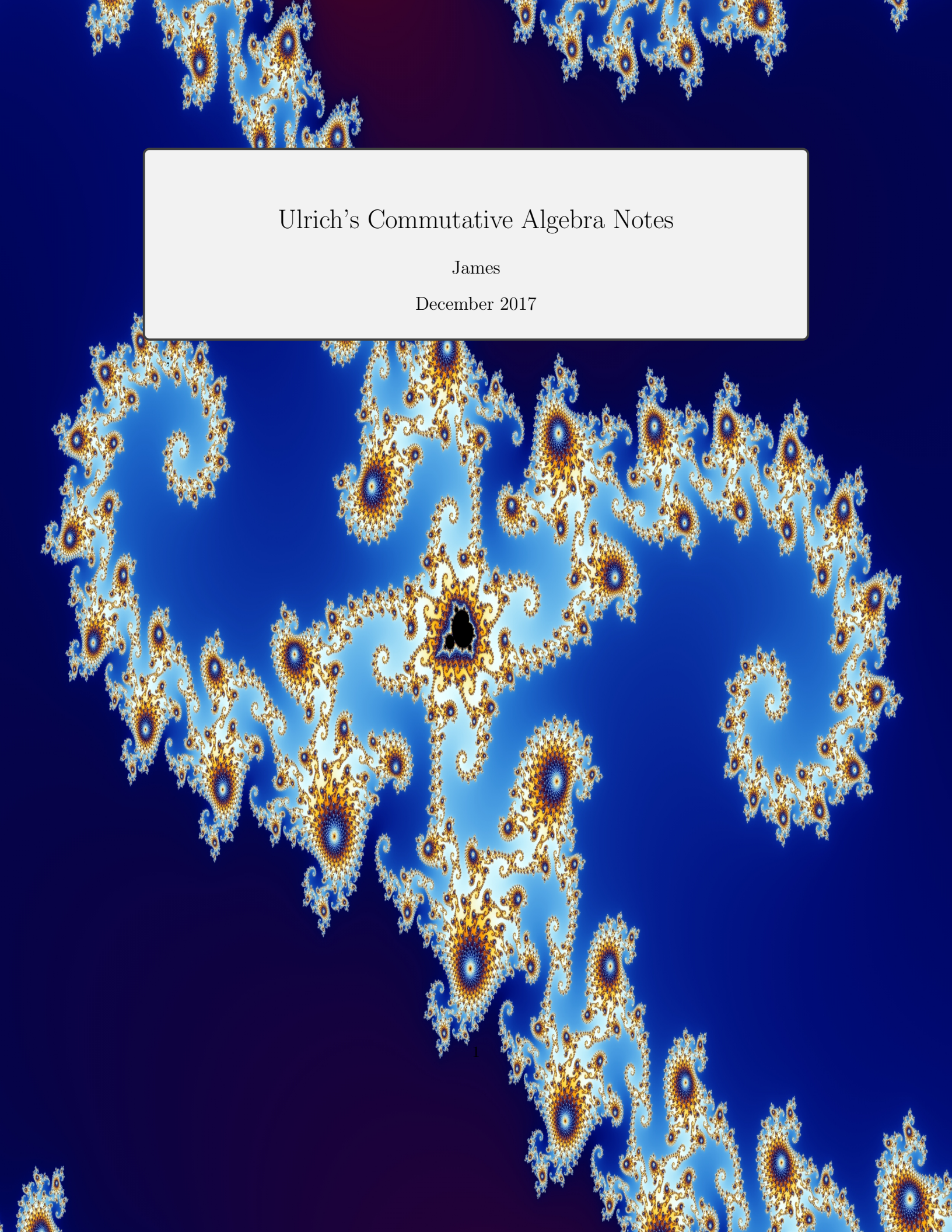


Ulrich's Commutative Algebra Notes

James

December 2017

Contents

Chapter 0: Preliminaries **3**

Chapter 1: Basics of Rings **5**
Ideals 5
Chinese Remainder Theorem 10

Chapter 2: Modules **13**
Operations on Modules 13
Tensor Products 15
Exact Sequences 21

Chapter 3: Noetherian/Artinian Modules and Ring **28**
Noetherian and Artinian Modules and Rings 28
Hilbert's Basis Theorem 33

Chapter 4: Localization and Spectrum **35**
Contraction and Extension of Ideals 38

Chapter 5: Associated Primes and Primary Decomposition. **42**

Chapter 6: Dimension and Hilbert's Nullstellensatz **47**
Dimension 47
Hilbert's Nullstellensatz 47

Chapter 7: Integral Extensions **52**

Chapter 8: DVR and Dedekind Domains **56**

Chapter 0: Preliminaries

These are things Ulrich never said in his lectures. Probably more basic than needed. Some things are stolen from Ben's Bridge to Algebra Lectures, and some are stolen from Wikipedia.

Definition (Binary Operation)**.** Let R be some set (informally a collection of objects). Then any function $f : R \times R \to R$ is called a binary operation.

Definition (Magma)**.** A magma structure on a set M is a binary operation $\cdot$.

Definition (Semigroup)**.** A semigroup structure on a set S is a binary operation $\cdot$ satisfying the following properties.

(a) (Associativity) For all $a, b, c \in S$, we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Definition (Monoid)**.** A monoid structure on a set M is a binary operation $\cdot$ such that the following properties are satisfied.

(a) (Associativity) For all $a, b, c \in M$ we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(b) (Identity element) There exists an element $e \in M$ such that for all $a \in M$ we have $a \cdot e = e \cdot a = a$.

Definition (Group)**.** A group is a set, denoted by G, together with some operation, denoted by $\cdot$, that combines any two elements $a, b \in G$ to form another element $a \cdot b$ in G. To qualify, the set along with the operation must satisfy four axioms.

(a) (Closure) For all $a, b \in G$, the result of the operation $a \cdot b$ is also in G.

(b) (Associativity) For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(c) (Identity element) There exists an element $e \in G$ such that for all $a \in G$ we have $a \cdot e = e \cdot a = a$.

(d) (Inverse element) For all $a \in G$, there exists an element $b \in G$ such that $a \cdot b = b \cdot a = e$ (generally, this b is denoted by a^{-1}).

Definition (Abelian/Commutative Group)**.** An abelian group is a set G with a binary operation $\cdot$ such that it satisfies these five properties.

1. (Closure) For all $a, b \in G$, the result of the operation $a \cdot b$ is also in G.
2. (Associativity) For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. (Identity element) There exists an element $e \in G$ such that for all $a \in G$ we have $a \cdot e = e \cdot a = a$.
4. (Inverse element) For all $a \in G$, there exists an element $b \in G$ such that $a \cdot b = b \cdot a = e$ (generally, this b is denoted by a^{-1}).
5. (Commutativity) For all $a, b \in G$ we have that $a \cdot b = b \cdot a$.

Theorem (Zorn's Lemma)**.** Suppose a partially ordered set P has the property that every chain in P has an upper bound in P. Then the set P contains at least one maximal element.

Theorem (Fundamental Theorem on Homomorphisms)**.** Given two algebraic structures (monoids, vector spaces, modules, rings, groups) G and H, and a homomorphism $f : G \to H$, let K be a set with which we can quotient by (normal group, ideal, etc.) in G and ϕ the natural surjective homomorphism $\phi : G \to G/K$. If K is a subset of $\ker f$, then there exists a unique homomorphism $h : G/K \to H$ such that $f = h \circ \phi$.

Definition (Monomorphism)**.** A monomorphism is an injective homomorphism.

Definition (Epimorphism)**.** An epimorphism is a surjective homomorphism.

Definition (Power Series Ring)**.** The ring of formal power series in x with coefficients in R is denoted by $R[[x]]$, and is defined as follows. The elements of $R[[x]]$ are infinite expressions of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

in which $a_n \in R$ for all $n \in \mathbb{N}$. Addition and multiplication are defined just as for the ring of polynomials $R[x]$. Notice that $R[[x]]$ is commutative because R is.

Definition (Equivalence Relation)**.** Let X be a set of objects. We define an equivalence relation on X to be a subset of $X \times X$; i.e., a collection R (not to be confused with ring) of ordered pairs of elements X satisfying certain properties. These properties are

1. It is reflexive; $(x, x) \in R$ for all $x \in X$.
2. It is symmetric; $(x, y) \in R$ implies $(y, x) \in R$ for all $x, y \in X$.
3. It is transitive; $(x, y) \in R$ and $(y, z) \in R$ implies $(x, z) \in R$.

Chapter 1: Basics of Rings

Ideals

Definition (Ring)**.** We say that R is a ring if

1. R is an abelian group with respect to addition.
2. R is commutative, associative, and has 1 with respect to multiplication. Multiplication is also distributive.

Definition (Homomorphism)**.** Let R and S be rings. We say $\varphi : R \to S$ is a homomorphism if it satisfies these three conditions:

1. $\varphi(x + y) = \varphi(x) + \varphi(y)$.
2. $\varphi(xy) = \varphi(x)\varphi(y)$.
3. $\varphi(1_R) = 1_S$.

Definition (Subring)**.** We say R is a subring of S if $R \subseteq S$, R is a ring with respect to the operations of S, and $1_R = 1_S$. Equivalently, we say it is a subring if there is a homomorphism $\varphi : R \to S$ which is injective.

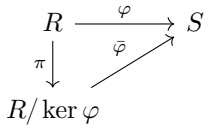
Definition (Ideal)**.** Let $I \subseteq R$ be a subset of R. We say that I is an R-ideal if I is a subgroup with respect to I and $RI \subseteq I$.

Fact (Fact 1)**.** If $\varphi : R \to S$ is a homomorphism, then $\operatorname{Im} R$ is a subring of S and $\ker \varphi$ is an ideal of R.

Definition (Factor Ring)**.** If I is an ideal, $I \subseteq R$: $R/I = \{x + I : x \in R\}$ is a ring. R/I called the factor ring of R.

Fact (Natural Projection)**.** Take $\pi : R \to R/I$. This is called the natural projection. Then π is an epimorphism, with $\ker \pi = I$. Thus, we see every ideal is a kernel.

Theorem (Theorem 1.1)**.** Given any $\varphi : R \to S$, and choose any $I \subseteq \ker \varphi$, where I is an R ideal. Then there is a unique homomorphism $\bar{\varphi} : R/I \to S$ so that $\varphi = \bar{\varphi} \cdot \bar{\pi}$. Moreover, $\operatorname{Im} \bar{\varphi} = \operatorname{Im} \varphi$, and $\ker \bar{\varphi} = \ker \varphi / I$. In particular, if you choose $I = \ker \varphi$, then $\bar{\varphi}$ is injective. Hence, there exists a unique monomorphism $\bar{\varphi} : R/\ker \varphi \to S$ where the following diagram commutes.



Proof. Proof is left as an exercise. **Q.E.D**

Proposition (Proposition 1.2)**.** Let $\pi : R \to R/I$ be surjective. Then there is a one-to-one correspondence with ideals of R containing I and ideals of R/I. Under this correspondence, factor ideals are preserved, i.e., $R/K \cong \frac{(R/I)}{(K/I)}$, where K is an ideal that contains I.

Definition (Principle Ideal)**.** (Principal Ideal) $I \subseteq R$ is called a principal ideal if $I = Rx$ for some x. Sometimes we denote this by $I = (x)$.

Definition (Unit)**.** We say that $x \in R$ is a unit if it has a multiplicative inverse, denoted by x^{-1}. Equivalently, we say that x is a unit if $(x) = R$.

Definition (Zero Divisor)**.** We say that $x \in R$ is a zero divisor if $xy = 0$ for some $y \neq 0$. Otherwise, it's a nonzero divisor.

Definition (Integral Domain)**.** We say that R is an integral domain if $R \neq 0$ and every $x \neq 0$ in R is a nonzero divisor.

Definition (Principle Ideal Domain)**.** We say that R is a principal ideal domain (shortened to PID) if R is a domain and every ideal is a principal ideal.

Proposition (Proposition 1.3)**.** Suppose $R \neq 0$ is a ring. Then the following are equivalent:

1. R is a field.
2. The only ideals in R are 0 and R.
3. Any homomorphism $\varphi : R \to S \neq 0$ is injective.

Proof. We show that 1 implies 2. Suppose we have an ideal $I \neq 0$. Then there exists a nonzero $x \in I$. But a nonzero element in a field is a unit, and so we have $xx^{-1} = 1$, and thus $1 \in I$. But this means that $I = R$.

We show that 2 implies 3. Notice that $\varphi \neq 0$, because $\varphi(1_R) = 1_S$, and since $S \neq 0$ then $1_S \neq 0$. Since $\varphi \neq 0$, $\ker \varphi \neq R$ and since $\ker \varphi$ is an ideal (Fact 1) then we must have $\ker \varphi = 0$ by assumption. Hence, $\ker \varphi = 0$ implies φ is injective.

We show that 3 implies 1. Take $x \in R$, $x \neq 0$. look at $\pi : R \to R/(x)$. Since $x \neq 0$ and $x \in \ker \pi$, π is not injective. By assumption, this means that $R/(x) = 0$. But for this to be true implies $(x) = R$, i.e. x is a unit. Since we chose arbitrary $x \neq 0$ in our ring R, this means that every $x \neq 0$ is a unit, and so this forces R to be a field. **Q.E.D**

Definition (Prime Ideal)**.** Let I be an R-ideal. Then I is a prime ideal if $I \neq R$ and whenever $xy \in I$, either $x \in I$ or $y \in I$.

Definition (Maximal Ideal)**.** Let I be an R-ideal. Then I is a maximal ideal if, whenever J is an ideal such that $I \subseteq J \subseteq R$, we have that either $I = J$ or $J = R$.

Fact (Fact 2)**.** We have that I is a prime ideal iff R/I is a domain, and I is a maximal ideal iff R/I is a field.

Fact (Fact 3)**.** We have that 0 is a prime ideal if and only if R is a domain.

Fact. Suppose $\varphi : R \to S$ is a homomorphism of rings, and p is a prime ideal in S. Then if $\bar{\varphi} : R/\varphi^{-1}(p) \to S/p$ is injective, we have that $\varphi^{-1}(p)$ is a prime ideal of R.

Theorem (Theorem 1.4)**.** Every nonzero ring has a maximal ideal.

Proof. Let $\Sigma = \{I : I \text{ is an } R\text{-ideal}, I \neq R\}$. This is a set which is partially ordered via inclusion. We need to then show that Σ has a maximal element. First, notice that $\Sigma \neq \varnothing$, since $(0) \in \Sigma$. To apply Zorn's Lemma, we need to check that every totally ordered subset $\{I_\alpha\}$ has an upper bound in Σ. Let $I = \cup_\alpha I_\alpha$, which is an ideal since the set is totally ordered. Notice that $1 \notin I_\alpha$ for all α since $I_\alpha \neq R$ for all α. Thus, 1 cannot be in the union, and so $1 \notin I$. Therefore, $I \in \Sigma$. Clearly, we have that this must be an upper bound, since $I_\alpha \subseteq I$ for all α. We apply Zorn's Lemma, and so there must be a maximal element. This must then be the maximal ideal. **Q.E.D**

Corollary (Corollary 1.5)**.** If $I \neq R$ is an R-ideal, then R has a maximal ideal containing I.

Proof. Notice $R/I \neq 0$, and so it must have a maximal ideal by Theorem 1.4. Denote this by $\bar{M}$. By Proposition 1.2, there is a corresponding ideal $M \subset R$ such that $I \subseteq M \subset R$. We now establish that this ideal is maximal. Assume it were not; that is to say, there is an ideal M' such that $M \subsetneq M' \subsetneq R$. Then we have that $M'/I = \bar{M'}$ is an ideal in R/I. We chose M to be maximal, however, and so $M'/I = M/I$. This gives us the resulting contradiction, since $M'/I = M/I$ implies $M = M'$. So, M is maximal. **Q.E.D**

Corollary (Corollary 1.6)**.** Let $R^\times$ denote the units of R. Then

$$R \backslash R^\times = \bigcup_{m \in m-\mathrm{Spec}(R)} m,$$

where $m - \mathrm{Spec}(R)$ denotes the set of maximal ideals of R.

Proof. For notational reasons, denote

$$Y := \bigcup_{m \in m-\mathrm{Spec}(R)} m.$$

We show $Y \subseteq R \backslash R^\times$. Let $x \in Y$. Then $x \notin R^\times$, since this contradicts the property of being a maximal ideal. So $x \in R/R^\times$.

We now show $R \backslash R^\times \subseteq Y$. By Corollary 1.5, every non-unit in R is contained in some maximal ideal. Moreover, every non-unit is in the union of maximal ideals. **Q.E.D**

Example. (1) The prime ideals in a PID are the prime elements which are not equal to 0. The maximal ideals are (p), where p is a prime element, if R is not a field.

(2) Let $0 \neq n \in \mathbb{Z}$. Then the set of prime ideals of $\mathbb{Z}/\mathbb{Z}n$ is equal to the set of maximal ideals which is equal to the set $(p)/(n)$ where p is a prime divisor of n, $p > 0$, and this has a one to one correspondence with the positive prime divisors of n.

(3) Suppose $f \in k[x_1, \ldots, x_n]$, k a field, and f irreducible. Then $k[x_1, \ldots, x_n]/(f)$ is a domain.

Definition (Local)**.** A ring R is called local if R has exactly one maximal ideal, m.

Definition (Residue Field)**.** Let R be a local ring with maximal ideal m. Then $k = R/m$ is called the residue field of R.

Definition (Semilocal)**.** A ring R is semilocal if it has at most finitely many maximal ideals.

Proposition (Proposition 1.7)**.** A ring R is local if and only if $R \backslash R^\times$ is an ideal.

Proof. We start with the implication. Since R is local, we have that $m - \text{Spec}(R) = \{m\}$. By Corollary 1.6, $R\backslash R^\times = m$, which is an ideal.

We show the converse. By Corollary 1.6 again, $R\backslash R^\times = \cup_{m \in m-\text{Spec}(R)} m$. Notice that this cannot be the whole ring (if it were, this would mean that there are no units in R, but R has 1, a contradiction), and so $R\backslash R^\times \neq R$. So, let $R\backslash R^\times = I$ be an R ideal by assumption. By Corollary 1.6, I contains every maximal ideal. Therefore, I must be every maximal ideal, meaning that there's only one. **Q.E.D**

Definition (Operations on Ideals)**.** Let I, J be R ideals. Then $I + J := \{x + y : x \in I, y \in J\}$, and this is an ideal. Also $IJ := \{\sum_{\text{Finite sums}} x_i y_i : x_i \in I, y_i \in J\}$ is again an ideal. One can also take intersections. Note that $IJ \subseteq I \cap J$. The union of two ideals is not necessarily an ideal.

Lemma (Lemma 1.8)**.** Suppose p is an R-ideal, $p \neq R$. Then p is a prime ideal if and only if whenever there are ideals $I, J \subset R$ such that $IJ \subset p$, then $I \subset p$ or $J \subset p$.

Proof. We start with the implication. Suppose $IJ \subset p$, and suppose $I \not\subset p$ and $J \not\subset p$. Then we can pick $x \in I/p$, $y \in J/p$. Notice $xy \in p$ by definition, and $xy \in IJ$. Since p is prime, we have either $x \in p$ or $y \in p$. But this grants us a contradiction; since if $x \in p$ then we have that $I \subset p$ and vice versa for y.

We show the converse. This follows by definition. Specifically, select arbitrary $x, y \in R$ so that $xy \in p$. If $xy \in p$, we have $(x)(y) \subset p$. By assumption, this forces either $(x) \subset p$ or $(y) \subset p$. If $(x) \subset p$, then this implies $x \in p$, and likewise for (y). Thus, if $xy \in p$, then either $x \in p$ or $y \in p$, and by definition this means p is prime. **Q.E.D**

Definition (Multiplicative Subset)**.** Let S be a subset of a ring R. We say S is a multiplicative subset if

1. $a, b \in S$ implies $ab \in S$.
2. $1 \in S$.

Example. (1) If $x \in R$, then $\{x^n : n \geqslant 0\}$ is a multiplicative subset of R.

(2) If p is a prime ideal of R, then we have that $S = R\backslash p$ is a multiplicative set. Not every multiplicative set is the complement of a prime ideal. The case where this is true is if we let (i) be if and only if.

Theorem (Theorem 1.9)**.** Let I be an R-ideal, S a multiplicative subset of R with $I \cap S \neq \varnothing$. Then

1. There exists an ideal p which is maximal with respect to the property that $I \subset p$ and $p \cap S = \varnothing$.
2. Such a p is prime.

Proof. We prove 1. Let Σ be the set of all ideals J where $I \subset J$ and $J \cap S = \varnothing$. Notice that this satisfies the assumption of Zorn's Lemma (proof of Theorem 1.4). Let p be the maximal ideal of Σ.

