Undergraduate Commutative Algebra

Robin Truax

December 2021

Contents

1 Basics

Commutative algebra is the study of (commutative) rings and their properties. In particular, a (commutative) ring is defined *with identity.* The applications of commutative algebra lie chiefly in algebraic geometry and homological algebra, as well as much of algebraic number theory. We will assume basic knowledge of ring theory, field theory, and Galois theory. Also, we expect knowledge of basic definitions in topology (axioms of topological spaces in terms of open and closed sets and Hausdorff spaces). These notes are created via a close reading of Miles Reid's *Undergraduate Commutative Algebra.*

We will adopt the following conventions:

1. All rings are commutative with identity.
2. The letter k will denote a field, even when not explicitly stated.
3. The letter A will denote a ring, even when not explicitly stated.
4. The font $\mathfrak{a}$ (known as fraktur font) denotes ideals without exception.
5. To denote proper containment of A in B, we write $A \subsetneq B$. To denote not-necessarily-proper containment of A in B, we will write $A \subseteq B$. In no cases we will use the ambiguous symbol $\subset$.
6. We use the symbol $\square$ to denote the conclusion of a proof (whether a proof is given, it is skipped because it is too easy, or it is skipped because it is too hard).

1.1 Rings

We assume a knowledge of rings, ideals, units, and basic results about them. In particular, you should know the definition of integral domains, UFDs, PIDs, Euclidean domains, and fields (and the proofs/definitions that imply each class of rings is contained in the next). Nonetheless, we'll recount the basic Isomorphism Theorems (since they're easy to forget):

Theorem 1 (Isomorphism Theorems for Rings)**.**

1. *If $\varphi : A \to B$ is a ring homomorphism, then $\ker\varphi \lhd A$, $\operatorname{im}\varphi$ is a subring of B, and $\operatorname{im}\varphi \simeq A/\ker\varphi$. In particular, if φ is surjective, then $B \simeq A/\ker\varphi$.*
2. *Let $B \subseteq A$ be rings and $I \lhd R$. Then the sum $B + I = \{b + a \mid b \in B, a \in I\}$ is a subring of A and the intersection $B \cap I$ is an ideal of B. Furthermore, $(B + I)/I \simeq B/(B \cap I)$.*
3. *If I is an ideal of A, then there is an inclusion-preserving bijection $A \leftrightarrow A/I$ between the ideals of A that contain I and the ideals of A/I. Similarly, there is an inclusion-preserving bijection $A \leftrightarrow A/I$ between the subrings of A that contain I and the subrings of A/I.*
4. *If $I \subseteq J$ are ideals of A, then $(R/I)/(J/I) \simeq R/J$.*

Problem 2. Prove that the inclusion-preserving bijection $A \leftrightarrow A/I$ restricts to a one-to-one correspondence of prime ideals and a one-to-one correspondence of maximal ideals.

Definition 3 (Prime Ideal)**.** An ideal $\mathfrak{p} \lhd A$ is called *prime* if $ab \in \mathfrak{p}$ implies that either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Contrapositively, this means that $\mathfrak{p}$ is prime if $a, b \notin \mathfrak{p} \Rightarrow ab \notin \mathfrak{p}$.

Definition 4 (Maximal Ideal)**.** A proper ideal $\mathfrak{m} \lhd A$ is called *maximal* if it is maximal with respect to inclusion among all proper ideals of A. Precisely, if $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A$, then $\mathfrak{m} = \mathfrak{a}$ or $\mathfrak{a} = A$.

Proposition 5. *A ring A is an integral domain if and only if the zero ideal (0) is prime, and a field if and only if the zero ideal (0) is maximal.*

Corollary 5.1. *An ideal $\mathfrak{a} \lhd A$ is prime if and only if $A/\mathfrak{a}$ is an integral domain, and maximal if and only if $A/\mathfrak{m}$ is a field.*

Corollary 5.2. *Maximal ideals are prime.*

Proposition 6. *Given a homomorphism of rings $\phi : A \to B$ and a prime ideal $\mathfrak{b} \lhd B$, the preimage of $\mathfrak{b}$, $\phi^{-1}(\mathfrak{b})$, is prime.*

In particular, the preimage of a maximal ideal is prime, but not always maximal. For an example of a maximal ideal whose preimage is not maximal, consider the natural embedding $\mathbb{Z} \hookrightarrow \mathbb{Q}$. The ideal (0) is maximal in $\mathbb{Q}$, but since the ring homomorphism is injective, its preimage is (0) in $\mathbb{Z}$ which is clearly not maximal.

Proposition 7. *If I and J are comaximal (i.e. $I + J = R$), then $IJ = I \cap J$.*

Proof. If $I + J = R$, then $I \cap J = (I \cap J)R = (I \cap J)(I + J) = (I \cap J)I + (I \cap J)J \subseteq IJ + JI = IJ$. Yet clearly $IJ \subseteq I \cap J$, whence the result follows. □

Definition 8 (Residue Field)**.** The *residue field* of a prime ideal $\mathfrak{p} \lhd A$ is the fraction field of the integral domain $A/\mathfrak{p}$. This is denoted $\kappa(\mathfrak{p})$. In particular, if $\mathfrak{p}$ is maximal, then $\kappa(\mathfrak{p}) \cong A/\mathfrak{p}$.

Proposition 9. *The prime ideals of A are precisely the kernels of homomorphisms from A to fields.*

Proof. The kernel of the map $A \to \kappa(\mathfrak{p})$ is $\mathfrak{p}$, so any prime ideal is the kernel of a homomorphism from A to a field. Conversely, if $\ker \phi$ is the kernel of a map $\phi : A \to k$ (with k a field), then

$$a, b \notin \ker \phi \Rightarrow \phi(a), \phi(b) \neq 0 \Rightarrow \phi(a)\phi(b) \neq 0 \Rightarrow \phi(ab) \neq 0 \Rightarrow ab \notin \ker \phi$$

precisely as desired. □

Definition 10 (Multiplicative Set)**.** A multiplicative set S is a subring of a ring A such that (i) $1 \in S$ and (ii) $a, b \in S \Rightarrow ab \in S$. In particular, an ideal $\mathfrak{p} \lhd A$ is prime iff $A \setminus \mathfrak{p}$ is a multiplicative set.

Definition 11 (Prime and Maximal Spectra)**.** Given a ring A, the *prime spectrum of* A is the set $\operatorname{Spec} A = \{\mathfrak{p} \mid \mathfrak{p} \lhd_{\text{pr}} A\}$. Similarly, the *maximal spectrum of* A is the set $\text{m-Spec}\, A = \{\mathfrak{m} \mid \mathfrak{m} \lhd_{\max} A\}$.

Lemma 12 (Existence of Maximal Ideals)**.** *If A is a ring and I is a proper ideal in A, then there exists $\mathfrak{m} \lhd_{\max} A$ containing I. In particular, there exists a maximal ideal containing any nonunit $a \in A$ (since in this case, (a) is a proper ideal).*

Proof. This is an elementary consequence of Zorn's Lemma: consider the set of proper ideals containing I, ordered by inclusion. It is nonempty (it contains I), and any chain has an upper bound (the union of all the ideals in the chain, which is itself a proper ideal). Thus, Zorn's Lemma implies there exists a maximal element. This maximal element, of course, is a maximal ideal containing I. □

Lemma 13 (Existence of Prime Ideals)**.** *If A is a ring, S is a multiplicative set in A, and I is an ideal disjoint from S, there exists a prime ideal $\mathfrak{p} \lhd_{\text{pr}} A$ containing I yet disjoint from S.*

Proof. Let $\mathscr{J} := \{J \lhd A \mid I \subseteq J, J \cap S = \varnothing\}$. This set is nonempty, as it contains I. Furthermore, any chain of ideals $\{J_\lambda\}$ has the upper bound $\bigcup_{\lambda \in \Lambda} J_\lambda$. Thus, by Zorn's Lemma, we have a maximal element which we call $\mathfrak{p}$. It suffices to prove that $\mathfrak{p}$ is prime.

Suppose that $f, g \in A \setminus \mathfrak{p}$. Define $J_1 := p + (f)$ and $J_2 := p + (g)$. Since these properly contain $\mathfrak{p}$, it must be that $J_1 \cap S, J_2 \cap S$ are nonempty. In particular, there exists $c, d \in \mathfrak{p}$ and $a, b \in A$ such that $c + af \in J_1 \cap S$ and $d + bg \in J_2 \cap S$. But then

$$(c + af)(d + bg) = cd + afd + bgc + abfg \in S$$

as S is a multiplicative set. Since $c, d \in \mathfrak{p}$, the first three terms are in $\mathfrak{p}$. To retain the condition $\mathfrak{p} \cap S = \varnothing$, it must be that $abfg \notin \mathfrak{p}$ whence $fg \notin \mathfrak{p}$. □

1.2 The Nilradical and Radical Ideals

Definition 14 (Nilpotent and Nilradical)**.** An element $x \in A$ is called *nilpotent* if there exists a positive integer n with $x^n = 0$. The set of all nilpotent elements in a ring A is called the *nilradical* of A and denoted $\mathfrak{N}(A)$. If $\mathfrak{N}(A) = 0$, then A is called *reduced*.

Proposition 15 (Nilpotents vs. Units)**.** *If x is nilpotent in A, then $1 - x$ is a unit in A.*

Proof. Suppose that n is such that $x^n = 0$. Then $(1 - x)(1 + x + x^2 + \cdots + x^{n-1}) = 1 + x^n = 1$. □

Proposition 16. *The nilradical $\mathfrak{N}(A)$ of a ring is an ideal.*

Proof. Since clearly $0 \in \mathfrak{N}(A)$, it suffices to prove that $ax + by \in \mathfrak{N}(A)$ for any $x, y \in \mathfrak{N}(A)$ and $a, b \in A$. To see why this holds, let m be such that $x^m = 0$ and n be such that $y^n = 0$. Then, using the binomial theorem, $(ax + by)^{m+n} = 0$, as desired. □

Definition 17 (Radical of an Ideal)**.** Suppose that I is an ideal in A. Then the *radical of I* is the set $\sqrt{I} = \{x \in A \mid \exists n, x^n \in I\}$. If $I = \sqrt{I}$, then I is called *radical*.

Proposition 18. *If $\eta_I : A \to A/I$ is the natural projection map, then $\sqrt{I} = \eta_I^{-1}(\mathfrak{N}(A/I))$. In particular, this demonstrates that the radical of an ideal is always an ideal.*

Lemma 19. *For any ring A,*

$$\mathfrak{N}(A) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$$

Proof. Pick some prime ideal $\mathfrak{p}$. If $f \in \mathfrak{N}(A)$, then $f^n = 0$ so $f^n \in \mathfrak{p}$. But since $\mathfrak{p}$ is prime, then $f \in \mathfrak{p}$. Conversely, if $f \notin N$, then let $S = \{1, f, f^2, \dots\}$ (a multiplicative set). Note $S \cap (0) = \varnothing$, so by Lemma 13 there exists a prime ideal $\mathfrak{p}$ with $S \cap \mathfrak{p} = \varnothing$. Thus in particular, it is not in $\bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$. □

Corollary 19.1. *By applying Proposition 18 and Lemma 19 to the ring A/I, we achieve*

$$\sqrt{I} = \bigcup_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ I \subseteq \mathfrak{p}}} \mathfrak{p}.$$

Corollary 19.2. *Any ideal which is the intersection of prime ideals is radical. In particular, any prime ideal is radical.*

Definition 20 (Radical Ideal)**.** An ideal is called *radical* if $I = \sqrt{I}$. Obviously, the radical of an ideal is a radical ideal (whence the nilradical, being $\sqrt{0}$, is a radical ideal).

Definition 21 (Idempotent)**.** An *idempotent* is an element $e \in A$ with $e^2 = e$.

Proposition 22. *A has an idempotent $e \neq 0, 1$ if and only if it is a nontrivial direct sum of rings $A = A_1 \oplus A_2$ with $A_1 = Ae$ and $A_2 = A(1 - e)$.*

Proof. If e is idempotent, then $(1-e)^2 = 1-2e+e^2 = 1-2e+e = 1-e$, so $e' = 1-e$ is also idempotent. In this case, $e + e' = 1$ and $ee' = 0$ (we call e and e' *complementary orthogonal idempotents*). By writing $a = ae + ae'$, we see that A is indeed the direct sum of A_1 and A_2 in the manner described. The reverse direction is similarly simple. □

Definition 23 (Zero Divisors)**.** In a ring A, a is a zero divisor if $a \neq 0$ and there exists $b \neq 0$ with $ab = 0$. In particular, a ring A is an integral domain if there exist no zero divisors.

Proposition 24 (Minimal Prime Ideals)**.** *Let A be a reduced ring with zero divisors. Then A has more than one minimal prime ideal.*

Proof. By Lemma 19, $0 = \bigcap \mathfrak{p}$ (where the intersection is over prime ideals in $\operatorname{Spec} A$). Yet, if $\mathfrak{p} \subseteq \mathfrak{q}$, we can simply omit $\mathfrak{q}$, so $0 = \bigcap \mathfrak{p}$, where the intersection is over minimal prime ideals in $\operatorname{Spec} A$. If there is only one such ideal, then 0 is a minimal prime ideal; a contradiction since this implies that A is an integral domain and thus has no zero divisors. □

1.3 Local Rings

Definition 25 (Local Ring)**.** A ring A with only one maximal ideal $\mathfrak{m}$ is called a *local ring*. In this case, we often write the ring as $(A, \mathfrak{m})$ or even $(A, \mathfrak{m}, k)$, where k is the *residue field* $A/\mathfrak{m}$.

Proposition 26. *A is a local ring if and only if all the nonunits of A form an ideal.*

Proof. As discussed in Lemma 12, any nonunit is contained in a maximal ideal. Thus, if there is just one maximal ideal, then it is the ideal of all nonunits (it cannot contain any units since an ideal which contains a unit is the whole ring). Conversely, if the nonunits of A form an ideal, clearly they are maximal among proper ideals; they contain every other proper ideal! □

Definition 27 (Jacobson Radical)**.** The Jacobson radical of a ring A is the intersection of all maximal ideals of A and is denoted by $\mathfrak{J}(A)$. It is not difficult to prove that it is a radical ideal.

Proposition 28. *An element $x \in A$ is in $\mathfrak{J}(A)$ if and only if $1 - yx$ is a unit for each $y \in A$.*

Proof. Suppose there exists y in A and $x \in \mathfrak{J}(A)$ with $1 - yx$ not a unit. Then $1 - yx$ is in some maximal ideal $M \triangleleft A$. But $x \in \mathfrak{J}(A) \Rightarrow x \in M \Rightarrow yx \in M \Rightarrow 1 - yx + yx = 1 \in M$, a contradiction with the assumption that M is a maximal ideal and in particular proper.

Conversely, suppose $x \notin J(A)$. Then there exists a maximal ideal $M \triangleleft R$ so that $x \notin M$. By the definition of M, $A = \langle M, \{x\} \rangle$, which implies that $1 = m + yx$ for $m \in M$, so $1 - yx \in M$. Thus $1 - yx$ is not a unit as M is a maximal ideal and in particular proper. □

Problem 29. Prove that $k[\![x]\!]$ (the ring of formal power series in x with coefficients in k) is a local ring with maximal ideal (x). This ring, and rings similar to it, appear often in analysis (especially when discussing functions analytic in a neighborhood of 0), or when discussing the p-adic integers.

1.4 Modules

Definition 30 (Module)**.** For any ring A, an *A-module* is an Abelian group M with a multiplication map $A \times M \to M$ (the image of (a, m) is denoted by am, as one expects) satisfying the following axioms:

1. $a(m + n) = am + an$ and $(a + b)m = am + bm$.
2. $(ab)m = a(bm)$.
3. $1_A m = m$.

The third condition is not always imposed: in some circles, only the first two axioms are required, and modules which additionally satisfy the third condition are called *unital*. Here, we require all our modules to be unital (just as we require all our rings to be unital).

