrak{p}_1, \ldots, \mathfrak{p}_{n-1}$.

So, we may assume $x \in M_n$ and $x \notin M_{n-1}$. Look at $(Ax) \cap M_{n-1}$. There are two cases.

(a) $(Ax) \cap M_{n-1} \neq (0)$. Then, $(Ax) \cap M_{n-1} \subseteq Ax$, where the latter is $\mathfrak{p}$-coprimary; it follows that $(Ax) \cap M_{n-1}$ is $\mathfrak{p}$-coprimary and $\mathrm{Ass}((Ax) \cap M_{n-1}) = \{\mathfrak{p}\}$. Yet, $(Ax) \cap M_{n-1} \subseteq M_{n-1}$, so,

$$\mathrm{Ass}((Ax) \cap M_{n-1}) \subseteq \mathrm{Ass}(M_{n-1}).$$

Therefore, $\mathfrak{p}$ is among $\mathfrak{p}_1, \ldots, \mathfrak{p}_{n-1}$, by the induction hypothesis.

(b) $(Ax) \cap M_{n-1} = (0)$. In this case, $Ax \cong Ax/((Ax) \cap M_{n-1}) \hookrightarrow M/M_{n-1} \cong A/\mathfrak{p}_n$, so, $\mathrm{Ass}(Ax) = \{\mathfrak{p}\} \subseteq \mathrm{Ass}(A/\mathfrak{p}_n) = \{\mathfrak{p}_n\}$. Therefore, $\mathfrak{p} = \mathfrak{p}_n$. □

The chain, (†), shows that M is a multiple extension of the "easy" modules $A/\mathfrak{a}_j$. That is, we have exact sequences

$$\begin{aligned}
&0 \longrightarrow M_1 = A/\mathfrak{p}_1 \longrightarrow M_2 \longrightarrow M_2/M_1 = A/\mathfrak{p}_2 \longrightarrow 0\\
&0 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow A/\mathfrak{p}_3 \longrightarrow 0\\
&\qquad\qquad\qquad\vdots\\
&0 \longrightarrow M_{n-1} \longrightarrow M \longrightarrow A/\mathfrak{p}_n \longrightarrow 0
\end{aligned}$$

We define $\mathrm{Ext}(M/N, N)$ as the set

$$\{M \mid 0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0\}/\sim,$$

where the equivalence relation $\sim$ is defined as in the case of group extensions. It turns out that not only is $\mathrm{Ext}(M/N, N)$ an abelian group, it is an A-module. If the A-modules $\mathrm{Ext}(A/\mathfrak{p}_j, M_{j-1})$ can be successively computed, we can classify all f.g. A-modules, M.

To attempt such a task, one should note the following:

Remarks:

(1) Say $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$ is exact, then

$$\mathrm{Supp}(M) = \mathrm{Supp}(N) \cup \mathrm{Supp}(M/N).$$

Proof. Localize at any prime $\mathfrak{p}$. We get

$$0 \longrightarrow N_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \longrightarrow (M/N)_{\mathfrak{p}} \longrightarrow 0 \quad \text{is exact.}$$

From this, (1) is clear. □

(2) If M and N are two f.g. modules, then

$$\mathrm{Supp}(M \otimes_A N) = \mathrm{Supp}(M) \cap \mathrm{Supp}(N).$$

Proof. We always have

$$(M \otimes_A N)_{\mathfrak{p}} \cong M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}}.$$

So, if $\mathfrak{p} \in \mathrm{Supp}(M \otimes_A N)$, the left hand side is nonzero which implies that $M_{\mathfrak{p}} \neq (0)$ and $N_{\mathfrak{p}} \neq (0)$. Consequently,

$$\mathrm{Supp}(M \otimes_A N) \subseteq \mathrm{Supp}(M) \cap \mathrm{Supp}(N).$$

Now, assume $\mathfrak{p} \in \mathrm{Supp}(M) \cap \mathrm{Supp}(N)$, then $M_{\mathfrak{p}} \neq (0)$ and $N_{\mathfrak{p}} \neq (0)$. As $M_{\mathfrak{p}}$ and $N_{\mathfrak{p}}$ are f.g. $A_{\mathfrak{p}}$-modules (since M and N are f.g. A-modules), Nakayama's lemma implies

$$M_{\mathfrak{p}}/\mathfrak{m}M_{\mathfrak{p}} \neq (0) \quad \text{and} \quad N_{\mathfrak{p}}/\mathfrak{m}N_{\mathfrak{p}} \neq (0).$$

As these are vector spaces over $\kappa(A_{\mathfrak{p}})$, we deduce that

$$M_{\mathfrak{p}}/\mathfrak{m}M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}}/\mathfrak{m}N_{\mathfrak{p}} \neq (0).$$

But, this is just $(M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}})/\mathfrak{m}(M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}})$; so, $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} \neq (0)$. □

(3) If M is a f.g. A-module, then $\mathfrak{p} \in \mathrm{Supp}(M)$ iff there exists a chain

$$(0) = M_0 < M_1 < M_2 \cdots < M_n = M \qquad (\dagger)$$

with $M_j/M_{j-1} \cong A/\mathfrak{p}_j$ and $\mathfrak{p}$ is one of these $\mathfrak{p}_j$.

Proof. If we have a chain (†) and $\mathfrak{p} = \mathfrak{p}_j$ for some j, then $A/\mathfrak{p}_j = A/\mathfrak{p}$ and $(A/\mathfrak{p})_{\mathfrak{p}} = \mathrm{Frac}(A/\mathfrak{p})$. Therefore, $(M_j/M_{j-1})_{\mathfrak{p}} \neq (0)$. By exactness, $(M_j)_{\mathfrak{p}} \neq (0)$. As $M_j \hookrightarrow M$ and localization is exact, $M_{\mathfrak{p}} \neq (0)$ and $\mathfrak{p} \in \mathrm{Supp}(M)$.

Conversely, if $\mathfrak{p} \in \mathrm{Supp}(M)$, then there is some $\mathfrak{q} \in \mathrm{Ass}(M)$ and $\mathfrak{p} \supseteq \mathfrak{q}$. So, $A/\mathfrak{q}$ is in a chain and $A/\mathfrak{p} = (A/\mathfrak{q})/(\mathfrak{p}/\mathfrak{q})$ implies (DX) $\mathfrak{p}$ is in a chain. □

Corollary 3.104 *The following are equivalent conditions:*

(1) $\mathfrak{p} \in \mathrm{Ass}(M/N)$*, for some submodule,* N*, of* M*.*

(2) $\mathfrak{p} \in \mathrm{Supp}(M)$*.*

(3) $\mathfrak{p} \supseteq \mathrm{Ann}(M)$ *(*$\mathfrak{p} \in V(\mathrm{Ann}(M))$*).*

(4) $\mathfrak{p}$ *contains some associated prime of* M*.*

Proof. (1) ⇒ (2). We have $\mathfrak{p} \in \mathrm{Ass}(M/N) \subseteq \mathrm{Supp}(M/N)$ and remark (1) shows that $\mathfrak{p} \in \mathrm{Supp}(M)$.