We prove 2. In order to do this, we must show that p is prime. Notice that $p \neq R$, since $S \neq \varnothing$ and $S \cap p = \varnothing$. Also notice that $p \neq 0$. We must establish the primality condition. let $x, y \in R/p$. Then by the maximality of p in Σ, we get that $(p, x) = p + (x)$ is an ideal which is strictly larger than p, along with (p, y). Thus, $(p, x)(p, y) \cap S \neq \varnothing$ since $xy \in S$. Therefore, it follows $(p, x)(p, y) \not\subset p$. Notice that $(p, x)(p, y) = p^2 + xp + yp + (xy)$, and so in particular we get that $xy \notin p$. By the contrapositive, we get what we desire. **Q.E.D**

Corollary (1.10)**.** Suppose I is an R-ideal, S a multiplicative set of R with $S \cap I = \varnothing$, then there is a prime ideal p with $I \cap p$ and $p \cap S = \varnothing$.

Definition (Radical Ideal)**.** Let I be an R-ideal. Then $\sqrt{I} = \{x \in R : x^n \in I \text{ for some } n > 0\}$ is called a radical ideal.

Definition (Nilpotent Element)**.** An element of a ring $x \in R$ is nilpotent if $x \in \sqrt{0}$.

Definition (Nilradical)**.** The nilradical of R is $\sqrt{0}$, or the set of nilpotent elements.

Definition (Reduced)**.** We say that R is reduced if $\sqrt{0} = 0$.

Remark. Every domain is reduced.

Remark (Remark 1.11)**.** 1. $\sqrt{I}$ is an ideal and $I \subseteq \sqrt{I}$.

2. $\sqrt{\sqrt{I}} = \sqrt{I}$. (Think of it as a closure operation)
3. $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$
4. $\sqrt{I} = R$ iff $I = R$.
5. $\sqrt{I + J} \neq \sqrt{I} + \sqrt{J}$ but rather $\sqrt{\sqrt{I} + \sqrt{J}}$.
6. $\sqrt{p^n} = p$ if p is prime and $n > 0$.

Proof. We first need a lemma.

Lemma. If I, J are R-ideals, and $I \subseteq J$, then $\sqrt{I} \subseteq \sqrt{J}$.

Proof. Let $x \in \sqrt{I}$. Then $x^n \in I$. By assumption, $x^n \in J$. But this means $x \in \sqrt{J}$. Thus, $\sqrt{I} \subseteq \sqrt{J}$. **Q.E.D**

We show 1. Notice that we need to establish that $\sqrt{I}$ is an ideal. Let $x, y \in \sqrt{I}$. Then by definition, we have $x^n \in I$ for some $n > 0$ and $y^m \in I$ for some $m > 0$. Assume without loss of generality that $n \leqslant m$. Then $(x + y)^m \in I$, $m > 0$, by the binomial theorem, and so $x + y \in \sqrt{I}$. We must then show $R\sqrt{I} \subseteq \sqrt{I}$. Let $r \in R$, $y \in \sqrt{I}$. Then $y^n \in I$ for some $n > 0$, and so $(yr)^n \in I$. Hence, $yr \in \sqrt{I}$. Since this applies for arbitrary $y \in \sqrt{I}$, $r \in R$, we have that $R\sqrt{I} \subseteq \sqrt{I}$. So, $\sqrt{I}$ is an ideal. We must then establish that $I \subseteq \sqrt{I}$. This, however, is clear (let $x \in I$, then $x^1 \in I$ and so $x \in \sqrt{I}$).

We show 2. From 1, it follows that $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$. It remains to show that $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$. Let $x \in \sqrt{\sqrt{I}}$. Then we have that $x^n \in \sqrt{I}$, $n > 0$. But if $x^n \in \sqrt{I}$, this means $(x^n)^m \in I$ for $m > 0$. In other words, $x^{mn} \in I$. But this means that $x \in \sqrt{I}$. So, $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$, and we get equality.

We show 3. Let $x \in \sqrt{IJ}$. Then we have $x^n \in IJ$. If $x^n \in IJ$, then $x^n \in I \cap J$ by definition and so we have $\sqrt{IJ} \subset \sqrt{I \cap J}$. Let $x \in \sqrt{I \cap J}$. Then we have $x^n \in I$ and $x^n \in J$. Therefore, we have $x^{2n} \in IJ$, or in other words $x \in \sqrt{IJ}$. Thus, we have $\sqrt{I \cap J} = \sqrt{IJ}$.

Next, we need to show $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$. Let $x \in \sqrt{I \cap J}$. Then we have $x^n \in I$ and $x^n \in J$. This means that $x \in \sqrt{I} \cap \sqrt{J}$. Next, let $x \in \sqrt{I} \cap \sqrt{J}$. Then $x^n \in I$ and $x^n \in J$. This means that $x \in \sqrt{I \cap J}$. Thus, $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

We show 4. We first show the implication. Assume $\sqrt{I} = R$. Then we have that for all $x \in \sqrt{I}$, $x^n \in I$. However, this means that for all $x \in R$, we have $x^n \in I$. More importantly, take $1 \in R$.

Then we have $1^n \in I$ for some $n > 0$. Hence, $I = R$. The converse follows (if $I = R$, then $x^n \in I$ for all $x \in R$ and so $\sqrt{I} = R$).

We show 5. We show $\sqrt{\sqrt{I} + \sqrt{J}} \subseteq \sqrt{I + J}$. Since $I, J \subseteq I + J$ (see Operations on Ideals), we get that $\sqrt{I}, \sqrt{J} \subseteq \sqrt{I + J}$ by the lemma. Hence, $\sqrt{I} + \sqrt{J} \subseteq \sqrt{I + J}$. By 1 and 2, we see that $\sqrt{\sqrt{I} + \sqrt{J}} \subseteq \sqrt{\sqrt{I + J}} = \sqrt{I + J}$. We show $\sqrt{I + J} \subseteq \sqrt{\sqrt{I} + \sqrt{J}}$. By 1, we have $I \subseteq \sqrt{I}$, $J \subseteq \sqrt{J}$, and so $I + J \subseteq \sqrt{I} + \sqrt{J}$. Using the lemma again, we get $\sqrt{I + J} \subseteq \sqrt{\sqrt{I} + \sqrt{J}}$. Combining these, we get $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

We show 6. Assume p is prime and $n > 0$. We show $\sqrt{p^n} \subseteq p$. Let $x \in \sqrt{p^n}$. Then $x^n \in p^n$. Notice that $p^n \subseteq p$, and so we have $x^n \in p$. Notice that p is prime, and so $x \in p$. We show that $p \subseteq \sqrt{p^n}$. Let $x \in p$. Then $x^n \in p^n \subseteq p$. But this means that $x \in \sqrt{p^n}$. Thus, $\sqrt{p^n} = p$. **Q.E.D**

Theorem (Theorem 1.12)**.** Let I be an ideal. Then

$$\sqrt{I} = \bigcap_{\substack{p \in \mathrm{Spec}(P) \\ I \subseteq p}} p.$$

Proof. We show the inclusion first. Suppose $I \subset p$, then $\sqrt{I} \subset \sqrt{p} = p$ (1.11.6).

We show other inclusion. We must show that if an element is not in $\sqrt{I}$, then it's not in $\cap p$ (this is the contrapositive of what we want). In other words, we must show there exists a prime ideal which contains I but it does not contain x. Let $\Sigma = \{x^n : n \geqslant 0\}$. Then $S \cap I = \varnothing$, since x is not in $\sqrt{I}$. By (1.10), there is a prime ideal $p \cap S = \varnothing$, $I \subseteq p$. Notice as well $x \notin p$. Thus, we have what we want. **Q.E.D**

Definition (Reduced Ring)**.** If R is a ring, then $R_{\mathrm{red}} = R/\sqrt{0}$ is a reduced ring.

Definition (Jacobson Radical)**.** We define the Jacobson Radical $\mathrm{Rad}(R)$ to be the intersection of all maximal ideals. Notice that by Theorem 1.12, we have $\sqrt{0} \subset \mathrm{Rad}(R)$.

Proposition (Proposition 1.13)**.** We have that $x \in \mathrm{Rad}(R)$ if and only if $1 + (x) \subseteq R^\times$.

Proof. We show the implication. Assume that $x \in \mathrm{Rad}(R)$. Then we have that x is in all maximal ideals. Since x is in all maximal ideals, we get that (x) is in all maximal ideals as well. Hence, $1 + (x)$ cannot be in any maximal ideals, so it must be a unit (by Corollary 1.6, since it's not in any maximal ideals, it's not in the union, and since it's not in the union it must lie in $R^\times$).

We show the converse. Suppose for contradiction that $x \notin m$ for some maximal ideal, and assume $1 + (x) \subseteq R^\times$. Then it follows that $m + (x) = R$, since m is maximal. Therefore, we get that $1 = n + ax$ for $n \in m$ and $a \in R$. Thus, $1 - ax = n \in m$, or in other words we have $1 + (x) \subseteq m$. But this is a contradiction, since we assumed that $1 + (x) \subseteq R^\times$. Hence, $x \in m$ for all maximal ideals. **Q.E.D**

Chinese Remainder Theorem

Definition (Comaximal)**.** Let I and J be R-ideals. We say that I and J are comaximal if $I + J = R$. We equivalently call this coprime.

Lemma (Comaximality Property)**.** If I and J are R-ideals which are comaximal, then $I \cap J = IJ$.

Proof. We show $I \cap J \subseteq IJ$. By Operations on Ideals, we have $IJ \subseteq I \cap J$. It remains to show that $I \cap J \subseteq IJ$. Let $x \in I \cap J$. Then $x \in I$ and $x \in J$. To show that it's in IJ, it suffices to show that $x = \sum_{i=1}^{n} a_i b_i$ for $a_i \in I$, $b_i \in J$. Since I and J are comaximal, we have that there is some $a \in I$ and $b \in J$ such that $a + b = 1$. Multiply both sides by x to get $ax + bx = x$. Thus, we have that $I \cap J \subseteq IJ$, and so we get $I \cap J = IJ$. **Q.E.D**

Proposition (Product Comaximality)**.** Let I, J, and K be R ideals. If I and J are comaximal, and I and K are comaximal, then $R = RR = (I + J)(I + K) \subseteq I + JK$. Thus, I and JK are comaximal.

Proof. The step $R = (I+J)(I+K)$ is clear (since they are comaximal, $(I+J) = R$ and $(I+K) = R$). It's also clear that $(I+J)(I+K) \subseteq I+JK$. Since $(I+J)(I+K) = R$, and by Operations on Ideals $I + JK$ is an R ideal, we get that $I + JK = R$. Hence, I and JK are comaximal as well. **Q.E.D**

Theorem (Theorem 1.14)**.** Let $I_1, \ldots, I_n$ be R ideals, and have $I_i + I_j = R$ for all $i \neq j$ (they are pairwise comaximal). Then $I_1 \cdots I_n = \cap_{i=1}^{n} I_i$.

Proof. We proceed by induction. The case $n = 1$ is both clear and non-illuminating. We proceed to the case $n = 2$. Denote these ideals by I and J for notational simplicity. Then we have that $I + J = R$, and by the Comaximality Property we get that $IJ = I \cap J$. Assume it holds for n_0. We must show it holds for $n_0 + 1$. Since it holds for n_0, we have $I_1 \cdots I_{n_0} = \cap_{i=1}^{n_0} I_i = J$, since by Operations on Ideals this is an ideal. Then take I_{n_0+1}, and assume it is pairwise comaximal with $I_1, \ldots, I_{n_0}$. By Product Comaximality, it's clear that I_{n_0+1} and J are comaximal. We then use Comaximality Property again with I_{n_0+1} and J to get $I_{n_0+1} \cap J = I_{n_0+1} J$, or $\cap_{i=1}^{n_0+1} I_i = \prod_{i=1}^{n_0+1} I_i$. Thus, our result follows by induction. **Q.E.D**

Corollary (Corollary 1.15)**.** Suppose R is a semilocal ring with maximal ideals $m_1, \ldots, m_n$. Then $\mathrm{Rad}(R) = \prod_{i=1}^{n} m_i$.

Proof. Let m_i, m_j be two maximal ideals. Then we must show they are comaximal. Notice that $m_i, m_j \subseteq m_i + m_j \subseteq R$. If $m_i = m_i + m_j$, then we have that $m_j = 0$ or m_i, which contradicts it being maximal and distinct from m_i. Hence, $m_i + m_j = R$, and so two maximal ideals which are distinct must be comaximal. Since $m_1, \ldots, m_n$ is a finite number of comaximal ideals, and $\mathrm{Rad}(R) = \cap_{i=1}^{n} m_i$, applying Theorem 1.14 gives us the result. **Q.E.D**

Definition (Product of Rings)**.** If R and A are two rings, we define $R \times A = \{(a, b) : a \in R, b \in A\}$ to be the direct product of the rings.

Theorem (Theorem 1.16 (Chinese Remainder Theorem))**.** Let $I_1, \ldots, I_n$ be R-ideals. Define a homomorphism

$$\phi : R \to \prod_{i=1}^{n} R/I_i$$

via $\phi(x) = (x + I_1, \ldots, x + I_n)$. Then

1. We have that ϕ is surjective if and only if $I_i + I_j = R$ for all $i \neq j$.
2. We have that $\ker \phi = \cap I_i$. In particular, if $I_1, \ldots, I_n$ are distinct maximal ideals, then $R/\ker \phi \cong R/I_1 \times \cdots \times R/I_n$.

Proof. We show 1. We first show the implication. Proceed by induction on n, the number of ideals. For $n = 1$, we clearly have that this is surjective. For illustration, we do $n = 2$. Assume ϕ is surjective. Then we have that there is an x in R so that $\phi(x) = (1, 0)$. Notice that $\phi(1-x) = (0, 1)$. So, we have that $x \in I_2$, and $1 - x \in I_1$. Adding these together grants us $x + (1 - x) = 1$, and so $I_1 + I_2$ are comaximal. Assume it holds for n, then we must show it holds for $n+1$. Denote R' as the ring $\prod_{i=1}^{n} R/I_i$. Denote $n_0 = n + 1$. Then examine the ring $R' \times R/I_{n_0}$, and assume ϕ is surjective onto this. We have then that there is some $x \in R$ so that $\phi(x) = (1, 0)$, and $\phi(1 - x) = (0, 1)$. Hence, we have $(1 - x) \in I_1 \cap \cdots \cap I_n$, $x \in I_{n_0}$, and so $I_1 \cap \cdots \cap I_n + I_{n_0} = R$. In other words, I_{n_0} is comaximal with each I_i (since we can find $(1 - x) \in I_i$, $x \in I_{n_0}$) and we are done.

We now show the converse. It suffices to show that we can find elements r_i so that the ith place is 1, that is, $\phi(r_i) = (0, \ldots, 0, 1, 0, \ldots, 0)$. Since $I_i + I_j = R$ for all $i \neq j$, choose I_i and notice that we can find $x \in I_i$ so that $(1 - x) \in I_j$ for all $j \neq i$. Hence, we get that $\phi(1 - x) = (0, \ldots, 0, 1, 0, \ldots, 0)$, and we're done. **Q.E.D**

Theorem (Theorem 1.17 (Prime Avoidance))**.** Let $p_1, \ldots, p_n$ be prime ideals in R and let I be an R-ideal contained in $\cup_{i=1}^{n} p_i$. Then $I \subseteq p_i$ for some i.

Proof. We prove 1. We use induction on n in the form

$$I \nsubseteq p_i \to I \nsubseteq \cup_{i=1}^{n} p_i.$$

This is clear for $n = 1$ by definition. For induction, assume it holds for $n - 1$, and we want to show it holds for n. If it holds for $n - 1$, then for each i there exists $x_i \in I$ such that $x_i \notin p_j$ whenever $j \neq i$. If for some i we have $x_i \notin p_i$, we are done. If not, then $x_i \in p_i$ for all i. Consider the element

$$y = \sum_{i=1}^{n} x_1 \cdots x_{i-1} x_{i+1} \cdots x_n;$$

we have $y \in I$ and $y \notin p_i$. Hence, $I \nsubseteq \cup_{i=1}^{n} p_i$. **Q.E.D**

Remark. I deviated from Ulrich's proof because I really didn't like it. This is from Atiyah MacDonald, Proposition 1.11 (i).

Corollary (Corollary 1.18)**.** Let S be a subset closed under addition and multiplication, let I be an R-ideal, and assume $S \nsubseteq I$. Let $p_1, \ldots, p_n$ be finitely many prime ideals, $n - 1$ of which are prime. If $S/I \subseteq \cup_{i=1}^{n}$, then $S \subseteq p_i$ for some i.

Proof. If $S \subseteq I \cup_{i=1}^{n} p_i$, then by the modified Theorem 1.17 (Prime Avoidance) (only $n - 2$ need be prime by Ulrich's version) $S \subseteq I$, which is impossible, or $S \subseteq p_i$ for some i, as desired. **Q.E.D**

Example. Notice that $R[[x_1, \ldots, x_n]]$ is the power series ring in n variables (see Power Series Ring).

1. $R[[x_1, \ldots, x_n]] = R^\times + (x_1, \ldots, x_n)$.
2. If $1 + (x_1, \ldots, x_n) \subseteq R[[x_1, \ldots, x_n]]^\times$ then $(x_1, \ldots, x_n) \subseteq \mathrm{Rad}(R[[x_1, \ldots, x_n]])$.
3. We have $R[[x_1, \ldots, x_n]]$ is a domain if and only if R is a domain.

Chapter 2: Modules

Operations on Modules

Definition (Module)**.** Let R be a ring. We say that M is an R-module if

1. M is an abelian group with respect to addition.
2. The scalar multiplication operation $\cdot : R \times M \to M$ is associative, distributive, and it has identity.

Example. If R is a ring, then R itself is an R-module.

Definition (Submodule)**.** We say that a subset $N \subseteq M$ is a submodule if it is closed under addition and multiplication.

Definition (Quotient Module)**.** The quotient of a module is a module.

Definition (Homomorphisms Of Modules)**.** Let M, N be R-modules. A mapping $f : M \to N$ is an R-module homomorphism if

1. $f(x + y) = f(x) + f(y)$
2. $f(ax) = a \cdot f(x)$

for all $a \in R$ and $x, y \in M$. Notice that these maps are sometimes called R-linear maps.

Example. (1) R-submodules of R are the ideals.

(2) $\mathbb{Z}$-modules are the abelian groups. If you have a homomorphism of groups, it's naturally a $\mathbb{Z}$-linear map.

(3) $k[x]$ modules, where k is a field, are the k-vector spaces together with the fixed endomorphisms $\phi : V \to V$.

Definition (Ideal Quotient)**.** If I, J are R-ideals, then their ideal quotient is

$$(I : J) = \{x \in R : rJ \subseteq I\}$$

which is an ideal.

Definition (Annihilator)**.** Let R be a ring, M a module. The annihilator of a module, denoted $\mathrm{Ann}_R(M) = (0_M :_R M) = \{x \in R : rM = 0\}$.

Definition (Faithful Module)**.** Let R be a ring, M a module. We say M is faithful if $\mathrm{Ann}_R(M) = 0$.

Definition (Operations on Modules)**.** Suppose $M_i : i \in \mathfrak{I}$ is a family of R-modules. Then we can define

$$\prod_{i \in \mathfrak{I}} M_i = \{(x_i)_{i \in \mathfrak{I}}\}$$

$$\bigoplus_{i \in \mathfrak{I}} M_i = \{(x_i)_{i \in \mathfrak{I}} : \text{ almost all } x_i = 0\}.\}$$

Notice that

$$\bigoplus_{i \in \mathfrak{I}} \subseteq \prod_{i \in \mathfrak{I}} M_i.$$

Definition (Free Module)**.** Let R be a ring, M a module. Then M is a free module if $M \cong \bigoplus_{i \in \mathfrak{I}} R$. In other words, M is a free module if and only if M has a basis.

Definition (Finitely Generated)**.** We say that M is finite, or finitely generated, if there are finitely many elements in M such that $M = Rx_1 + \cdots + Rx_n$. In other words, we say M is finitely generated if and only if there is a free module with n-basis elements $R^n \to M$ which surjects.

Lemma (Lemma 2.1)**.** Suppose M is an R module, $\{x_1, \ldots, x_n\} \subseteq M$, A is an $n \times n$ matrix with entries in R. If

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

then $(\det(A))x_i = 0$ for all i.

Proof. By assumption, we have

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

Multiplying both sides by $\operatorname{adj}(A)$ gives us

$$0 = (\operatorname{adj}A)(A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}) = ((\operatorname{adj}A)A) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Recall that $((\operatorname{adj}A)A) = \det(A)$, and so $\det(A)(x_1, \ldots, x_n)^T = 0$. So for all i, we have $\det(A)x_i = 0$. **Q.E.D**

Theorem (Theorem 2.2 (Nakayama's Lemma))**.** Suppose M is a finitely generated R-module, I is an R-ideal, if $M = IM$, then there exists $a \in 1 + I$ so that $aM = 0$.