Definition 31 (Submodule)**.** A *submodule* of an A-module M is an A-module N with $N \subseteq M$.

Problem 32. Prove that the submodules of A (considered as an A-modules in the obvious way) are precisely the ideals of A.

Definition 33 (Module Homomorphism)**.** An map between A-modules $\varphi : M \to N$ is called *A-linear* or an *A-module homomorphism* if $\varphi(ax + by) = a\varphi(x) + b\varphi(y)$ for any $a, b \in A$ and $x, y \in M$. Notice, among other things, that such a map is an abelian group homomorphism $M \to N$.

Theorem 34 (Isomorphism Theorems for Modules)**.** *Let A be a ring and M and N be A-modules.*

1. *If $\varphi : M \to N$ is an A-module homomorphism, then $\ker \varphi$ is a submodule of M, $\operatorname{im} \varphi$ is a submodule of N, and $\operatorname{im} \varphi \simeq M/\ker \varphi$. In particular, if φ is surjective, then $N \simeq M/\ker \varphi$.*

2. *If $N_1, N_2 \subseteq M$, then $(N_1 + N_2)/N_2 = N_1/(N_1 \cap N_2)$.*
3. *If N is an submodule of M, then there is an inclusion-preserving bijection $M \leftrightarrow M/N$ between the submodules of M that contain N and the submodules of M/N.*
4. *If $N_1 \subseteq N_2$ are submodules of M, then $(M/N_1)/(N_2/N_1) \simeq M/N_2$.*

You might notice that these isomorphism theorems are quite simpler; much simpler than the ones for rings. This is because, in a categorical sense, modules are much "nicer" objects than rings (which have two subobjects: ideals and subrings).

Definition 35 (Generated Submodules)**.** If M is an A-module and $(m_\lambda)_{\lambda\in\Lambda}$ is a set of elements in M, then the *submodule generated by* $(m_\lambda)_{\lambda\in\Lambda}$ is the submodule

$$\sum_{\lambda\in\Lambda} Am_\lambda = \left\{ \sum_{\lambda\in\Lambda} f_\lambda m_\lambda \in M \mid f_\lambda \in A \right\}$$

In the case that the family of elements is countable, i.e. it can be expressed in the form $\{m_1, m_2, \dots\}$ (and even sometimes, by abuse of notation, when it cannot), we denote this submodule by $(m_1, m_2, \dots)$.

Definition 36 (Direct Sum)**.** The direct sum of a family $(M_\lambda)_{\lambda\in\Lambda}$ of A-modules is defined as expected:

$$\bigoplus_{\lambda\in\Lambda} M_\lambda = \{(m_\lambda)_{\lambda\in\Lambda} \mid \text{only finitely many } a_\lambda \neq 0\}$$

Of special interest is the case $A^{|\Lambda|} = \bigoplus_{\lambda\in\Lambda} A$ (adding A to itself $|\Lambda|$ times). This is because, given any set of elements $(m_\lambda)_{\lambda\in\Lambda}$, there is a A-module homomorphism

$$\eta : A^{|\Lambda|} \to M \text{ given by } (f_\lambda)_{\lambda\in\Lambda} \mapsto \sum_{\lambda\in\Lambda} f_\lambda m_\lambda.$$

Definition 37 (Definitions Based on η)**.** Let η be the map, as described above, associated with the set $\mathcal{G}$ of elements $(m_\lambda)_{\lambda\in\Lambda}$ in an A-module M.

1. If η is surjective, then we say $\mathcal{G}$ is a *family of generators of* M.
2. If there exists a finite set of elements that generate M, we say that M is a *finite A-module.*
3. If η is an isomorphism, then we say $\mathcal{G}$ is a *basis for* M.
4. If an A-module M has a basis, then we call it a *free module.*

Theorem 38. *If m and n are finite, then $A^m \simeq A^n$ (as A-modules) implies that $m = n$ for any ring A.*

Proof. If $A^m \simeq A^n$, then $A/\mathfrak{m} \otimes A^m \simeq A/\mathfrak{m} \otimes A^n$, which implies that $(A/\mathfrak{m})^m \simeq (A/\mathfrak{m})^n$. But these can be viewed as $A/\mathfrak{m}$-modules, and since $A/\mathfrak{m}$ is a field, they are vector spaces of dimension m and n respectively. We have thus reduced the theorem to the well-known case of finite-dimensional vector spaces, which tells us that $m = n$. □

1.5 The Determinant Trick and Nakayama's Lemma

Theorem 39 (Cayley-Hamilton Theorem)**.** *Let A be a commutative ring, $N = (a_{ij})$ an $n \times n$ matrix with entries in A, and write $p(x) = \det(xI - N)$. Then $p(x)$ is a monic polynomial in $A[x]$ of degree n such that $p(N) = 0$.*

Proof. Laborious and thus omitted. □

The following result is proven in exactly the same way:

Theorem 40 (Determinant Trick). *Let M be a finite A-module generated by n elements. Further let $\varphi : M \to M$ be an A-module homomorphism and suppose that I is an ideal of A such that $\varphi(M) \subseteq IM$. Then φ satisfies*

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

for some $a_i \in I^i$ for each $i \in \{1, \ldots, n\}$.

Proof. Let $M = \langle m_1, \ldots, m_n \rangle$ with $\phi(m_i) \in IM$. Then $\phi(m_i) = \sum_j a_{ij}m_j$ with $a_{ij} \in I$. We also have the equation $\sum_j(\delta_{ij}\phi - a_{ij})(m_j) = 0$ for each i, where $\delta_{ij}\phi - a_{ij} \in \operatorname{End} M$. Then let Δ be the matrix with the (i, j) element $\delta_{ij}\phi - a_{ij} \in \operatorname{End} M$. Recall that $\operatorname{adj}\Delta \cdot \Delta = \det\Delta \cdot I_n$ (where I_n is the $n \times n$ identity matrix). Now consider the fact that:

$$\Delta \cdot \begin{bmatrix} m_1 \\ m_2 \\ \cdots \\ m_n \end{bmatrix} = 0 \Rightarrow \operatorname{adj}\Delta \cdot \Delta \cdot \begin{bmatrix} m_1 \\ m_2 \\ \cdots \\ m_n \end{bmatrix} = 0$$

But then this implies that $(\det\Delta)$ (as an endomorphism over M) is 0 over all the m_i, which means that it is identically 0 over all of M as the m_i generate M). And now we're done, since taking the determinant of Δ gives us the desired polynomial in ϕ which is 0. In particular, using the Leibniz permutation formula for determinants, each a_i is the sum of elements which are the product of i elements in I; thus $a_i \in I^i$, as desired. □

Corollary 40.1. *If M is a finite module and $M = IM$, then there exists $x \in A$ such that $1 + I = x + I \in A/I$ and $xM = 0$.*

Proof. This follows from applying the determinant trick to the identity map id_M. Since $(\operatorname{id}_m)^i = \operatorname{id}_M$, we see that $(1 + b)\operatorname{id}_M = 0$ for some $b = a_1 + \cdots + a_n \in I$, as desired. □

Corollary 40.2 (Nakayama's Lemma). *Let $(A, \mathfrak{m})$ be a local ring and M a finite A-module. Then $M = \mathfrak{m}M$ implies that $M = 0$.*

Proof. By the previous corollary, there exists $x \in A$ congruent to 1 mod $\mathfrak{m}$ (in particular, $x \notin \mathfrak{m}$ whence x is a unit) such that $xM = 0$. But then $M = x^{-1}(xM) = x^{-1} \cdot 0 = 0$, as desired. □

Corollary 40.3. *Suppose $(A, \mathfrak{m})$ is a local ring, M is an A-module, and $N \subseteq M$ is a submodule of M. Further suppose that M/N is finite over A and $M = N + \mathfrak{m}M$. Then $N + M$.*

In particular, if M is finite over A, and $s_1, \ldots, s_n \in M$ are elements whose images span the $A/\mathfrak{m}$-vector space $M/\mathfrak{m}M$, then $s_1, \ldots, s_n$ generate M.

Proof. The given condition gives that $\mathfrak{m}(M/N) = M/N$ (quotient both sides by N), whence by Nakayama's Lemma, $M/N = 0$ and $M = N$. □

1.6 Exact Sequences

Definition 41 (Exact Sequence). Suppose L, M, N are A-modules and $L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ is a sequence of A-module homomorphisms. Then this sequence is called *exact at M* if $\operatorname{im}\alpha = \ker\beta$. A longer sequence $\cdots \to M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} M_3 \to \cdots$ is called *exact* if it is exact at every "interior" term.

Proposition 42 (Special Exact Sequences).

1. *$0 \to L \xrightarrow{\alpha} M$ is exact if and only if α is injective.*
2. *$M \xrightarrow{\beta} N \to 0$ is exact if and only if β is surjective.*
3. *In particular, $0 \to L \xrightarrow{\iota} M \to 0$ is exact if and only if ι is an isomorphism.*

4. $0 \to L \overset{\alpha}{\to} M \overset{\beta}{\to} N \to 0$ is exact if and only if $L \hookrightarrow M$ and $N = M/L$.

Definition 43 (Short Exact Sequence)**.** An exact sequence of the form $0 \to L \overset{\alpha}{\to} M \overset{\beta}{\to} N \to 0$ is called a *short exact sequence.*

Proposition 44 (Split Exact Sequences)**.** *Let*

$$0 \to L \overset{\alpha}{\to} M \overset{\beta}{\to} N \to 0$$

be a short exact sequence of A-modules. Then the following are equivalent:

1. *There exists an isomorphism $M \simeq L \oplus N$ under which α is given by $m \mapsto (m, 0)$ and β by $(m, n) \mapsto n$.*
2. *There exists an A-module homomorphism $s : N \to M$ with $\beta \circ s = \mathrm{id}_N$.*
3. *There exists an A-module homomorphism $r : M \to L$ such that $r \circ \alpha = \mathrm{id}_L$.*

*Clearly **1** implies **2** and **3**. Thus, assume **2**. Then s must be injective (it has a left inverse). We argue that $M = \alpha(L) \oplus s(N)$ (which would prove **1** since $\alpha(L) \simeq L$ and $s(N) \simeq N$ by virtue of the injectivity of α and s). To see this, notice that $m \in M$ can be expressed as*

$$m = (m - s(\beta(m))) + s(\beta(m))$$

*The first term is clearly in $\ker\beta = \alpha(L)$ yet the second is obviously in $s(N)$. Furthermore, $\alpha(L) \cap s(N) = 0$, since if $n \in N$ is such that $s(n) \in \alpha(L) = \ker\beta$ then $n = \beta(s(n)) = 0$. Thus **1** holds. The implication **3** $\Rightarrow$ **1** is similar.*

Definition 45 (Split Exact Sequences)**.** If any of the conditions in Proposition 44 hold, the short exact sequence is called a *split exact sequence.*

2 Noetherian Rings

Definition 46 (Ascending Chain Condition)**.** A partially ordered set $\mathscr{S}$ is said to satisfy the *ascending chain condition* (*ACC* for short) if every chain $s_1 \leq s_2 \leq s_3 \leq \cdots$ eventually stabilizes (that is, if $s_k = s_{k+1} = \cdots$ for some k). Obviously, a poset has the ascending chain condition if and only if every nonempty set has a maximal element.

Proposition 47 (Rings Satisfying ACC)**.** *Let A be a ring. Then the following are equivalent:*

1. *The set $\mathscr{S}$ of ideals of A satisfy the ascending chain condition.*
2. *Every nonempty set $S \subseteq \mathscr{S}$ of ideals has a maximal element.*
3. *Every ideal of A is finitely generated.*

Definition 48 (Noetherian Rings)**.** If A is a ring such that the equivalent conditions in Proposition 47 hold, then we call A a *Noetherian ring.*

2.1 Noetherian Modules

Proposition 49 (Modules Satisfying ACC)**.** *Let A be a ring and M an A-module. Then the following are equivalent:*

1. *The set $\mathscr{S}$ of submodules of M satisfy the ascending chain condition.*
2. *Every nonempty set $S \subseteq \mathscr{S}$ of submodules has a maximal element.*
3. *Every submodule of M is finite.*

Definition 50 (Noetherian Modules)**.** If M is an A-module such that the equivalent conditions in Proposition 49 hold, then we call M a *Noetherian A-module.* Notice that since the submodules of a ring A considered as a A-module are precisely its ideals, a ring A is a Noetherian ring if and only if it is an Noetherian A-module.

Proposition 51 (A S.E.S. of Noetherian Modules)**.** *Suppose that*

$$0 \to L \overset{\phi}{\to} M \overset{\psi}{\to} N \to 0$$

is a short exact sequence of A-modules. Then M is Noetherian if and only if L and N are Noetherian.

Proof. Obviously, if M is Noetherian, then L is Noetherian (an infinitely ascending chain of submodules in L is also an infinitely ascending chain of submodules in M). Similarly, if M is Noetherian, then N is Noetherian, since by the Third Isomorphism Theorem for Modules (see Theorem 34), an infinitely ascending chain of submodules of $N \simeq M/L$ corresponds to an infinitely ascending chain of submodules of M containing L.

Assume L and N are Noetherian. Take an ascending chain $M_1 \subseteq M_2 \subseteq \cdots$. First, intersect it with L (formally, intersect it with $\phi(L)$, but L and $\phi(L)$ can be identified) to get $L \cap M_1 \subseteq L \cap M_2 \subseteq \cdots$, an ascending chain of submodules of L. Similarly, apply ψ to get a chain $\psi(M_1) \subseteq \psi(M_2) \subseteq \cdots$ of submodules of N. For some k, both of these chains must stabilize.

Thus, it suffices to prove that for $M_k \subseteq M_{k+1} \subseteq M$, $L \cap M_k = L \cap M_{k+1}$ and $\psi(M_1) = \psi(M_2)$ implies $M_1 = M_2$. To prove this, take $m \in M_{k+1}$, so $\psi(m) \in \psi(M_{k+1}) = \psi(M_k)$. In particular, there is some $n \in M_k$ with $\psi(m) = \psi(n) \Rightarrow \psi(m-n) = 0$. Yet $\ker\psi$ is precisely L, so $m - n \in M_{k+1} \cap L = M_k \cap L$. Thus $m - n \in M_k$, whence $m \in M_k$. This allows us to conclude that $M_k = M_{k+1}$, as desired. □

Corollary 51.1. *The quotient ring A/I of a Noetherian ring A by an ideal $I \lhd A$ is also Noetherian.*

Proof. Notice that

$$0 \to I \to A \to A/I \to 0$$

is a short exact sequence of A-modules, and A is Noetherian, so A/I is Noetherian. □

Corollary 51.2 (Conditions on Noetherian Modules)**.**

1. *If $M_1, \ldots, M_r$ are Noetherian modules, then $\bigoplus_{i=1}^{r} M_i$ is a Noetherian module.*
2. *If A is a Noetherian module, then an A-module M is Noetherian if and only if it is finite.*
3. *In particular, any submodule N of a finite module M over a Noetherian ring A is finite.*
4. *If A is a Noetherian ring, $\varphi : A \to B$ is a ring homomorphism, and B is a finite A-module (where the A-module structure of B is given by φ), B is a Noetherian ring.*

Proof.
1: This follows by noticing that $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$ is a short-exact-sequence, applying Proposition 51, and then using induction.

2: If M is finite, then we have a short exact sequence $0 \to N \to A^r \to M \to 0$ for some r and $N \subseteq A^r$. Notice that by Part 1 and the assumption that A is Notherian, A^r is Noetherian whence, by Proposition 51, M is Noetherian.

3: This is trivial from Part 2.