(2) ⇒ (3). This has already been proved in Section 3.3, Proposition 3.21.

(3) ⇒ (4). If $\mathfrak{p} \supseteq \mathrm{Ann}(M)$, then $\mathfrak{p} \supseteq \sqrt{\mathrm{Ann}(M)}$. However, $\sqrt{\mathrm{Ann}(M)} = \bigcap_{j=1}^{t} \mathfrak{p}_j$, where the $\mathfrak{p}_j$'s are the primes associated with $\mathrm{Ann}(M)$. So,

$$\mathfrak{p} \supseteq \bigcap_{j=1}^{t} \mathfrak{p}_j \supseteq \prod_{j=1}^{t} \mathfrak{p}_j,$$

and it follows that $\mathfrak{p} \supseteq \mathfrak{p}_j$, for some j. By Corollary 3.100, we have $\mathfrak{p}_j \in \mathrm{Ass}(M)$ and $\mathfrak{p} \supseteq \mathfrak{p}_j$, proving (4).

(4) ⇒ (1). Say $\mathfrak{p} \supseteq \mathfrak{q}$ and $\mathfrak{q} \in \mathrm{Ass}(M)$. By our theorem, we know that there is some $x \in M$ so that $\mathfrak{q} = \mathrm{Ann}(x)$, i.e., $A/\mathfrak{q} \hookrightarrow M$. But, $\mathfrak{p}/\mathfrak{q} \hookrightarrow A/\mathfrak{q} \hookrightarrow M$. Let $N = \mathfrak{p}/\mathfrak{q}$, then,

$$A/\mathfrak{p} \cong (A/\mathfrak{q})/(\mathfrak{p}/\mathfrak{q}) \hookrightarrow M/N,$$

so $\{\mathfrak{p}\} = \mathrm{Ass}(A/\mathfrak{p}) \subseteq \mathrm{Ass}(M/N)$. □

Corollary 3.105 *The minimal elements of* $\mathrm{Supp}(M)$ *and the minimal elements of* $\mathrm{Ass}(M)$ *are the same set.*

Proof. Let $\mathfrak{p} \in \mathrm{Supp}(M)$ be minimal. By Corollary 3.104 (4), we have $\mathfrak{p} \supseteq \mathfrak{q}$, for some $\mathfrak{q} \in \mathrm{Ass}(M)$. But $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$, so, $\mathfrak{q} \in \mathrm{Supp}(M)$. Since $\mathfrak{p}$ is minimal, we get $\mathfrak{p} = \mathfrak{q} \in \mathrm{Ass}(M)$. Now, $\mathfrak{p}$ is minimal in $\mathrm{Supp}(M)$, so it is also minimal in $\mathrm{Ass}(M)$.

Now, let $\mathfrak{p} \in \mathrm{Ass}(M)$ be minimal. As $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$, we have $\mathfrak{p} \in \mathrm{Supp}(M)$. If $\mathfrak{p} \supseteq \mathfrak{q}$ for some $\mathfrak{q} \in \mathrm{Supp}(M)$, then, by Corollary 3.104 (4), we have $\mathfrak{q} \supseteq \widetilde{\mathfrak{q}}$, for some $\widetilde{\mathfrak{q}} \in \mathrm{Ass}(M)$. So, $\mathfrak{p} \supseteq \widetilde{\mathfrak{q}}$; since $\mathfrak{p}$ is minimal, we get $\mathfrak{p} = \widetilde{\mathfrak{q}}$. □

Remark: We saw in Section 3.3 that $\mathrm{Supp}(M)$ is closed in $\mathrm{Spec}\, A$. In fact, $\mathrm{Supp}(M)$ is a finite (irredundant) union of irreducible subsets (recall, a set is irreducible iff it is not the union of two proper closed subsets). In this decomposition, the irreducible components are $V(\mathfrak{p})$, for $\mathfrak{p}$ an isolated prime in $\mathrm{Ass}(M)$ (= a minimal element of $\mathrm{Supp}(M)$). Thus, the minimal elements of $\mathrm{Ass}(M)$ are exactly the generic points of $\mathrm{Supp}(M)$.

Corollary 3.106 *If A is a noetherian ring, then*

$$\{x \in A \mid x \text{ is a zero divisor in } A\} = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(A)} \mathfrak{p}.$$

Proof. Say $\xi \in \bigcup_{\mathfrak{p}\in \mathrm{Ass}(A)} \mathfrak{p}$, so $\xi \in \mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{Ass}(A)$. By Theorem 3.99, we have $\mathfrak{p} = \mathrm{Ann}(y)$, for some $y \in A$. Clearly $y \neq 0$ and $y\xi \in y\mathfrak{p} = (0)$, so ξ is a zero divisor.

Conversely, pick $x \notin \bigcup_{\mathfrak{p}\in \mathrm{Ass}(A)} \mathfrak{p}$ and let $S = A - \bigcup_{\mathfrak{p}\in \mathrm{Ass}(A)} \mathfrak{p}$. We know from previous work that S is a multiplicative set. Now, we have a primary decomposition $(0) = \bigcap \mathfrak{q}$, where $\sqrt{\mathfrak{q}} = \mathfrak{p} \in \mathrm{Ass}(A)$. We get $S((0)) = \bigcap_{\mathfrak{q}} S(\mathfrak{q})$ and we know that $S(\mathfrak{q}) = \mathfrak{q}$ iff $S \cap \mathfrak{p} = \emptyset$. By definition of S, we conclude that $S((0)) = (0)$. If $xy = 0$, as $x \in S$, we get $y \in S((0)) = (0)$. Therefore, $y = 0$ and x is not a zero divisor. □

Corollary 3.107 *Say $M = \bigcup_\alpha M_\alpha$, for some submodules, M_α, of M. Then,*

$$\mathrm{Ass}(M) = \bigcup_\alpha \mathrm{Ass}(M_\alpha).$$

Proof. Since $M_\alpha \subseteq M$, we get $\mathrm{Ass}(M_\alpha) \subseteq \mathrm{Ass}(M)$, so, $\bigcup_\alpha \mathrm{Ass}(M_\alpha) \subseteq \mathrm{Ass}(M)$. If $\mathfrak{p} \in \mathrm{Ass}(M)$, then there is some $m \in M$ so that $\mathfrak{p} = \mathrm{Ann}(m)$. But, $m \in M_\alpha$ for some α; Theorem 3.99 implies that $\mathfrak{p} \in \mathrm{Ass}(M_\alpha)$. □

Corollary 3.108 *Given an A-module, M, and any nonempty subset, $\Phi \subseteq \mathrm{Ass}(M)$, then there is some submodule, N, of M so that $\mathrm{Ass}(N) = \Phi$.*