Proof. We have that M is finitely generated, so we have that $M = Rx_1 + \cdots + Rx_n$ (see Finitely Generated). So $M = IM$ gives us $(x_1, \ldots, x_n)^T = A(x_1, \ldots, x_n)^T$, where A is some $n \times n$ matrix with entries in I. This then gives us $(I - A)(x_1, \ldots, x_n)^T = 0$. By Theorem 2.2 (Nakayama's Lemma), we get $\det(I - A)x_i = 0$ for all i (recall that the x_i come from the generating set). Hence, $\det(I - A)x_1 + \cdots + \det(I - A)x_n = 0 + \cdots + 0 = 0$. Thus, $\det(I - A) \in 1 + I$, since $\det(I - A) \equiv I \pmod{I}$. **Q.E.D**

Corollary (Corollary 2.3)**.** Suppose N, M are R-modules with M/N finitely generated, and assume $I \subseteq \operatorname{Rad}(R)$ an ideal. IF $M = N + IM$, then $N = M$.

Proof. If $M = N + IM$, $(N + IM)/N = \{(\sum_{i=1}^n (a_i m_i) + N : n \in \mathbb{N}, a_i \in I, m_i \in M\} = \{\sum_{i=1}^n a_i(m_i + N) : n \in \mathbb{N}, a_i \in I, m_i \in M\} = I(M/N)$. Thus, $M/N = I(M/N)$, and using Theorem 2.2 (Nakayama's Lemma) we get $M/N = 0$. Since $M/N = 0$, this implies $M = N$. **Q.E.D**

Definition (Minimal Generating Set)**.** W is called a minimal generating set of a module M if W generates M, but no proper subset of W does generate M.

Example. Let $M = R = \mathbb{Q} \times \mathbb{Q}$. Then $\{(1,1)\}$ is a minimal generating set of M as an R-module. On the other hand $\{(0,1),(1,0)\}$ is a minimal generating set. The reason is because R is not local.

Theorem (Theorem 2.4)**.** Assume R is a local ring with maximal ideal m, M is a f.g. R-module, $\bar{M} = M/mM$, $k = R/m$. For an element $x \in M$, write $\bar{x}$ for its image in $\bar{M}$.

1. $\{x_1, \ldots, x_n\}$ is a minimal generating set of M if and only if $\{\bar{x_1}, \ldots, \bar{x_n}\}$ is a basis for $\bar{M}$ as a k-vector space. In particular, every minimal generating set of M has the same cardinality. Furthermore, this cardinality is finite.

2. Suppose $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_n\}$ are two minimal generating sets of M. Then $(y_1, \ldots, y_n)^T = A(x_1, \ldots, x_n)^T$ for some invertible $n \times n$ matrix A with entries in R.

Proof. We show 1. For the implication, we proceed by contradiction. We have to show $\{\bar{x_1}, \ldots, \bar{x_n}\}$ is a minimal generating set of $\bar{M}$. Suppose not. Then we could take out one of the $\bar{x_i}$. Therefore, $\{x_1, \ldots, x_n\}$ is not a minimal generating set, a contradiction.

We show the converse. In order to do that, we show that $\{x_1, \ldots, x_n\}$ is a generating set. Note that it's automatically minimal. We know $\bar{M} = k\bar{x_1} + \cdots + k\bar{x_n}$, hence $M = Rx_1 + \cdots + Rx_n + mM$. Since R is local with maximal ideal m, $m = \mathrm{Rad}(R)$, and hence by Corollary 2.3 this implies $M = Rx_1 + \cdots + Rx_n$. Thus $\{x_1 \ldots, x_n\}$ is a generating set.

We show 2. There exists an $n \times n$ matrix in A, with entries in R with $(y_1, \ldots, y_n)^T = A(x_1, \ldots, x_n)^T$. Now $(\bar{y_1}, \ldots, \bar{y_n})^T = \bar{A}(\bar{x_1}, \ldots, \bar{x_n})^T$. By (a), $\{\bar{y_1}, \ldots, \bar{y_n}\}$ and $\{\bar{x_1}, \ldots, \bar{x_n}\}$ are k-vector spaces bases of $\bar{M}$. So $\bar{A}$ has an inverse; in other words, $\det(\bar{A}) \neq \bar{0}$. Hence $\det(A) \neq \bar{0}$. Then $\det(A) \notin m$ and it's a unit. Hence, the A is invertible, since $\frac{1}{\det(A)}\mathrm{adj}(A)$ is the inverse of A. **Q.E.D**

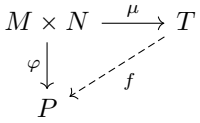
Definition (Minimal Number of Generators)**.** Let M be a finite module over a local ring R with maximal ideal m and residue field k. Then the minimal number of generators of M, denote $\mu(M)$, is the cardinality of any minimal generating set. Notice that $\mu(M) = \dim_k(\bar{M})$, where $\bar{M} = M/mM$. If M happens to be a vector space already, then $\mu(M) = \dim_k(M)$. So we have a notion of dimension of modules. In Noetherian rings, submodules of finitely generated modules will be finitely generated.

Theorem (Theorem 2.5)**.** Let M be a finite R-module, $\varphi \in \mathrm{Hom}_R(M, M)$. Suppose φ is surjective. Then φ is injective, i.e. it's an isomorphism. Furthermore, $\varphi^{-1} = f(\varphi)$ for some $f \in R[x]$.

Proof. M is an $R[x]$-module via $x \cdot n = \varphi(n)$. By extension, any polynomial $f \in R[x]$ and $f(x) \cdot n = (f(\varphi))(n)$. Notice that M is in particular a finite $R[x]$-module. Since φ is surjective, $\varphi(M) = M$. Recall $\varphi(M) = xM$ then $(x)M = M$. Applying Theorem 2.2 (Nakayama's Lemma), we have that $(1 + (x))M = 0$. Thus, we have $(1 - xf)M$. So $(1 - xf) \cdot n = 0$ for all $n \in M$. Thus, distributing, we get $n = nxf$ for all $n \in M$. Then we get that $n = (\varphi \circ f(\varphi))(n)$ for all n in N, which is equivalent to $\varphi \circ f(\varphi) = 1_M$. Thus, $f(\varphi) \circ \varphi = 1_M$. Since φ has an inverse and it's surjective, it is a bijective homomorphism (isomorphism). **Q.E.D**

Tensor Products

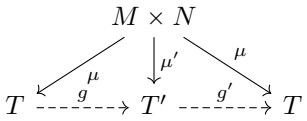
Theorem (Theorem 2.6 (Tensor Product))**.** There exists an R-module $T = T(M, N)$ and an R-bilinear map $\mu : M \; times N \to T$ so that for any R-bilinear map $\varphi : M \times N \to P$ there exists a unique R-linear map $f : T \to P$ so that $\varphi = f \circ \mu$. Notice that it commutes. This is called the tensor product.



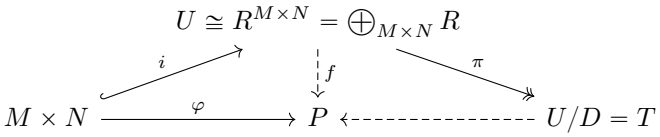
Proof. Proof omitted. **Q.E.D**

Remark. Let T' and μ' have the same property as T and μ, then there exists a unique R-linear map $g : T \to T'$ which is an isomorphism, and furthermore $\mu' = g \circ \mu$.

Proof. (Proof of remark) We begin with uniqueness. Notice that we have the commutative diagram below. For now, assume existence. Let the first dotted line be g and let the second dotted line be g'. Then we get $g \circ g' = \mathrm{Id}$, and likewise $g \circ g' = \mathrm{Id}$, and so it is an isomorphism, as the remark required.



We now show existence. Using the universal property, we get the diagram below. The problem is, however, that i is not bilinear, so T is a submodule generated by all elements of the form $(r_1m_1 + r_2m_2, n) - r_1(m_1, n) - r_2(m_2, n)$ and $(m, r_1n_1 + r_2n_2) - r_1(m, n_1) - r_2(m, n_2)$. Then μ is bilinear. By the Fundamental Theorem on Homomorphisms, f exists if and only if $D \subseteq \ker(f)$. It's enough to check this for the generators of D. Indeed, $F((r_1m_1+r_2m_2, n)) - r_1(m_1, n) - r_2(m_2, n)) = F((r_1m_1+r_2m_2, n) - r_1F(m_1, n)) - r_2F((m_2, n)) = \phi(r_1m_1+r_2m_2, n) - r_1\phi(m_1, n) - r_2\phi(m_2, n) = 0$, since ϕ is bilinear. Finally, f is uniquely determined by ϕ, because T is generated as an R-module by $\mu(M \times N)$, and moreover the f is eternined uniquely on $\mu(M \times N)$, and f is R-linear.



Q.E.D

Definition (Tensor Product)**.** We call $T = T(M, N)$ the tensor product of M and N, and we write $M \otimes_R N$. We also write $x \otimes_R y$ for $\mu(x, y)$.

Remark. If V and W are generating sets of M and N respectively, then $M \otimes_R N = \{\sum_{\text{finite}} x_i \otimes_R y_i : x_i \in M, y_i \in N\} = \{\sum_{\text{finite}} r_i(v_i \otimes_R w_i) : v_i \in V, w_i \in W, r_i \in R\}$.

Theorem (Theorem 2.7)**.** Let M, N, P be R modules. The following properties hold.

(a) $M \otimes_R N \cong N \otimes_R M$.
(b) $(M \otimes_R N) \otimes_R P \cong M \otimes_R N \otimes_R P \cong M \otimes_R (N \otimes_R P)$.
(c) $(M \oplus N) \otimes_R P \cong (M \otimes_R P) \oplus (N \otimes_R P)$.
(d) $R \otimes_R M \cong M$.

Proof. (a) Note that $M \times N \cong N \times M$ via $(m,n) \mapsto (n,m)$. We then have $M \times N \to N \times M \to N \otimes_R M$ is a bilinear mapping from $M \times N$ into $N \otimes_R M$ via $(m,n) \mapsto n \otimes m$. Note then by the universal property we have that there is a unique linear mapping from $M \otimes_R N$ to $N \otimes_R M$ by sending $m \otimes n \mapsto n \otimes m$. There is an analogous argument for $N \otimes_R M \to M \otimes_R N$. Let $h : M \otimes_R N \to N \otimes_R M$ and $\bar{h} : N \otimes_R M \to M \otimes_R N$. We must show that these are inverses on the on the generators. This is, however, clear; if $m \otimes n$ is a generating element, then $\bar{h}(h(m \otimes n)) = m \otimes n$ and likewise $h(\bar{h}(n \otimes m)) = n \otimes m$. Hence, $h^{-1} = \bar{h}$, and we have $M \otimes_R N \cong N \otimes_R M$. Hence, the tensor product is symmetric.

(b) We must construct homomorphisms f, g such that $f : (M \otimes_R N) \otimes_R P \to M \otimes_R N \otimes_R P$ and $g : M \otimes_R N \otimes_R P \to (M \otimes_R N) \otimes_R P$, and we will show that $f \circ g = g \circ f = \mathbb{1}$. Fixing an element $p \in P$, we must show that the homomorphism $(m,n) \mapsto m \otimes n \otimes p$ is bilinear. The function is well-defined, since the selection of representatives is arbitrary. We have $m \otimes n \otimes p = m' \otimes n' \otimes p$. Notice that $(a_1 m_1 + a_2 m_1, n) \mapsto (a_1 m_1 + a_2 m_2) \otimes n \otimes p = a_1 m_1 \otimes n \otimes p + a_2 m_2 \otimes n \otimes p = a_1(m_1 \otimes n \otimes p) + a_2(m_2 \otimes n \otimes p)$ which is equivalent to $a_1(m_1, n) + a_2(m_2, n) \mapsto a_1(m_1 \otimes n \otimes p) + a_2(m_2 \otimes n \otimes p)$, and so it's linear in the first component. Linearity for the second component follows similarly. By the universal property this induces a homomorphism $f_p : M \otimes_R N \to M \otimes_R N \otimes_R P$. Consider then the mapping of $(\alpha, p) \mapsto f_p(\alpha)$ of $(M \otimes_R N) \times P$ into $M \otimes_R N \otimes_R P$. Denote this mapping $\bar{f}$. It's clear that this is well-defined, and bilinearity follows readily. Linearity in the first component is clear, and we have $\bar{f}((m \otimes n), ap) = m \otimes (n \otimes ap) = m \otimes a(n \otimes p) = a(m \otimes (n \otimes p)) = a\bar{f}(m \otimes n, p)$ and $\bar{f}(m \otimes n, p + p') = m \otimes (n \otimes (p + p')) = m \otimes ((n \otimes p) + (n \otimes p')) = (m \otimes (n \otimes p)) + (m \otimes (n \otimes p')) = \bar{f}(m \otimes n, p) + \bar{f}(m \otimes n, p')$. Thus bilinearity follows. Then by the universal property this induces another homomorphism $f : (M \otimes_R N) \otimes_R P \to M \otimes_R N \otimes_R P$, where $f((m \otimes n) \otimes p) = m \otimes n \otimes p$. Note that g is easier to construct; consider the mapping $(m,n,p) \mapsto (m \otimes n) \otimes p$ of $M \times N \times P$ into $(M \otimes_R N) \otimes_R P$. This is clearly linear in each variable (and hence multilinear) and so we have that by the universal property this induces a mapping $g : M \otimes_R N \otimes_R P \to (M \otimes_R N) \otimes_R P$. On the generators of $(M \otimes_R N) \otimes_R P$ and $M \otimes_R N \otimes_R P$ we can clearly see that $f \circ g = g \circ f = \mathbb{1}$, and so it follows readily that $f = g^{-1}$ and so we have an isomorphism.

We must construct again isomorphisms f, g such that $f : M \otimes_R (N \otimes_R P) \to M \otimes_R N \otimes_R P$ and $g : M \otimes_R N \otimes_R P \to M \otimes_R (N \otimes_R P)$ where $f \circ g = g \circ f = \mathbb{1}$. Fix an element $m \in M$. Then we have $(n,p) \mapsto m \otimes n \otimes p$ is bilinear by above (the argument is near identical), and so by the universal property this induces a homomorphism $f_m : N \otimes_R P \to M \otimes_R N \otimes_R P$, where $f_m(n,p) = m \otimes n \otimes p$. Consider the mapping $(m, \alpha) \mapsto f_m(\alpha)$ of $M \times (N \otimes_R P)$ into $M \otimes_R N \otimes_R P$. Then by the universal property this induces a homomorphism $f : M \otimes_R (N \otimes_R P) \to M \otimes_R N \otimes_R P$, where $f(m \otimes (n \otimes p)) = m \otimes n \otimes p$. Note again g is easier; consider the mapping $(m,n,p) \mapsto m \otimes (n \otimes p)$ of $M \times N \times P$ into $M \otimes_R (N \otimes_R P)$. Then this induces a homomorphism $g : M \otimes_R N \otimes_R P \to M \otimes_R (N \otimes_R P)$ where $g(m \otimes n \otimes p) = m \otimes (n \otimes p)$. We have f and g are clearly inverses on the generators of these modules, and so $f \circ g = g \circ f = \mathbb{1}$, and so we have an isomorphism. Hence, the tensor product is associative.

(c) Let $f : (M \oplus N) \times P \to (M \otimes_R P) \oplus (N \otimes_R P)$ be the mapping defined by $((m,n),p) \mapsto (m \otimes p, n \otimes p)$. Note that this is clearly well-defined. We must show that this is bilinear. Let $r \in R$, $m, m' \in M$, $p, p' \in P$ and $n, n' \in N$. Then we have that

$$f(r(m,n),p) = f((rm,rn),p) = (rm \otimes p, rn \otimes p) =$$

$$(r(m \otimes p), r(n \otimes p)) = r(m \otimes p, n \otimes p) = rf((m,n),p),$$

$$f((m,n),rp) = (m \otimes rp, n \otimes rp) = (r(m \otimes p), r(n \otimes p)) =$$

$$r(m \otimes p, n \otimes p) = rf((m,n),p),$$

$$f((m,n)+(m',n'),p) = f((m+m',n+n'),p) = ((m+m') \otimes p, (n+n') \otimes p) =$$

$$(m \otimes p, n \otimes p) + (m' \otimes p, n' \otimes p) = f((m,n),p) + f((m',n'),p),$$

$$f((m,n),p+p') = (m \otimes (p+p'), n \otimes (p+p') = (m \otimes p, n \otimes p) + (m \otimes p', n \otimes p') =$$

$$f((m,n),p) + f((m,n),p').$$

So, we have that f is bilinear. By the universal property, this induces a linear mapping $g : (M \oplus N) \otimes_R P \to (M \otimes_R P) \oplus (N \otimes_R P)$, which can be defined as $g((m,n) \otimes p) = (m \otimes p, n \otimes p)$. Now, we must find an inverse function from $(M \otimes_R P) \oplus (N \otimes_R P) \to (M \oplus N) \otimes_R P$. Likewise, we must use the universal property of direct sums to find the inverse. Let $j_1 : M \times P \to (M \oplus N) \otimes_R P$ be defined by $j_1(m,p) = (m,0) \otimes p$, and $j_2 : N \times P \to (M \oplus N) \otimes_R P$ be defined by $j_2(n,p) = (0,n) \otimes p$. These are clearly well-defined. We then get the linear maps $j_1' : M \otimes_R P \to (M \oplus N) \otimes_R P$ and $j_2' : N \otimes_R P \to (M \oplus N) \otimes_R P$ defined in the canonical fashion. We then have by the universal property of direct sums a function $j : (M \otimes_R P) \oplus (N \otimes_R P) \to (M \oplus N) \otimes_R P$ defined by $j(m \otimes p, n \otimes p) = (m,0) \otimes p + (0,n) \otimes p$.

Let $(m,n) \otimes p \in (M \oplus N) \otimes_R P$ be a generator. We have then that

$$j(g((m,n) \otimes p)) = j(m \otimes p, n \otimes p) = (m,0) \otimes p + (0,n) \otimes p = (m,n) \otimes p,$$

as required, and so $j \circ g = \mathbb{1}$ on the generators. Likewise, let $(m \otimes p, 0)$ and $(0, n \otimes p)$ in $(M \otimes_R P) \oplus (N \otimes_R P)$ be generators. We have

$$g(j(m \otimes p, 0)) = g((m,0) \underset{p}{\otimes}) = (m \otimes p, 0)$$

and likewise for $(0, (n \otimes p)$. Thus, $g \circ j = \mathbb{1}$, and so we have g and j are inverses and form an isomorphism.

(d) Let $f' : R \times M \to M$ be a homomorphism $f(r,m) = rm$. We must show that this is a bilinear map. Notice $f(a_1r_1 + a_2r_2, m) = (a_1r_1 + a_2r_2)m = a_1r_1m + a_2r_2m = a_1f(r_1,m) + a_2f(r_2,m)$. The argument for the linearity of the second component is similar. Then we have that this is a bilinear map from $R \times M \to M$, and so we have that this must induce a linear map $f : R \otimes_R M \to M$ where $f(r \otimes m) = rm$. Let $g : M \to R \otimes_R M$ be the linear mapping $g(m) = 1 \otimes m$. This is clearly linear, and so it suffices to show that these maps are inverses. Let $m \in M$ be a generator of M, $r \in R$. Then we have

$$f(g(m)) = f(1 \otimes m) = m$$

and

$$g(f(r \otimes m)) = g(rm) = 1 \otimes rm = r(1 \otimes m) = r \otimes m.$$

Thus, we have that they are inverses and this creates an isomorphism from $M \to R \otimes_R M$. **Q.E.D**

Definition (Bimodules)**.** Suppose R and S are two rings. Then we say that N is an R-S bimodule if it is an R-module and an S-module. Furthermore, $r(sn) = s(rn)$ for all r in R, s in S, and n in N.

Proposition (Proposition 2.8)**.** Let R and S be rings. Suppose M is an R-module, N is an R-S bimodule, and P is an S-module. Then

(a) $M \otimes_R N$ is an R-S bimodule.

(b) $(M \otimes_R N) \otimes_P S \cong_{R-S} M \otimes_R (N \otimes_P S)$

Proof. (a) We must show that $M \otimes_R N$ is an $R - S$ bimodule. Fix some $s \in S$. Let there be a map $M \times N$ into $M \otimes_R N$ defined via $(m, n) \mapsto m \otimes sn$. We also have the natural map from $M \times N$ into $M \otimes_R N$ defined via $(m, n) \mapsto (m \otimes n)$. Hence, by the universal property this induces a unique and linear map from $M \otimes_R N$ to $M \otimes_R N$ via $m \otimes n \mapsto m \otimes sn$. Hence, let $M \otimes_R N$ be our module T, and so we want to show that $T \times S \to T$ is well-defined. If $(t, s) = (t', s')$ then we have $ts = t's'$ but $(t, s) = (t', s') \to s = s'$ since S is a ring. Hence, we have that our function $f : (M \otimes_R N) \times S \to M \otimes_R N$ is well-defined, and is given essentially by our function above. Denote this map $\phi : (M \otimes_R N) \times S \to M \otimes_R N$. Then we have $\mu(\sum m_i \otimes n_i) = \sum \mu(m_i \otimes n_i) = \sum m_i \otimes sn_i$ as required. So, it follows that $M \otimes_R N$ is an $R - S$ bimodule.