4: The ideals of B are A-submodules of B, so if B isn't a Noetherian ring, then it isn't a Noetherian A-module. Yet by Part 2, B is Noetherian as an A-module (whence B must be a Noetherian ring). □

2.2 Hilbert's Basis Theorem

Theorem 52 (Hilbert Basis Theorem)**.** *If A is a Noetherian ring then so is the polynomial ring $A[x]$.*

Proof. Let $I \lhd A[x]$ be an ideal which is not finitely generated. Then let f_1 be an element of minimal degree in I, f_2 be an element of minimal degree in $I \setminus (f_1)$, f_3 be an element of minimal degree in $I \setminus (f_1, f_2)$, and so on (we can continue this forever by virtue of the non-finitely-generated nature of I). Let a_j be the leading coefficient of f_j, so $(a_1, a_2, \dots) \lhd A$ is generated by $(a_1, \dots, a_m)$ for some m. In particular, $a_{m+1} = \sum_{j=1}^m b_j a_j$ for some $b_j \in A$.

Notice that

$$g = \sum_{j=1}^{m} b_j f_j x^{\deg f_{m+1} - \deg f_j} \in (f_1, \dots, f_m)$$

is well-defined ($\deg f_{m+1} - \deg f_j$ is nonnegative since f_j was chosen with $\deg f_j \leq \deg f_{m+1}$) and has the same leading coefficient and degree as f_{m+1}. Yet $f_{m+1} - g$ is not in $(f_1, \dots, f_m)$; if it was, then f_{m+1} would be in $(f_1, \dots, f_m)$, a contradiction. But $f_{m+1} - g$ is in I and has strictly smaller degree than f_{m+1}, a contradiction with our choice of f_{m+1}. This tells us that our initial assumption, that we could choose an ideal which was not finitely generated, was wrong, so we're done. □

Corollary 52.1. *If A is a Noetherian ring then so is $A[x_1, \dots, x_n]$.*

Proof. This follows trivially by induction. □

Corollary 52.2. *If A is a Noetherian ring, then any finitely generated A-algebra is Noetherian.*

Proof. Let B be a finitely-generated A-algebra. By hypothesis, $B \simeq A[x_1, \dots, x_n]/I$ for some ideal $I \lhd A[x_1, \dots, x_n]$. The result follows by first applying Corollary 52.1 and then Corollary 51.1. □

Corollary 52.3. *For any field k, $k[x_1, \dots, x_n]$ is a Noetherian ring.*

Proof. This is immediate from Corollary 52.1 and the fact that all fields are Noetherian, since the only ideals in a field are the zero ideal and the field itself, which are generated by 0 and 1 respectively. □

3 Finite Extensions

Definition 53 (Algebraic and Integral Elements)**.** If $k \subseteq K$ is a field extension, an element $y \in K$ is *algebraic over k* if it satisfies an algebraic dependence $a_n y^n + \cdots + a_1 y + a_0 = 0$. If, furthermore, y satisfies a monic algebraic dependence $y^n + \cdots + a_1 y + a_0 = 0$, we say that y is *integral over k*.

Definition 54 (Algebra)**.** If A is a ring, then an *A-algebra B* is a ring B with a give ring homomorphism $\varphi : A \to B$. In this case, B is an A-module, with multiplication $a \cdot b$ defined as $\varphi(a)b$.

One naturally generalizes the notions of an algebraic or integral element of B over A: $y \in B$ is algebraic over A if there exists a polynomial $f(Y) = a_n Y^n + a_{n-1} Y^{n-1} + \cdots + a_0 \in A'[Y]$ such that $f(y) = 0$ (where $A' = \varphi(A)$). Similarly, $y \in B$ is integral over A if there exists a monic polynomial $f(Y) = Y^n + a_{n-1} Y^{n-1} + \cdots + a_0 \in A'[Y]$ such that $f(y) = 0$.

Definition 55 (Finite, Algebraic, and Integral Algebras)**.** Let B be an A-algebra. Then B is a *finite A-algebra* if it is finite as an A-module. An algebra B is *algebraic* over A if every $b \in B$ is algebraic over A, and it is *integral* over A if every $b \in B$ is integral over A.

Proposition 56 (Facts About Algebras Pt. 1)**.** *Let B be an A-algebra and $y \in B$. Then the following are equivalent:*

1. *y is integral over A.*

2. *If $A' = \varphi(A)$, then the algebra $A'[y]$ is finite over A.*
3. *There exists an A-subalgebra $C \subseteq B$ such that $A'[y] \subseteq C$ and C is finite over A.*

Proof. **1** implies **2** because, if y satisfies integral relation, then $A'[y]$ is generated by $1, y, \dots, y^{n-1}$ (where n is the degree of the polynomial). It's trivial to notice that **2** implies **3**. Finally, **3** implies **3** because we can use the A-module homomorphism $\mu_y : C \to C$ defined by multiplication by y (since C is a finite A-module), so we get a relation

$$\mu_y^n + a_{n-1}\mu_y^{n-1} + \cdots + a_0 = 0$$

Then, by plugging in 1 to μ_y, we get an integral relation, as desired. □

Proposition 57 (Facts About Algebras Pt. 2)**.** *Let B be an A-algebra*

1. *If $A \subseteq B \subseteq C$ are extension rings such that C is a finite B-algebra and B a finite A-algebra, then C is finite over A.*
2. *If $y_1, \dots, y_m \in B$ are integral over A¡ then $A[y_1, \dots, y_m]$ is finite over A, so in particular, every $f \in A[y_1, \dots, y_m]$ is integral over A.*
3. *If $A \subseteq B \subseteq C$ with C integral over B and B integral over A, then C is integral over A.*
4. *The subset $\widetilde{A} = \{y \in B \mid y \text{ is an integral over } A\}$ is a subring of B; moreover, if $y \in B$ is integral over $\widetilde{A}$ then $y \in \widetilde{A}$, so $\widetilde{\widetilde{A}} = \widetilde{A}$.*

Proof. **1** is trivial (it is proven the same way as for field extensions). **2** follows by induction using Proposition 56 and (a). To prove **3**, one can constructs a monic polynomial $z^n + b_{n-1}z^{n-1} + \cdots + b_0 = 0$ for $z \in C$. Yet since each b_i is integral over A, $A \subseteq A[b_0, \dots, b_{n-1}] \subseteq A[b_0, \dots, b_{n-1}, z]$ is a sequence of finite extensions (hence finite), so z belongs to a finite A-algebra and is integral by Proposition 56. The first part of **4** follows from noticing that if $\alpha, \beta \in \widetilde{A}$, then $\alpha \pm \beta$ and $\alpha\beta$ are elements of $A[\alpha, \beta]$, which by **2** is finite (and thus integral) over A. The second part of **4** is obvious by **3**. □

3.1 Integral Closures

Definition 58 (Integral Closure)**.** The ring $\widetilde{A}$ is called the *integral closure of A in B*. If $A = \widetilde{A}$, then A is *integrally closed* in B. An integral domain A is *integrally closed* if it's integrally closed in $\operatorname{Frac} A$. The integral closure of an integral domain A in $\operatorname{Frac} A$ is called the *integral closure of A*.

Here, we see links to algebraic number theory and algebraic geometry. Firstly, a *number field* is a finite field extension $\mathbb{Q} \subseteq K$. Then the *ring of integers $\mathcal{O}_K$* of K is the integral closure of $\mathbb{Z}$ in K. This is a hugely important concept in algebraic number theory. Suppose k is an algebraically closed field, $f \in k[X, Y]$ an irreducible polynomial, and $C \subseteq k^2$ is the plane curve defined by $f(X, Y) = 0$. Then $A = k[X, Y]/(f) = k[C]$ is the ring of polynomial functions on C.

We say that C is *singular at P* if $(\partial f/\partial x)(P) = 0$ and $(\partial f/\partial y)(P) = 0$ (and, of course, C is nonsingular if it is not singular at any point). This is a very important fact, and it is critical towards algebraic geometry. Interestingly, A is integrally closed if and only if C is nonsingular! In fact, an integral closure of A corresponds precisely to a resolution of singularities!

3.2 Noether Normalization

Definition 59 (Algebraic Independence)**.** Suppose that k is a field and A is a k-algebra. Then elements $y_1, \dots, y_n \in A$ are *algebraically independent over k* if the natural surjection $k[Y_1, \dots, Y_n] \to k[y_1, \dots, y_n]$ is an isomorphism. In particular, there are no nonzero polynomial relations $F(y_1, \dots, y_n) = 0$ with coefficients in k.

Our proof of Noether Normalization, which is used to prove the Nullstellensatz, is adapted from here.

First, we begin with a technical lemma which outlines a useful automorphism of polynomial rings:

Lemma 60. *Suppose that k is a field and $f \in k[x_1, \dots, x_n]$ is a nonzero polynomial in n variables over f. Let N be an integer greater than* $\deg(f)$*. Now define $\phi : k[x_1, \dots, x_n] \to k[x_1, \dots, x_n]$ to be the k-algebra automorphism given as follows:*

$$x_1 \mapsto x_1 + x_n^N \qquad x_2 \mapsto x_2 + x_n^{N^2} \qquad \cdots \qquad x_{n-1} \mapsto x_{n-1} + x_n^{N^{n-1}} \qquad x_n \mapsto x_n.$$

Then $\phi(f)$ is equal to a nonzero scalar of k times a polynomial g which is monic in x_n when considered as a polynomial in one variable over $k[x_1, \dots, x_{n-1}]$. That is, the term of $\phi(f)$ in which x_n appears to the highest power has the form cx_n^m for some $c \in k^\times$.

Proof. First simplify f by combining like terms. Then, consider any nonzero monomial $cx_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ in f (note that $c \in k^\times$). Then the image of this monomial under ϕ is

$$\phi(cx_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}) = (x_1 + x_n^N)^{a_1}(x_2 + a_n^{N^2})_2^a \cdots (x_{n-1} + x_n^{N^{n-1}})x_n^{a_n}.$$

When expanded, the term of this polynomial in which x_n appears to the highest power is plainly equal to $c(x_n^N)^{a_1}(x_n^{N^2})^{a_2}\cdots(x_n^{N^{n-1}})^{a_{n-1}}x_n^{a_n} = cx_n^{a_n+a_1N+a_2N^2+\cdots+a_{n-1}N^{n-1}} = cx_n^m$.

Now, $N > \deg(f)$ implies $N > a_1, \dots, a_n$. Now take any two distinct monomials f_1, f_2 of f (recall that we have combined like terms, so the powers of $x_1, \dots, x_n$ cannot be the same in both monomials). Since any integer has a unique base N representation, the terms of $\phi(f_1)$ and $\phi(f_2)$ in which x_n appears to the highest power must have different degree. In other words, there is a unique nonzero monomial of f whose image has the term with the strictly greatest power of x_n, and said term has the form cx_n^m for some $c \in k^\times$. □

Lemma 61 (Noether Normalization Lemma)**.** *Let k be a field and A a finitely-generated k-algebra. Then, there are elements $z_1, \dots, z_m \in A$ such that $z_1, \dots, z_m$ are algebraically independent over k, and A is finite (in particular integral) over $k[z_1, \dots, z_m]$.*

Proof. We will use induction on the number n of generators of A over k. Now, in the base case $n = 0$, $A = k$ and the result is trivial. For the inductive step, suppose that $n > 0$ and that the result holds whenever the number of generators is less than n. Let $y_1, \dots, y_n$ generate A over k. If the y_i are algebraically independent over k, then we may assign $z_i = y_i$ and we are done.

On the other hand, suppose that the y_i are not algebraically independent over k. Then there is a nonzero polynomial $f \in k[x_1, \dots, x_n]$ such that $f(y_1, \dots, y_n) = 0$. Now, define $y_1' = y_1 - y_n^N, \dots, y_{n-1}' = y_{n-1} - y_n^{N^{n-1}}$, and $y_n' = y_n$, where $N > \deg(f)$; these elements also generate A over k. Now, recalling how ϕ was defined in Lemma 60, notice that $y_1, \dots, y_n$ satisfy the polynomial $\phi(f) = g$. By Lemma 60, by replacing g by $c^{-1}g$, we may assume that g is monic in x_n with coefficients in $k[x_1, \dots, x_{n-1}]$. Therefore y_n' is integral over $k[x_1, \dots, x_{n-1}]$, so $A = k[y_1', \dots, y_n']$ is a finite $k[y_1', \dots, y_{n-1}']$-module. But then, by the inductive hypothesis, there exist algebraically independent $z_1, \dots, z_m \in k[y_1', \dots, y_{n-1}']$ such that $k[y_1', \dots, y_{n-1}']$ is a finite $k[z_1, \dots, z_m]$-module. But then A is a finite $k[z_1, \dots, z_m]$-module, so we are done. □

3.3 Zariski's Lemma

Proposition 62 (Integral Extension of Integral Domains)**.** *Let $A \subseteq B$ be an integral extension of integral domains. Then A is a field if and only if B is a field.*

Proof. Assume that A is a field and take $0 \neq x \in B$. Then there is a monic relation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ with $a_i \in A$. We may assume that $a_0 \neq 0$. Now, A is a field, therefore

$$x^{-1} = -a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_2x + a_1) \in B$$

so B is a field. Similarly, assume that B is a field and $0 \neq x \in A$. Then $x^{-1} \in B$, so x^{-1} is integral over A. Then there is a relation of the form

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

whence $x^{-1} = x^{-1} = -a_{n-1} - a_{n-2}x - \cdots - x^{n-1}a_0 \in A$, so A is indeed a field, as desired. □

Lemma 63 (Zariski's Lemma)**.** *If L/k be a field extension such that L is a finitely-generated k-algebra. Then L/k is a finite field extension.*

Proof. By Noether's Normalization Lemma, there exists an injective morphism $\phi : k[z_1, \ldots, z_r] \hookrightarrow L$. In particular, L is finite over $k[z_1, \ldots, z_r]$, so it is integral over $k[z_1, \ldots, z_r]$. By Proposition 62, since L and $k[z_1, \ldots, z_r]$ are both integral domains, L is a field if and only if $k[z_1, \ldots, z_r]$ is a field. Yet $k[z_1, \ldots, z_r]$ is a field if and only if $r = 0$, so L is finite over k and we are done. □

4 The Nullstellensatz and the Prime Spectrum

Definition 64 (Affine n-Space)**.** The *affine n-space* over a field k is the underlying set of k^n: that is,

$$\mathbb{A}^n_k = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in k\}$$

Definition 65 (Evaluating Polynomials)**.** Suppose that $P = (a_1, \ldots, a_n) \in \mathbb{A}^n_k$. Then ε_P is the k-algebra homomorphism $k[x_1, \ldots, x_n] \to k$ given by fixing k and sending $x_i \to a_i$ for each $i \in \{1, \ldots, n\}$. Furthermore, if $f \in k[x_1, \ldots, x_n]$, then we denote $\varepsilon_P(f)$ by $f(P)$ and say this is f *evaluated at* P.

Definition 66 (Algebraic Sets)**.** Let k be a field. Then an *algebraic set* in $\mathbb{A}^n_k$ is a subset of the form

$$V(J) = \{P \in \mathbb{A}^n_k \mid f(P) = 0 \text{ for all } f \in J\}$$

where $J \subseteq k[x_1, \ldots, x_n]$ is an arbitrary subset. $V(J)$ is called *the zero set* of J.

Ostensibly, it looks like to understand algebraic sets in $\mathbb{A}^n_k$ we must consider the zero set of any arbitrary set in $k[x_1, \ldots, x_n]$. Yet this is not the case: it's easy to prove that $V(J) = V((J))$ (where (J) is the ideal generated by J). Furthermore, by Corollary 52.3, polynomial rings are Noetherian, so (J) is finitely generated. Thus, any algebraic set is the zero set of a finite number of polynomials.

Definition 67 (Ideals of Affine Sets)**.** Let k be a field and $X \subseteq \mathbb{A}^n_k$ an arbitrary set. Then $I(X)$ is the set of polynomials in $k[x_1, \ldots, x_n]$ that vanish on all points of X, i.e.,

$$I(S) = \{f \in k[x_1, \ldots, x_n] \mid f(P) = 0 \text{ for all } P \in X\}$$

This is not only an ideal (easy to check), but a radical ideal, since $f^m(P) = 0 \Rightarrow f(P) = 0$.