Proof. Let $\Phi = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$. By proposition 3.97, there are some submodules, P_j, of M so that $\mathrm{Ass}(P_j) = \{\mathfrak{p}_j\}$. I claim, the map $\coprod_{j=1}^t P_j \longrightarrow M$ is injective and $\mathrm{Ass}(\coprod_{j=1}^t P_j) = \Phi$. First, consider the case $t = 2$. Look at the map $P_1 \coprod P_2 \longrightarrow P_1 + P_2 \subseteq M$. This is an isomorphism iff $P_1 \cap P_2 = (0)$. But, $P_1 \cap P_2 \subseteq P_j$ for $j = 1, 2$, so, $\mathrm{Ass}(P_1 \cap P_2) \subseteq \{\mathfrak{p}_1\}$ and $\mathrm{Ass}(P_1 \cap P_2) \subseteq \{\mathfrak{p}_2\}$; as $\mathfrak{p}_1 \neq \mathfrak{p}_2$, we conclude that $P_1 \cap P_2 = (0)$. Then, the sequence

$$0 \longrightarrow P_1 \longrightarrow P_1 \coprod P_2 \longrightarrow P_2 \longrightarrow 0$$

is exact and split. Consequently, $\mathrm{Ass}(P_1 \coprod P_2) = \{\mathfrak{p}_1, \mathfrak{p}_2\}$. For $t > 2$, we proceed by induction (DX). □

Proposition 3.109 *If $N \subseteq M$ and N possesses a primary decomposition in M, then*

$$\mathrm{Rad}_M(N) = \bigcap_{\substack{\mathfrak{p}\in \mathrm{Ess}_N(M) \\ \mathfrak{p} \text{ isolated}}} \mathfrak{p}.$$

In fact, the isolated primes of $\mathrm{Rad}_M(N)$ are just the isolated essential primes of N in M (The hypothesis holds if A is noetherian and M is f.g.).

Proof. As $\mathrm{Rad}_M(N) = \mathrm{Rad}_{M/N}((0)) = \sqrt{\mathrm{Ann}(M/N)}$ and $\mathrm{Ess}_M(N) = \mathrm{Ass}(M/N)$, we may assume that $N = (0)$. We must show that

$$\sqrt{\mathrm{Ann}(M)} = \bigcap_{\substack{\mathfrak{p}\in \mathrm{Ass}(M) \\ \mathfrak{p} \text{ isolated}}} \mathfrak{p}.$$

Now, we have a reduced primary decomposition $(0) = \bigcap_{j=1}^t Q_j$, so

$$\mathrm{Ann}(M) = (M \longrightarrow (0) = \bigcap_{j=1}^t (M \longrightarrow Q_j).$$

But, $(M \longrightarrow Q_j)$ is $\mathfrak{p}_j$-primary, by previous work, so,

$$\sqrt{\mathrm{Ann}(M)} = \sqrt{(M \longrightarrow (0)} = \bigcap_{j=1}^t \sqrt{(M \longrightarrow Q_j)} = \bigcap_{\mathfrak{p}\in \mathrm{Ass}(M)} \mathfrak{p} = \bigcap_{\substack{\mathfrak{p}\in \mathrm{Ass}(M) \\ \mathfrak{p} \text{ isolated}}} \mathfrak{p}.$$

The rest should be clear. □

3.7 Theorems of Krull and Artin–Rees

We begin with a generalization of the power lemma.

Lemma 3.110 *(Herstein's Lemma) If A is a noetherian ring, $\mathfrak{A}$ is some ideal, M is a f.g. A-module and N is a submodule of M, then there is some $n >> 0$ (depending on A, $\mathfrak{A}$, M, N) so that*

$$\mathfrak{A}^n M \cap N \subseteq \mathfrak{A}N.$$

Proof. By reducing modulo $\mathfrak{A}N$, we may assume $\mathfrak{A}N = (0)$ and we must prove $\mathfrak{A}^n M \cap N = (0)$. Let $\mathcal{S} = \{F \subseteq M \mid F \cap N = (0)\}$. Clearly, $\mathcal{S}$ is nonempty and since M is f.g. and A is noetherian, $\mathcal{S}$ has a maximal element, call it F, again. Let $m_1, \ldots, m_t$ be generators of M and pick $a \in \mathfrak{A}$. Given m_j, for any $n \geq 0$, consider

$$F_n^{(j)}(a) = (a^n m_j \longrightarrow F) = \{x \in A \mid xa^n m_j \in F\}.$$

The $F_n^{(j)}(a)$'s are ideals of A and we have

$$F_1^{(j)}(a) \subseteq F_2^{(j)}(a) \subseteq F_3^{(j)}(a) \subseteq \cdots.$$

By the ACC in A, there is some $N_j(a)$ so that

$$F_{N_j(a)}^{(j)}(a) = F_{N_j(a)+1}^{(j)}(a), \quad \text{for } j = 1, \ldots, t.$$

Let $N(a) = \max_{1 \leq j \leq t}\{N_j(a)\}$. I claim that $a^{N(a)} M \subseteq F$.

Of course, if we show that $a^{N(a)} m_j \in F$ for $j = 1, \ldots, t$, we will have proved the claim.

If the claim is false, there is some j so that $a^{N(a)} m_j \notin F$. Then, $F + Aa^{N(a)} m_j > F$, and by maximality of F, we must have $(F + Aa^{N(a)} m_j) \cap N \neq (0)$. So, there is some $f \in F$ and some $\alpha \in A$ so that

$$0 \neq f + \alpha a^{N(a)} m_j \in N. \tag{$\dagger$}$$

If we multiply ($\dagger$) by a, we get

$$af + \alpha a^{N(a)+1} m_j \in aN = (0),$$

since $\mathfrak{A}N = (0)$ and $a \in \mathfrak{A}$. Thus, $\alpha a^{N(a)+1} m_j = -af \in F$, and so,

$$\alpha \in (a^{N(a)+1} m_j \longrightarrow F) = F_{N(a)+1}^{(j)}(a) = F_{N(a)}^{(j)}(a).$$

It follows that $\alpha a^{N(a)} m_j \in F$; so, $f + \alpha a^{N(a)} m_j \in F$, which means that $F \cap N \neq (0)$, a contradiction. Therefore, $a \in \sqrt{(M \longrightarrow F)}$; as $\mathfrak{A}$ is f.g., by the power lemma, we get $\mathfrak{A}^\rho M \subseteq F$. Thus, finally, $\mathfrak{A}^\rho M \cap N \subseteq F \cap N = (0)$. $\square$

Theorem 3.111 *(Krull Intersection Theorem) Say A is a noetherian ring, M is a f.g. A-module and $\mathfrak{A}$ is an ideal of A. Write $S = 1 - \mathfrak{A}$ $(= \{1 - \alpha \mid \alpha \in \mathfrak{A}\})$. Then,*

$$\bigcap_{n \geq 0} \mathfrak{A}^n M = S(0) = \operatorname{Ker}(M \longrightarrow S^{-1}M).$$