(b) Fix $p \in P$. Then let $f_p : M \times N \to (M \otimes_R N) \otimes_S P$ be defined by $(m, n) \mapsto m \otimes (n \otimes p)$. This is clearly well-defined. The biadditivity property is similar to Problem 4 (c) above, and so it remains to show that this is bilinear by showing the scalar property. Let $r \in R$. Then we have

$$f_p(rm, n) = rm \otimes (n \otimes p) = r(m \otimes (n \otimes p)) = rf_p(m, n)$$

and likewise

$$f_p(m, rn) = m \otimes (rn \otimes p) = m \otimes r(n \otimes p) = r(m \otimes (n \otimes p)) = rf_p(m, n).$$

Hence, it is bilinear. By the universal property, we have that this induces a linear mapping $f'_p : M \otimes_R N \to M \otimes_R (N \otimes_S P)$ by taking $f'_p(m \otimes n) = m \otimes (n \otimes p)$. Let p vary. Then we have a mapping $f : (M \otimes_R N) \times P \to M \otimes_R (N \otimes_S P)$ defined by $f((m \otimes n), p) = f'_p(m \otimes n)$. We must show that this mapping is bilinear. It is clearly biadditive. It's also R-linear in the first variable by definition of f'_p. Hence, it remains to show that it is S-bilinear. Let $s \in S$. Then we have

$$f((m \otimes n)s, p) = f(m \otimes ns, p) = m \otimes (ns \otimes p) =$$

$$m \otimes (n \otimes p)s = (m \otimes (n \otimes p))s = f(m \otimes n, p)s$$

and

$$f(m \otimes n, ps) = m \otimes (n \otimes ps) = m \otimes (n \otimes p)s = (m \otimes (n \otimes p))s = f(m \otimes n, p)s.$$

By the universal property, we get that since this is bilinear, it induces a linear mapping $f' : (M \otimes_R N) \otimes_S P \to M \otimes_R (N \otimes_S P)$, where $f'((m \otimes_R n) \otimes_S p) = m \otimes_R (n \otimes_S p)$.

We now must find the inverse. Fix $m \in M$. Then we define $f_m : N \times P \to M \otimes_R (N \otimes_S P)$ by taking $(n, p) \mapsto (m \otimes n) \otimes p$ The biadditivity is clear, and it remains to show the scalar property. Let $s \in S$. Then we have

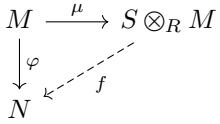
$$f_m(ns, p) = (m \otimes ns) \otimes p = (m \otimes n)s \otimes p = ((m \otimes n) \otimes p)s = f_m(n, p)s$$

and likewise

$$f_m(n, ps) = (m \otimes n) \otimes ps = ((m \otimes n) \otimes p)s = f_m(n, p)s.$$

Hence it is bilinear. By the universal property, we have that this induces a linear mapping $f'_m : N \otimes_S P \to (M \otimes_R N) \otimes_S P$ by taking $f'_m(n \otimes p) = (m \otimes n) \otimes p$. Let m vary now. Then we have the mapping $f : M \times (N \otimes_S P) \to (M \otimes_R N) \otimes_S P$ defined by $f(m, (n \otimes p)) = f'_m(n \otimes p)$. The process is similar to above to show that it is bilinear. It is clear that is also biadditive, and it's S-linear in the second variable by definition of f'_m. Also by above, it's clear to show that it's R-bilinear. Then this induces a linear mapping $g' : M \otimes_R (N \otimes_S P) \to (M \otimes_R N) \otimes_S P$, where $g'(m \otimes_R (n \otimes_S p)) = (m \otimes_R n) \otimes_S p$. Now we note that they're inverses; $f'(g'(m \otimes_R (n \otimes_S p))) = f'((m \otimes_R n) \otimes_S p) = m \otimes_R (n \otimes_S p)$ and likewise $g'(f'((m \otimes_R n) \otimes_S p)) = g'(m \otimes_R (n \otimes_S p)) = (m \otimes_R n) \otimes_S p$. Thus, $M \otimes_R (N \otimes_S P) \cong (M \otimes_R N) \otimes_S P$. **Q.E.D**

Theorem (Theorem 2.9)**.** Let R and S be rings, $\varphi : R \to S$ a homomorphism of rings, and M an R-module. Then $S \otimes_R M$ is an S-module by Proposition 2.8, and $\mu : M \to S \otimes_R M$ where $\mu(m) = 1 \otimes_R m$ is an R-linear map. Furthermore, for every S-module N and any R-linear map $\varphi : M \to N$, there exists a unique S-linear map $f : S \otimes_R M \to N$ with $\varphi = f \circ \mu$. Thus, we have the following commutative diagram.



Proof. (It was unclear on what to do for this one, so I tried the best I could.)

We begin by construction a map from $S \times M$ into $S \otimes_R M$ via $(s, m) \mapsto s \otimes m$. We then construct another map from $S \times M$ into $S \times N$ via $(s, m) \mapsto (s, \phi(n))$. This is clearly bilinear, as was the map before, and so we have an induced linear mapping from $S \otimes_R M$ into $S \times N$. Next we have the projection map of $S \times N$ into N via $(s, n) \mapsto n$. We then have a function from $S \times N$ into $S \otimes_S N$ via $(s, n) \mapsto s \otimes_S n$. Denote this map g. This induces a unique S-linear mapping from $S \otimes_S N$ into N via $s \otimes n \mapsto n$. Finally, we have the mapping $S \otimes_R M$ into $S \otimes_S N$ via $s \otimes m \mapsto s \otimes \psi(m)$ by the previous maps constructed. Denote this map h. Then we can define $f = g \circ h$, and we have that it makes the prior map commute and is unique. Note that it commutes since $\psi = f \circ \mu$ since for all m we have $f(\mu(m)) = f(1 \otimes m) = \psi(m)$. **Q.E.D**

Definition (Algebra)**.** Let $\psi : R \to S$ be a homomorphism of rings, then S is an R-algebra. This is equivalent to R and S being both rings, then S is an R-S bimodule. Equivalently, R and S are rings, S is an R module, and $r(s_1 s_2) = s_1(r s_2)$.

Proposition (Proposition 2.10)**.** Suppose we have two R-algebras, S and T. Then $S \otimes_R T$ is again an R-algebra, via $(s \otimes_R t)(s' \otimes_R t') = (ss' \otimes_R tt')$.

Proof. Recall that we define an R-algebra to be a ring S together with a ring homomorphism $f : R \to S$. In this case, let $f : R \to S$ be the corresponding homomorphism for S an R-module and let $g : R \to T$ be the corresponding homomorphism for T an R-module. Then we have that S and T are R-algebras. Consider then the mapping $S \times T \times S \times T \to S \otimes_R T$ defined by $(s, t, s', t') \mapsto (ss', tt')$. This is clearly R-linear in each factor, and therefore by the multilinear tensor product this induces an R-module homomorphism $S \otimes_R T \otimes_R S \otimes_R T \to S \otimes_R T$. Using Problem 4 (b) we have then that this is $(S \otimes_R T) \otimes_R (S \otimes_R T) \to (S \otimes_R T)$. By the universal property, this corresponds to some R-bilinear mapping $\mu : (S \otimes_R T) \times (S \otimes_R T) \to S \otimes_R T$ which is $\mu(s \otimes t, s' \otimes t') = ss' \otimes tt'$.

We now show that this is a commmutative ring. First, note that this clearly forms an additive abelian group by the properties of tensor products. Next, note that it's closed under multiplication clearly, and it has identity $1 \otimes 1$, since $(s \otimes t)(1 \otimes 1) = s \otimes t = (1 \otimes 1)(s \otimes t)$. Associativity under multiplication is clear by properties of tensor products. Note that it's also abelian under multiplication: $(s \otimes t)(s' \otimes t') = ss' \otimes tt' = s's \otimes t't = (s' \otimes t')(s \otimes t)$. Finally, we show that it's distributive; let $s_1, s_2, s_3 \in S$, $t_1, t_2, t_3 \in T$, then $(s_1 \otimes t_1)((s_2 \otimes t_2) + (s_3 \otimes t_3)) = (s_1 \otimes t_1)((s_2 + s_3) \otimes (t_2 + t_3)) = (s_1 s_2 + s_2 s_3) \otimes (t_1 t_2 + t_1 t_3) = (s_1 s_2 \otimes t_1 t_2) + (s_1 s_3 \otimes t_1 t_3) = (s_1 \otimes t_1)(s_2 \otimes t_2) + (s_1 \otimes t_1)(s_3 \otimes t_3)$. The argument for the other direction of distributivity is similar. Hence, it's a commutative ring with identity.

Finally, to show it's an R-algebra we need to show that there is a ring homomorphism $h : R \to S \otimes_R T$. Let $h(a) = f(a) \otimes g(a)$, where f and g are defined above. The properties follow clearly; $h(a+b) = f(a+b) \otimes g(a+b) = f(a) + f(b) \otimes g(a) + g(b) = f(a) \otimes g(a) + f(b) \otimes g(b) = h(a) + h(b)$, $h(ab) = f(ab) \otimes g(ab) = f(a)f(b) \otimes g(a)g(b) = (f(a) \otimes g(a))(f(b) \otimes g(b)) = h(a)h(b)$, and $h(1) = f(1) \otimes g(1) = 1 \otimes 1$ which is the identity in the ring, as we showed earlier. Hence, we have that $S \otimes_R T$ is an R-algebra by definition. **Q.E.D**

Exact Sequences

Definition (Complex)**.** Suppose we have $\delta_i : M_i \to M_{i-1}$ R-linear maps, where $i \in \mathbb{Z}$. Then we can put them together as follows.

$$\cdots \xrightarrow{\delta_{i+2}} M_{i+1} \xrightarrow{\delta_{i+1}} M_i \xrightarrow{\delta_i} M_{i-1} \xrightarrow{\delta_{i-1}} \cdots$$

Such a sequence is called a complex of R modules if $\delta i \circ \delta_{i+1} = 0$ for all i. Notice that this is equivalent to $\operatorname{Im}(\delta_{i+1}) \subseteq \ker(\delta_i)$ for all i.

Definition (Exact Sequences)**.** If we have a complex of R-modules such that $\operatorname{Im}(\delta_{i+1}) = \ker(\delta_i)$ for all i, then we call it an exact sequence of R modules.

Definition (Short Exact Sequence)**.** If you have a sequence

$$0 \to M' \to M \to M'' \to 0.$$

it is called a short exact sequence.

Remark. Notice that $0 \to M' \xrightarrow{\varphi} M$ is exact if and only if φ is injective. Notice as well that $M \xrightarrow{\psi} M'' \to 0$ is exact if and only if ψ is surjective. Notice that $M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$ is exact if and only if ψ induces an isomorphism between $M/\operatorname{Im}(\varphi)$ and M''.

Definition (Cokernel)**.** The cokernel of a map $f : M' \to M$ is $M/\operatorname{Im}(f)$. This is generally denoted $\operatorname{Coker}(f)$.

Theorem (Theorem 2.11 (Snake Lemma))**.** If we have the following commutative diagram, then diagram following has induced mappings and they give a six term exact sequence. Moreover, if φ is injective, then so is $\bar{\varphi}$, and if ψ is surjective then so is $\bar{\psi}$.

$$\begin{array}{ccccccccc}
 & & \ker(f') & \xrightarrow{\bar{\varphi}} & \ker(f) & \longrightarrow & \ker(f'') & & \\
 & & \downarrow{\scriptstyle i_{f'}} & & \downarrow{\scriptstyle i_f} & & \downarrow{\scriptstyle i_{f''}} & & \\
 & & M' & \xrightarrow{\varphi} & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\
0 & \longrightarrow & N' & \longrightarrow & N & \xrightarrow{\psi} & N'' & & \\
 & & \downarrow{\scriptstyle \pi_{f'}} & & \downarrow{\scriptstyle \pi_f} & & \downarrow{\scriptstyle \pi_{f''}} & & \\
 & & \mathrm{Coker}(f') & \longrightarrow & \mathrm{Coker}(f) & \xrightarrow{\bar{\psi}} & \mathrm{Coker}(f'') & &
\end{array}$$

$$\begin{array}{ccccccc}
\ker(f') & \longrightarrow & \ker(f) & \longrightarrow & \ker(f'') & \multirow{2}{*}{$\Big)$} & \\
 & & & & & \multirow{2}{*}{δ} & \\
\hookrightarrow \mathrm{Coker}(f') & \longrightarrow & \mathrm{Coker}(f) & \longrightarrow & \mathrm{Coker}(f'') & &
\end{array}$$

Proof. Proof omitted. **Q.E.D**

Theorem (Five Lemma)**.** If we have the following commutative diagram with exact rows, then f is an isomorphism.

$$\begin{array}{ccccccccc}
A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & D & \longrightarrow & E \\
\downarrow & & \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \cong} & & \downarrow \\
A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & D' & \longrightarrow & E'
\end{array}$$

Proof. Proof omitted. **Q.E.D**

Definition (Hom)**.** Let M, M', N be R-modules such that we have a map $\varphi : M' \to M$. Then we define $\mathrm{Hom}_R(\varphi, N) : \mathrm{Hom}_R(N, N') \to \mathrm{Hom}_R(N, M)$ via $f \mapsto \varphi \circ f$. Note that this is R-linear.

Define $\mathrm{Hom}_R(\varphi, N) : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N)$ via $f \mapsto f \circ \varphi$. Note that this is R-linear.

Define $\varphi \otimes_R N : M' \otimes_R N \to M \otimes_R N$ via $m' \otimes_R n \mapsto \varphi(m') \otimes_R n$.

Remark. $\mathrm{Hom}_R(N, \varphi\varphi') = \mathrm{Hom}_R(N, \varphi) \circ \mathrm{Hom}_R(N, \varphi')$ is covariant, since the order of the maps stay the same. Notice $\mathrm{Hom}_R(\varphi\varphi', N) = \mathrm{Hom}_R(\varphi', N) \circ \mathrm{Hom}_R(\varphi, N)$. This is contravariant, since the order of the maps is reversed. Notice that $\varphi\varphi' \otimes_R N = (\varphi \otimes_R N) \circ (\varphi' \otimes_R N)$. We have that this is covariant.

Theorem (Theorem 2.12)**.** (a) The following are equivalent.

(i) $0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M''$ is exact.

(ii) $0 \to \mathrm{Hom}_R(N, M') \xrightarrow{\mathrm{Hom}_R(N,\varphi)} \mathrm{Hom}_R(N, M) \xrightarrow{\mathrm{Hom}_R(N,\psi)} \mathrm{Hom}_R(N, M'')$ is exact for all N.

(b) The following are equivalent.

(i) $M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$ is exact.

(ii) $0 \to \mathrm{Hom}_R(M'', N) \xrightarrow{\mathrm{Hom}_R(\psi, N)} \mathrm{Hom}_R(M, N) \xrightarrow{\mathrm{Hom}_R(\varphi, N)} \mathrm{Hom}_R(M', N)$ is exact for all N.

(iii) $M' \otimes_R N \xrightarrow{\varphi \otimes_R N} M \otimes_R N \xrightarrow{\psi \otimes_R N} M'' \otimes_R N \to 0$ is exact for all N.

Proof. (a) Denote $\bar{\varphi} = \mathrm{Hom}_R(N, \varphi)$ and $\bar{\psi} = \mathrm{Hom}_R(N, \psi)$. We begin with (i) implies (ii). Since the sequence in (i) is exact, we get that φ is injective. We want to then establish that $\bar{\varphi}$ is also injective. Recall that by definition $\bar{\varphi} : \mathrm{Hom}_R(N, M') \to \mathrm{Hom}_R(N, M)$ where $f \mapsto \varphi \circ f$. Assume that this is not injective, then we get that the kernel is nontrivial. Notice that the kernel of $\bar{\varphi}$ are the functions $f \in \mathrm{Hom}_R(N, M')$ with $\varphi \circ f = 0$. But φ is injective, so if $\varphi(f(x)) = 0$ for all $x \in N$, then this must mean that $f(x) = 0$ for all $x \in N$. In other words, the kernel is trivial, and we get a contradiction. So $\bar{\varphi}$ is injective.

Next, we must show that $\mathrm{Im}(\bar{\varphi}) = \ker(\bar{\psi})$, and thus the sequence will be exact. We begin with $\mathrm{Im}(\bar{\varphi}) \subseteq \ker(\bar{\psi})$. Let $f \in \mathrm{Hom}_R(N, M')$. Then $\bar{\varphi}(f) = \varphi \circ f$. Notice that $\bar{\psi}(\varphi \circ f) = \psi \circ (\varphi \circ f)$. By assumption, $\psi(\varphi \circ f(x)) = 0$ for all $x \in M'$ and all $f \in \mathrm{Hom}_R(N, M')$, since $\ker(\psi) = \mathrm{Im}(\varphi)$. So, we get that $\mathrm{Im}(\bar{\varphi}) \subseteq \ker(\bar{\psi})$. Next, we show the other direction; that is, $\ker(\bar{\psi}) \subseteq \mathrm{Im}(\bar{\varphi})$. But this also just follows since $\ker(\varphi) = \mathrm{Im}(\psi)$. Hence, we have (i) implies (ii).

For the other direction, notice that $\bar{\varphi}$ is injective. This means that if $\varphi(f_1(x)) = \varphi(f_2(y))$ then $f_1(x) = f_2(y)$. This automatically gives us that φ is injective then; for if we have $\varphi(x) = \varphi(y)$ but $x \neq y$, then we could construct homomorphisms f, g such that $f(x) = x$ and $g(y) = y$, and we have then that $\varphi(f(x)) = \varphi(g(y))$, which results in a contradiction. Thus, φ must also be injective. We again must check that $\mathrm{Im}(\varphi) = \ker(\psi)$. Notice that $\bar{\psi} \circ \bar{\varphi} = 0$ by assumption. Then this gives us $\psi \circ \varphi \circ f = 0$ for all $f \in \mathrm{Hom}_R(N, M')$. Take f to be the identity function where $N = M'$, then we have $\psi \circ \varphi = 0$. Then we have that $\mathrm{Im}(\psi) \subseteq \ker(\psi)$. Now, let $N = M/\mathrm{Im}(\varphi)$. Let π be the projection map from M onto N. Then we have $\pi \in \ker(\bar{\psi})$. Then we have $k : M'' \to N$ such that π factors through, giving us the desired inequality. Thus, we have (i) if and only if (ii).

(b) We show that we have (i) if and only if (ii). Let $\bar{\psi} = \mathrm{Hom}_R(\psi, N)$ and let $\bar{\phi} = \mathrm{Hom}_R(\phi, N)$ for notational simplicity. First, we show that $\mathrm{Hom}_R(M'', N)$ is exact. In order to do so, we must show that $\bar{\psi}$ is injective. Notice that the kernel of $\bar{\psi}$ consists of the functions f where $f \circ \psi = 0$. Notice as well that since we have (i) then ψ is surjective. Hence, we must show that $(f \circ \psi)(x) = 0$ for all $x \in M$. Since ψ is surjective, we have that $\psi(x) = m$ for some unique $m \in M''$. Hence, we must have all functions f such that for all $m \in M''$ we have $f(m) = 0$. We have that f must be the zero mapping, and so we have that $\ker(\bar{\psi}) = \{0\}$. Hence, the mapping is injective, as we required.

Next, we are given that $\psi \circ \phi = 0$. We must then show that $\bar{\phi} \circ \bar{\psi} = 0$. Notice that $\bar{\phi}(\bar{\psi}(f)) = \bar{\phi}(f \circ \psi) = f \circ \psi \circ \phi$ for all $f \in \mathrm{Hom}_R(M'', N)$ per definition. Since we have $\psi \circ \phi = 0$, then we have $f \circ \psi \circ \phi = f \circ 0 = 0$. Hence, we have $\bar{\phi} \circ \bar{\psi} = 0$, and so $\mathrm{Im}(\bar{\psi}) \subseteq \ker(\bar{\phi})$.

Next, we show that $\ker(\bar{\phi}) \subseteq \mathrm{Im}(\bar{\psi})$ and hence we have equality, making the sequence exact. If $f \in \ker(\bar{\phi})$, then we have $f \circ \phi = 0$. By exactness of the first sequence and this, we have $\mathrm{Im}(\phi) = \ker(\psi) \subseteq \ker(f)$. Hence we have that there is some function $\bar{f}$ in $\mathrm{Hom}_R(M'', N)$ where $f = \bar{f} \circ \psi = \bar{\psi}(f)$ and so $\mathrm{Im}(\bar{\psi}) \subseteq \ker(\bar{\phi})$ and hence we have equality. Thus, the sequence is exact.

Next, we show that (ii) $\to$ (i). It's clear that ψ is surjective, since we have that $\bar{\psi}$ is injective. So we must show then that $\ker(\psi) = \mathrm{Im}(\phi)$. Notice that $\bar{\psi} \circ \bar{\phi} = 0$. Then it follows that $\phi \circ \psi \circ f = 0$ for all $f \in \hom M''$. Let f be the identity function and N to be M'' (we can do so since it holds for any R-module N and any function) then it follows that $\phi \circ \psi = 0$. So, we have $\mathrm{Im}(\phi) \subseteq \ker(\psi)$. Next, let $N = M/\mathrm{Im}(\phi)$. Let π be the projection from M onto N. Then it follows that we must have $\pi \in \ker(\bar{\phi})$; hence, there exists $k : M'' \to N$ such that π factors through. Hence, $\mathrm{Im}(\phi) = \ker(\psi)$ and so the sequence is exact. Thus, we have (i) $\leftrightarrow$ (ii).