Proposition 68 (Properties of The Zero Set and Ideal Operators)**.**

1. $J_1 \subseteq J_2 \subseteq k[x_1, \ldots, x_n] \Rightarrow V(J_2) \subseteq V(J_1)$
2. $X_1 \subseteq X_2 \subseteq \mathbb{A}^n_k \Rightarrow I(X_2) \subseteq I(X_1)$
3. *If $X_1, X_2 \subseteq \mathbb{A}^n_k$, then $I(X_1 \cup X_2) = I(X_1) \cap I(X_2)$.*
4. *If $J_1, J_2 \lhd k[x_1, \ldots, x_n]$, then $V(J_1J_2) = V(J_1) \cup V(J_2)$.*
5. *For any $X \subseteq \mathbb{A}^n_k$, $X \subseteq V(I(X))$; indeed, $V(I(X))$ is the smallest algebraic set containing X.*

6. *In particular, if X is an algebraic set, $X = V(I(X))$.*
7. *$J \subseteq I(V(J))$. Furthermore, $I(V(J))$ is a radical ideal, so $\sqrt{J} \subseteq I(V(J))$.*

Proof. **1** follows because all polynomials in J_1 vanish on any point that all polynomials in the larger set J_2 vanish on. **2** follows because any polynomials that vanish on X_2 vanish on the smaller set X_1.

For **3**, suppose that $x \in V(J_1) \cup V(J_2)$ and f is any polynomial in $J_1 J_2$. Then $f = p_i p_j$ for some $p_i \in J_1$ and $p_j \in J_1$. In particular, since either $p_i \in J_1$ vanishes on x or $p_i \in J_2$ vanishes on x, $p_i p_j$ vanishes on x so $x \in V(J_1 J_2)$. This implies that $V(J_1) \cup V(J_2) \subseteq V(J_1 J_2)$. Conversely, suppose that $x \in V(J_1 J_2)$. If there exist $p_i \in J_1$ *and* $p_j \in J_2$ such that p_i and p_j both do not vanish on x, then $p_i p_j \in J_1 J_2$ does not vanish on x, a contradiction. Thus, either $x \in V(I)$ or $x \in V(J)$, which implies that $x \in V(I) \cup V(J)$ and allows us to conclude that $V(J_1 J_2) \subseteq V(J_1) \cup V(J_2)$. This, combined with our earlier result, gives $V(J_1 J_2) = V(J_1) \cup V(J_2)$.

$I(X_1 \cup X_2)$ is the set of polynomials which vanish on all points in X_1 and X_2; clearly, this is the intersection of the set of polynomials which vanish on all points in X_1 and the set of polynomials which vanish on all points in X_2. Thus $I(X_1 \cup X_2) = I(X_1) \cap I(X_2)$.

The first part of **5** is the tautology "the set of all polynomials that vanish on X vanishes on X". The second part is simple bashing, and it means **6** follows instantly. The first part of **7** is the tautology "all polynomials in J are in the set of all polynomials that vanish on the set of points that J vanishes on", and the second part follows from the fact that $\sqrt{J}$ is the smallest radical ideal containing J. □

4.1 The Algebro-Geometric Dictionary

For the rest of this section, assume that k is algebraically closed. In particular, any finite extensions of k (since such an extension is algebraic) will be equal to k itself. In this context, we can further develop our link between geometric sets in affine space and algebraic ideals in polynomial rings.

Proposition 69 (The Weak Nullstellensatz)**.** *Maximal ideals of $k[x_1, \dots, x_n]$ correspond precisely to points of $\mathbb{A}_k^n$. More precisely, every maximal ideal of $A = k[x_1, \dots, x_n]$ is of the form*

$$\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n) \text{ for some } a_1, \dots, a_n \in k$$

and every ideal of the form $(x_1 - a_1, \dots, x_n - a_n)$ for some $a_1, \dots, a_n \in k$ is maximal.

Proof. Clearly every ideal of the form $\mathfrak{a} = (x_1 - a_1, \dots, x_n - a_n)$ for some $a_1, \dots, a_n \in k$ is maximal, since $k[x_1, \dots, x_n]/\mathfrak{a} \simeq k$, a field (this isomorphism is obvious since taking said quotient is like "replacing x_i with a_i"). On the other hand, $k[x_1, \dots, x_n]/\mathfrak{m}$ is a finitely generated k-algebra for any ideal $\mathfrak{m} \lhd k[x_1, \dots, x_n]$. If, furthermore, $\mathfrak{m}$ is maximal, $K = k[x_1, \dots, x_n]/\mathfrak{m}$ is a field, so by Zariski's Lemma (see 63), K is a finite extension over k. Yet k is algebraically closed, so $K = k$.

By taking a_i to be the image of x_i for each $i \in \{1, \dots, n\}$, we see that $(x_1 - a_1, \dots, x_n - a_n) \subseteq \mathfrak{m}$. Yet we already know that $(x_1 - a_1, \dots, x_n - a_n)$ is maximal, so $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$, as desired. □

We can use this result to get a condition for a common zero of a set of polynomials:

Corollary 69.1. *If $J \lhd k[x_1, \dots, x_n]$, then J is equal to $k[x_1, \dots, x_n]$ if and only if $V(J) = \varnothing$.*

Proof. If J is a proper ideal, it is contained in a maximal ideal $\mathfrak{m}$. Then $V(\mathfrak{m}) \subseteq V(J)$, but $V(\mathfrak{m})$ is a single point (by the Weak Nullstellensatz) so $V(J)$ is nonempty. On the other hand, if J is not a proper ideal (it is the whole ring), then $V(J) = \varnothing$ since the polynomial 1 vanishes nowhere. □

Now that we have a correspondence $\mathbb{A}_k^n \leftrightarrow \text{m-Spec}\, k[x_1, \dots, x_n]$, we can generalize this result to learn more about maximal ideals in related commutative rings.

Corollary 69.2. *Suppose that $A = k[x_1, \dots, x_n]/J$ is a finitely generated k-algebra. Write $\overline{x_i}$ to mean the image of x_i in A. Then, there is a one-to-one correspondence*

$$V(J) \leftrightarrow \text{m-Spec}(A) \text{ given by } (a_1, \dots, a_n) \leftrightarrow (x_1 - a_1, \dots, x_n - a_n).$$

Proof. This follows immediately from the fact that the maximal ideals of A correspond precisely to the maximal ideals of $k[x_1, \dots, x_n]$ containing J, and an maximal ideal $\mathfrak{m}$ can only contain J if $V(\mathfrak{m}) = \{(a_1, \dots, a_n)\} \subseteq V(J)$ (see Proposition 68). □

Corollary 69.3 (Multi-Dimensional Fundamental Theorem of Algebra)**.** *If k is an a algebraically closed field and $f \in k[x_1, \dots, x_n]$ is nonconstant, then $\exists \lambda_1, \dots, \lambda_n \in k$ such that $f(\lambda_1, \dots, \lambda_n) = 0$.*

Proof. If f is nonconstant, it is not a unit, so it is contained in a maximal ideal $\mathfrak{m} = (x_1 - \lambda_1, \dots, x_n - \lambda_n)$. In particular, f is a linear combination of polynomials which vanish when $\lambda_1, \dots, \lambda_n$ are plugged in, so it also vanishes when $\lambda_1, \dots, \lambda_n$ are plugged in. □

4.2 Hilbert's Nullstellensatz

Notice that this correspondence misses "powers". For example, given $(x) \neq (x^2) \lhd k[x]$, $V((x)) = V((x^2)) \subseteq \mathbb{A}^1_k$. In fact, more generally, this correspondence *never* "catches" powers:

Proposition 70. *If $J \lhd k[x_1, \dots, x_n]$, then $V(J) = V(\sqrt{J})$.*

Hilbert's Nullstellensatz says this is the main issue:

Theorem 71 (Hilbert's Nullstellensatz)**.** *For any $J \lhd k[x_1, \dots, x_n]$, $I(V(J)) = \sqrt{J}$.*

Proof. As discussed in Proposition 68, $\sqrt{J} \subseteq I(V(J))$. Thus it suffices to show that $I(V(J)) \subseteq \sqrt{J}$; more specifically, we will take some $g \in I(V(J))$ and show that $g^m \in J$ for some $m \in \mathbb{N}$. To do this, we will use Rabinowitsch's trick, which goes as follows.

Let $f_1, \dots, f_m$ generate J. Then $f_1, \dots, f_m, x_{n+1}g - 1$ have no common zeros in $\mathbb{A}^{n+1}_k$. This is because, in $V(J)$, the former polynomials are all 0, but the last polynomial is -1. But all of $f_1, \dots, f_m$ cannot vanish outside $V(J)$ (by definition), so there are no common zeros outside of $V(J)$ either. Thus, by Proposition 69.1, these polynomials generate the entirety of $k[x_1, \dots, x_n, x_{n+1}]$. In particular:

$$1 = p_1 f_1 + \cdots + p_m f_m + p_{m+1}(x_{n+1}g - 1)$$

for some $p_1, \dots, p_{m+1} \in k[x_1, \dots, x_{n+1}]$. Under the homomorphism $k[x_1, \dots, x_{n+1}] \to k(x_1, \dots, x_n)$ given by fixing $k[x_1, \dots, x_n]$ and sending $x_{n+1} \mapsto g^{-1}$, we see that that

$$1 = p_1(x_1, \dots, x_n, g^{-1}) f_1 + \cdots + p_m(x_1, \dots, x_n, g^{-1}) f_m$$

whence, by letting j be the largest power to which g^{-1} appears in any of the f_i, we see that

$$g^j = q_1 f_1 + \cdots + q_m f_m \in J$$

for some $q_1, \dots, q_m \in k[x_1, \dots, x_n]$, as desired. □

Corollary 71.1. *There is a 1-to-1 inclusion-reversing correspondence between algebraic sets in $\mathbb{A}^n_k$ and radical ideals in $k[x_1, \dots, x_n]$. This correspondence is given by $X \mapsto I(X)$ in one direction and $Z(J) \mapsto J$ in the other.*

Corollary 71.2. *$I(V(I(X))) = I(X)$ and $V(I(V(J))) = V(J)$.*

Proof. $I(V(I(X)) = \sqrt{I(X)}$ but $I(X)$ is a radical ideal so $I(V(I(X))) = \sqrt{I(X)} = I(X)$. Similarly, $V(I(V(J))) = V(\sqrt{J}) = V(J)$, as desired. □

4.3 Algebraic Varieties

Definition 72 (Variety)**.** An algebraic set $X \subseteq \mathbb{A}_k^n$ is an *(algebraic) variety* if it is irreducible: that is, if it is nonempty and not the union of two proper sub-algebraic sets. Explicitly, we require that

$$X = X_1 \cup X_2 \text{ for algebraic sets } X_1, X_2 \Rightarrow X = X_1 \text{ or } X = X_2.$$

Proposition 73. *An algebraic set X is a variety if and only if $I(X)$ is prime.*

Proof. Let $J = I(X)$; if J is not prime, then there exist $f, g \notin J$ such that $fg \in J$. But then $J_1 = (J, f)$ and $J_2 = (J, g)$ are such that $V(J_1) \subsetneq X$ and $V(J_2) \subsetneq X$ (since $f \notin I(X)$), but $X = V(J_1) \cup V(J_2)$, so X is reducible. The converse is virtually identical. □

Corollary 73.1. *There is a* 1*-to-*1 *inclusion-reversing correspondence between algebraic varieties in $\mathbb{A}_k^n$ and prime ideals in $k[x_1, \ldots, x_n]$. This correspondence* $\operatorname{Spec} k[x_1, \ldots, x_n] \leftrightarrow \{$*varieties in* $\mathbb{A}_k^n\}$ *is given by $X \mapsto I(X)$ in one direction and $Z(J) \mapsto J$ in the other.*

Just as we used this result to understand maximal ideals in more general classes of rings, we will use this result to understand prime ideals in a more general class of rings.

Corollary 73.2. *Suppose that $A = k[x_1, \ldots, x_n]/J$ is a finitely generated k-algebra. Write $\overline{x_i}$ to mean the image of x_i in A. Then, there is a one-to-one correspondence*

$$\operatorname{Spec}(A) \leftrightarrow \textit{subvarieties of } X \subseteq V(J)$$

4.4 A Refresher on Irreducible Topological Spaces

Definition 74 (Irreducible Topological Space)**.** A non-empty topological space X is called *irreducible* if X cannot be decomposed into two proper closed subsets. Precisely, this means that if $X_1, X_2 \subseteq X$ are closed in X and $X_1 \cap X_2$, then either $X = X_1$ or $X = X_2$.

Proposition 75. *An irreducible topological space X is Hausdorff if and only if it is a single point.*

Proof. Suppose X is a single point. Then clearly it is irreducible and Hausdorff. Otherwise, suppose X is an space with at least 2 points (say p and q). For the sake of contradiction, assume X is Hausdorff. By hypothesis, we can take choose p-neighborhood P and q-neighborhood Q such that $P \cap Q = \varnothing$. In this case, $(X \setminus P)$ and $(X \setminus Q)$ are closed sets (their complements are open). Neither of $(X \setminus P)$ and $(X \setminus Q)$ are equal to X (they don't contain p and q, respectively). Finally, $(X \setminus P) \cup (X \setminus Q) = X \setminus (P \cap Q) = X$, so X is not irreducible. □

Proposition 76. *Suppose X is an irreducible topological space and $\varnothing \neq U \subseteq X$ is a nonempty open subset. Then U is irreducible as its own topological space.*

Proof. Suppose U is not irreducible in X, so $U = V_1 \cup V_2$ for closed sets $V_1, V_2 \subseteq U$. By the definition of the subspace topology, we may conclude that $U = (W_1 \cap U) \cup (W_2 \cap U)$ for some closed sets $W_1, W_2 \in X$. Yet, since U is nonempty and $U \not\subseteq W_1$, $W_1 \cup (X \setminus U)$ is a proper closed subset of X. Similarly, $(W_2 \cup (X \setminus U))$ is a proper closed subset of X. Yet $(W_1 \cup (X \setminus U)) \cup (W_2 \cup (X \setminus U)) = X$ is a contradiction with the hypothesis that X is irreducible. Thus U is irreducible in X. □

Proposition 77. *Conversely, if X is an irreducible topological space contained in another topological space Y, then $\overline{X}$ (the closure of X) is irreducible in Y.*

Proof. $X \subseteq Y$ is irreducible if and only if any two nonempty open subsets in X intersect. Since the open subsets in X are the same as the open subsets in $\overline{X}$ (its closure in Y), $\overline{X}$ is still irreducible. □

4.5 The Zariski Topology on Affine Space

Proposition 78. *The algebraic sets $X \subseteq \mathbb{A}_k^n$ satisfy the axioms for closed sets of a topology.*

Proof. $\varnothing$ is the algebraic set $V(1)$ and $\mathbb{A}_k^n$ is the algebraic set $V(0)$. On the other hand, as discussed earlier, $V(I) \cup V(J) = V(I \cap J) = V(IJ)$ (so the union of a finite number of algebraic sets is an algebraic set). Similarly, if $X_i = V(J_i)$ is any family of algebraic sets, then their intersection $\bigcap X_i$ is the algebraic set $V(\sum J_i)$. □

Definition 79 (Zariski Topology)**.** As justified by Proposition 78, we can give $\mathbb{A}_k^n$ a topology (called *the Zariski topology*) by defining the algebraic sets of $\mathbb{A}_k^n$ to be the closed sets.