Proof. Write $N = \bigcap \mathfrak{A}^n M$. By Herstein's lemma there exists $\rho > 0$ so that $\mathfrak{A}^\rho M \cap N \subseteq \mathfrak{A}N$. But, $N \subseteq \mathfrak{A}^\rho M$, so $\mathfrak{A}^\rho M \cap N = N$ and it follows that $N \subseteq \mathfrak{A}N$. Of course, we get $\mathfrak{A}N = N$. Now, N is f.g., say $n_1, \ldots, n_t$ are some generators. As $\mathfrak{A}N = N$, there exist some $\alpha_{ij} \in A$ so that

$$n_j = \sum_{i=1}^{t} \alpha_{ij} n_i, \quad \text{for } j = 1, \ldots, t.$$

Therefore, $0 = \sum_{i=1}^{t}(\alpha_{ij} - \delta_{ij})n_i$, for $j = 1, \ldots, t$; so, the matrix $(\delta_{ij} - \alpha_{ij})$ kills the vector $(n_1, \ldots, n_t)$. By linear algebra, if $\Delta = \det(\delta_{ij} - \alpha_{ij}) \in A$, then

$$\Delta n_j = 0, \quad \text{for } j = 1, \ldots, t.$$

(This can be seen as follows: If T is the linear map given by the matrix $(\delta_{ij} - \alpha_{ij})$, then by the Cayley–Hamilton theorem, $\chi(T) = T^t + \beta_1 T^{t-1} + \cdots + \beta_{t-1}T + \beta_t I = 0$. But, $\beta_t = \pm\Delta$ and if we apply $\chi(T)$ to $(n_1, \ldots, n_t)$, then $\chi(T)$ and all the nonnegative powers of T kill it. Consequently, $\beta_t I(n_1, \ldots, n_t) = 0$.) Now, $\Delta = 1 - d$, for some $d \in \mathfrak{A}$. Thus, $\Delta \in S$. For all j, we have $n_j \in S(0)$, so $N \subseteq S(0)$. On the other hand, if $\xi \in S(0)$, then there is some $s \in S$ with $s\xi = 0$. Yet, $s = 1 - \alpha$, for some $\alpha \in \mathfrak{A}$. Thus, $(1 - \alpha)\xi = 0$, i.e., $\xi = \alpha\xi$. An immediate induction yields $\xi = \alpha^n\xi$, for all $n \geq 0$. However, $\alpha^n\xi \in \mathfrak{A}^n M$, for every $n \geq 0$, so $\xi \in \bigcap \mathfrak{A}^n M$; this proves that $S(0) \subseteq N$. □

Corollary 3.112 *Under the hypotheses of Theorem 3.111, if $\mathfrak{A} \subseteq \mathcal{J}(A)$, then $\bigcap \mathfrak{A}^n M = (0)$.*

Proof. Since $S = 1 - \mathfrak{A} \subseteq 1 - \mathcal{J}(A) \subseteq$ units of A, we get $S(0) = (0)$. □

Corollary 3.113 *(Original Krull theorem) If A is local noetherian and $\mathfrak{m}$ is its maximal ideal, then $\bigcap \mathfrak{m}^n = (0)$.*

Proof. As A is local, $\mathfrak{m} = \mathcal{J}(A)$; the result follows from Corollary 3.112 applied to $M = A$. □

Corollary 3.114 *Say X is a real or complex manifold and $x \in X$. Write $\mathcal{O}_{X,x}$ for the local ring of germs of C^∞-functions at x. Then, $\mathcal{O}_{X,x}$ is never noetherian.*

Proof. As the question is local on X, we may assume X is an open ball in $\mathbb{R}^n$ and $x = 0$ in this ball (with n even in case of a complex manifold). Let

$$f(x) = \begin{cases} e^{-1/(x,x)} & \text{for } x \in \mathbb{R}^n,\ x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

(Here, (x, y) is the usual euclidean inner product on $\mathbb{R}^n$.) We have $f(x) \in C^\infty(\text{ball})$. Moreover $f^{(n)}(0) = 0$, for all $n \geq 0$. But, in $\mathcal{O}_{X,x}$, observe that $\mathfrak{m}^n$ consists of the classes of functions defined near zero so that the n-th derivative and all previous derivatives are 0 at the origin. So, $\text{germ}(f) \in \bigcap \mathfrak{m}^n$; by the Krull intersection theorem, our ring $\mathcal{O}_{X,x}$ is *not* noetherian. □

$\mathfrak{A}$-adic Topologies.

Let A be a ring, $\mathfrak{A}$ be an ideal in A and M be an A-module. At the origin in M, take as basis of opens (= fundamental system of neighborhoods at 0) the subsets $\mathfrak{A}^n M$, for $n = 0, 1, 2, \ldots$. Topologise M by translating these so that $\{m + \mathfrak{A}^n M\}_{n \geq 0}$ is a neighborhood basis around m. When $M = A$, the ring A receives a topology and A is a topological ring in this topology which is called the $\mathfrak{A}$-*adic topology*. Similarly, the module M is a topological module in this topology also called the $\mathfrak{A}$-*adic topology*. The $\mathfrak{A}$-adic topology is *pseudo-metric*, i.e., set

$$\text{ord}_{\mathfrak{A}}(m) = \begin{cases} n & \text{if } m \in \mathfrak{A}^n M, \text{ yet } m \notin \mathfrak{A}^{n+1} M \\ \infty & \text{if } m \in \bigcap_{n \geq 0} \mathfrak{A}^n M, \end{cases}$$

and define

$$d(m_1, m_2) = e^{-\text{ord}_{\mathfrak{A}}(m_1 - m_2)}.$$

Then, we have

(1) $d(m_1, m_2) \geq 0$.

(2) $d(m_1, m_2) = d(m_2, m_1)$.

(3) $d(m_1, m_3) \leq \max(d(m_1, m_2), d(m_2, m_3))$ (ultrametric property).

Yet, it can happen that $d(m_1, m_2) = 0$ and $m_1 \neq m_2$. The $\mathfrak{A}$-adic topology is Hausdorff iff d *is* a metric (i.e., $d(m_1, m_2) = 0$ iff $m_1 = m_2$)) iff $\bigcap_{n \geq 0} \mathfrak{A}^n M = (0)$.

If the $\mathfrak{A}$-adic topology is Hausdorff, then we have Cauchy sequences, completeness and completions. The reader should check: The completion of M in the $\mathfrak{A}$-adic topology (Hausdorff case) is equal to $\varprojlim_n M/\mathfrak{A}^n M \stackrel{\text{def}}{=} \widehat{M}$. The first person to make use of these ideas was Kurt Hensel (1898) in the case $A = \mathbb{Z}$, $M = \mathbb{Q}$, $\mathfrak{p} = (p)$, where p is a prime. But here, Hensel used $\text{ord}_p(\frac{r}{s}) = \text{ord}_p(r) - \text{ord}_p(s)$.