We now show (i) if and only if (iii). By (i) if and only if (ii), we have

$$M' \underset{R}{\otimes} P \to M \underset{R}{\otimes} P \to M'' \underset{R}{\otimes} P \to 0$$

is exact if and only if

$$0 \to \mathrm{Hom}_R(M'' \underset{R}{\otimes} P, N) \to \mathrm{Hom}_R(M \underset{R}{\otimes} P, N) \to \mathrm{Hom}_R(M' \underset{R}{\otimes} P, N)$$

is exact for all N. Notice that this sequence is isomorphic to

$$0 \to \mathrm{Hom}_R(M'', \mathrm{Hom}_R(N, P)) \to \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)) \to \mathrm{Hom}_R(M', \mathrm{Hom}_R(N, P))$$

for all N, since $\mathrm{Hom}_R(M \otimes_R N, P) \cong \mathrm{Bil}(M \times N, P)$ (b y the universal property), and this is isomorphic to $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$. By (i) if and only if (ii), we get that this is true if and only if $M' \to M \to M'' \to 0$ is exact. **Q.E.D**

Corollary (Corollary 2.13)**.** We have $M \otimes_R R/I \cong M/IM$.

Proof. Notice that the sequence

$$0 \to I \xrightarrow{i} R \xrightarrow{\pi} R/I \to 0$$

is exact. We now tensor with M to get

$$M \underset{R}{\otimes} I \to M \underset{R}{\otimes} R \to M \underset{R}{\otimes} R/I \to 0$$

which is right exact by Theorem 2.12. By Theorem 2.7 d, we have $M \otimes_R \cong R$. Hence, this sequence is

$$M \underset{R}{\otimes} I \to M \to M \underset{R}{\otimes} R/I \to 0.$$

By exactness, if $f : M \otimes_R I \to M$, then $M \otimes_R R/I \cong \mathrm{Coker}(f)$. We now must show that $\mathrm{Coker}(f) \cong M/IM$. Moreover, it suffices to see that the kernel of f is IM (since $\mathrm{Coker}(f) = M/\ker(f)$ by Cokernel). But this follows since $f(m \otimes_R m') = mm'$ (see Theorem 2.7 d). This completes the proof. **Q.E.D**

Remark. Let M, N be R-modules. You can get exact sequences

$$0 \to U \xrightarrow{i} F \to M \to 0$$

and

$$0 \to V \xrightarrow{i} G \to N \to 0$$

where F and G are free modules, F has basis $\{e_i\}$ for some indexing set, and G has basis $\{y_j\}$ for some indexing set. We tensor the first sequence with N to get

$$U \underset{R}{\otimes} N \to F \underset{R}{\otimes} N \to M \underset{R}{\otimes} N \to 0$$

which is exact by Theorem 2.12. Similarly, we tensor the second sequence with F to get

$$F \underset{R}{\otimes} V \to F \underset{R}{\otimes} G \to F \underset{R}{\otimes} N \to 0.$$

We see then that

$$M \underset{R}{\otimes} N \cong F \underset{R}{\otimes} N / \mathrm{Im}(U \underset{R}{\otimes} N)$$

via the first sequence. We then need a lemma.

Lemma.

$$M \underset{R}{\otimes} N \cong F \underset{R}{\otimes} G/(\mathrm{Im}(F \underset{R}{\otimes} V) + \mathrm{Im}(U \underset{R}{\otimes} G))$$

Proof. By the second sequence, we see that

$$F \underset{R}{\otimes} N \cong F \underset{R}{\otimes} G/\,\mathrm{Im}(F \underset{R}{\otimes} V).$$

Q.E.D

Recall $F \otimes_R G$ is a free module with basis $\{e_i \otimes_R g_i\}$.

Definition (Split Exact)**.** The following are equivalent for an exact sequence of R-modules

$$0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$$

(1)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & M'' & \longrightarrow & 0 \\ \downarrow{=} & & \downarrow{=} & & \downarrow{\cong} & & \downarrow{=} & & \downarrow{=} \\ 0 & \longrightarrow & M' & \xrightarrow{i} & M' \oplus M'' & \xrightarrow{\pi} & M'' & \longrightarrow & 0 \end{array}$$

(2) There exists an $\epsilon : M \to M'$ where $\epsilon \circ \varphi = \mathrm{Id}_{M'}$.
(3) There exists a $\mu : M'' \to M$ where $\psi \circ \mu = \mathrm{Id}_{M''}$.
These maps are called splittings, and such a sequence is called split exact.

Definition (Projective Module)**.** Let R be a ring and N an R-module. Then the following are equivalent.

(i) N is projective.

(ii) If ψ surjective, then $\mathrm{Hom}_R(N, \psi)$ is surjective.

(iii) $\mathrm{Hom}_R(N, \cdot)$ preserves exact sequences.

Definition (Injective Module)**.** Let R be a ring and N an R-module. Then the following are equivalent.

(i) N is injective.

(ii) If φ is injective, then $\mathrm{Hom}_R(\varphi, N)$ is surjective.

(iii) $\mathrm{Hom}_R(\cdot, N)$ preserves exact sequences.

Definition (Flat Module)**.** Let R be a ring and N an R-module. Then the following are equivalent.

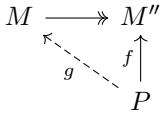
1. N is flat.
2. If φ is injective, then $\varphi \otimes_R \cdot$ is injective.
3. $\cdot \otimes_R N$ preserves exact sequences.

Proposition (Proposition 2.14)**.** Let R be a ring.

(a) The following are equivalent.

(i) P is a projective module.

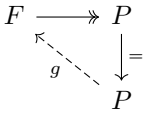
(ii) For all surjective $\psi : M \to M''$ and $f : P \to M''$, there exists a $g : P \to M$ making the following diagram commute.



(iii) There exists an R-module M where $P \oplus M$ is free.

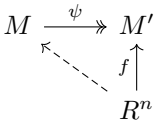
(b) We have free $\to$ projective $\to$ flat.

Proof. We start with (a). Notice that (i) if and only if (ii) follows from the definition, Projective Module. Next, we prove (ii) implies (iii). Using (ii), let M'' be P and let M be F, a free module. Then we have the following diagram.



We then use the equivalences of Split Exact. We now prove (iii) implies (ii). Notice that every free module is projective, and a direct summand of a projective module is projective, since $\mathrm{Hom}_R(P \oplus M, \psi) = \mathrm{Hom}_R(P, \psi) \oplus \mathrm{Hom}_R(M, \psi)$. So ψ is surjective implies $\mathrm{Hom}_R(P \oplus M, \psi)$ is surjective, which implies $\mathrm{Hom}_R(P, \psi)$, giving us the desired result.

We now prove (b). First, we establish free implies projective. Examine the following diagram.



Let $\{e_i\}$ be the basis of R^n. Examine $f(e_i)$. For each i, choose $x_i \in \psi^{-1}(f(e_i))$. Define $g : F \to M$ by $g(e_i) = x_i$. Then by Projective Module, we get that it's projective. Since the projective is a direct summand of free modules, it must also be flat, via Flat Module. **Q.E.D**

Remark. Notice that the arrows for Proposition 2.14 b cannot be reversed.

Theorem (Theorem 2.15)**.** Let (R, m, k) be a local ring, M a finite R-module. Then M is free if and only if it is projective.

Proof. Let M be projective. Let $n = \mu(M)$ (recall Minimal Number of Generators). Then we have $M = Rx_1 + \cdots + Rx_n$. Let $F = R^n$. So we take

$$0 \to K \to F \to M \to 0.$$

(Here, K denotes the kernel of the mapping $F \to M$.) Notice that $K \subseteq mF$. Since $\sum a_i e_i \in k$, then $\sum a_i x_i = 0$ implies no a_i can be a unit. Since R is local, $a_i \in m$. Since M is projective, we get the following diagram.

$$\begin{array}{ccc} F & \twoheadrightarrow & M \\ & \nwarrow & \downarrow = \\ & & M \end{array}$$

By Split Exact, we get $F \cong k \oplus M$, and also K is finitely generated. So $R^n \cong k \oplus M$. Tensor this with k to get that $k \otimes_R R^n \cong k^n$, and so we have $k^n \cong (k \otimes_R k) \oplus (m \otimes_R k)$. Notice that $m \otimes_R k \cong k^n$, since

$$K \to F \to k \underset{R}{\otimes} k \to F \underset{R}{\otimes} k$$

because $k \subseteq mF$. Thus

$$0 \to F \underset{R}{\otimes} k \to M \underset{R}{\otimes} k \to 0,$$

so $M \otimes_R k \cong k^n$. Thus, $k^n \cong (K \otimes_R k) \oplus (k^n)$ gives us $K \otimes_R k = 0$, which gives us $K/mK = 0$. So by Theorem 2.2 (Nakayama's Lemma), we get $K = 0$. Hence,

$$0 \to K \to F \to M \to 0$$

implies

$$0 \to F \to M \to 0$$

and hence $F \cong M$, as desired. **Q.E.D**

Chapter 3: Noetherian/Artinian Modules and Rings

Noetherian and Artinian Modules

Lemma (Lemma 3.1)**.** Let Γ be a partially ordered set with respect to $\leqslant$ (in other words, $\leqslant$ is transitive, $(x \leqslant y) \wedge (y \leqslant x) \to x = y$). Then the following are equivalent.

(i) Every increasing sequence $x_1 \leqslant x_2 \leqslant x_3 \leqslant \cdots$ is stationary or stabilizes. In other words, there exists an n such that $x_n = x_{n+1} = \cdots$.

(ii) Every nonempty subset of Γ has a maximal element.

Proof. We show (i) implies (ii). We proceed by contradiction. Suppose $\Gamma' \subseteq \Gamma$ does not have a maximal element, and $\Gamma' \neq \varnothing$. By induction on n, we construct elements $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n$ in Γ' which are all distinct. For $n = 1$, arbitrarily choose any. Suppose it holds for $n-1$, i.e. we have a chain $x_1 \leqslant \cdots \leqslant x_{n-1}$ which are distinct for all x_i. Since x_{n-1} cannot be a maximal element (assuming (ii) is false), there must exists an $x_n \in \Gamma'$ such that $x_{n-1} \leqslant x_n$, and $x_{n-1} \leqslant x_n$ (otherwise x_{n-1} would be maximal). Thus, by induction the case n holds. Since by induction we can increase this chain to be arbitrarily long, we see that (i) does not hold, and so we have a contradiction. Hence, we must have (ii) if we have (i).

We show (ii) implies (i). This, however, is clear. Let $x_1 \leqslant \cdots$ be an arbitrary chain, and let them all be contained in Γ'. Then we apply (ii) to Γ' to find an x_n such that $x_1 \leqslant \cdots \leqslant x_n$ and if $x_n \leqslant x_{n+1}$ then we must have $x_n = x_{n+1}$ by the second property of partially ordered sets. Hence, we have that this chain stabilizes, giving us (i) as desired. **Q.E.D**

Remark (Ascending Chain Condition)**.** We call the above property (Lemma 3.1) the Ascending Chain Condition. If Γ satisfies the properties above, then it has the Ascending Chain Condition.

Definition (Descending Chain Condition)**.** If we have the properties in Lemma 3.1 but with respect to $\geqslant$ as opposed to $\leqslant$, then we call it the Descending Chain Condition.

Definition (Noetherian Module)**.** Let M be an R-module, R a ring. Then M is Noetherian if the set of all submodules of M satisfies the ascending chain condition.

Definition (Artinian Ring)**.** Let M be an R-module, R a ring. Then M is Artinian if the set of all submodules of M satisfies the descending chain condition.

Definition (Noetherian/Artinian Ring)**.** Let R be a ring. We say R is Noetherian as a ring (respectively Artinian) if R is Noetherian (respectively Artinian) as an R-module.

Proposition (Proposition 3.2)**.** Let R be a ring, M an R-module. We have that M is Noetherian if and only if every submodule of M is finitely generated.

Proof. We start with the implication. Let N be a submodule of M. Let Γ' be the finitely generated submodules of N. Note that Γ' is nonempty (Γ' must contain at least N). By the Noetherian property, Γ' as a maximal element, M'. We would like to show that $M' = N$. We proceed by contradiction; assume that $M' \neq N$. Then there exists an $x \in N$ such that $x \notin M'$. Now, consider $M' + Rx$. This is a finitely generated N-module, and $M' \subseteq M' + Rx$, which contradicts the maximality of M'. Thus, we have that $N = M'$, and N is finitely generated.

We prove the converse. Let $M_1 \subseteq M_2 \subseteq \cdots$ be a chain of submodules. Define

$$M' = \bigcup_{i=1}^{\infty} M_i.$$

Then M' is a submodule of M. Hence, M' is a finitely generated module. By definition, $M' = Rx_1 + \cdots + Rx_n$. So $x_j \in M_{i_j}$ for some i_j. Let $r = \max\{i_j : 1 \leqslant j \leqslant n\}$. Then $x_j \in M_r$ for all j. Notice that $M' = Rx_1 + \cdots + Rx_n \subseteq M_r \subseteq \cup_{i=1}^{\infty} M_i \subseteq M'$, hence we have that $M' = M_r$, and therefore for all j greater than or equal to r, we have $M_r = M_j$. So it stabilizes. **Q.E.D**

Corollary (Corollary 3.2.1)**.** A ring is Noetherian if and only if every R ideal is finitely generated.

Lemma (Lemma 3.3)**.** Let R be a ring, M an R-module, $M' \subseteq M$ a submodule, and let $N_1 \subseteq N_2 \subseteq M$ be submodules. Then we have $N_1 = N_2$ if and only if $N_1 \cap M' = N_2 \cap M'$ and $(N_1 + M')/M' = (N_2 + M')/M'$. (Not an isomorphism, actual equality.)

Proof. For the implication, it follows clearly. If $N_1 = N_2$, then it's clear that $N_1 \cap M' = N_2 \cap M'$, since M' is the same in both. It's also clear that $(N_1 + M')/M' = (N_2 + M')/M'$ since $N_1 = N_2$.

For the converse, there is more work. We know $N_2 \subseteq N_2 \cap (N_1 + M')$ because $N_1 + M' = N_2 + M'$ (since $(N_1 + M')/M' = (N_2 + M')/M'$). Then $N_2 \cap (N_1 + M') = (N_2 \cap N_1) + (N_2 \cap M') = (N_2 \cap N_1) + (N_1 \cap M') \subseteq N_1$. Hence $N_2 \subseteq N_1$. By a symmetry argument, $N_1 \subseteq N_2$, and thus $N_1 = N_2$, as required. **Q.E.D**

Proposition (Proposition 3.4)**.** If

$$0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$$

is an exact sequence, then

(a) M is Noetherian if and only if M' and M'' Noetherian.

(b) M is Artinian if and only if M' and M'' are Artinian.

Proof. You may start with assuming $M' \subseteq M$ and $M'' = M/M'$, since the sequence is exact. We start with the implication of (a) and (b). Let $M_1' \subseteq M_2' \subseteq \cdots$ be any sequence in M'. Since we may assume $M' \subseteq M$, it's clear that this is a sequence in M, and so it must eventually stabilize. We can apply this same logic for (b). For M'', let $M_1'' \subseteq M_2'' \subseteq \cdots$. Since $M'' = M/M'$, we have that this is $M_1/M' \subseteq M_2/M' \subseteq \cdots$ for $M_i \subseteq M$. But this stabilizes, since $M_1 \subseteq M_2 \subseteq \cdots$ stabilizes by assumption. Apply similar logic for (b).

We now prove the converse of (a) and (b). Assume M' and M'' are Noetherian (respectively Artinian). Then select some arbitrary chain $M_1 \subseteq M_2 \subseteq \cdots$ in M. The corresponding chain in M' is then $M_1 \cap M' \subseteq \cdots$ in M', and the corresponding chain in M'' is $(M_1 + M'')/M'' \subseteq \cdots$. We know that both stabilize eventually (by assumption), and so we apply Lemma 3.3 on these sequences to get that they stabilize in M as well. Therefore, every chain eventually stabilizes in M. **Q.E.D**

Corollary (Corollary 3.5)**.** $M_1, \ldots, M_n$ are Noetherian (respectively Artinian) if and only if $M_1 \oplus \cdots \oplus M_n$ is Noetherian (respectively Artinian).

Proof. We proceed via induction. The case where $n = 1$ is trivial. The case where $n = 2$ is more illuminating. Notice that we have

$$0 \to M_2 \xrightarrow{i} M_1 \oplus M_2 \xrightarrow{\pi} M_1 \to 0$$

is a short exact sequence, where i indicates the natural injection and π indicates the natural projection. We then apply Lemma 3.3, and we get the result. We now assume that it holds for $n_0 > 0$. We want to then show that it holds for $n_0 + 1$. Notice now we have the short exact sequence

$$0 \to M_{n_0+1} \xrightarrow{i} \bigoplus_{i=1}^{n_0} M_i \oplus M_{n_0+1} \xrightarrow{\pi} \bigoplus_{i=1}^{n_0} M_i \to 0$$

where, once again, i indicates the natural injection and π indicates the natural projection. Applying Lemma 3.3 again, we get the result that we wish, and so it holds for all $n \in \mathbb{N}_{\geqslant 1}$. **Q.E.D**

Corollary (Corollary 3.6)**.** Let R be a Noetherian ring (respectively Artinian), and let M be an R-module. If M is finite, then M is Noetherian (respectively Artinian).

Proof. There exists a short exact sequence

$$0 \to U \xrightarrow{i} R^n \xrightarrow{\pi} M \to 0.$$

where $U = \ker(\pi)$ (this follows from Finitely Generated). By Corollary 3.5, R^n is a Noetherian (respectively Artinian) ring module. Applying Proposition 3.4, we get that M is Noetherian (respectively Artinian). **Q.E.D**

Corollary (Corollary 3.7)**.** Let R and S be rings, and let $R \to S$ be a homomorphism of rings which makes S a finite R-module. So if R is Noetherian (respectively Artinian) then S is Noetherian (respectively Artinian) as a ring.

Proof. By Corollary 3.6 we know S is a Noetherian (respectively Artinian) R-module. In particular, it is a Noetherian (respectively Artinian) S-module. **Q.E.D**

Remark. The converse does not necessarily follow.

Example. (1) Notice that $\mathbb{Z}$ is a Noetherian ring. Notice, however, it is not an Artinian ring; take (2^k).

(2) We have that $\mathbb{Z}[\sqrt{-5}]$ is Noetherian by Corollary 3.7, but it is not Artinian.

(3) Let k be a field. It is both Artinian and Noetherian.

(4) Let k be a field. Then $k[\{x_i : i \in \mathbb{N}\}]$ is neither Noetherian nor Artinian. Take the ideals generated by the generators – they never stabilize.

Proposition (Proposition 3.8)**.** Suppose M is a Noetherian R-module. Then $R/\mathrm{Ann}_R(M)$ is a Noetherian ring.

Remark. Over this ring, the module is faithful.

Proof. Since M is a Noetherian R-module, it is finitely generated via Proposition 3.2. Thus, we can rewrite M as $M = Rx_1 + \cdots + Rx_n$. Notice $Rx_i \subseteq M$, and it is a cyclic module. Thus, $R/\mathrm{Ann}_R(x_i) \cong Rx_i$. By Proposition 3.4, $R/\mathrm{Ann}_R(x_i)$ is Noetherian, therefore, by Corollary 3.5, we have $R/\mathrm{Ann}_R(x_1) \oplus \cdots \oplus R/\mathrm{Ann}_R(x_n)$ is a Noetherian R-module. Hence, by Theorem 1.16 (Chinese Remainder Theorem), we get

$$R/(\mathrm{Ann}_R(x_1) \cap \cdots \cap \mathrm{Ann}_R(x_n)) \hookrightarrow \bigoplus_{i=1}^{n} R/\mathrm{Ann}_R(x_i).$$

By Proposition 3.4, $R/(\mathrm{Ann}_R(x_1) \cap \cdots \cap \mathrm{Ann}_R(x_n))$ is Noetherian as an R-module, hence as a ring. Therefore, this is just $R/\mathrm{Ann}_R(M)$. **Q.E.D**

Remark. This is not true if we replace Noetherian by Artinian.

Theorem (Theorem 3.9)**.** Suppose R is a ring. We have that R is Noetherian if and only if every prime ideal of R is finitely generated.