Proposition 80. $\mathbb{A}_k^n$ *(with the Zariski topology) is irreducible for any n.*

Proof. Any algebraic set $Z(f_1, \dots, f_n)$ is contained in $Z(f_1)$, which is a hypersurface in $\mathbb{A}_k^n$. Intuitively, if two such hypersurfaces cover all of $\mathbb{A}_k^n$, then one or the other must be $\mathbb{A}_k^n$. □

Corollary 80.1. $\mathbb{A}_k^n$ *(with the Zariski topology) is not Hausdorff if $n > 0$.*

Proof. $\mathbb{A}_k^n$ is non-Hausdorff is because it is an irreducible space with multiple points. Indeed, it is extremely non-Hausdorff since any two nonempty open sets intersect. □

The Zariski topology is often cited as an example of a topological space which is extremely interesting despite the fact that it isn't Hausdorff, but its usefulness goes far beyond just being an example.

Definition 81 (Irreducible Decomposition)**.** If X is a topological space, then a decomposition of X of the form

$$X = \bigcup_{\lambda \in \Lambda} X_\lambda$$

where the X_λ are irreducible and $X_\alpha \not\subseteq X_\beta$ for any $\alpha, \beta \in \Lambda$ with $\alpha \neq \beta$ (this is called the *essentiality condition*) is an *irreducible decomposition of* X with *irreducible components* $\{X_\lambda\}_{\lambda \in \Lambda}$.

This definition is a general topological one, but it does have special meaning when we are discussing $\mathbb{A}_k^n$ under the Zariski topology. In particular, an irreducible decomposition of X corresponds to a way of writing $I(X)$ as the intersection of prime ideals $I(X_\lambda)$.

Definition 82 (Noetherian Topological Spaces)**.** Let X be a topological space. Then X is *Noetherian* if any descending sequence of closed sets $X \supseteq X_1 \supseteq X_2 \dots$ eventually stabilizes.

Proposition 83. $\mathbb{A}_k^n$ *(with the Zariski toplogy) is Noetherian.*

Proof. A descending chain of closed sets corresponds to an ascending chain of ideals in $k[x_1, \dots, x_n]$. Since $k[x_1, \dots, x_n]$ is Noetherian, the ideal chain stabilizes, so the closed set chain stabilizes. □

Lemma 84. *If an irreducible set Z is in the union $X_1 \cup \cdots \cup X_r$ of some irreducible closed sets $X_1, \dots, X_r$, then $Z \subseteq X_j$ for some $j \in \{1, \dots, r\}$.*

Proof. In this case, $X_i \cap Z$ is a closed set for each i. In particular, $Z = (X_1 \cap Z) \cup \cdots \cup (X_r \cap Z)$, so since Z is irreducible, $Z = X_i \cap Z$ for some i, implying that $Z \subseteq X_i$, as desired. □

Theorem 85. *Assume X is a Noetherian topological space and $\varnothing \neq Y \subseteq X$ is closed. Then $Y = Y_1 \cup \cdots \cup Y_r$ where the Y_i are irreducible closed subsets. If in addition $Y_i \subsetneq Y_j$ for all $i \neq j$, then the $Y_1, \dots, Y_r$ are unique up to permutation and are called the irreducible components of Y.*

Proof. Let $\mathscr{S}$ be the set of subsets of X that cannot be written as the union of irreducible subsets. If $\mathscr{S} = \varnothing$, we are done, so assume it is nonempty. Since X is Noetherian, $\mathscr{S}$ has a minimal element $Y \in \mathscr{S}$. Yet Y cannot be irreducible (else it is the union of irreducible subsets), so we can write $Y' \cup Y'' = Y$. By the minimality of Y, both Y' and Y'' are not in $\mathscr{S}$, so they can be written as the union of irreducible subsets. Yet then Y is the union of these two unions, a contradiction.

Now assume the extra condition and suppose there are two such decompositions $Y = Y_1 \cup \cdots \cup Y_r = Y'_{1'} \cup \cdots \cup Y'_{r'}$. Then, for any i, $Y_i \in Y'_{1'} \cup \cdots \cup Y'_{r'}$, so by the above Lemma, $Y_i \subseteq Y'_j$ for some j. By identical logic, $Y'_j \subseteq Y_k$ for some k. Thus $Y_i \subseteq Y'_j \subseteq Y_k$, so by the extra condition $Y_i = Y'_j = Y_k$. By repeating this argument, we see that the irreducible sets in the first decomposition are identical, up to some permutation, to the irreducible sets in the second decomposition. □

Corollary 85.1. *For any algebraic set $X \subseteq \mathbb{A}^n_k$, $X = X_1 \cup \cdots \cup X_r$ (where the X_i are algebraic varieties) in a unique way (up to permutation) if we require $X_i \not\subseteq X_j$ for all $i \neq j$.*

Proof. $\mathbb{A}^n_k$ is a Noetherian topological space. □

Corollary 85.2. *Suppose B is a finitely generated k-algebra and $J \lhd B$. Then $\sqrt{J} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ for some prime ideals $\mathfrak{p}_i \lhd_{\text{pr}} B$. Furthermore, this decomposition is unique up to permutation if we require $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for $i \neq j$.*

Proof. If B is a finitely generated k-algebra, then $B = k[x_1, \ldots, x_n]/I$ for some $I \lhd k[x_1, \ldots, x_n]$. Let $\overline{J} \lhd k[x_1, \ldots, x_n]$ be the preimage in $k[x_1, \ldots, x_n]$ of $J \lhd B$. Now consider the irreducible decomposition $Z(\overline{J}) = X = X_1 \cup \cdots \cup X_r$ and let $\overline{\mathfrak{p}}_i = I(X_i)$. Then $\sqrt{\overline{J}} = I(X) = \overline{\mathfrak{p}}_1 \cap \cdots \cap \overline{\mathfrak{p}}_r$ (by the Nullstellensatz). Let $\mathfrak{p}_i = \overline{\mathfrak{p}}_i/I$. Then $\sqrt{J} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$, as desired. The uniqueness of this intersection follows through the exact same correspondence. □

4.6 The Zariski Topology on the Prime Spectrum

Recall that the *prime spectrum*, denoted by $\operatorname{Spec} A$, is the set of prime ideals of A.

Proposition 86. *For any ring A, $\operatorname{Spec} A$ can be given a topological structure by assigning the closed sets to be all sets of the form $\mathcal{V}(I) = \{\mathfrak{p} \in \operatorname{Spec} A \mid I \subseteq \mathfrak{p}\}$, where I is an ideal of A.*

Proof. $\mathcal{V}(A) = \varnothing$ and $\mathcal{V}(0) = \operatorname{Spec} A$. Similarly, one can verify that $\bigcap_{\lambda \in \Lambda} \mathcal{V}(I_\alpha) = \mathcal{V}(\sum I_\alpha)$ and

$$\mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1 I_2) = \mathcal{V}(I_1 \cap I_2)$$

□

Definition 87 (Zariski Topology on $\operatorname{Spec} A$)**.** As justified by Proposition 86, $\operatorname{Spec} A$ can be given a topology (also called the *Zariski topology*) by assigning all subsets of the form $\mathcal{V}(I)$ (for some $I \lhd A$) to be the closed sets.

Proposition 88. *For any ring A and ideal $I \lhd A$, $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$.*

Proof. This follows immediately from Corollary 19.1. □

Definition 89 (An Inverse to $\mathcal{V}$)**.** For any $X \subseteq \operatorname{Spec} A$, we define $\mathcal{I}(X)$ to be $\bigcap_{\mathfrak{p} \in X} \mathfrak{p}$.

Proposition 90 (The Nullstellensatz for $\operatorname{Spec} A$)**.** *For any $J \lhd A$, $\mathcal{I}(\mathcal{V}(J)) = \sqrt{J}$.*

Proof. This follows immediately from Proposition 88 and Corollary 19.1. □

Corollary 90.1. *For any ring A, $\mathcal{V}(\_\_)$ and $\mathcal{I}(\_\_)$ offer a one-to-one correspondence between the radical ideals of A and the closed sets of* $\operatorname{Spec} A$.

Proposition 91. *$X = \mathcal{V}(J)$ is an irreducible closed set iff $\sqrt{J} = \mathcal{I}(X) = \mathcal{I}(\mathcal{V}(J))$ is prime.*

Proof. Exactly the same as Proposition 73. □

Proposition 92. *If A is a Noetherian ring, then the topology on* Spec *A is Noetherian.*

Corollary 92.1. *If A is a Noetherian ring and $I \lhd A$, then there are finitely many prime ideals over I that are minimal (with respect to inclusion) over I.*

Corollary 92.2. *If A is a Noetherian ring and $I \lhd A$, then since $\sqrt{I}$ is the intersection of all minimal prime ideals over I, $\sqrt{I}$ is a finite intersection.*

Corollary 92.3. *In particular, a nonzero ring A which is not an integral domain either has nonzero nilpotents or at least* 2 *minimal primes.*

Proof. There are two cases:

1. $0 = \sqrt{0}$. In this case, 0 is the intersection of the minimal primes of A, but since 0 is not a prime ideal (A is not an integral domain), there must be at least 2 minimal primes.
2. $0 \neq \sqrt{0}$. In this case, A has nonzero nilpotent elements, as desired.

The result follows. □

5 Localization and Primary Decomposition

Definition 93 (Ring of Fractions)**.** Let A be a ring and $S \subseteq A$ a multiplicative set (see Def. 10). Then define a relation $\sim$ on $A \times S$ by $(a, s) \sim (b, t)$ if there exists $u \in S$ such that $u(at - bs) = 0$. One can check that $\sim$ is an equivalence relation; we write $\frac{a}{s}$ for the equivalence class of (a, s). Indeed, we get a ring $S^{-1}A = A \times S/\sim$, called the *ring of fractions of A with respect to S*, with operations

$$\frac{a}{s} \pm \frac{b}{t} = \frac{(at \pm bs)}{st} \text{ and } \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Note that A naturally embeds into $S^{-1}A$ by sending $a \mapsto \frac{a}{1}$: we will denote this map by φ.

Problem 94. Prove that $\ker \varphi = \{a \in A \mid \exists s \in S \text{ such that } sa = 0\}$.

Problem 95. Prove that $S^{-1}A = 0$ if and only if $0 \in S$ if and only if S contains a nilpotent element.

Theorem 96 (Universal Mapping Property)**.** *Let $\varphi : A \to S^{-1}A$ be the natural embedding. First, φ takes every element of S to a unit in $S^{-1}A$, and secondly, φ is universal for this process: if $\psi : A \to B$ is a ring homomorphism which maps every element of S to a unit in B, then there exists a unique $\xi : S^{-1}A \to B$ with $\psi = \xi \circ \varphi$.*

Definition 97. Given $f \in A$, define A_f to be $S^{-1}A$ with $S = \{1, f, f^2, \dots\}$ the multiplicative subset of A generated by f. Notice that $A_f = A[x]/(xf - 1)$, since this is akin to adding a new symbol x with the property that $xf = 1$.

Definition 98 (Extension and Restriction)**.** Given a ring homomorphism $\varphi : A \to B$, we define *extension* and *restriction* as so:

1. If $I \lhd A$, the *extension of I* $e(I) = \varphi(I)B = IB$.
2. If $J \lhd B$, the *restriction of J* $r(J) = \varphi^{-1}(J)$.

Lemma 99. *Let A be a ring and $S \subseteq A$ a multiplicative subset.*

1. *For any ideal J of $S^{-1}A$, $e(r(J)) = J$.*

2. *For any ideal I of J, $r(e(I)) = \{a \in A \mid as \in I \text{ for some } s \in S\}$.*

3. *If $\mathfrak{p} \lhd_{\text{pr}} A$, then either $e(\mathfrak{p}) = S^{-1}\mathfrak{p} \lhd_{\text{pr}} S^{-1}A$ (if $\mathfrak{p} \cap S = \varnothing$) or $e(\mathfrak{p}) = S^{-1}\mathfrak{p} = S^{-1}A$.*

Proof.
1: If $\frac{b}{s} \in J$, then $b \in \varphi^{-1}(J)$, so $\frac{b}{s} \in e(r(J))$. Thus $J \subseteq e(r(J))$. The other direction is trivial).
2: If $a \in r(e(I))$, then $\frac{a}{1} = \frac{b}{t} \in S^{-1}A$ for some $b \in I$ and $t \in S$. Now there exists $u \in S$ such that $uta = ub \in I$, so $s = ut \in S$ is such that $sa \in I$, thus $r(e(I))$ is included in the right-hand side. The reverse direction is again trivial.
3: Trivial. □

Corollary 99.1. *There e and r define inverse one-to-one correspondences between ideals of A such that $as \in I \Rightarrow a \in I$ for all $s \in S$ and ideals of $S^{-1}A$. In particular, $S^{-1}A$ is Noetherian if A is Noetherian.*

Corollary 99.2. $r(e(I)) = A \Leftrightarrow e(I) = S^{-1}A \Leftrightarrow I \cap S \neq \varnothing$.

Corollary 99.3. *The natural map $\phi^{-1} : \operatorname{Spec} S^{-1}A \to \operatorname{Spec} A$ (which takes a prime ideal in $S^{-1}A$ to its preimage, which is a prime ideal in A) identifies $\operatorname{Spec} S^{-1}A$ with $\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \cap S = \varnothing\}$. In particular, $\operatorname{Spec} S^{-1}A$ is identified with $\{p \in \operatorname{Spec} A \mid p \cap S = \varnothing\}$.*

Proposition 100. *Localization commutes with taking quotients. Precisely, take a ring A, a proper ideal $\mathfrak{a} \lhd A$, and a multiplicative set $S \subseteq A$. Further let S' be the image of S under the quotient projection $\pi : A \to A/\mathfrak{a}$. Then:*

$$S'^{-1}(A/\mathfrak{a}) \cong \frac{S^{-1}A}{S^{-1}\mathfrak{a}}$$

Proof. Elements in $S'^{-1}(A/\mathfrak{a})$ are of the form $\frac{r+\mathfrak{a}}{s+\mathfrak{a}}$. Elements in $\frac{S^{-1}A}{S^{-1}\mathfrak{a}}$ are of the form $\frac{r}{s} + \mathfrak{a}$. It can be easily verified that the inverse maps

$$\varphi : \frac{S^{-1}A}{S^{-1}\mathfrak{a}} \to S'^{-1}(A/\mathfrak{a}) \text{ given by } \frac{r}{s} + \mathfrak{a} \to \frac{r+\mathfrak{a}}{s+\mathfrak{a}}$$
$$\varphi^{-1} : \frac{S^{-1}A}{S^{-1}\mathfrak{a}} \to S'^{-1}(A/\mathfrak{a}) \text{ given by} \frac{r+\mathfrak{a}}{s+\mathfrak{a}} \to \frac{r}{s} + \mathfrak{a}$$

are both homomorphisms, giving an isomorphism pair, as desired. □

Definition 101 (Localization at Prime Ideal)**.** Given a prime ideal $\mathfrak{p} \lhd A$, we set $S = A \setminus \mathfrak{p}$. Then the localization $S^{-1}A$ is called the *localization of A at $\mathfrak{p}$* and denoted $A_{\mathfrak{p}}$.