Corollary 3.115 *The $\mathfrak{A}$-adic topology on a f.g. module M over a noetherian ring is Hausdorff if $\mathfrak{A} \subseteq \mathcal{J}(A)$. In particular, this holds if A is local and $\mathfrak{A} = \mathfrak{m}_A$.*

Corollary 3.116 *Say A is a noetherian domain and $\mathfrak{A}$ is any proper ideal (i.e., $\mathfrak{A} \neq A$). Then, the $\mathfrak{A}$-adic topology on A is Hausdorff.*

Proof. We have $S = 1 - \mathfrak{A} \subseteq$ nonzero elements of A. Thus, S consists of nonzero divisors. If $\xi \in S(0)$, then $s\xi = 0$, for some $s \in S$, so, $\xi = 0$. Therefore, $S(0) = (0)$ and the topology is Hausdorff. □

Theorem 3.117 *(Artin–Rees) Let A be a noetherian ring, $\mathfrak{A}$ be some ideal, M be a f.g. A-module and N a submodule of M. Then, there is some k (depending on A, $\mathfrak{A}$, M and N) so that for all $n \geq k$,*

$$\mathfrak{A}^n M \cap N = \mathfrak{A}^{n-k}(\mathfrak{A}^k M \cap N).$$

Proof. Define the graded ring $\text{Pow}_{\mathfrak{A}}(A) \subseteq A[X]$, where X is an indeterminate by

$$\begin{aligned} \text{Pow}_{\mathfrak{A}}(A) &= \coprod_{n \geq 0} \mathfrak{A}^n X^n \\ &= \{z_0 + z_1 X + \cdots + z_r X^r \mid r \geq 0,\ z_j \in \mathfrak{A}^j\}. \end{aligned}$$

Now, M gives rise to a graded module, M', over $\text{Pow}_{\mathfrak{A}}(A)$, namely

$$\begin{aligned} M' &= \coprod_{n \geq 0} \mathfrak{A}^n M X^n \\ &= \{z_0 + z_1 X + \cdots + z_r X^r \mid r \geq 0,\ z_j \in \mathfrak{A}^j M\}. \end{aligned}$$

Observe that $\text{Pow}_{\mathfrak{A}}(A)$ is a noetherian ring. For, if $\alpha_1, \ldots, \alpha_q$ generate $\mathfrak{A}$ in A, then the elements of $\mathfrak{A}^n$ are sums of degree n monomials in the α_j's, i.e., if $Y_1, \ldots, Y_q$ are independent indeterminates the map

$$A[Y_1, \ldots, Y_q] \longrightarrow \text{Pow}_{\mathfrak{A}}(A)$$

via $Y_j \mapsto \alpha_j X$ is surjective, and as $A[Y_1, \ldots, Y_q]$ is noetherian, so is $\text{Pow}_{\mathfrak{A}}(A)$.

Let $m_1, \ldots, m_t$ generate M over A. Then, $m_1, \ldots, m_t$ generate M' over $\text{Pow}_{\mathfrak{A}}(A)$. Therefore, M' is a noetherian module. Set

$$N' = \coprod_{n \geq 0} (\mathfrak{A}^n M \cap N) X^n \subseteq M',$$

a submodule of M'. Moreover, N' is a homogeneous submodule of M and it is f.g. as M' is noetherian. Consequently, N' possesses a finite number of homogeneous generators: $u_1 X^{n_1}, \ldots, u_s X^{n_s}$, where $u_j \in \mathfrak{A}^{n_j} M \cap N$. Let $k = \max\{n_1, \ldots, n_s\}$. Given any $n \geq k$ and any $z \in \mathfrak{A}^n M \cap N$, look at $zX^n \in N'_n$. We have

$$zX^n = \sum_{l=1}^{s} a_l X^{n - n_l} u_l X^{n_l},$$

where $a_l X^{n-n_l} \in \big(\mathrm{Pow}_{\mathfrak{A}}(A)\big)_{n-n_l}$. Thus,

$$a_l \in \mathfrak{A}^{n-n_l} = \mathfrak{A}^{n-k}\mathfrak{A}^{k-n_l}$$

and

$$a_l u_l \in \mathfrak{A}^{n-k}(\mathfrak{A}^{k-n_l}u_l) \subseteq \mathfrak{A}^{n-k}(\mathfrak{A}^{k-n_l}(\mathfrak{A}^{n_l}M \cap N)) \subseteq \mathfrak{A}^{n-k}(\mathfrak{A}^k M \cap N).$$

It follows that $z = \sum_{l=1}^{s} a_l u_l \in \mathfrak{A}^{n-k}(\mathfrak{A}^k M \cap N)$, so

$$\mathfrak{A}^n M \cap N \subseteq \mathfrak{A}^{n-k}(\mathfrak{A}^k M \cap N).$$

Now, it is clear that the righthand side is contained in $\mathfrak{A}^n M \cap N$, as $\mathfrak{A}^{n-k}N \subseteq N$. □

Remark: If we choose $n = k+1$ in the Artin–Rees theorem, we get $\mathfrak{A}^n M \cap N = \mathfrak{A}(\mathfrak{A}^k M \cap N) \subseteq \mathfrak{A}N$, hence a new proof of Herstein's lemma.

Corollary 3.118 *If A is a noetherian ring, $\mathfrak{A}$ is an ideal, M is a f.g. module and N is a submodule, then the topology on N induced by the $\mathfrak{A}$-adic topology on M is just the $\mathfrak{A}$-adic topology on N.*

Proof. The induced topology has as neighborhood basis at 0 the sets $\mathfrak{A}^n M \cap N$. By the Artin–Rees theorem,

$$\mathfrak{A}^n M \cap N = \mathfrak{A}^{n-k}(\mathfrak{A}^k M \cap N) \subseteq \mathfrak{A}^{n-k}N,$$

for all $n \geq k$, for some fixed k. It follows that the induced topology is finer. But, $\mathfrak{A}^\rho N \subseteq \mathfrak{A}^\rho M \cap N$, for all ρ; so, the $\mathfrak{A}$-adic topology on N is in its turn finer than the induced topology. □

We turn now to two very famous theorems of Wolfgang Krull. Recall that a power of a prime ideal need not be primary. In the proof of the first of the Krull theorems, the principal ideal theorem, we need to remedy this situation. We are led to the notion of the *symbolic powers*, $\mathfrak{p}^{(n)}$, of a prime ideal, $\mathfrak{p}$.