Proof. The implication follows via Corollary 3.2.1. We now prove the converse. Let $\Gamma = \{\text{R-ideals that are not finitely generated}\}$. Suppose $\Gamma \neq \varnothing$. To apply Zorn's Lemma, we check that every totally ordered subset has an upper bound. Let $\{I_\alpha\}$ be our totally ordered set. Let $I = \cup_\alpha I_\alpha$, which is an ideal. We need to show that I is not finitely generated. Suppose, for contradiction, that it is finitely generated. Then $I = Rx_1 + \cdots + Rx_n$, $x_i \in I_{\alpha_i}$ for some α_i. Let $r = \max\{\alpha_i\}$. Then $\alpha_i \leqslant r$ and hence $I_{\alpha_i} \subseteq I_r$, and therefore $x_i \in I_r$ for all i. This shows that the whole ideal is in I_r, and thus $I = I_r$. Remember I_r is in Γ, and all elements in Γ are not finitely generated, and so I is not finitely generated, resulting in a contradiction. By Zorn's Lemma, Γ has a maximal element, denote it p. We need to show p is a prime ideal. It's clear that p is proper, because R is finitely generated. We need to then show that if $\alpha, \beta \in p$, then $\alpha \in p$ or $\beta \in p$. Suppose there exist elements $\alpha \in R/p$, $\beta \in R/p$ with $\alpha\beta \in p$. Look at $p + R\alpha$. This is an ideal, and is strictly bigger than p. Likewise, $p + R\beta$ is an ideal. Notice we also have $p \subsetneq p + R\beta \subseteq (p : \alpha)$. By the maximality of p in Γ, we have $p + R\alpha$ and $(p : \alpha)$ are both finitely generated. So we can write $p = (p + R\alpha) \cap p = (I + R\alpha) \cap p = I + p \cap R\alpha = I + \{\lambda \in R : \lambda \in p\}\alpha$. By definition, this is just $I + (p : \alpha)\alpha$, and so we get p is finitely generated. **Q.E.D**

Definition (Composition Series)**.** Let M be an R-module. Then a composition series of M is a strictly decreasing chain of submodules $0 = M_n \subsetneq \cdots \subsetneq M_1 \subsetneq M_0 = M$ which cannot be properly refined. Equivalently, M_{i-1}/M_i are simple modules if and only if $M_{i-1}/M_i \cong R/\mathfrak{m}_i$, $\mathfrak{m}_i$ some maximal ideal.

Lemma (Lemma 3.10)**.** Let M be a module with the composition series of length n. Then every chain of submodules of M has length less than or equal to n.

Proof. We proceed via induction. It's clear that this holds for $n = 1$. Assume M has a composition series $0 = M_n \subsetneq M_{n-1} \subsetneq \cdots \subsetneq M_1 \subsetneq M_0 = M$, and $0 = N_r \subsetneq \cdots \subsetneq N_1 \subsetneq N_0 = M$. Let $M' = N_{n-1}$. Then M/M' has a composition series of length $n - 1$. Hence, by the induction hypothesis, the chain $0 = N_r/(M' \cap N_r) \subseteq \cdots \subseteq N_1/(M' \cap N_1) \subseteq N_0/(M' \cap N_0) = M/M'$. This chain has length at most $n - 1$. Since M' is simple, $M' \cap N_i = \{M' \text{or} 0\}$. Let t be maximum with $M' \cap N_t = M'$. Then $N_r \subsetneq \cdots \subsetneq N_{t-1}/0 \subseteq N_t/M' \subseteq \cdots \subseteq N_0/M' = M/M'$. The length of this chain is at least $r - 1$. Via the induction hypothesis, $r - 1 \leqslant n - 1$, and hence $r \leqslant n$. **Q.E.D**

Corollary (Corollary 3.11)**.** Let M be a module with a composition series. Then every composition series has the same length. Furthermore, every chain of submodules can be refined to a composition series.

Proof. Folows directly from Lemma 3.10. **Q.E.D**

Definition (Length of a Composition Series)**.** Let R be a ring and M be an R-module. We define $l(M) = l_R(M)$ to be the length of the composition series of M if M has a composition series. Otherwise, we define it to be infinite.

Proposition (Proposition 3.12)**.** Let R be a ring, and M an R-module. Then $l(M) < \infty$ if and only if M is Noetherian and Artinian.

Proof. For the implication, we notice it follows directly from Lemma 3.10. For the converse, let Γ be the set of submodules of M having finite length. Notice that this set is nonempty, clearly, and must also contain 0. Since M is Noetherian, M has a maximal element, denote it by N. If $N = M$, then we're done (this sequence cannot be properly refined). Assume otherwise. Let Δ be the set of submodules of M properly containing N. Notice this set contains M. Since M is Artinian, Δ has a minimal element, call it M'. Now $N \subsetneq M'$ and also M'/N is a simple module, since M' is minimal. Hence, M' has a composition series. This contradicts the maximality of N, and thus $N = M$, completing the proof. **Q.E.D**

Remark (Remark 3.13)**.** Let

$$0 \to M' \to M \to M'' \to 0$$

be an exact sequence of R-modules. Then $l(M) = l(M') + l(M'')$.

Remark (Remark 3.14)**.** Let M be a k-vector space. Then the following are equivalent.

(i) M is Noetherian.

(ii) M is Artinian.

(iii) M has finite length.

(iv) M has finite dimension.

We also have $l(M) = \mathrm{Dim}_k(M)$.

Proof. It suffices to prove (ii) implies (iv); this, however, follows from a simple generator argument. Suppose $\mathrm{Dim}_k(M) = \infty$; then this means that M has an infinite minimal generating set. Denote it b W. So $\cdots \subsetneq W_1 \subsetneq W_0 = W$. Then thre exists an infinite chain of submodules $\cdots RW_2 \subsetneq RW_1 \subsetneq RW_0 = M$ because W is a minimal generating set. So by the contrapositive, we get what we desire. **Q.E.D**

Lemma (Lemma 3.15)**.** Suppose R is a ring which is Artinian or Noetherian. Let I be any ideal. Then there exists N with $0 :_R I^n = 0 :_R I^{n+1}$. For this n, we write $\bar{R} = R/(0 :_R I^n)$ and $\bar{I}$ for the image of I in $\bar{R}$. Then $\mathrm{ann}_R(\bar{I}) = \bar{0} = \bar{0} :_{\bar{R}} \bar{I}$.

Proof. It suffices to show that $\bar{0} :_{\bar{R}} \bar{I} = \bar{0}$. Equivalently, in R, $(0 :_R I^n) :_R I = 0 :_R I^n$. But notice that $(0 : I^n) : I = 0 : (I^n I) = 0 : I^{n+1} = 0 : I^n$. **Q.E.D**

Lemma (Lemma 3.16)**.** Let R be an Artinian ring. Then there exists n with $\mathrm{Rad}(R)^n = 0$. In particular, this gives us $\mathrm{nil}(R) = \mathrm{Rad}(R)$.

Proof. Let $I = \mathrm{Rad}(R)$. By Lemma 3.15, there exists an n so that $\mathrm{ann}_R(\bar{I}) = 0$, where $\bar{R} = R/(0 : I^n)$. We then show $\bar{R} = \bar{0}$, since if $\bar{R} = \bar{0}$ then $0 : I^n = R$ if and only if $I^n = 0$. Suppose for contradiction $\bar{R} \neq \bar{0}$. Since $\bar{R}$ is an Artinian ring, $\bar{R}$ has a simple submodule, call it $N \neq 0$ (see Remark 3.14). In particular, N is a finite R-module. Notice $IN = \{0, N\}$. If $IN = N$, then $N = 0$. If $IN = 0$, then $N = 0$, since $\mathrm{ann}_{\bar{R}}(\bar{I}) = 0$. We get a contradiction either way, and so we're done. **Q.E.D**

Theorem (Theorem 3.17)**.** Every Artinian ring is Noetherian.

Proof. We will have a better proof in Chapter 7, so I will omit it here. **Q.E.D**

Hilbert's Basis Theorem

Theorem (Theorem 3.18 (Hilbert's Basis Theorem))**.** If R is a Noetherian ring, then so is $R[X_1, \ldots, X_n]$.

Proof. It's clear that once we show it holds for $R[X_1]$, it must hold for all $n \in \mathbb{N}$. Assume it holds for n, then we must show it holds for $n + 1$. We have the ring $R[X_1, \ldots, X_n, X_{n+1}] = R[X_1, \ldots, X_n][X_{n+1}]$. Let $R' = R[x_1, \ldots, X_n]$. Then we may rewrite this as $R'[X_{n+1}]$. Since it holds for n, we have that R' is Noetherian, and we use the case where $n = 1$ to establish that $R'[X_{n+1}]$ is Noetherian. Thus, by induction, it holds. It remains to show the case for $n = 1$.

For $n = 1$, we proceed via contradiction. Assume there is an ideal I of $R[X]$ that is not finitely generated (see Proposition 3.2). Set $I_0 := (0)$. For each $i \geqslant 1$, choose inductively $f_i \in I - I_{i-1}$ of least degree d_i, and set $I_i = (f_1, \ldots, f_i)$. Let I_i be the leading coefficient of f_i, and J the ideal generated by all the I_i. Since R is Noetherian, $J = (I_1, \ldots, I_n)$ for some n. Then $I_{n+1} = r_1 I_1 + \cdots + r_n I_n$ for $r_i \in R$.

By construction, $d_i \leqslant d_{i+1}$ for all i. Set

$$f := f_{n+1} - (r_1 f_1 X^{d_{n+1} - d_1} + \cdots + r_n f_n X^{d_{n+1} - d_n}).$$

Then $\deg(f) < d_{n+1}$, so $f \in I_n$. Therefore, $f_{n+1} \in I_n$, a contradiction. **Q.E.D**

Corollary (Corollary 3.19)**.** Every finitely generated algebra over a Noetherian ring is a Noetherian ring.

Proof. Let S be a finitely generated R-algebra, R a Noetherian ring. Then $S \cong R[X_1, \ldots, X_n]/J$, and so we apply Theorem 3.18 (Hilbert's Basis Theorem). **Q.E.D**

Theorem (Theorem 3.20)**.** Let R be a ring, M an R-module, $\Gamma = \{IM : I \text{ an } R\text{-module}\}$. If M is finitely generated and Γ satisfies Ascending Chain Condition, then M is Noetherian.

Proof. Suppose M is not Noetherian. We will get to the case where M/aM is Noetherian for all $0 \neq a \in R$, and M/M' is not faithful for all submodules $0 \neq M' \subseteq M$. In this case, we are done: suppose $0 \neq M' \subseteq M$ a submodule. Then M/M' is not faithful. Hence, there exists $0 \neq a \in R$ with $a(M/M') = 0$. Hence, $aM \subseteq M'$. Now, M'/aM is a submodule of M/aM and by the first assumption M/aM is Noetherian. Hence, M'/aM is finitely generated, and therefore M' is finitely

generated (since M is finitely generated) and so aM is finitely generated. Since every submodule of M is finitely generated, M is Noetherian. Hence, by contradiction, we have the statement.

We must now get to the assumptions. Let $\Delta = \{IM : I \text{ is an ideal with } M/IM \text{ not Noetherian}\}$. Δ is nonempty, since $0 \in \Delta$. By Ascending Chain Condition, Δ has a maximal element, denote it by I_0M. Replace M by M/I_0M and R by $R/\text{ann}_R(M/IM)$. Let $a \neq 0 \in R'$, then $aM \neq 0$, since M is faithful now. Therefore, in the old module, $I_0M \subsetneq (I_0, a)M$. By the maximality of I_0M in Δ, $M/(I_0, a)M$ is Noetherian. For the new module, this is simply M/aM. Hence, we have the first assumption. Notice M is still not Noetherian, because $I_0 \in \Delta$.

We now must show the second assumption. Consider $0 \in \Sigma = \{N : N \text{ submodule of } M,\ M/N \text{ is faithful}\}$. Hence, Σ is nonempty. Let $\{N_\alpha\}$ be a chain of Σ. Let $N = \cup_\alpha N_\alpha$. Then N is a submodule. We claim M/N is faithful. Let $M = Rm_1 + \cdots + Rm_n$ since M is finitely generated. Let $a \in R$ which annihilates the module. This means that $aM \subseteq N$. Therefore $am_i \in N$ for all i. So there exists α_i so that $am_i \in N_{\alpha_i}$ for all i. So let $\beta = \max\{\alpha_i\}$. Then $N_{\alpha_i} \subseteq N_\beta$ for all α_i. Therefore $a \in \text{ann}(M/N\beta) = 0$. Hence $a = 0$, and our module N is faithful. By Zorn's Lemma, we have there is a maximal element in Σ; call it N. Replace M by M/N. By the maximality of $N \in \Sigma$, then M/M' is not faithful for all $M' \neq 0$ a submodule of M. So we need to check that our new module is not Noetherian. Suppose it is Noetherian. Recall this M is M/N, $N \in \Sigma$. Therefore, this M/N is faithful, and so this gives us that the ring is Noetherian (Proposition 3.8). If the ring is Noetherian, then since the old M is finitely generated, M would be Noetherian, which gives us a contradiction. So we have all of our assumptions, as we wanted. **Q.E.D**

Corollary (Corollary 3.21 (Eakin's Theorem))**.** Suppose $R \subseteq S$ is a ring extension making S a finitely generated R-module. If S is Noetherian, then R is Noetherian.

Proof. Examine $\Gamma = \{SI : I \text{ an } R\text{-ideal}\} \subseteq \{S\text{-ideals}\}$. Since S is Noetherian, then $\{S$-ideals$\}$ satisfies Ascending Chain Condition, and so any subset satisfies Ascending Chain Condition. In particular, this means that Γ satisfies Ascending Chain Condition. Hence by Theorem 3.20, we get that S is a Noetherian R-module. Since $R \subseteq S$, S is a fiathful R-module (i.e. the annihilator is 0). Hence, R is a Noetherian ring by Proposition 3.8. **Q.E.D**

Chapter 4: Localization and Spectrum

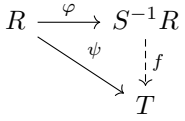
Definition (Localization)**.** Let R be a commutative ring, and let S be a Multiplicative Subset. On $S \times R$ we define $\sim$: $(s,x) \sim (s',x')$ if and only if $t(sx' - s'x) = 0$ for some $t \in S$. Notice that this is an Equivalence Relation. We define $S^{-1}R = R_s = S \times R/\sim = \{(s,x) : s \in S, x \in R\} = \{\frac{x}{s}\}$. We can define multiplication and addition in the obvious way. These operations are well-defined. With these operations, $S^{-1}R$ is a commutative ring with $0 = \frac{0}{1}$ and $1 = \frac{1}{1}$.

Remark (Remark 4.1)**.** $S^{-1}R$ is a ring, φ is a homomorphism of rings, $\varphi(S) \subseteq (S^{-1}R)^\times$.

Proof. Let $s \in S$. We want to show $s/1$ is invertible in $S^{-1}R$. The inverse is $s/1 \cdot 1/s = 1/1$. **Q.E.D**

Definition (Quotient Ring)**.** Let $S^{-1}R$ be as above. We call $S^{-1}R$ the quotient ring, or the ring of fractions.

Proposition (Proposition 4.2)**.** Let $\psi : R \to T$ be a homomorphism of rings with $\psi(S) \subseteq T^\times$. Then there exists a unique homomorphism of rings $f : S^{-1}R \to T$ so that $\psi = f \circ \varphi$.



Remark. This property determines $S^{-1}R$ and φ up to canonical isomorphism.

Proof. We define $f : S^{-1}R \to T$ via $\frac{x}{s} \mapsto \psi(x)\psi(s)^{-1}$. So we must check f is well-defined. We need to show that $\frac{x}{s} = \frac{x'}{s'}$ then $\psi(x)\psi(s)^{-1} = \psi(x')\psi(s')^{-1}$. By definition (Localization), $ts'x = tsx'$ for some $t \in S$. Apply ψ to get $\psi(t)\psi(s')\psi(x) = \psi(t)\psi(s)\psi(x')$. This then gives us $\psi(s')\psi(x) = \psi(s)\psi(x')$, which then implies $\psi(x')\psi(s')^{-1} = \psi(x)\psi(s)^{-1}$, as required. **Q.E.D**

Definition (Localization at a Prime)**.** Let p be a prime ideal of R. Then $S = R/p$ is a multiplicative set, which we generally denote by $R_p := S^{-1}R$. This is called the localization of R at p.

Definition (Localization at an Element)**.** Let $x \in R$, $S = \{x^n : n \geqslant 0\}$. Then S is a multiplicatively closed set, and $R_x := S^{-1}R$.

Definition (Total Ring of Quotients)**.** Let S be the set of all nonzerodivisors in R. We then get $\mathrm{Quot}(R) = S^{-1}R$ or the total ring of quotients.

Definition (Quotient Field)**.** If R is a domain, then the Total Ring of Quotients is a field, and we call it the quotient field.

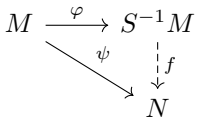
Remark (Remark 4.3)**.** Let $\varphi : R \to S^{-1}R$ be the map such that $x \mapsto x/1$. Then notice that $\ker(\varphi) = \{x \in R : x/1 = 0/1\} = \{x \in R : sx = 0, s \in S\}$. We get the following.

(a) φ is injective if and only if S consists of nonzerodivisors. In particular, $\varphi : R \to \mathrm{Quot}(R)$ is always injective.

(b) $S^{-1}R = 0$ if and only if $\varphi = 0$ if and only if $0 \in S$ if and only if S contains a nilpotent element.

Definition (Inverse of a Module)**.** Let R be a ring, and let M be an R-module. Let $S \subseteq R$ is a multiplicative subset. We define $S^{-1}M = M_s = S \times M/\sim$ where $(s,m) \sim (s',m')$ if and only if $t(sm' - s'm) = 0$ for some $t \in S$. We define addition and scalar multiplication in the obvious way. We check that this is well-defined and that this new object is a module. It turn out $S^{-1}M$ is an $S^{-1}R$-module, hence an R-module via $R \to S^{-1}R$. Define M_p and M_x as before, where p is a prime ideal and x is an element. We also get a map $\varphi : M \to S^{-1}M$ via $m \mapsto m/1$. It can only be an R-linear map, with $\ker(\varphi) = \{m \in M : sm = 0, s \in S\}$.

Proposition (Proposition 4.4)**.** Let M be an R-module, N an $S^{-1}R$ module. Then for every R linear map $\psi : M \to N$, there exists a unique $S^{-1}R$-linear map $f : S^{-1}M \to N$ so that $\psi = f \circ \varphi$.



Proof. Proof omitted. **Q.E.D**

Corollary (Corollary 4.5)**.** $S^{-1}R \otimes_R M$ has exactly the same property. So $S^{-1}R \otimes_R M \cong S^{-1}M$ via $r/s \otimes_R m \mapsto rm/s$.

Proof. It follows from Theorem 2.9 and Proposition 4.4. **Q.E.D**

Corollary (Corollary 4.6)**.** $S{-}1R$ is flat as an R-module.

Proof. In order to show that it is flat, we need to show that if $\varphi : M \to N$ is an injective R-linear map, then $S^{-1}R \otimes_R \varphi : S^{-1}R \otimes_R M \to S^{-1}R \otimes_R N$ is injective. Notice that $S^{-1}R \otimes_R M \cong S^{-1}M$ and $S^{-1}R \otimes_R N \cong S^{-1}N$ via Corollary 4.5. Then we must show that $\varphi : S^{-1}M \to S^{-1}N$ is injective, where $\psi(m/s) = \psi(m)/s$. Let $m/s \in S^{-1}M$ with $\psi(m/s) = 0$. Then $\psi(m)/s = 0$ in $S^{-1}N$. Hence, $t\psi(m) = 0$ for some $t \in S$. Notice if φ is R-linear, then we have $\varphi(tm) = 0$ and since φ is injective we have $tm = 0$ in N. But then $tm/ts = 0$ implies $m/s = 0$ in $S^{-1}M$, which means that the kernel is trivial and so the mapping is injective. **Q.E.D**

Example. Every quotient field of a domain R is flat as an R module.

Corollary (Corollary 4.7)**.** Let N be a submodule of an R-module M. Then $S^{-1}N$ is a submodule of $S^{-1}M$ and $S^{-1}M/S^{-1}N \cong S^{-1}(M/N)$.

Proof. Since N is a submodule of M, we have the short exact sequence

$$0 \to N \to M \to M/N \to 0.$$

Tensor this with $S^{-1}R$ to get

$$0 \to S^{-1}R \underset{S^{-1}R}{\otimes} N \to S^{-1}R \underset{S^{-1}R}{\otimes} M \to S^{-1}R \underset{S^{-1}R}{\otimes} M/N \to 0.$$

This is exact via Corollary 4.6. By Corollary 4.5, we're granted the short exact sequence

$$0 \to S^{-1}N \to S^{-1}M \to S^{-1}(M/N) \to 0$$

which also gives us $S^{-1}N/S^{-1}M \cong S^{-1}(M/N)$. **Q.E.D**

Corollary (Corollary 4.8)**.** Let N and P be submodules of an R-module M. Then we have the following

(a) $S^{-1}(N+P) = S^{-1}N + S^{-1}P$ as submodules of $S^{-1}M$.

(b) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.

(c) $S^{-1}(N : P) = S^{-1}N : S^{-1}P$ if P is finitely generated.

(d) $S^{-1}\text{ann}_R(M) = \text{ann}_{S^{-1}R}(S^{-1}M$ if M is finitely generated.

Proof. For now, we omit the proof of (a).