Proposition 102. *$A_{\mathfrak{p}}$ is a local ring (see Def. 25) with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$ (that is, the ideal of all fractions with numerator in $\mathfrak{p}$ and denominator in $A \setminus \mathfrak{p}$).*

Proof. Let $\mathfrak{a} \lhd A_{\mathfrak{p}}$ be such that $\mathfrak{a} \not\subseteq \mathfrak{p}A_{\mathfrak{p}}$. Then there is an element $\frac{a}{b} \in \mathfrak{a}$ with $a, b \notin \mathfrak{p}$. But then $\frac{b}{a} \in A_{\mathfrak{p}}$, so $\frac{a}{b}\frac{b}{a} = 1 \in \mathfrak{a}$, whence $\mathfrak{a} = A_{\mathfrak{p}}$. Hence any proper ideal in $A_{\mathfrak{p}}$ is contained in $\mathfrak{p}A_{\mathfrak{p}}$. □

Theorem 103. *There is an isomorphism between $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ and $\kappa(\mathfrak{p})$.*

Proof. Let $S = A \setminus \mathfrak{p}$. Then $S' = (A/\mathfrak{p}) \setminus 0$. But this implies that $\kappa(\mathfrak{p}) = S'^{-1}(A/\mathfrak{p}) \cong \frac{S^{-1}A}{S^{-1}\mathfrak{p}}$ by Prop. 100. But both $\mathfrak{p}A_{\mathfrak{p}}$ and $S^{-1}\mathfrak{p}$ are those fractions in $A_{\mathfrak{p}}$ with numerator in $\mathfrak{p}$, whence $\frac{S^{-1}A}{S^{-1}\mathfrak{p}} = \frac{A_{\mathfrak{p}}}{\mathfrak{p}A_{\mathfrak{p}}}$. □

Problem 104. Let $S \subseteq T$ be multiplicative subsets of a ring A. Write $A' = S^{-1}A$, let $\varphi : A \hookrightarrow A'$ be the natural map, and define $T' = \varphi(T)$. Prove that then $T^{-1}A = T'^{-1}A$. This demonstrates that the composition of two localizations is one large localization.

5.1 Modules of Fractions

Proposition 105. *Let A be a ring and S a multiplicative set of A. Then modules over $S^{-1}A$ can be naturally identified with A-modules M having the property that the multiplication map $\mu_s : M \to M$ (given by $m \mapsto sm$) is bijective for all $s \in S$.*

Proof. If M is an $S^{-1}A$-module, then one can consider it as an A-module by $(a, m) \mapsto (a/1, m)$. It is an easy exercise to see that in this case μ_s is bijective. In the other direction, if M is an A-module such that $\mu_s : M \to M$ is bijective for all $s \in S$, then one can define an action of $S^{-1}A$ on M by setting $(a/s)m = a \cdot \mu_s^{-1}(m)$. Again, it is an easy exercise to prove that this is a well-defined action. □

Definition 106 (Ring of Fractions of Modules)**.** Let M be an A-module and S be a multiplicative set in A. Then *ring of fractions of M with respect to S* is the set $M \times S$ mod the equivalence relation $(x, s) \sim (y, t)$ if $\exists u \in S$ such that $u(tx - sy) = 0$. This is denoted by $S^{-1}M$ and is naturally an $S^{-1}A$-module (thus naturally an A-module). Again, the equivalence class of (x, s) is denoted by $\frac{x}{s}$.

The following section relies on an understanding of functors and tensor products (for example, the knowledge that the tensor product functor is right-exact and the universal property of tensor products), which we do not cover here. It also assumes you know the definition and basic properties of complexes.

Lemma 107. $S^{-1}M \simeq M \otimes_A S^{-1}A$

Proof. It is a simple exercise to check that $S^{-1}M$ satisfies the universal property of tensor products (i.e. for any bilinear morphism $\phi : M \times S^{-1}A \to N$ there exists a unique morphism $\psi : S^{-1}M \to N$ such that $\psi \circ \eta = \phi$ (where η is the natural map $M \times S^{-1}A \to S^{-1}M$). Any two viable tensor products are uniquely isomorphic, so the result follows. □

Lemma 108. *The localization map $S^{-1}(\_\_)$ given by $M \mapsto S^{-1}M$ is a covariant functor.*

Proof. This follows from $S^{-1}(\_\_) = \_\_ \otimes_A S^{-1}A$. Indeed, this demonstrates that A is right-exact. One may also notice that a map $\phi : M \to N$ gives us a map $S^{-1}\phi : S^{-1}M \to S^{-1}N$ given by $\frac{x}{s} \mapsto \frac{\phi(x)}{s}$ and then conclude the result by definition. □

Lemma 109. *The localization map $S^{-1}(\_\_)$ given by $M \mapsto S^{-1}M$ is an exact functor.*

Proof. Let

$$L \overset{\psi}{\to} M \overset{\phi}{\to} N$$

be an exact complex of A-modules (so $\ker \phi = \operatorname{im} \psi$). Then we have a new complex of A-modules

$$S^{-1}L \overset{S^{-1}\psi}{\longrightarrow} S^{-1}M \overset{S^{-1}\phi}{\longrightarrow} S^{-1}N$$

after application of $S^{-1}(\_\_)$. We seek to show that $\ker S^{-1}\phi = \operatorname{im} S^{-1}\psi$. To do this, take $\frac{x}{s}$ such that $S^{-1}\phi(\frac{x}{s}) = \frac{\phi(x)}{s} = 0$ in $S^{-1}N$. By definition, this means $\exists u \in S$ such that $u \cdot \phi(x) = \phi(ux) = 0$. But $\ker \phi = \operatorname{im} \psi$, so there exists $y \in L$ such that $\psi(y) = ux$. Then

$$S^{-1}\psi\left(\frac{y}{us}\right) = \frac{\psi(y)}{us} = \frac{ux}{us} = \frac{x}{s}$$

so $\frac{x}{s} \in \operatorname{im} S^{-1}\psi$ (and $\ker S^{-1}\phi \subseteq \operatorname{im} S^{-1}\psi$). Since the definition of a complex gives us $\ker S^{-1}\phi \supseteq \operatorname{im} S^{-1}\psi$, we may conclude that $\ker S^{-1}\phi = \operatorname{im} S^{-1}\psi$, as desired. □

We can know also conclude many of our earlier results more trivially.

Corollary 109.1. *The localization of a quotient is the quotient of the localization. In other words, $S^{-1}(M/N) = (S^{-1}M)/(S^{-1}N)$.*

Corollary 109.2. *If $\mathfrak{p} \lhd_{pr} A$, then $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \simeq \operatorname{Frac}(A/\mathfrak{p}) \simeq \kappa(\mathfrak{p})$.*

We will now do a similar version of Lemma 3 for modules.

Lemma 110. *Take $N' \subseteq S^{-1}M$ (a $S^{-1}A$-submodule). Let $N \subseteq M$ be the preimage of N' along $M \to S^{-1}M$. Then $N' = S^{-1}N$.*

Proof. Take $\frac{x}{s} \in N'$. Then $\frac{x}{1} = s \cdot \frac{x}{s} \in N'$. But then $x \in N$, thereby showing that $\frac{x}{s} \in S^{-1}N$. This proves us $N' \subseteq S^{-1}N$. Conversely, take $\frac{x}{s} \in S^{-1}N$. Then $x \in N$ (by definition) and hence $\frac{x}{1} \in N'$. But then $\frac{x}{s} = \frac{1}{s} \cdot \frac{x}{1} \in N'$, so $S^{-1}N \subseteq N'$. Combining the two results finishes the proof. □

Corollary 110.1. *If $A \subseteq B$ is a ring extension and $S \subseteq A$ is a multiplicative set, then any $J' \lhd S^{-1}B$ is of the form $S^{-1}J$ for some $J \lhd B$. Furthermore, prime ideals correspond to prime ideals.*

Proof. Clearly the only part that needs proving is the part about prime ideals. But notice $S^{-1}(B/J) \sim (S^{-1}B)/(S^{-1}J)$, so by the fact that a quotient is an integral domain if and only if the divisor is a prime ideal, J and $S^{-1}J$ are either both prime ideals or neither prime ideals. □

This result is similar to the one we started the section with.

Theorem 111 (Universal Property of Ring of Fractions for Modules)**.** *Let A be a ring, S be a multiplicative set, and M, N be A-modules. Assume that all $s \in S$ acts on N as an automorphism (that is, s is invertible on N). Then the natural morphism $\varphi : M \to S^{-1}M$ induces an isomorphism:*

$$\alpha : \operatorname{Hom}_A(S^{-1}M, N) \xrightarrow{\sim} \operatorname{Hom}_A(M, N)$$

Proof. Let $\phi : M \to N$, $\frac{x}{s} \in S^{-1}M$, and choose $y \in N$ to be the unique element with $sy = \phi(x)$. Define $\psi : S^{-1}M \to N$ by $\frac{x}{s} \mapsto y$. To prove ψ is well-defined, suppose that $\frac{x}{s} = \frac{x'}{s'}$ and let $y' \in N$ be such that $s'y' = \phi(x')$. Then there exists $u \in S$ such that $us'x = usx'$, so $us'\phi(x) = s\phi(x')$. But u is invertible on N, $s'sy = s'\phi(x) = s\phi(x') = ss'y'$ and then $y = y'$. Thus ψ is well-defined and α is surjective. But α is also injective: take $\psi : S^{-1}M \to N$ and $\frac{x}{s}$ such that $\alpha(\psi) = 0$. Then $s\psi(\frac{x}{s}) = \psi(x/1) = 0$ whence $\psi(x/s) = 0$. □

Of course, this can be restated equivalently in the form of a universal property:

Theorem 112. *Let A be a ring, S be a multiplicative set, and M, N be A-modules. Assume that all $s \in S$ acts on N as an automorphism (that is, s is invertible on N). Then for any A-module homomorphism $\psi : M \to N$, there exists a unique $\xi : S^{-1}M \to N$ such that $\xi \circ \varphi = \psi$.*

5.2 Localization and Integrality

Proposition 113. *Let $A \subseteq F$ where A is a ring and F is a field. Let B be the integral closure of A in F. Then $S^{-1}B$ is the integral closure of $S^{-1}A$ in F for any multiplicative subset S of A.*

Proof. First, we will demonstrate that $S^{-1}B$ is integral over $S^{-1}A$. To do this, notice that any element of $S^{-1}B$ can be written as $\frac{b}{1} \cdot \frac{1}{s}$ for some $b \in B$ and $s \in S$, and furthermore that $\frac{1}{s}$ is in $S^{-1}A$ (and thus integral over $S^{-1}A$) for each $s \in S$. Thus, since the product of integral elements is integral, it suffices to demonstrate that $\frac{b}{1}$ is integral over $S^{-1}A$. Yet this is simple: since b is integral over A, there exist $a_0, \dots, a_{n-1}$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0 \Rightarrow \left(\frac{b}{1}\right)^n + \frac{a_{n-1}}{1}\left(\frac{b}{1}\right)^{n-1} + \cdots + \frac{a_1}{1}\left(\frac{b}{1}\right) + \frac{a_0}{1} = 0,$$

whence $\frac{b}{1}$ is indeed integral over $S^{-1}A$.

Next, we want to show that if $x \in F$ is integral over $S^{-1}A$, then $x \in S^{-1}B$. Now, if $x \in F$ is integral over $S^{-1}A$, then there exist $a_i \in A$ and $s_i \in S \subseteq A$ such that

$$x^n + \frac{a_{n-1}}{s_{n-1}}x^{n-1} + \cdots + \frac{a_1}{s_1}x + \frac{a_0}{s_0} = 0.$$

But then, if $s = s_0 \cdots s_{n-1}$, by multiplying through by s^n we find that

$$(sx)^n + \frac{a_{n-1}s}{s_{n-1}}(sx)^{n-1} + \cdots + \frac{a_1 s^{n-1}}{s_1}(sx) + \frac{a_0 s^n}{s_0} = 0$$

and since $s_i \mid s$ for each i, each of the coefficients of this relation is in A. Then, this is indeed an integral relation for $sx \in F$ over A. But then since B is the integral closure of A, $sx \in B$, whence $x \in S^{-1}B$ as desired. □

Corollary 113.1. *Suppose A is an integrally closed ring. Then $S^{-1}A$ is integrally closed for any multiplicative subset S of A.*

Lemma 114. *Suppose A is an integral domain. Then*

$$A = \bigcap_{\mathfrak{p} \lhd_{\mathrm{pr}} A} A_{\mathfrak{p}} = \bigcap_{\mathfrak{m} \lhd_{\max} A} A_{\mathfrak{m}},$$

where the intersection formally happens within the field of fractions of A.

Proof. Now, since A is an integral domain, $A \subseteq A_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$. Thus, $A \subseteq \bigcap_{\mathfrak{p} \lhd_{\mathrm{pr}} A} A_{\mathfrak{p}}$. Then, clearly $\bigcap_{\mathfrak{p} \lhd_{\mathrm{pr}} A} A_{\mathfrak{p}} \subseteq \bigcap_{\mathfrak{m} \lhd_{\max} A} A_{\mathfrak{m}}$. Hence it suffices to show that $A \subseteq \bigcap_{\mathfrak{m} \lhd_{\max} A} A_{\mathfrak{m}}$.

For this, take $x \in \bigcap_{\mathfrak{m} \lhd_{\max} A} A_{\mathfrak{m}}$. Then let $I_x = \{a \in A \mid xa \in A\}$. Our goal is to demonstrate that $1 \in A$, since then $1 \cdot x = x \in A$. To do this, fix any $\mathfrak{m} \lhd_{\max} A$. Then since $x \in A_{\mathfrak{m}}$, there exists $p \in A$ and $q \in A \setminus \mathfrak{m}$ such that $x = \frac{p}{q}$. But then $q \in I_x$, since $qx = p \in A$. Thus I_x is not contained in $\mathfrak{m}$, and indeed not contained in any maximal ideal of A. Thus $I_x = A$, so $1 \in I_x$, as desired. □

Lemma 115. *A is integrally closed if and only if $A_{\mathfrak{p}}$ is integrally closed for every prime ideal $\mathfrak{p}$ of A if and only if $A_{\mathfrak{m}}$ is integrally closed for every maximal ideal $\mathfrak{m}$ of A.*

Proof. In light of Corollary 113.1, the first condition implies the second. Now, the second condition trivially implies the third. Therefore, it suffices to show that if $A_{\mathfrak{m}}$ is integrally closed for every maximal ideal $\mathfrak{m}$ of A, then A is integrally closed. For this, suppose $x \in F$ is integral over A. Then x is clearly integral over $A_{\mathfrak{m}}$ for each $\mathfrak{m}$. Since $A_{\mathfrak{m}}$ is integrally closed, then $x \in A_{\mathfrak{m}}$ for each maximal $\mathfrak{m}$. But then, by applying Lemma 114, we find that $x \in A$. Thus A is integrally closed, as desired. □

5.3 The Support of a Module

Definition 116 (Support)**.** If M is an A-module, then the *support of M* is the subset

$$\operatorname{Supp} M = \{\mathfrak{p} \in \operatorname{Spec} A \mid M_{\mathfrak{p}} \neq 0\} \subseteq \operatorname{Spec} A$$

Definition 117 (Annihilator and Zero Divisor)**.** If M is an A-modle, then the *annihilator of* $m \in M$ is the ideal $\operatorname{Ann} m = \{f \in A \mid fm = 0\} \lhd A$. Similarly, the *annihilator of* M is the ideal $\operatorname{Ann} M = \{f \in A \mid fM = 0\} \lhd A$. Finally, recall that $f \in A$ is a *zerodivisor* on M if $fm = 0$ for some $0 \neq m \in M$.

Proposition 118 (Properties of the Support)**.**

1. *If M is a cyclic module with generator x and $I = \operatorname{Ann} x$ (so $M \simeq A/I$), then $\operatorname{Supp} M = \mathcal{V}(I)$.*

2. *If* $M = \sum_{\lambda \in \Lambda} M_\lambda$*, then* $\operatorname{Supp} M = \bigcup_{\lambda \in \Lambda} \operatorname{Supp} M_\lambda$*.*
3. *If* $0 \to L \to M \to N \to 0$ *is a short exact sequence,* $\operatorname{Supp} M = \operatorname{Supp} L \cup \operatorname{Supp} N$*.*
4. *If* M *is finite over* A*, then* $\operatorname{Supp} M = \mathcal{V}(\operatorname{Ann} M)$*; in particular, it is a closed subset of* $\operatorname{Spec} A$*.*
5. *If* $\mathfrak{p} \in \operatorname{Supp} M$ *then* $\mathcal{V}(P) \subseteq \operatorname{Supp} M$*.*

Proof. **1:** $M_\mathfrak{p}$ will be zero if and only if $\frac{x}{1} = 0 \in M_\mathfrak{p}$. Yet this follows if and only if $sx = 0$ for some $s \notin \mathfrak{p}$, which follows if and only if $\operatorname{Ann} x \not\subseteq \mathfrak{p}$. The result follows.