Let A be a ring and let $\mathfrak{p} \in \operatorname{Spec} A$. Look at $A_{\mathfrak{p}} = S^{-1}A$, where $S = A - \mathfrak{p}$. Take the powers of $\mathfrak{p}$, extend and contract them to and from $A_{\mathfrak{p}}$, to get

$$\mathfrak{p}^{(n)} \stackrel{\text{def}}{=} (\mathfrak{p}^n)^{ec} = S(\mathfrak{p}^n).$$

Lemma 3.119 *The ideal $\mathfrak{p}^{(n)}$ is always a $\mathfrak{p}$-primary ideal.*

Proof. The ideal $\mathfrak{p}^e$ is maximal in $A_{\mathfrak{p}}$. Hence, $(\mathfrak{p}^e)^n$ is $\mathfrak{p}^e$-primary, by previous work. But, $(\mathfrak{p}^e)^n = (\mathfrak{p}^n)^e$. Therefore, $(\mathfrak{p}^n)^e$ is $\mathfrak{p}^e$-primary. Now, $S \cap \mathfrak{p} = \emptyset$, so $(\mathfrak{p}^n)^{ec}$ is $\mathfrak{p}$-primary. □

Further, we have the descending chain

$$\mathfrak{p} \supseteq \mathfrak{p}^{(2)} \supseteq \mathfrak{p}^{(3)} \supseteq \cdots.$$

Theorem 3.120 *(Krull Principal Ideal Theorem (1928)) If A is a noetherian domain and $\mathfrak{p} \in \operatorname{Spec} A$, then* $\operatorname{ht}(\mathfrak{p}) \leq 1$ *iff $\mathfrak{p}$ is an isolated prime of a principal ideal.*

Proof. ($\Rightarrow$) (easy part). By hypothesis, $\operatorname{ht}(\mathfrak{p}) \leq 1$ and $\mathfrak{p} \supseteq (0)$; hence, if $\operatorname{ht}(\mathfrak{p}) = 0$, then $\mathfrak{p} = (0)$, an isolated prime of (0). If $\operatorname{ht}(\mathfrak{p}) = 1$, pick $a \neq 0$ in $\mathfrak{p}$. As $\mathfrak{p} \supseteq (a)$, the ideal $\mathfrak{p}$ must contain one of the isolated primes of (a), say $\mathfrak{P}$. So, $\mathfrak{p} \supseteq \mathfrak{P} > (0)$, and as $\operatorname{ht}(\mathfrak{p}) = 1$, we must have $\mathfrak{p} = \mathfrak{P}$.

($\Leftarrow$) (hard part). Here, we may assume $\mathfrak{p}$ is an isolated prime of (a), where $a \neq 0$ (else, if $a = 0$, then $\mathfrak{p} = (0)$ and $\operatorname{ht}(\mathfrak{p}) = 0$). We must show $\operatorname{ht}(\mathfrak{p}) = 1$. Hence, we must prove that

$$\text{if } \mathfrak{P} \in \operatorname{Spec} A \text{ and } \mathfrak{p} > \mathfrak{P}, \text{ then } \mathfrak{P} = (0). \qquad (\dagger)$$

Step 1. If we localize at $\mathfrak{p}$, there is a one-to-one correspondence between primes contained in $\mathfrak{p}$ and all primes in $A_{\mathfrak{p}}$. Therefore, we may assume $A = A_{\mathfrak{p}}$, i.e., A is local, $\mathfrak{p}$ is maximal and $\mathfrak{p}$ is an isolated prime of (a), with $a \neq 0$. We must prove (†). Now, given $\mathfrak{P} \in \operatorname{Spec} A$ with $\mathfrak{p} > \mathfrak{P}$, could $a \in \mathfrak{P}$? If so, we would have $\mathfrak{p} > \mathfrak{P} \supseteq (a)$. As $\mathfrak{p}$ is isolated, $\mathfrak{p} = \mathfrak{P}$, a contradiction; so, $a \notin \mathfrak{P}$. It follows that the ring $A/(a)$ has precisely *one* prime ideal and it is maximal. Since A is noetherian, by Akizuki's theorem, $A/(a)$ is artinian (i.e., it has the DCC).

Step 2. Pick $\mathfrak{P} \in \operatorname{Spec} A$ with $\mathfrak{P} < \mathfrak{p}$. Of course, $a \notin \mathfrak{P}$. Examine the symbolic powers $\mathfrak{P}^{(n)}$. We have

$$\mathfrak{P} \supseteq \mathfrak{P}^{(2)} \supseteq \mathfrak{P}^{(3)} \supseteq \cdots .$$

I claim this chain stops. To see this, consider the descending chain

$$\mathfrak{P} + (a) \supseteq \mathfrak{P}^{(2)} + (a) \supseteq \mathfrak{P}^{(3)} + (a) \supseteq \cdots .$$

This chain is in one-to-one correspondence with a chain in $A/(a)$. By step 1, the ring $A/(a)$ has the DCC, so, there is some n_0 so that for all $n \geq n_0$,

$$\mathfrak{P}^{(n)} \subseteq \mathfrak{P}^{(n+1)} + aA.$$

Given $x \in \mathfrak{P}^{(n)}$, there is some $y \in \mathfrak{P}^{(n+1)}$ and some $z \in A$ so that $x = y + za$. As $x - y \in \mathfrak{P}^{(n)}$, we have $za \in \mathfrak{P}^{(n)}$; since $a \notin \mathfrak{P} = \sqrt{\mathfrak{P}^{(n)}}$, we get $z \in \mathfrak{P}^{(n)}$. Hence,

$$\mathfrak{P}^{(n)} \subseteq \mathfrak{P}^{(n+1)} + \mathfrak{P}^{(n)}a \subseteq \mathfrak{P}^{(n+1)} + \mathfrak{P}^{(n)}\mathfrak{p}.$$

Read this in the local ring $\overline{A} = A/\mathfrak{P}^{(n+1)}$ whose maximal ideal is $\overline{\mathfrak{p}}$. We get

$$\overline{\mathfrak{P}^{(n)}} = \overline{\mathfrak{P}^{(n)}}\,\overline{\mathfrak{p}}. \tag{‡}$$

As $\overline{\mathfrak{P}^{(n)}}$ is a f.g. $\overline{A}$-module, by Nakayama's lemma, $\overline{\mathfrak{P}^{(n)}} = (0)$. Therefore,

$$\mathfrak{P}^{(n)} = \mathfrak{P}^{(n+1)}, \quad \text{for all } n \geq n_0. \tag{$*$}$$

Step 3. By $(*)$, we get $\bigcap_{n\geq 1} \mathfrak{P}^{(n)} = \mathfrak{P}^{(n_0)}$. But, $(\mathfrak{P}^{(n_0)})^e = \left(\bigcap_{n\geq 1} \mathfrak{P}^{(n)}\right)^e \subseteq \bigcap_{n\geq 1}(\mathfrak{P}^{(n)})^e$. Consequently,

$$(\mathfrak{P}^{(n_0)})^e \subseteq \bigcap_{n\geq 1} (\mathfrak{P}^n)^e = \bigcap_{n\geq 1} (\mathfrak{P}^e)^n.$$

However, $\mathfrak{P}^e$ is the maximal ideal of A, so by the Krull intersection theorem, the righthand side is (0). Therefore,

$$(\mathfrak{P}^e)^{n_0} = (\mathfrak{P}^{n_0})^e = (0).$$

But, A is an integral domain, therefore, $\mathfrak{P}^e = (0)$; so, $\mathfrak{P} = (0)$, as contended. □

Now, consider the case where A is just a ring (not necessarily an integral domain).