We prove (b). Notice that we have the short exact sequence

$$0 \to N \cap P \xrightarrow{\delta} N \oplus P \to N + P \to 0.$$

By Corollary 4.5 and Corollary 4.6 we get that the following sequence is also exact

$$0 \to S^{-1}(N \cap P) \to S^{-1}N \oplus S^{-1}P \to S^{-1}N + S^{-1}P \to 0.$$

Notice $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$. This completes it.

We skip (c) and show (d). Since M is finitely generated, we have $M = Rx_1 + \cdots + Rx_n$. We proceed via induction on n, the number of generators. For $n = 1$, we have $M = Rx_1 \cong R/\text{ann}_R(x)$. Let $I = \text{ann}_R(x)$. Then $M \cong R/I$. We then get that $S^{-1}M \cong S^{-1}(R/I)$. So $\text{ann}_{S^{-1}R}(S^{-1}M) = S^{-1}\text{ann}_R(M)$, since $\text{ann}_{S^{-1}R)(S^{[}-1}M) = S^{-1}\text{ann}_R(x)$.

For the general case, we have that, by (a), $S^{-1}M = S^{-1}R(x_1/1) + \cdots + S^{-1}R(x_n/1)$. Therefore, we have $\text{ann}_{S^1R}(S^{-1}M) = \cap_i \text{ann}_{S^{-1}R}(S^{-1}R(x_i/1)) = \cap_i S^{-1}\text{ann}_R(Rx_i) = S^{-1}(\cap_i \text{ann}_R(Rx_i)) = S^{-1}\text{ann}_R(M)$.

Notice that (c) follows immediately from (d).

Q.E.D

Theorem (Theorem 4.9 (Local to Global Principle))**.** Suppose M is an R-module, then the following are equivalent.

(i) $M = 0$.

(ii) $M_p = 0$ for all p a prime ideal.

(iii) $M_m = 0$ for all m a maximal ideal.

Proof. Notice that (i) implies (ii) and (iii) clearly. We show (iii) implies (i), and we're done, since (ii) implies (iii) as well. For (iii) implies (i), suppose M is not equal to 0. Then there exists $y \in M - \{0\}$. Notice that $I = \text{ann}(y)$ is not the whole ring. Hence, $I \subseteq m$ for some m. We choose this m. For this m, $0/1 = y/1 \subseteq 0 = M_m$ implies that in M, $ay = 0$ for some $a \in R - m \subseteq R - \text{ann}(y)$. So $a \notin \text{ann}(y)$ but also $a \in \text{ann}(y)$, so we have a contradiction. **Q.E.D**

Contraction and Extension of Ideals

Definition (Extension of an Ideal)**.** Let $\varphi : R \to T$ be a homomorphism of rings (a typical example is the inclusion map). Let I be an R-ideal. Then $I^e = IT = \varphi(I)T$ is a T-ideal. This is called the extension of I.

Definition (Contraction of an Ideal)**.** Let $\varphi : R \to T$ be a homomorphism of rings. Let J be an T-ideal. Then $J^c = J \cap R = \varphi^{-1}(J)T$ is called the contraction of J, and it is a T-ideal.

Remark (Remark 4.10)**.** Suppose I an R-ideal and J is a T-ideal.

(a) $I^e = I^{ece}$. In particular, every extended ideal is extended from its own contraction.

(b) $J^c = J^{cec}$. In particular, every contracted ideal is contracted from its own extension.

Proof. We show (a). Since $I \subseteq I^{ec}$, we get $I^e \subseteq I^{ece}$. On the other hand, $I^e = (I^e)^c e \subseteq I^e$. Hence, $I^e = I^{ece}$. The proof of (b) is similar. **Q.E.D**

Remark (Remark 4.11)**.** Assume T is a flat R-module, I is an R-ideal. Then $I^e \cong I \otimes_R T$ via $i \otimes_R t \mapsto \varphi(i)t$.

Proof. $0 \to I \xrightarrow{i} R$, and so $0 \to I \otimes_R T \to R \otimes_R T$ remains exact. Remember $R \otimes_R T \cong T$, so we have $0 \to I \otimes_R T \to T$. Take $i \otimes_R t \mapsto i \cdot t$ via multiplication in T as an R-module, and $i \cdot t = \varphi(i)t$. Therefore, the image of $I \otimes_R T$ in T is I^e, and so $I \otimes_R T \cong I^e$. **Q.E.D**

Definition (Primary Ideal)**.** Let I be an R-ideal. An ideal I is called primary if and only if $I \neq R$, $xy \in I$ implies $x \in I$ or $y^n \in I$ for some n. This is equivalent to saying that $I \neq R$ and if $xy \in I$ then $x \in I$ or $y \in I$ and x and y are in $\sqrt{I}$. This is equivalent to saying that $R/I \neq 0$ and every zero divisor in nilpotent in R/I.

Remark (Remark 4.12)**.** Suppose J is a T-ideal, then if J is prime (resp. primary) then so is J^c.

Proof. Notice that $\varphi : R \to T$ induces an embedding and $R \xrightarrow{i} T/J$ is injective, and the kernel is J^c. **Q.E.D**

Remark. Notice this is not true if you replace contraction with extension.

Theorem (Theorem 4.13)**.** Let S be a multiplicatively closed set, $\varphi : R \to S^{-1}R$, I an R-ideal.

(a) $I^e \cong I \otimes_R S^{-1}R \cong S^{-1}I$ and $S^{-1}R/I^e \cong \bar{S}^{-1}(R/I)$ as rings, where $\bar{S}$ is the image of S in R/I.

(b) Every ideal of $S^{-1}R$ is extended from R.

(c) $I^{ec} = \{x \in R : sx \in I, s \in S\}$. In particular, we know exactly when the extension of the ideal becomes the whole ring; $I^e = S^{-1}R$ if and only if $I \cap S \neq \varnothing$, and for p a prime ideal $IR_p \neq R_p$ if and only if $I \subseteq p$.

Proof. We prove (a). This follows from Corollary 4.5, Corollary 4.6, Corollary 4.7, Remark 4.11.

We prove (b). Let J be an $S^{-1}R$ ideal. We just need to show $J = J^{ce}$. From Remark 4.10, we know that all we need to show is $J \subseteq J^{ce}$. Let $x = r/s \in J$. Hence $s/1 \cdot x = r/1 \in J$, hence $r \in \varphi^{-1}(J) = J^c$. Hence, $1/s \cdot r/1 = x \in J^{ce}$. **Q.E.D**

Lemma (Lemma 4.13)**.** I is an R-ideal.

(a) $I^e \cong I \otimes S^{-1}R \cong S^{-1}I$ as $S^{-1}R$ modules, and $S^{-1}R/I^e \cong \bar{S}^{-1}(R/I)$ as rings.

(b) Every ideal from $S^{-1}R$ is extended.

(c) $I^{ec} = \{r \in R : sr \in I, s \in S\}$. In particular, $I^e = S^{-1}R$ if and only if $I \cap S = \varnothing$, and for a prime ideal p, $IR_p \neq R_p$ if and only if $I \subseteq p$.

(d) There is a one-to-one correspondence between $\{p : p$ a prime ideal of R with $S \cap p = \varnothing\} \leftrightarrow$ {prime ideals of $S^{-1}R$}.

(e) Same as (d) for primary.

Proof. We skip (a) and (b) and proceed to (c). Notice $S^{-1}R/I^e \cong S^{-1}(R/I)$. Notice φ induces a map from $R/I \to S^{-1}(R/I)$. WE then know that the kernel is $\ker(\varphi) = \{\bar{x} \in R/I : \exists s \in S$ such that $s\bar{x} = 0 \in R/I\}$. Alternatively, this is just $\{\bar{x} \in R/I : \exists s \in S$ with $sx \in I$ in $R\}$. Notice that the kernel I^{ec}/I, and so I^{ec}/I, and so $I^{ec} = \{x \in R : \exists s \in S$ with $sx \in I$ in $R\}$, since both contain I.

We show the first part of (d). We have $e \circ c = \mathrm{id}$ holds, because every ideal in $S^{-1}R$ is extended by (b), and by Proposition 4.2 we have it's the identity. Also the map is well-defined, since for all q a prime ideal in $S^{-1}R$, q^c is a prime ideal in R, and hence $q^c \cap S = \varnothing$.

We show the second part of (d). We need to show that $c \circ e = \mathrm{id}$. Let p be in the left hand side. We need to show $p^{ec} = p$. By (c), we know $p^{ec} = \{x \in R : sx \in p, s \in S\} = p$, since p is prime and s can never be in p. We need to show that this map is well-defined. Hence, if p is a prime ideal, then p^e is a prime ideal of $S^{-1}R$. We know $p^e = S^{-1}R$ by (c), since $S \cap p = \varnothing$. Let $x, y \in S^{-1}R$ so that $xy \in p^e$. We need to show $x \in p^e$ or $y \in p^e$. Write $x = r/s$, $y = r'/s'$. Since $xy \in p^e = S^{-1}p$, we have $rr'/ss' = a/t$ for $a \in p$, $t \in S$. Then in R we have $t'(rr't - ss'a) = 0$ for some $t' \in S$. Notice $tss'a \in p$ and $tt' \in S$, and since p is prime we have either r or r' is in p. This forces either x or y to be in p^e. **Q.E.D**

Corollary (Corollary 4.14)**.** Suppose R is a Noetherian or Arterian ring, then so is $S^{-1}R$.

Proof. This follows from Lemma 4.13 (b) and Remark 4.10. Hence every chain of ideals is extended from its contraction to R. **Q.E.D**

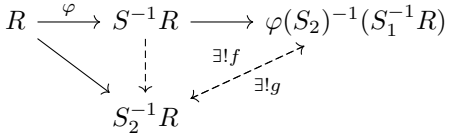
Corollary (Corollary 4.15)**.** If P is a prime ideal in R. then R_p is a local ring. The unique maximal ideal is pR_p, and $R_p/pR_p \cong (R/p)_{\bar{0}} \cong$ Quotient field. This motivates the term 'localization.'

Proof. Lemma 4.13 (d) and Lemma 4.13 (a). **Q.E.D**

Definition (Spectrum of Rings)**.** We define Spec(R) = spectrum of R = $\{p : p$ a prime ideal of R$\}$ This contains m-spec = maximal spectrum = {m : m a maximal ideal of R }

Proposition (Proposition 4.16)**.** Suppose S_1, S_2 are multiplicative sets such that $S_1 \subseteq S_2$. We have $\varphi : R \to S_1^{-1}R$. Then $\varphi(S_2)^{-1}(S_1^{-1}R) \cong S_2^{-1}R$.

Proof. By the universal property Proposition 4.2, we have the following diagram, and it's clear that $f \circ g = g \circ f = \text{id}$.



and it's clear that $f \circ g = g \circ f = id$. **Q.E.D**

Corollary (Corollary 4.17)**.**

$$p \in \text{Spec}(R), p \cap s = \varnothing. \text{ Then } pS^{-1}R \in \text{Spec}(S^{-1}R) \text{ and } (S^{-1}R)_{pS^{-1}R} \cong R_p.$$

In particular, if $p \subseteq q$ are two prime ideals of R_1 then $pR_q \in \text{Spec}(R_q)$

Definition (Saturated)**.** Suppose S is a multiplicative set of R. Then we say S is saturated if and only if we have that $xy \in S$ if and only if $x \in S$ and $y \in S$. Equivalently we have that S is saturated if and only if

$$S = R - \cup_{p \in \text{Spec}(R), p \bigcap S = \varnothing} p.$$

Definition (Saturation)**.** The saturation of S is denoted by $\widetilde{S} = \{x \; in R : xy \in S, y \in R\}$. It is the smallest saturated set containing S.

Proposition (Proposition 4.18)**.** Let φ be the map $\varphi : R \to S^{-1}R$. Then $\widetilde{S}$ is the unique smallest saturated multiplicative set containing S.

Proof. Proof omitted. **Q.E.D**

Theorem (Theorem 4.19)**.** Let R be a domain, and $S \subseteq R$ a multiplicative set which doesn't contain 0. Then we may consider $R \subseteq S^{-1}R \subseteq (S^{-1}R)_0 = R_0 = \text{Quot}(R)$. With these identifications, we have $R = \cap_{m \in m-\text{Spec}(R)} R_m$.

Proof. It's sufficient to show $\cap_m R_m \subseteq R$. Let $z \in \cap_m R_m \subseteq \text{Quot}(R)$. Consider $I = \{x \in R \backslash 0 : z = y/x, y \in R\} \cup \{0\} = \{x \in R : xz \in R\} = (R : Z)$ is an R-ideal. We want to show that $I = R$. Suppose $I \neq R$. Then we have $I \subseteq m$, m a maximal ideal. Now $I_m \neq R_m$ by Lemma 4.13 (c). Notice $I_m = (R : z)_m$ by Corollary 4.8 (c), and $(R : z)_m = R_m : (z/1) = R_m$, which is a contradiction. Hence, $I = R$. **Q.E.D**

Remark (Remark 4.20 (Zariski Topology))**.** (a) $V(0) = \text{Spec}(R)$.

(b) $V(R) = \varnothing$.

(c) $V(I_1 \cap \cdots \cap I_n) = \bigcup_{i=1}^n V(I_i) = V(I_i \cdots I_n)$.

(d) $V(\sum I_i) = \cap_i V(I_i)$.

Then $T = \{V(I) : I \text{ an } R\text{-ideal}\}$ induces a topology on $\text{Spec}(R)$, where T is the closed sets of $\text{Spec}(R)$. This is called the Zariski Topology. The topology induced on the maximal ideals is also called the Zariski topology.

Example. $m\text{-Spec}(R)(\mathbb{C}[x]) = \{(x - a) : a \in \mathbb{C}\} \leftrightarrow \mathbb{C}$. The closed sets are: $\varnothing$, $\mathbb{C}$, and finite subsets of points. Notice that the topology is not Hausdorff.

Remark (Notice)**.** $V(I) = V(J)$ if and only if $\sqrt{I} = \sqrt{J}$. So there is a one-to-one correspondence with T and the set of all the radical ideals.

Remark (Remark 4.21)**.**

1. $V(I) \leftrightarrow \mathrm{Spec}(R/I)$ (they have a one-to-one correspondence), and they are homeomorphic.
2. $D_x \leftrightarrow \mathrm{Spec}(R_x)$ (see Lemma 4.13 (d)), and they are homeomorphic.
3. $\{D_x : x \in R\}$ form a basis of the topology.
4. $\mathrm{Spec}(R)$ is quasicompact (compact, but not Hausdorff).
5. If R is Noetherian, then every open set is quasicompact.

Proof. The only nontrivial remark is (d). We must show $\varnothing = \cap_i V(I_i)$. This means $\varnothing = V(I_1) \cap \cdots \cap V(I_n)$. Now $V(R) = V(\sum I_i)$, which implies $R = \sqrt{\sum I_i}$. This then gives us $R = \sum I_i$, or $1 = f_{i_1} + \cdots + f_{i_n}$ for $f_{i_j} \in I_{i_j}$, which gives us $\varnothing V(I_1) \cap \cdots \cap V(I_n)$. **Q.E.D**

Remark. Suppose $\varphi : R \to T$ is a homomorphism of rings, then we have $\varphi^* : \mathrm{Spec}(T) \to \mathrm{Spec}(R)$ which sends $p \mapsto p^c$. This should be a homomorphism of topological spaces.

Remark (Remark 4.22 (Contravariant Functor))**.** (a) φ^* is continuous

(b) $(\psi\varphi)^* = \varphi^* \circ \psi^*$

(c) $\mathrm{id}^* = \mathrm{id}$

This is called a contravariant functor.

Definition (Support of a Module)**.** If M is an R-module, then the support of M is defined by $\mathrm{Supp}(M) := \{p \in \mathrm{Spec}(R) : M_p \neq 0\}$.

Remark (Remark 4.23)**.** If M is a finitely generated module, then $\mathrm{Supp}(M) = V(\mathrm{ann}_R(M))$. In particular, $\mathrm{Supp}(M)$ is closed (topologically).

Proof. Since M is finitely generated, we can rewrite it as $M = Rx_1 + \cdots + Rx_n$. In particular, $\mathrm{Supp}_R(M) = \cup_{i=1}^M \mathrm{Supp}_R(Rx_i) = \cup_{i=1}^n \mathrm{Supp}(R/\mathrm{ann}_R(x_i)) = \cup_{i=1}^n V(\mathrm{ann}_R(x_i)) = V(\cap_{i=1}^n \mathrm{ann}_R(x_i)) = V(\mathrm{ann}_R(M))$, as required. **Q.E.D**

Remark. Suppose $p \in \mathrm{Spec}(R)$, and look at $k(p) :=$ residue field of $p = R_p/pR_p = \mathrm{Quot}(R/p)$.

Proposition (Proposition 4.24)**.** Suppose M is a finite module. Then M=0 iff $M \otimes_R k(m) = 0$, for all m in m-Spec(R).

Proof. We prove the converse (the implication is clear). We have $0 = M \otimes_R k(m)$ by assumption, which gives us $M \otimes_R R_m/mR_m \cong M \otimes_R (R_{m_{R_m}} \otimes_R R_m/mR_m) \cong (M \otimes_R R_{mR_m}) \otimes_R R_m/mR_m \cong M_m \otimes_R R_m/mR_m \cong M_m M_m$, hence $M_m = mR_m M_m$ implies $M_m = 0$ by Theorem 2.2 (Nakayama's Lemma), and since this applies for all m we get $M = 0$. **Q.E.D**

Chapter 5: Associated Primes and Primary Decomposition

Definition (Associated Prime)**.** If M is an R-Module, we say p is an associated prime of M if p is prime and there exists an x in M such that p = ann(x). $\mathrm{Ass}(M) = \mathrm{Ass}_R M = \{\text{associated primes of M}\}$

Theorem (Theorem 5.1)**.** Suppose R is a Noetherian ring, and M is a nonzero R-module. Then

(a) $\Lambda = \{\mathrm{ann}(x) : 0 \neq x \in M\}$. Every maximal element in Λ is an associated prime of M. In particular, there are associated primes. ($\mathrm{Ass}(M) \neq 0$)

(b) $\{\text{zero divisors on M}\} = \cup_{p \in \mathrm{Ass}(M)} p$.

Notice in particular (a) says that if R is Noetherian, then $M = 0$ if and only if $\mathrm{Ass}(M) = \varnothing$.

Proof. (a) Let $p \in \Lambda$ be a maximal element. We need to prove it is prime. It's clear that $p \neq R$. Next, if $xy \in p$, then we must show either $x \in p$ or $y \in p$. Let $p = ann(x), x \in M$. If $xy \in p$ then $xy \in ann(x)$. If $b \notin ann(x) = p_1$ then $bx \neq 0$. Hence $ann(bx) \in \Lambda$. Hence $ann(x) \subseteq ann(bx)$. But by maximality, we get $ann(x) = ann(bx)$. Hence, $a \in ann(x) = p$. So we are done.

(b) We only need to prove the inclusion. A zero divisor is an element which annihilates some nonzero divisors, and so by definition $\{\text{zero divisors on M}\} = \cup_{I \in \Lambda} I = \cup_{p \in \Lambda \text{maximal}} \subseteq \cup_{p \in \mathrm{Ass}(M)} p$.
Q.E.D

Theorem (Theorem 5.2)**.** Let S be any multiplicative set of R, identify $\mathrm{Spec}(S^{-1}R)$ with a subset of $\mathrm{Spec}(R)$ by Lemma 4.13 (d).

(a) Suppose N is an $S^{-1}R$ module. Then it's also an R-module, and so $\mathrm{Ass}_{S^{-1}R}(N) = \mathrm{Ass}_R(N)$.

(b) If R is Noetherian and M is an R-module, then $\mathrm{Ass}_{S^{-1}R}(S^{-1}M) = \mathrm{Ass}_R(M) \cap \mathrm{Spec}(S^{-1}R)$.

Proof. We show (a). Let $p \in \mathrm{Ass}_R(N)$. Then $p = \mathrm{ann}_R(x)$, $x \in N$, and $x \neq 0$. Hence, $x \in S^{-1}N$. Therefore, $\mathrm{ann}_{S^{-1}R}(x/1) \neq S^{-1}R$. Notice this is equivalent to $S^{-1}(\mathrm{ann}_R(x))$ by Corollary 4.8 (c). So this is really $S^{-1}p$ and since it's not the whole ring, this gives us $S^{-1}p$ is prime by Lemma 4.13. So $pS^{-1}R \in \mathrm{Ass}_{S^{-1}R}(N)$. Hence, $\mathrm{Ass}_R(N) \subseteq \mathrm{Ass}_{S^{-1}R}(N)$. Suppose $q \in \mathrm{Ass}_{S^{-1}R}(N)$, say $q = \mathrm{ann}_{S^{-1}R}(x)$, where $x \in N$. Let $p = q^c = q \cap R$. Then $p = q \cap R = \mathrm{ann}_R(X)$. Also $p \in \mathrm{Spec}(R)$, so $p \in \mathrm{Ass}_R(N)$.