2: The exactness of the localization functor means that sums commute with localization. In particular:

$$M_\mathfrak{p} = \sum_{\lambda \in \Lambda} (M_\lambda)_\mathfrak{p}$$

Thus, $\mathfrak{p} \notin \operatorname{Supp} M$ iff $\mathfrak{p} \notin \operatorname{Supp} M_\lambda$ for any $\lambda \in \Lambda$. The result follows by taking the complement.

3: The exactness of the localization functor means that we have an exact sequence $0 \to L_\mathfrak{p} \to M_\mathfrak{p} \to N_\mathfrak{p} \to 0$. Notice that $M_\mathfrak{p}$ is 0 iff $L_\mathfrak{p}$ and $N_\mathfrak{p}$ are 0: the result follows by taking the complement.

4: If $\{m_1, \ldots, m_k\}$ is a family of generators of M, by applying **2**, then **1**, then definitions,

$$\operatorname{Supp} M = \bigcup_{i=1}^{k} \operatorname{Supp} A m_i = \bigcup_{i=1}^{k} \mathcal{V}(\operatorname{Ann}(m_i)) = \mathcal{V}\left(\bigcap_{i=1}^{k} \operatorname{Ann}(m_i)\right) = \mathcal{V}(\operatorname{Ann} M)$$

5: $\mathfrak{q} \in \mathcal{V}(\mathfrak{p})$ implies $\mathfrak{p} \subseteq \mathfrak{q}$ implies $A \setminus \mathfrak{q} \subseteq A \setminus \mathfrak{p}$, whence $M_\mathfrak{p}$ is a localization of $M_\mathfrak{q}$. In other words, if $M_\mathfrak{p}$ is nonzero then so is $M_\mathfrak{q}$. The result follows. □

5.4 Associated Primes of a Module

Definition 119 (Assassin or Associated Primes)**.** If M is an A-module, then an *assassin* or *associated prime* of M is a prime ideal $\mathfrak{p} \lhd_{\text{pr}} A$ such that $\exists x \in M$ such that $\mathfrak{p} = \operatorname{Ann} x$ (equivalently, there exists $N \subseteq M$ with $N \simeq A/\mathfrak{p}$). We write $\operatorname{Ass} M = \{\text{assassins of } M\}$.

Obviously, each $\mathfrak{p} \in \operatorname{Ass} M$ contains $\operatorname{Ass} M = \bigcap_{m \in M} \operatorname{Ann} M$.

Proposition 120 (Properties of Assassins)**.**

1. *Let* $x \in M$ *be such that* $\operatorname{Ann} x = \mathfrak{p}$ *is prime. Then for any nonzero* $y \in Ax$*,* $\operatorname{Ann} y = \mathfrak{p}$*.*
2. *Any maximal element of the set of ideals* $\{\operatorname{Ann} x \mid 0 \neq x \in M\}$ *is prime, so it will be in* $\operatorname{Ass} M$*.*
3. *If* A *is Noetherian, then* $M \neq 0 \Rightarrow \operatorname{Ass} M \neq \varnothing$*.*
4. *If* $0 \to L \to M \to N$ *is a short exact sequence, then* $\operatorname{Ass} M \subseteq \operatorname{Ass} L \cap \operatorname{Ass} N$*.*

Proof. **1:** Note that the submodule $Ax \subseteq M$ is isomorphic to $A/\mathfrak{p}$. When we view $A/\mathfrak{p}$ as a ring (indeed, an integral domain) and an A-module at once, it is clear that any $y \in A/\mathfrak{p}$ has $\operatorname{Ann} y = \mathfrak{p}$.

2: Suppose $x \in M$ is chosen so that $\operatorname{Ann} x$ is maximal among annihilating ideals. If $fg \in \operatorname{Ann} x$, then $fgx = 0$. There are two possibilities: if $gx = 0$, then $g \in \operatorname{Ann}(x)$, and if $gx \neq 0$ then $\operatorname{Ann}(gx) \supseteq \operatorname{Ann}(x)$, so $\operatorname{Ann}(gx) = \operatorname{Ann}(x)$ by maximality, whence $fgx = 0$ gives $f \in \operatorname{Ann}(x)$.

3: This follows immediately because if A is Noetherian and $M \neq 0$, then $\{\operatorname{Ann} x \mid 0 \neq x \in M\}$ is nonempty and thus has a maximal element (recall one equivalent criteria discussed in Def. 48 for being Noetherian is that any nonempty set of ideals has a maximal element).

4: If M contains a submodule isomorphic to $A/\mathfrak{p}$, then either $(A/\mathfrak{p}) \cap L = 0$ (then $A/\mathfrak{p}$ maps isomorphically to a submodule of N), whence $\mathfrak{p} \in \operatorname{Ass} N$, or $(A/\mathfrak{p} \cap L \neq 0)$. In the latter case, any $0 \neq x \in A/\mathfrak{p} \cap L$ has $\operatorname{Ann} x = \mathfrak{p}$ (see **1**), giving $\mathfrak{p} \in \operatorname{Ass} L$, as desired. □

Corollary 120.1. *If A is Noetherian and M is an A-module, then*

$$\{\textit{zerodivisors of } M \textit{ in } A\} = \bigcup_{\mathfrak{p}\in \operatorname{Ass} M} \mathfrak{p}.$$

Proof. Clearly every element in an assassin of M is a zerodivisor. On the other hand, if $f \in A$ is a zerodivisor, then $f \in \operatorname{Ann} m$ for some $0 \neq m \in M$, yet $\operatorname{Ann} m$ is contained in a maximal annihilating ideal $\operatorname{Ann} x$, which is an associated prime. Thus $f \in \mathfrak{p} \in \operatorname{Ass} M$, as desired. □

Theorem 121. *Let M be a module over a ring A. Then $\operatorname{Ass} M \subseteq \operatorname{Supp} M$ (in fact, $\mathfrak{p} \in \operatorname{Ass} M \Rightarrow \mathcal{V}(P) \subseteq \operatorname{Supp} M$). Also, if A is Noetherian, then any minimal element $\mathfrak{p} \in \operatorname{Supp} M$ is in $\operatorname{Ass} M$.*

Proof. Omitted; long and not very fun. □

Corollary 121.1. *Let M be a finite module over a Noetherian ring A. Then*

$$\operatorname{Supp} M = \bigcup_{i=1}^{n} \mathcal{V}(\mathfrak{p}_i)$$

where the $\mathfrak{p}_i$ for $i = 1, \ldots, n$ are the finitely many minimal primes containing $\operatorname{Ann} M$. Furthermore, each $\mathfrak{p}_i$ is in $\operatorname{Ass} M$ (since they are minimal).

Proof. As we know from Prop. 118, $\operatorname{Supp} M = \mathcal{V}(\operatorname{Ann} M)$. Then, by Cor. 92.1, this set has finitely many minimal elements $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$, whence the result follows. □

Theorem 122. *If A is a Noetherian ring and M is a finite A-module, then there exists a chain*

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$$

such that $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$, each $\mathfrak{p}_i$ is a prime ideal of A, and $\operatorname{Ass} M \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ (in particular it is finite).

Proof. Proposition 120 implies that there exists $\mathfrak{p}_1 \in \operatorname{Ass} M$. Let $M_1 \subseteq M$ be such that $M_1 \simeq A/\mathfrak{p}_1$. Construct the rest of the chain by the same argument applied to M/M_i: suppose that $M_0 \subseteq M_1 \subseteq \cdots \subseteq M_i$ are already constructed, and $M/M_i \neq 0$. Then $\operatorname{Ass}(M/M_i) \neq \varnothing$, so there exists a submodule $M' \subseteq M/M_i$ with $M' \simeq A/\mathfrak{p}_{i+1}$. Write $M_{i+1} \subseteq M$ for the inverse image of M' continuing the chain. Finally, the chain must eventually stop with $M_n = M$ because M is Noetherian (see Cor. 51.2). □

5.5 Primary Ideals and Primary Decomposition

Definition 123 (Primary Ideals)**.** A proper ideal $\mathfrak{q} \lhd A$ is called *primary* if $fg \in \mathfrak{q}$ implies that either $f \in \mathfrak{q}$ or $g^n \in \mathfrak{q}$ for some $n > 0$. Clearly, this is equivalent to saying that a proper ideal $\mathfrak{q}$ is primary if all zerodivisors in $A/\mathfrak{q}$ are nilpotent.

Proposition 124. *If $\mathfrak{q}$ is primary, then $\mathfrak{p} = \sqrt{\mathfrak{q}}$ is prime.*

Proof. If $fg \in \mathfrak{p}$, then $f^n g^n \in \mathfrak{q}$ for some n, which implies that either f^n or g^{mn} is in $\mathfrak{q}$ for some m, which implies that either f or g is in $\mathfrak{p}$. □

Definition 125 ($\mathfrak{p}$-Primary Ideals)**.** An ideal $\mathfrak{q}$ is called $\mathfrak{p}$-*primary* (or *primary belonging to* $\mathfrak{p}$) if $\mathfrak{q}$ is primary and $\mathfrak{p} = \sqrt{\mathfrak{q}}$.

Lemma 126. *If $\mathfrak{q}$ is a ideal such that $\sqrt{\mathfrak{q}} = \mathfrak{m}$ is maximal, then $\mathfrak{q}$ is $\mathfrak{m}$-primary.*

Proof. Suppose $f \in A \setminus \mathfrak{q}$, and let $I = \{g \in A \mid fg \in Q\}$. Then I is an ideal of A and $\mathfrak{q} \subseteq I \subsetneq A$ (since I cannot contain 1). Thus I must be contained in a maximal ideal: however, $\mathfrak{m}$ is the only prime ideal containing $\mathfrak{q}$ (by properties of radical ideals), hence $I \subseteq \mathfrak{m}$. This demonstrates

$$fg \in \mathfrak{q} \text{ and } f \notin \mathfrak{q} \Rightarrow g \in I \Rightarrow g \in \mathfrak{m} = \sqrt{\mathfrak{q}}$$

whence $g^n \in \mathfrak{q}$ for some n, as desired. □

Theorem 127. *If A is a Noetherian ring and $\mathfrak{q} \lhd A$, then $\mathfrak{q}$ is $\mathfrak{p}$-primary iff* $\operatorname{Ass}(A/\mathfrak{q}) = \{\mathfrak{p}\}$.

Proof. If $\mathfrak{q}$ is $\mathfrak{p}$-primary, then the zerodivisors of $A/\mathfrak{q}$ are contained in $\mathfrak{p}$ (since they are the preimage of $\sqrt{0} = \sqrt{\overline{q}}$). Thus, for any nonzero $x \in A/\mathfrak{q}$, so $\mathfrak{q} \subseteq \operatorname{Ann} x \subseteq \mathfrak{p} = \sqrt{\mathfrak{q}}$, therefore $\sqrt{\operatorname{Ann} x} = \mathfrak{p}$. In particular, since all prime ideals are radical, $\operatorname{Ann} x$ can only be a prime if it is equal to $\mathfrak{p}$. Yet by Proposition 120, we know that $\operatorname{Ass}(A/\mathfrak{q})$ is nonempty, so it must equal $\{\mathfrak{p}\}$.

In the opposite direction, if $\operatorname{Ass}(A/\mathfrak{p})$, take any nonzero module $M \subseteq A/\mathfrak{q}$. By Corollary 19.1, $\sqrt{\operatorname{Ann} M}$ is the intersection of prime ideals containing $\operatorname{Ann} M$. Indeed, we can take the intersection of the minimal prime ideals containing containing $\operatorname{Ann} M$; but these are the minimal elements of $\operatorname{Supp} M$, so by Theorem 121, they are in $\operatorname{Ass}(M)$. Yet $\operatorname{Ass}(M) = \{\mathfrak{p}\}$, so $\sqrt{\operatorname{Ann} M} = \mathfrak{p}$. In particular, $\mathfrak{q} = \operatorname{Ann}(A/\mathfrak{q})$ satisfies $\sqrt{q} = \mathfrak{p}$. Let $f, g \in A$ be elements with $fg \in \mathfrak{q}$ but $f \notin \mathfrak{q}$. Then $\overline{f} \in A/\mathfrak{q}$ is such that $g \in \operatorname{Ann} \overline{f} \subseteq \sqrt{\operatorname{Ann} \overline{f}} = \mathfrak{p}$, so $g^n \in \mathfrak{q}$, as desired. □

Lemma 128. *If $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are $\mathfrak{p}$-primary then so is $\mathfrak{q}_1 \cap \mathfrak{q}_2$.*

Proof. Suppose that $xy \in \mathfrak{q}_1 \cap \mathfrak{q}_2$ but $x \notin \mathfrak{q}_1 \cap \mathfrak{q}_2$. In either case we get $y \in \mathfrak{p}$, then $y^n \in \mathfrak{q}_1$ and $y^m \in \mathfrak{q}_2$ for some n and m. Yet then $y^{nm} \in \mathfrak{q}_1 \cap \mathfrak{q}_2$, making $\mathfrak{q}_1 \cap \mathfrak{q}_2$ primary. It is easy to see that the radical is $\mathfrak{p}$: $\mathfrak{q}_1 \cap \mathfrak{q}_2 \subseteq \mathfrak{q}_1$, so $\mathfrak{q}_1 \cap \mathfrak{q}_2 \subseteq \mathfrak{p}$. If $f \in \mathfrak{p}$, then as argued above there is k with $f^k \in \mathfrak{q}_1 \cap \mathfrak{q}_2$, so $f \in \sqrt{\mathfrak{q}_1 \cap \mathfrak{q}_2}$, whence $\mathfrak{p} \subseteq \sqrt{\mathfrak{q}_1 \cap \mathfrak{q}_2}$ and indeed $\mathfrak{p} = \sqrt{\mathfrak{q}_1 \cap \mathfrak{q}_2}$. □

Definition 129 (Primary Decomposition)**.** Let A be a ring and $I \lhd A$ be an ideal. Then a *primary decomposition of I* is an expression

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_k$$

with each $\mathfrak{q}_i$ primary. We call such a decomposition a *shortest primary decomposition of I* if $I \subsetneq \cap_{i \neq j} \mathfrak{q}_i$ for any J (that is, no term $\mathfrak{q}_j$ is redundant) and $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary for $\mathfrak{p}_i \neq \mathfrak{p}_j$ for $i \neq j$ (no two primary ideals can be combined using Lemma 128).

Definition 130 (Indecomposable Ideal)**.** An ideal $I \lhd A$ is *indecomposable* if it cannot be written as an intersection of two strictly bigger ideals: that is, if $I = J \cap K$ with J, K ideals implies that $I = J$ or $I = K$. For example, prime ideals are indecomposable.