Corollary 3.121 *If A is a noetherian ring and $\mathfrak{p}$ is an isolated prime of some $(a) \subseteq A$, then* $\operatorname{ht}(\mathfrak{p}) \leq 1$.

Proof. Now, $\mathfrak{p}$ is an isolated prime of some $(a) \subseteq A$. If $a = 0$, then $\mathfrak{p}$ is a minimal prime, i.e., $\operatorname{ht}(\mathfrak{p}) = 0$. Therefore, we may assume $a \neq 0$. Suppose $\operatorname{ht}(\mathfrak{p}) \geq 2$, then we must have a chain

$$\mathfrak{p} > \mathfrak{q} > \mathfrak{q}'.$$

Look in $\overline{A} = A/\mathfrak{q}'$, a noetherian domain. Here, we have

$$\overline{\mathfrak{p}} > \overline{\mathfrak{q}} > (0) = \overline{\mathfrak{q}'}, \tag{$**$}$$

yet, $\overline{\mathfrak{p}}$ is an isolated prime of $(\overline{a})$, so the theorem in the domain case implies that $\operatorname{ht}(\overline{\mathfrak{p}}) = 1$, contradicting $(**)$. □

To prove the next and last Krull theorem, we need the *chain detour lemma*:

Lemma 3.122 *(Chain detour lemma) Say A is a noetherian ring and*

$$\mathfrak{p}_0 > \mathfrak{p}_1 > \cdots \mathfrak{p}_{m-1} > \mathfrak{p}_m$$

is a given chain in $\operatorname{Spec} A$. *Given a finite set of primes $S = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_t\}$, suppose $\mathfrak{p}_0 \not\subseteq \mathfrak{q}_i$, for $i = 1, \ldots, t$. Then, there exists an alternate chain (the detour)*

$$\mathfrak{p}_0 > \widetilde{\mathfrak{p}_1} > \cdots \widetilde{\mathfrak{p}}_{m-1} > \mathfrak{p}_m$$

so that no $\widetilde{\mathfrak{p}_i}$ is contained in any $\mathfrak{q}_j$.

Proof. Say the lemma is known when $m = 2$, i.e., given a chain $\mathfrak{p}_0 > \mathfrak{p}_1 > \mathfrak{p}_2$, we can change $\mathfrak{p}_1$. Given our chain

$$\mathfrak{p}_0 > \mathfrak{p}_1 > \cdots \mathfrak{p}_{m-1} > \mathfrak{p}_m$$

and the set S, we can replace $\mathfrak{p}_1$ by $\widetilde{\mathfrak{p}_1}$ with $\widetilde{\mathfrak{p}_1} \not\subseteq \mathfrak{q}_i$ for $i = 1, \ldots, t$. But, then, we have the chain

$$\widetilde{\mathfrak{p}_1} > \mathfrak{p}_2 > \cdots \mathfrak{p}_{m-1} > \mathfrak{p}_m$$

and we can use induction to obtain the desired chain.

Thus, we are reduced to the main case: $\mathfrak{p}_0 > \mathfrak{p}_1 > \mathfrak{p}_2$. Now, $\mathfrak{p}_0 > \mathfrak{p}_2$ and $\mathfrak{p}_0 \not\subseteq \mathfrak{q}_\mathfrak{j}$ for $j = 1, \ldots, t$. By the prime avoidance lemma,

$$\mathfrak{p}_0 \not\subseteq \mathfrak{p}_2 \cup \bigcup_{j=1}^{t} \mathfrak{q}_j.$$

Hence, there is some $x \in \mathfrak{p}_0$ so that $x \notin \mathfrak{p}_2$ and $x \notin \mathfrak{q}_j$ for $j = 1, \ldots, t$. Look in $\overline{A} = A/\mathfrak{p}_2$, a noetherian domain. In $\overline{A}$, we have

$$\overline{\mathfrak{p}_0} > \overline{\mathfrak{p}_1} > \overline{\mathfrak{p}_2} = (0)$$

and so, $\operatorname{ht}(\overline{\mathfrak{p}_1}) \geq 2$. Now, $\overline{x} \in \overline{\mathfrak{p}_0}$ and it follows that some isolated prime of $\overline{x}$, say $\mathfrak{B}$, is contained in $\overline{\mathfrak{p}_0}$. As $x \notin \mathfrak{p}_2$, we have $\overline{x} \neq 0$ and $\mathfrak{B}$ is an isolated prime of $\overline{x}$; by the principal ideal theorem, $\operatorname{ht}(\mathfrak{B}) = 1$. As $\operatorname{ht}(\overline{\mathfrak{p}_0}) \geq 2$, we have $\overline{\mathfrak{p}_0} > \mathfrak{B} > (0)$ and $\overline{x} \in \mathfrak{B}$. Let $\widetilde{\mathfrak{p}_1}$ be the inverse image of $\mathfrak{B}$ in A. We get:

(1) $\mathfrak{p}_0 > \widetilde{\mathfrak{p}_1} > \mathfrak{p}_2$.

(2) $x \in \widetilde{\mathfrak{p}_1}$; $x \notin \mathfrak{q}_j$, for $j = 1, \ldots, t$.

(3) $\widetilde{\mathfrak{p}_1} \not\subseteq \mathfrak{q}_j$, for $j = 1, \ldots, t$. □

Theorem 3.123 *(Krull Height Theorem (1928)) If $\mathfrak{A}$ is an ideal of the noetherian ring, A, suppose $\mathfrak{A}$ is generated by r elements and $\mathfrak{p}$ is an isolated prime of $\mathfrak{A}$. Then* $\operatorname{ht}(\mathfrak{p}) \leq r$.

Proof. We proceed by induction on r. Hypothesis: The theorem holds for all isolated primes, $\mathfrak{p}$, of $\mathfrak{A}$ and all $\mathfrak{A}$ generated by at most r elements.