Lemma 131. *In a Noetherian ring A, every indecomposable ideal $\mathfrak{q}$ is primary.*

Proof. Notice that $\mathfrak{q} \subseteq A$ is indecomposable if and only if $0 \subseteq A/\mathfrak{q}$ is indecomposable (and similarly for primary ideals). Thus, it suffices to prove that if B is a Noetherian ring, then $0 \subseteq B$ is indecomposable implies $0 \subseteq B$ is primary. Thus let $x, y \in B$ with $xy = 0$. Then $y \in \operatorname{Ann} x$. Consider the ascending chain

$$\operatorname{Ann} x \subseteq \operatorname{Ann}(x^2) \subseteq \cdots \subseteq \operatorname{Ann}(x^n) \subseteq \cdots,$$

because B is Noetherian, $\operatorname{Ann}(x^n) = \operatorname{Ann}(x^{n+1})$. Now, if $a \in (x^n) \cap (y)$, then $ax = 0$ (since a is a multiple of y) and $a = bx^n$, but then $ax = bx^{n+1}$, so $b \in \operatorname{Ann}(x^{n+1})$. But then, since $\operatorname{Ann}(x^{n+1}) = \operatorname{Ann}(x^n)$ and $a = bx^n$, we see that $a = 0$. This proves that $(x^n) \cap (y) = 0$. Hence if 0 is indecomposable, then $xy = 0$ implies that $x^n = 0$ or $y = 0$, so 0 is primary. □

Theorem 132. *In a Noetherian ring A, every ideal I has a primary decomposition.*

Proof. Let $\mathscr{S}$ be the set of ideals not expressible as an intersection of indecomposable ideals. If $\mathscr{S} \neq \varnothing$, then by Cor. 51.2, $\mathscr{S}$ has a maximal element $I \in \mathscr{S}$. I cannot be indecomposable, so it must be of the form $I = J \cap K$ for strictly bigger ideals J and K. By the maximality of I, neither J or K can be contained in $\mathscr{S}$, whence J and K are each are the intersection of finitely many indecomposable ideals. But then I is also the intersection of finitely many indecomposable ideals! This is a contradiction with the assumption that $\mathscr{S}$ is nonempty, so $\mathscr{S}$ must be empty; the result follows. □

Theorem 133 (1st Uniqueness Theorem)**.** *Let A be Noetherian, $I \subseteq A$ an ideal, and let $I = \bigcap_{i=1}^k \mathfrak{q}_i$ be a shortest primary decomposition, where each $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. Then* $\operatorname{Ass}(A/I) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$ *(in particular, the set of primes $\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$ is uniquely determined by I).*

Proof. From $I = \bigcap_{i=1}^k \mathfrak{q}_i$ it follows that there is a natural inclusion map

$$A/I \hookrightarrow \bigoplus_{i=1}^{k} A/\mathfrak{q}_i.$$

Hence $\operatorname{Ass}(A/I) \subseteq \bigcup \operatorname{Ass}(A/\mathfrak{q}_i) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$. On the other hand, by the irredundancy conditions, for any j, we have that

$$0 \neq N = \bigcap_{i \neq j} \mathfrak{q}_i/I \subseteq A/I$$

In the earlier inclusion, N maps to zero in each decomponent $A/\mathfrak{q}_i$ for $i \neq j$. Hence $0 \neq N \hookrightarrow A/\mathfrak{q})j$. By Theorem 127, $\operatorname{Ass}(A/\mathfrak{q}_j) = \{\mathfrak{p}_j\}$. Therefore A/I contains a submodule N with $\varnothing \neq \operatorname{Ass} N \subseteq \{\mathfrak{p}_j\}$, so $\mathfrak{p}_j \in \operatorname{Ass}(A/I)$, as desired. □

Here we generalize earlier results on prime ideals and passing to a ring of fractions to primary ideals.

Proposition 134. *Let A be a ring and S a multiplicative set of A. Further let $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ be a shortest primary decomposition, where each $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. Order the factors so that $S \cap \mathfrak{p}_i = \varnothing$ if $i \in \{1, \dots, m\}$ and $S \cap \mathfrak{p}_i \neq \varnothing$ if $i \in \{m+1, \dots, n\}$. Then*

$$S^{-1}I = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i \text{ and } \varphi^{-1}(S^{-1}I) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m.$$

where φ is the natural map $\varphi : A \to S^{-1}A$.

Proof. Not included here, as it is too similar to earlier results on localization. □

Corollary 134.1. *Let $I = \bigcap \mathfrak{q}_i$ be a shortest primary decomposition of I where each $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. Suppose that $\mathfrak{p}_i$ is a minimal element of $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$. Then setting $S = A \backslash \mathfrak{p}_i$, we have $\mathfrak{q}_i = \varphi^{-1}(S^{-1}I)$; in particular, $\mathfrak{q}_i$ is uniquely determined by I and $\mathfrak{p}_i$. Thus the primary component belonging to a minimal prime is uniquely determined.*

6 Discrete Valuation Rings

Definition 135 (Discrete Valuation)**.** If k is a field, then a *discrete valuation* of K is a surjective map $\nu : K \to \mathbb{Z} \cup \{\infty\}$ with the properties that

1. $\nu(x) = \infty$ if and only if $x = 0$.
2. $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in k$.
3. $\nu(x \pm y) \geq \min\{\nu(x), \nu(y)\}$ for all $x, y \in k$.

Note that (2) forces $\nu(1) = 0$. The *valuation ring* of a discrete valuation ν is the subset $A = \{x \in K \mid \nu(x) \geq 0\}$. One can easily check that this is a ring; a ring of this form is a *discrete valuation ring or DVR.*

Proposition 136. *If A is a DVR with discrete valuation ν, then A is a local ring with maximal ideal $\mathfrak{m} = \{x \in K \mid \nu(x) > 0\}$. Furthermore, A is a principal ideal domain.*

Proof. For the first part, notice that by Axiom 2 for DVRs, $\nu(x^{-1}) = -\nu(x)$. Thus, x is a unit if and only if $\nu(x) = 0$, the set of nonunits in A are those with valuation greater than 0. By Axiom 3 for DVRs, this set is closed under addition and thus an ideal; by our characterization of local rings in Proposition 26, the result follows.

For the second part, let $t \in k$ be any element such that $v(t) = 1$. Then it is easy to check that $\mathfrak{m} = (t)$, and indeed every ideal I of A is of the form (t^n) for some n. Thus, we are done. □

Lemma 137. *Let A be a Noetherian integral domain and $t \in A$ a nonunit. Then $\bigcap_{n=1}^{\infty}(t^n) = 0$.*

Proof. Choose $x \in \bigcap_{n\in\mathbb{N}}(t^n)$. Then $x = a_1t = a_2t^2 = a_3t^3 = a_4t^4 = \cdots$ for some $a_1, a_2, \cdots \in A$. By the Noetherian assumption, the ascending chain of ideals $(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \cdots$ must eventually stabilize; in particular $a_n \in (a_1, \ldots, a_{n-1})$ for some n. Thus for some $b_1, \ldots, b_{n-1} \in A$, $a_n = b_1a_1 + \cdots + b_{n-1}a_{n-1}$. Then, by multiplying t^n on both sides and recalling that $x = a_nt^n$,

$$x = a_nt^n = b_1a_1t^n + \cdots + b_{n-1}a_{n-1}t^n = b_1xt^{n-1} + \cdots + b_{n-1}xt = x(b_1t^{n-1} + \cdots + b_{n-1}t).$$

Yet this implies that $x = 0$, since if x is nonzero, then the cancellation property gives us $b_1t^{n-1} + \cdots + b_{n-1}t = 1 \Leftrightarrow (b_1t^{n-2} + \cdots b_{n-1})t = 1$, a contradiction with the assumption that t is not a unit. □

Proposition 138. *Let $(A, \mathfrak{m})$ be a local integral domain with principal maximal ideal $\mathfrak{m} = (t)$ for some $t \neq 0$. Also assume that $\bigcap_{n=1}^{\infty}(t^n) = 0$ (this holds if A is Noetherian by Lemma 137). Then:*

1. *Every $0 \neq x \in A$ is of the form $x = t^nu$ with $n \geq 0$ and u a unit.*
2. *Define $\nu(x) = n$, where $x = t^nu$ as in (1), and $\nu(x/y) = \nu(x) - \nu(y)$ for all $x/y \in \operatorname{Frac} A$. Then ν is a discrete valuation of $\operatorname{Frac} A$ and A is its valuation ring.*
3. *Every nonzero ideal I of A is of the form $I = (t^n)$ for some $n \geq 0$.*

Proof.
1: If $x \in (t^n) \setminus (t^{n+1})$, then $x = t^nu$ with $u \neq \mathfrak{m}$ (i.e. U is a unit). This eventually happens because the intersection of all the (t^n) tends to 0. The first part follows.
2: This is a matter of simple computation.
3: Let $n = \min\{k \mid I \text{ contains an element } x = t^ku \text{ with } u \text{ a unit}\}$. Then clearly $I = (t^n)$. □

In particular, if $(A, \mathfrak{m})$ is a Noetherian local ring and $\mathfrak{m} = (t)$, either A is a DVR or t is nilpotent.

6.1 An Equivalent Condition for DVRs

Theorem 139 (The Main Result on DVRs)**.** *A ring A is a DVR if and only if A is a local integrally closed Noetherian integral domain with $\operatorname{Spec} A = \{0, \mathfrak{m}\}$.*

Proof. ($\Rightarrow$): If A is a DVR, then it is a local ring by Proposition 136. Since it is a PID by the same proposition, it is Noetherian. Finally, since it is a PID, it is a UFD, so it is an integrally closed domain. To see why $\operatorname{Spec} A = \{0, \mathfrak{m}\}$, take a proper ideal I of A. If it is equal to 0 or $\mathfrak{m} = (t)$, then it is clearly prime. Otherwise, by Proposition 138, $I = (t^n)$ for some $n \geq 2$. But then $t, t^{n-1} \notin I$ (since A is a domain and t cannot be a unit) whereas $t^n = t \cdot t^{n-1} \in I$, so I is not a prime ideal.

($\Leftrightarrow$): First, notice that because A is Noetherian, any ideal I of A is a finite A-module. Since A is a local ring, by Nakayama's Lemma, Corollary 40.2, $I\mathfrak{m} = I$ implies that $I = 0$. In particular, since $\mathfrak{m} \neq 0$, $\mathfrak{m} \neq \mathfrak{m}^2$. Therefore, we may choose an element $x \in \mathfrak{m} \setminus \mathfrak{m}^2$.

I claim that $\mathfrak{m} = (x)$. To see why, suppose for the sake of contradiction that $\mathfrak{m}/(x) \neq 0$. Then by Proposition 120, $\operatorname{Ass} M \neq \varnothing$. Hence, there exists some element $y \in \mathfrak{m} \setminus (x)$ such that $\mathfrak{m}y \subseteq (x)$. Now consider $y/x \in \operatorname{Frac} A$; on one hand, $y/x \notin A$ but on the other hand, $(y/x)\mathfrak{m}$ is an ideal of A. Now, we cannot have $(y/x)\mathfrak{m} = A$, since then $ym/x = 1 \Rightarrow x = ym$ for some $m \in \mathfrak{m}$, implying that $x \in \mathfrak{m}^2$, a contradiction. Therefore, $(y/x)\mathfrak{m} \subseteq \mathfrak{m}$.

In this case, y/x is integral over A using the same argument as in the determinant trick; $\mathfrak{m}$ is a finite A-module since A is Noetherian, and multiplication by y/x is a linear map $\varphi : \mathfrak{m} \to \mathfrak{m}$. Hence φ satisfies a monic relation $\varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_0 = 0$ with $a_i \in A$ for each i. But then applying this to any nonzero $z \in \mathfrak{m}$ gives $((y/x)^n + a_{n-1}(y/x)^{n-1} + \cdots + a_0)z = 0$, whence $((y/x)^n + a_{n-1}(y/x)^{n-1} + \cdots + a_0) = 0$ since A is an integral domain.

But then since y/x is integral over A, it belongs to A since A is integrally closed. Hence $y/x \in A$, so $y \in (x)$, a contradiction. Therefore the assumption that $\mathfrak{m} \neq (x)$ must have been false, and we are done by Proposition 138. □

6.2 General Valuation Rings

Definition 140 (Valuation Rings). Let A be an integral domain and $K = \operatorname{Frac} A$ its field of fractions. Then A is a *valuation ring* if for every nonzero element $x \in K$, either x or $x^{-1} \in A$.

Definition 141 (Ordered Group). Recall that a partial order $>$ on a set Γ is a *total order* if, for all $a, b \in \Gamma$, exaclty one of $a > b$, $a = b$, or $a < b$ holds. An *order group* Γ is an additive Abelian group with a total order $>$ compatible with the addition law, in the sense that $a \geq b$ and $a' > b'$ implies $a + a' > b + b'$.

Let A be an integral domain and $K = \operatorname{Frac} A$. Let $\Gamma = K^\times/A^\times$; notice that $\overline{a} + \overline{b} = \overline{ab}$ for $a, b \in K^\times$. We may give Γ the partial order $>$ defined by $\overline{b} \geq \overline{a}$ if and only if $b/a \in A$.

Proposition 142. *Suppose that A is an integral domain with $K = \operatorname{Frac} A$.*

1. *Then A is a valuation ring if and only if $>$ is a total order on $\Gamma = K^\times/A^\times$. If this holds, the quotient map $\nu : K^\times \to \Gamma$ satisfies $\nu(xy) = \nu(x) + \nu(y)$ and $\nu(x \pm y) \geq \min\{\nu(x), \nu(y)\}$.*
2. *Similarly, if Γ is an ordered group and $\nu : K^\times \to \Gamma$ a surjective map that satisfies $\nu(xy) = \nu(x) + \nu(y)$ and $\nu(x \pm y) \geq \min\{\nu(x), \nu(y)\}$, then $A = \{a \in K \mid \nu(a) \geq 0\}$ is a valuation ring, and $\Gamma = K^\times/A^\times$.*

In this set-up, $\nu : K^\times \to \Gamma$ is called a valuation, and $\Gamma = K^\times/A^\times$ the value group of ν.

Proof. To say that $>$ is a total order means that for $a, b \in K$, exactly one of the three cases $a/b \in A$ but $b/a \notin A$, $a/b \in A^\times$, or $b/a \in A$ but $a/b \notin A$, which is the same thing as the definition of a valuation ring. The rest is simple computation from here. □

Theorem 143. *Let A be a valuation ring. Then A is Noetherian if and only if A is a DVR.*

Proof. We have already discussed the direction $\Leftarrow$. To prove $\Rightarrow$, note that in a valuation ring A, any finitely generated ideal I is principal. For $I = (x_1, \ldots, x_n)$, then assuming each $x_i \neq 0$, either $x_1/x_2 \in A$, so that $I = (x_2, \ldots, x_n)$, or $x_2/x_1 \in A$, so $I = (x_1, x_3, \ldots, x_n)$. Assume that A is Noetherian: then the maximal $\mathfrak{m}$ of A is finitely generated, so principal. Thus $\mathfrak{m} = (t)$ and A is a DVR by Proposition 138. □

Lemma 144. *Let A be a integrally closed Noetherian ring. Then if $\mathfrak{p}$ is a minimal nonzero prime ideal of A then $A_{\mathfrak{p}}$ is a DVR. Now, if $0 \neq I = (x) \subseteq A$ is a principal ideal, then $\mathfrak{p} \in \operatorname{Ass} A/I \Rightarrow \mathfrak{p}$ is a minimal nonzero prime ideal.*

Proof. Boring to prove. You may see it on pages 119-120 of *Undergraduate Commutative Algebra.* □

Theorem 145. *Let A be a integrally closed Noetherian ring, $K = \operatorname{Frac} A$, and $K \subseteq L$ a finite separable field extension. Let $B \subseteq L$ be the integral closure of A in L. Then B is a finite A-module (in particular, a Noetherian ring).*

Proof. Boring to prove. You may see it on pages 123 of *Undergraduate Commutative Algebra.* □

Corollary 145.1.

1. *Let A be an integral domain that is finitely generated over a field k. Then $\widetilde{A}$ is a finite A-module.*
2. *Suppose that L is an algebraic number field. Then $\mathcal{O}_L$ is a finite $\mathbb{Z}$-module.*

Proof. For part **1**, notice that by the Noetherian Normalization Lemma, one can assume that $k \subseteq k[z_1, \ldots, z_r] \subseteq A$ where $z_1, \ldots, z_r$ are algebraically independent over k and A is finite over $k[z_1, \ldots, z_r]$. We can assume that $K = \operatorname{Frac} A$ is a separable extension of $k(z_1, \ldots, z_r)$. Then $\widetilde{A}$ is the integral closure of $k[z_1, \ldots, z_r]$ in K, so we can apply the above theorem. From this, **2** follows directly. □