The principal ideal theorem yields the cases $r = 0, 1$. Next, let $\mathfrak{A} = (x_1, \ldots, x_r)$ and $\mathfrak{B} = (x_1, \ldots, x_{r-1})$. If $\mathfrak{A} = \mathfrak{B}$, there is nothing to prove. Thus, we may assume that $x_r \notin \mathfrak{B}$. If $\mathfrak{p}$ (some isolated prime of $\mathfrak{A}$) is an isolated prime of $\mathfrak{B}$, the induction hypothesis implies $\operatorname{ht}(\mathfrak{p}) \leq r - 1$. So, we may assume that $\mathfrak{p}$ is an isolated prime of $\mathfrak{A}$, *not* an isolated prime of $\mathfrak{B}$ and $x_r \notin \mathfrak{B}$ (obviously, $\mathfrak{A} \neq \mathfrak{B}$). Let $S = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_t\}$ be the finite set of isolated primes of $\mathfrak{B}$, let $\mathfrak{p} = \mathfrak{p}_0$ and look at some chain

$$\mathfrak{p} = \mathfrak{p}_0 > \mathfrak{p}_1 > \cdots \mathfrak{p}_{m-1} > \mathfrak{p}_m$$

of $\operatorname{Spec} A$, so that $\operatorname{ht}(\mathfrak{p}_0) \geq m$. If $\mathfrak{p}_0 \subseteq \mathfrak{q}_j$, then

$$\mathfrak{B} \subseteq \mathfrak{A} \subseteq \mathfrak{p}_0 \subseteq \mathfrak{q}_j,$$

contradicting the fact that $\mathfrak{p}_0$ is not an isolated prime of $\mathfrak{B}$. Therefore, $\mathfrak{p}_0 \not\subseteq \mathfrak{q}_j$, for $j = 1, \ldots, t$, and by the detour lemma, there is a chain of the same length

$$\mathfrak{p}_0 > \widetilde{\mathfrak{p}_1} > \cdots \widetilde{\mathfrak{p}}_{m-1} > \mathfrak{p}_m$$

so that no $\widetilde{\mathfrak{p}_i}$ is contained in any $\mathfrak{q}_j$. Our goal is to show that $m \leq r$. let $\overline{A} = A/\mathfrak{B}$. Then $\overline{\mathfrak{A}}$ becomes principal $(\overline{A}\overline{x}_r)$ in $\overline{A}$ and as $\overline{\mathfrak{p}_0}$ is an isolated prime of $\overline{\mathfrak{A}}$, the principal ideal theorem in $\overline{A}$ implies $\mathrm{ht}(\overline{\mathfrak{p}_0}) = 1$. ($\mathrm{ht}(\overline{\mathfrak{p}_0}) > 0$ because $\mathfrak{p}_0$ is *not* an isolated prime of $\mathfrak{B}$).

Now, $\mathfrak{p}_0 \supseteq \widetilde{\mathfrak{p}}_{m-1}$ and $\mathfrak{p}_0 \supseteq \mathfrak{B}$, so,

$$\mathfrak{p}_0 \supseteq \widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}.$$

Then, observe that $\overline{\mathfrak{p}_0} \supseteq \overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}}$ and as $\mathfrak{B} \subseteq \mathfrak{q}_i$, for all i and $\widetilde{\mathfrak{p}}_{m-1} \not\subseteq \mathfrak{q}_i$, for all i, we have $\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B} \not\subseteq \mathfrak{q}_i$, for all i; thus, $\overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}} \not\subseteq \overline{\mathfrak{q}_i}$, for all i (here, the $\overline{\mathfrak{q}_i}$ are the isolated primes of (0) in $\overline{A}$, i.e., those of height 0 in $\overline{A}$).

Claim. The ideal $\overline{\mathfrak{p}_0}$ is an isolated prime of $\overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}}$.

As $\overline{\mathfrak{p}_0} \supseteq \overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}}$, we find $\overline{\mathfrak{p}_0} \supseteq \mathfrak{m}$, where $\mathfrak{m}$ is some isolated prime of $\overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}}$. If $\overline{\mathfrak{p}_0} \neq \mathfrak{m}$, then as $\mathrm{ht}(\mathfrak{m}) \geq 1$ (because $\overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}} \not\subseteq \overline{\mathfrak{q}_i}$, for all i) we'd see that $\mathrm{ht}(\overline{\mathfrak{p}_0}) \geq 2$. But, $\mathrm{ht}(\overline{\mathfrak{p}_0}) = 1$, a contradiction. Therefore, $\overline{\mathfrak{p}_0} = \mathfrak{m}$, as claimed.

Now, let $\overline{\overline{A}} = A/\widetilde{\mathfrak{p}}_{m-1}$. As $\mathfrak{p}_0 \supseteq \widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}$, we get

$$\overline{\overline{\mathfrak{p}_0}} \supseteq \overline{\overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}}} = \overline{\overline{\mathfrak{B}}}.$$

Moreover, as $\overline{\mathfrak{p}_0}$ is an isolated prime of $\overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}}$, we see that $\overline{\overline{\mathfrak{p}_0}}$ is an isolated prime of $\overline{\overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}}} = \overline{\overline{\mathfrak{B}}}$. But, the number of generators of $\overline{\overline{\mathfrak{B}}}$ is at most $r - 1$. If we apply the induction hypothesis to $\overline{\overline{A}}$, we get $\mathrm{ht}(\overline{\overline{\mathfrak{p}_0}}) \leq r - 1$. Finally, by applying double bar to our detored chain, we get

$$\overline{\overline{\mathfrak{p}_0}} > \overline{\overline{\widetilde{\mathfrak{p}_1}}} > \cdots > \overline{\overline{\widetilde{\mathfrak{p}}}}_{m-2} > (0),$$

a chain of length $m - 1$. Therefore, $m - 1 \leq r - 1$, that is, $m \leq r$. □

Corollary 3.124 *In a noetherian ring, the prime ideals satisfy the descending chain condition. In particular, every prime ideal contains a minimal prime.*

Proof. Given a prime, $\mathfrak{p}$, it is finitely generated, say by r elements. Therefore, $\mathrm{ht}(\mathfrak{p}) \leq r$ and any descending chain starting at $\mathfrak{p}$ must stop. □

Corollary 3.125 *If A is a noetherian ring, then for every $\mathfrak{p} \in \operatorname{Spec} A$, the Krull dimension, $\dim(A_\mathfrak{p})$, is finite.*

Corollary 3.126 *Say A is noetherian, $a \neq 0$ is any given element in A and $\mathfrak{p}$ is an isolated prime of Aa. Then, every prime ideal, $\mathfrak{q}$, strictly contained in $\mathfrak{p}$ is an isolated prime of (0), i.e., consists of zero-divisors.*

Proof. By the principal ideal theorem, $\mathrm{ht}(\mathfrak{p}) \leq 1$, and $\mathrm{ht}(\mathfrak{p}) = 1$, as $\mathfrak{q} < \mathfrak{p}$. It follows that $\mathrm{ht}(\mathfrak{q}) = 0$, which means that $\mathfrak{q}$ is an isolated prime of (0).

Proposition 3.127 *(Converse of the height theorem) Let A be a noetherian ring. For every $\mathfrak{p} \in \operatorname{Spec} A$, if $\mathrm{ht}(\mathfrak{p}) \leq r$, then there is some ideal, $\mathfrak{A}$, of A generated by at most r elements and $\mathfrak{p}$ is an isolated prime of $\mathfrak{A}$.*

Proof. (DX). □

3.8 Further Readings

There is a vast literature on commutative rings and commutative algebra. Besides some of the references already given in Section 2.9, such as Atiyah MacDonald [3], Lafon [32, 33], Eisenbud [13], Matsumura [39], Malliavin [38], let us mention Bourbaki [6, 8, 7] Zariski and Samuel [50, 51], Jacobson [28] and Serre [46].