We show (b). Let $P \in \mathrm{Ass}_R(M) \cap \mathrm{Spec}(S^{-1}R)$. So $p \cap S = \varnothing$. Then $S^{-1}p$ is, again, a prime ideal. Also, $p \in \mathrm{Ass}_R(M)$, $p = \mathrm{Ann}_R(x)$ for some x. So by Corollary 4.8 (c), we have $S^{-1}p = pS^{-1}R = \mathrm{Ann}_{S^{-1}R}(x/1)$. Hence, $p \in \mathrm{Ass}_{S^{-1}R}(S^{-1}M)$. Let $p \in \mathrm{Ass}_{S^{-1}R}(S^{-1}M)$. We only need to show that $p \in \mathrm{Ass}_R(M)$. By (a), $\mathrm{Ass}_{S^{-1}R}(S^{-1}M) = \mathrm{Ass}_R(S^{-1}M)$. We then have $p = \mathrm{Ann}_R(x/t)$, $x \in M$ and $t \in S$. Since R is Noetherian, p is finitely generated, say $p = Ra_1 + \cdots + Ra_n$. Now $a_0 \cdot x/t = 0$ in $S^{-1}M$ for all i. Hence, there exists $s_i \in S$ with $s_i a_i x = 0$ in M. Since there are finitely many a_i, then there exists $s \in S$ such that $sa_i x = 0$. Since the a_i's generate p, we have $psx = 0$ in M. So we get $p \subseteq \mathrm{Ann}_R(sx) \subseteq \mathrm{Ann}_R(sx/1) = \mathrm{Ann}_R(x/t) = p$. This forces $p = \mathrm{Ann}_R(sx)$. So p is an associated prime of M; $p \in \mathrm{Ass}_R(M)$.
Q.E.D

Corollary (Corollary 5.3)**.** If M is an R-module, R a Noetherian ring, then $p \in \mathrm{Ass}_R(M)$ if and only if $pR_p \in \mathrm{Ass}_{R_p}(M_p)$.

Remark (Remark 5.4)**.** Suppose M is an R-module, then $\mathrm{Ass}_R(M) \subseteq \mathrm{Supp}_R(M)$.

Proof. Suppose $p \in \mathrm{Ass}_R(M)$. Then $R/p \cong R/\mathrm{Ann}_R(x) \cong Rx \subseteq M$. This gives $p \in \mathrm{Supp}_R(Rx) \subseteq \mathrm{Supp}_R(M)$. **Q.E.D**

Theorem (Theorem 5.5)**.** Suppose we have the following exact sequence of R-modules

$$0 \to M' \to M \to M'' \to 0.$$

Then

(a) $\mathrm{Supp}_R(M) = \mathrm{Supp}_R(M') \cup \mathrm{Supp}_R(M'')$.

(b) (i) $\mathrm{Ass}_R(M') \subseteq \mathrm{Ass}_R(M)$.
(ii) $\mathrm{Ass}_R(M) \subseteq \mathrm{Ass}_R(M') \cup \mathrm{Ass}_R(M'')$.

Proof. We prove (a). Let $P \in \mathrm{Spec}(R)$. Then we have

$$0 \to M'_p \to M_p \to M''_p \to 0$$

is exact. Hence $M_p \neq 0$ if and only if $M'_p \neq 0$ or $M''_p \neq 0$.

We prove (b). Part (i) is clear. For (ii), let p be in $\mathrm{Ass}_R(M)$. Say $p = \mathrm{Ann}_R(x)$, $x \in M$. Assume $M' \subseteq M$ and $M'' = M/M'$. Let $N = Rx \subseteq M$. Then $\mathrm{Ass}_R(N) = \mathrm{Ass}_R(R/p) = \{p\}$. We then have two cases. In the first case, we have that $N \cap M' = 0$. In this case, $N/N \cap M' = N$ which injects into $M/M' = M''$. Therefore, $p \in \mathrm{Ass}_R(M'')$, and moreover $\mathrm{Ass}_R(N) \subseteq \mathrm{Ass}_R(M'')$. In the second case, $M' \cap N \neq 0$, and so $N \cap M' \subseteq R/p$. Therefore, taking any $x \neq 0$ in $N \cap M'$, we have $\mathrm{Ann}_R(x) = p$. Therefore, $p \in \mathrm{Ass}_R(M')$. **Q.E.D**

Theorem (Theorem 5.6)**.** Let R be a Noetherian ring and $M \neq 0$ a finite R-module. Then there is a chain of submodules $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ so that $M_i/M_{i-1} \cong R/p_i$ with $p_i \in \mathrm{Spec}(R)$ for all $1 \leqslant i \leqslant n$. Moreover, $\mathrm{Ass}_R(M) \subseteq \{p_i\}$.

Proof. Examine $\Lambda = \{N \neq 0 : N \text{ a submodule of M with a prime filtration}\}$. We first prove $\Lambda \neq \varnothing$. Since R is Noetherian and $M \neq 0$, there exists a $p \in \mathrm{Ass}_R(M)$ by Theorem 5.1. Hence, there exists an $x \in M$ with $\mathrm{Ann}_R(x) = p \in \mathrm{Spec}(R)$. Let $N = Rx$. Clearly, this is nonzero and since this is a generator, we get $N \in \Lambda$ and $N \cong R/p$. Thus, $\Lambda \neq \varnothing$. Since M is a Noetherian module, we get Λ has a maximal element in N. Suppose $N \subsetneq M$. Then $M/N \neq 0$. So by the first step of the proof, M/N has a submodule N' with $N' \cong R/p$ for some $p \in \mathrm{Spec}(R)$. The preimage of N' in M contains N properly, and furthermore it is in Λ. This contradicts the maximality of N. For the additional claim, we use induction on n. If $n = 1$, then $M = M_1 = R/p$ for some $p \in \mathrm{Spec}(R)$. Then $\mathrm{Ass}_R(M) = \{p\}$. Assume it holds for $n-1$. Then we get

$$0 \to M_{n-1} \to M_n \to R/p^n \to 0.$$

Hence, by Theorem 5.5 (b), $\mathrm{Ass}_R(N) \subseteq \mathrm{Ass}_R(M_{n-1}) \cup \mathrm{Ass}_R(R/p^n) \subseteq \{p_0, \ldots, p_{n-1}\} \cup \{p_n\}$. **Q.E.D**

Theorem (Theorem 5.7)**.** Let R be a Noetherian ring and M a finitely generated R-module. Then

(a) $\mathrm{Ass}_R(M)$ is finite.

(b) The minimal elements of $\mathrm{Ass}_R(M)$ and $\mathrm{Supp}_R(M)$ coincides. Furthermore, there are only finitely many elements, and they exist if $M \neq 0$; moreover, every element in the support contains a minimal element.

Proof. Notice that (a) follows from Theorem 5.6 We prove (b). We already know $\text{Ass}_R(M) \subseteq \text{Supp}_R(M)$ and $\text{Ass}_R(M) \neq \varnothing$ if $M \neq \varnothing$. The only thing we need to show is that for all $p \in \text{Supp}_R(M)$, there exists $q \in \text{Ass}_R(M)$ with $q \subseteq p$. Now $\text{Ass}_R(M) \cap \{\text{prime ideals contained in p}\} = \text{Ass}_R(M) \cap \text{Spec}(R_p) = \text{Ass}_R(M_p) \neq \varnothing$ because R_p is Noetherian and $p \in \text{Supp}_R(M)$. **Q.E.D**

Corollary (Corollary 5.8)**.** Suppose R is a Noetherian ring.

(a) If M is a finite R-module, then {zero divisors on M} is a finite union of prime ideals.

(b) R has only finitely many minimal primes.

Proof. We prove (a). By Theorem 5.1, {zero divisors on M} $= \cup_{p \in \text{Ass}_R(M)} p$. By Theorem 5.7, this is a finite set of primes. We prove (b). Notice $\text{Spec}(R) = V(0) = \text{Supp}_R(R)$. The result then follows by Theorem 5.7 (b). **Q.E.D**

Remark. Recall that $I \subsetneq R$ is primary if and only if for every zero divisor $\bar{a}$ in the ring R/I, we have $\bar{a} \in \text{nil}(R)$ if and only if for every zero divisor $a \in R$ on the R-module R/I, we have that there exists n with $a^n \in \text{Ann}_R(R/I)$. Saying it this way generalizes it to modules.

Definition (Primary Submodule)**.** Let N be a submodule of a module M, $N \subsetneq M$. We say N is a primary submodule of M if and only if for every zero divisor $a \in R$ on M/N, there exists n with $a^n \in \text{Ann}_R(M/N)$.

Proposition (Proposition 5.9)**.** Suppose R is a Noetherian ring, M a finite R-module, and N is a proper submodule $N \subsetneq M$. Then N is the primary submodule of M if and only if $\text{Ass}_R(M/N)$ consists of exactly one element. If this happens, we write $I = \text{Ann}_R(M/N)$ and p for the unique element in $\text{Ass}_R(M/n)$. Then I is a primary ideal and $\sqrt{I} = p$.

Proof. IF N is primary in M, then $\cup_{p \in \text{Ass}_R(M/N)} p = \sqrt{\text{Ann}_R(M/N)}$ so $\cup_{p \in \text{Ass}_R(M/N)} p = \cap_{p \in \text{Supp}_R(M/N)} p$ since $V(\text{Ann}_R(M/N)) = \text{Supp}_R(M/N)$ and $\sqrt{I} = \cap_{p \in V(I)} p$. Now we use Theorem 5.7 to note that the intersection over all primes is equivalent to the intersection over the minimal primes, and every minimal prime is in the associated primes. So $\cup_{p \in \text{Ass}_R(M/N)} p = \cap_{p \in \text{Ass}_R(M/N)} p$ then $|\text{Ass}_R(M/N)| = 1$. Write $M/N = Rx_1 + \cdots + Rx_n$, then $R/I = R/\cap_{i=1}^n \text{Ann}_R(x_i)$. By Theorem 1.16 (Chinese Remainder Theorem), we have $R/\cap_{i=1}^n \text{Ann}_R(x_i) \hookrightarrow \bigoplus_{i=1}^n R/\text{Ann}_R(x_i) = \bigoplus_{i=1}^n Rx_i$. Hence, $\text{Ass}_R(R/I) \subseteq \text{Ass}_R(\bigoplus_{i=1}^n Rx_i) \subseteq \cup_{i=1}^n \text{Ass}_{Rx_i}(\subseteq)\text{Ass}_R(M/N)$. Hence, $\text{Ass}_R(R/I) = \{p\}$, and we immediately see I is primary. Furthermore, p is the unique minimal prime of I (Theorem 5.7) and hence $\sqrt{I} = p$. **Q.E.D**

Definition (P-Primary Submodule of M)**.** If there is only one associated prime in M/N, we say N is a p-primary submodule of M.

Proposition (Proposition 5.10)**.** Suppose R is a Noetherian ring, M is a finite R-module, and N and N' are p-primary submodules of M. Then $N \cap N'$ is p-primary.

Proof. We have $M/N \cap N' \hookrightarrow M/N \oplus M/N'$. Hence $\text{Ass}_R(M/N \cap N') \subseteq \text{Ass}_R(M/N \oplus M/N') \subseteq \text{Ass}_R(M/N) \cup \text{Ass}_R(M/N') = \{p\}$. Notice $M/N \cap N' \neq 0$, and so $\text{Ass}_R(M/N \cap N') = \{p\}$. Therefore, $N \cap N'$ is a p-primary submodule of M, per definition. **Q.E.D**

Definition (Irreducible Submodule)**.** If N is a submodule of M¡ $N \subsetneq M$, then N is an irreducible submodule of M if, whenever $N = N_1 \cap N_2$ with N_1, N_2 submodules of M, then $N_1 = N$ or $N_2 = N$. It's called reducible otherwise.

Remark. N is an irreducible submodule of M if and only if 0 is an irreducible submodule of M/N.

Theorem (Theorem 5.11)**.** Let R be a Noetherian ring, M a finite R-module, and $N \subsetneq M$ a submodule. If N is an irreducible submodule of M, then N is a primary submodule of M.

Proof. Suppose otherwise for contradiction. Then M/N has at least two associated primes, denote them by p and q. Let $M = M/N$, we may assume $N = 0$. Now $p \neq q$ are in $\mathrm{Ass}_R(M)$. Then there are cyclic submodules N_1, N_2 of M where $N_1 \cong R/p$ and $N_2 \cong R/q$. We now examine $\mathrm{Ass}_R(N_1 \cap N_2) \subseteq \mathrm{Ass}_R(N_1) \cap \mathrm{Ass}_R(N_2) = \mathrm{Ass}_R(R/p) \cap \mathrm{Ass}_R(R/q) = \{p\} \cap \{q\} = \varnothing$. So this means that $N_1 \cap N_2 = 0$. But $N_1, N_2 \neq 0$, so 0 is not an irreducible submodule of M. This completes the proof. **Q.E.D**

Proposition (Proposition 5.12)**.** Suppose R Noetherian, M finite R-module. Then any proper submodule $N \subsetneq M$ is a finite intersection of irreducible submodules of M.

Proof. Let $\Gamma = \{N \subsetneq M : N \text{ submodule and } N \text{ is not a finite intersection of irreducible submodules}\}$. Suppose $\Gamma \neq \varnothing$. Then by the Noetherian property of M, Γ has a maximal element; denote it by N. Notice N cannot be irreducible. Since it's not irreducible, $N = N_1 \cap N_2$ for some submodules $N \subsetneq N_1$ and $N \subsetneq N_2$. Notice both N_1 and N_2 must be proper. By the maximality of N, we have both N_1 and N_2 are the finite intersection of irreducible submodules, then so is N, a contradiction. Then $\Gamma = \varnothing$ and the statement follows. **Q.E.D**

Theorem (Theorem 5.13)**.** Suppose R is a Noetherian ring, M a finite R-module, $N \subsetneq M$ submodule. Then $N = N_1 \cap \cdots \cap N_n$ with N_i p_i-primary submodules of M and p_i's are pairwise distinct.

Proof. Follows by Proposition 5.12, Theorem 5.11, Proposition 5.10. **Q.E.D**

Definition (Primary Decomposition)**.** Suppose $N = N_1 \cap \cdots \cap N_n$ with N_i primary submodules of M, then we call this the primary decomposition of N. The primary decomposition is irreducible; i.e. none of the N_i can be dropped. In other words, $N_1 \cap \cdots \cap N_{i-1} \cap N_{i+1} \cap \cdots \cap N_n \nsubseteq N_i$ for all i. A primary decomposition is called the shortest if it is irredundant and the p_i's are pairwise distinct. If $N = N_1 \cap \cdots \cap N_n$ is a shortest primary decomposition with N_i as before, then N_i is called a p_i-primary component of N.

Theorem (Theorem 5.14)**.** R is a Noetherian ring, M a finite R-module, and $N \subsetneq M$ a submodule. Suppose there is a primary decomposition, and suppose it's irredundant.

(a) $\{p_1, \ldots, p_n\}$ is unique, and it's exactly the set of associated primes, $\mathrm{Ass}_R(M/N)$.

(b) Let S be any multiplicative set, $\varphi : M \to S^{-1}M$. Then $\cap_{p_i \cap S = \varnothing} N_i = \varphi^{-1}(S^{-1}N)$. In particular, this is uniquely determined by N.

Proof. We begin with (a). We prove the inclusion. Replace M by M/N, we may assume $N = 0$. Now we have $0 = N_1 \cap \cdots \cap N_n$ irredundant, N_i p_i-primary. We need to show $p_1 \in \mathrm{Ass}_R(M)$. By irredundancy of the decomposition, $0 \neq N_2 \cap \cdots \cap N_n \hookrightarrow M/N_1$. So $\mathrm{Ass}_R(M)$ contains $\mathrm{Ass}_R(N_2 \cap \cdots \cap N_n)$ is contained in $\mathrm{Ass}_R(M/N_1) = \{p_1\}$. Hence $\mathrm{Ass}_R(N_2 \cap \cdots \cap N_n) = \{p_1\}$ and so $\{p_1\} \subseteq \mathrm{Ass}_R(M)$. We prove the reverse inclusion. Notice that $M/N = M/N_1 \cap \cdots \cap N_n \hookrightarrow M/N_1 \oplus \cdots \oplus M/N_n$ implies that $\mathrm{Ass}_R(M/N) \subseteq \mathrm{Ass}_R(M/N_1 \oplus \cdots \oplus M/N_n) = \cup_{i=1}^n \mathrm{Ass}_R(M/N_i) = \{p_1, \ldots, p_n\}$.

We prove (b). We start with $\varphi^{-1}(S^{-1}M) = \varphi^{-1}(S^{-1}N_1 \cap \cdots \cap S^{-1}N_n) = \varphi^{-1}(S^{-1}N) \cap \cdots \cap \varphi^{-1}(S^{-1}N_n)$. It remains to show that if we let N' be a p-primary submodule of M, then $\varphi^{-1}(S^{-1}N') = \begin{cases} M \text{ if } p \cap S \neq \varnothing \\ N' \text{ if } p \cap S = \varnothing \end{cases}$. If $p \cap S \neq \varnothing$, then $S^{-1}p = S^{-1}R = S^{-1}\sqrt{\mathrm{Ann}_R(M/N')} = \sqrt{\mathrm{Ann}_R(S^{-1}M/S^{-1}N)}$ then $S^{-1}R = \mathrm{Ann}_R(S^{-1}M/S^{-1}N)$ which implies $S^{-1}M = S^{-1}N'$, which finally gives us $\varphi^{-1}(S^{-1}N') = M$. If $p \cap S = \varnothing$, then S consists of only nonzerodivisors of M/N', since p is the only associated prime of this module and $\{\text{zerodivisors of } M/N'\} = p$. This means the natural map $M/N' \hookrightarrow S^{-1}(M/N')$ is injective. This is the same as $S^{-1}M/S^{-1}N'$. The kernel of the map is $\varphi^{-1}(S^{-1}N')/N'$. Since this is zero, $\varphi^{-1}(S^{-1}N') = N'$. Hence, we have the two cases, as required. **Q.E.D**

Corollary (Corollary 5.15)**.** With the same setting as in Theorem 5.14, let P be a minimal element in $\mathrm{Ass}_R(M/N)$. Then the p-primary component in any shortest primary decomposition of N is uniquely determined.

Proof. By Theorem 5.14, using the notation from there, and taking $S := R\backslash p : \varphi^{-1}(N_p) = \cap_{p_i \subseteq p} N)i$. But p is minimal, so $\varphi^{-1}(N_p) = p$-primary component. **Q.E.D**

Chapter 6: Dimension and Hilbert's Nullstellensatz

Dimension

Definition (Krull Dimension)**.** We define $\dim(R) = \sup\{n : \exists p_0 \subsetneq p_1 \subsetneq \cdots \subsetneq p_n \text{ with } p_i \in \operatorname{Spec}(R)\}$. We call this the Krull Dimension of R.

Theorem (Theorem 6.1)**.** A ring R is Artinian if and only if it is Noetherian and $\dim(R) = 0$.

Proof. We show the implication. We know that R is Noetherian and so R is semilocal. Say $m\text{-Spec}(R) = \{m_1, \ldots, m_n\}$. Furthermore, $\operatorname{Rad}(R) = \sqrt{0}$. To show $\dim(0) = 0$, we show $m\text{-Spec}(R) = \operatorname{Spec}(R)$. Let $p \in \operatorname{Spec}(R)$. Then we know $\sqrt{0} \subseteq p$, since $\operatorname{Rad}(R) = \sqrt{0}$, we have $m_1 \cap \cdots \cap m_n \subseteq p$ implies $p = m_i$ for some i, and so p is maximal.

We show the converse. By assumption, $\dim(R) = 0$, and so every maximal ideal is minimal. Hence, $\operatorname{Rad}(R) = \sqrt{0}$. Furthermore, since R is Noetherian, $\sqrt{0}$ is finitely generated, hence $(\sqrt{0})^r = 0$ for some r, and hence $(\operatorname{Rad}(R))^r = 0$. Every maximal ideal of R is the minimal prime ideal, hence an associated prime. But there are only finitely many associated primes since R is Noetherian. Hence, R is semilocal. The rest follows as in proof of Theorem 3.17, since R is semilocal and $(\operatorname{Rad}(R)))^r = 0$, thus we have R Artinian if and only if R is Noetherian. **Q.E.D**

Example. If R is a PID which is not a field, then $\dim(R) = 1$.

Definition (Height of a Prime)**.** Suppose we have a $p \in \operatorname{Spec}(R)$, then $\operatorname{ht}(p) = \operatorname{height}(p) = \dim(R_p) = \sup\{n : \exists p_0 \subsetneq \cdots \subsetneq p_n \subsetneq p \text{with } p_i \in \operatorname{Spec}(R)\}$.

Definition (Dimension of a Prime)**.** We have that $\dim(p) =$ dimension of p $= \dim(R/p) = \sup\{n : p \subseteq p_0 \subsetneq \cdots \subsetneq p_n, p_i \in \operatorname{Spec}(R)\}$.

Remark. Notice that $\operatorname{ht}(p) + \dim(p) \leqslant \dim(R)$ for all $p \in \operatorname{Spec}(R)$.

Definition (Height of an Ideal)**.** Let I be any R-ideal: $\operatorname{ht}(I) =$ height of I $= \inf\{\operatorname{ht}(p) : p \in V(I)\} = \inf\{\operatorname{ht}(p) : p \text{ minimal prime in } V(I)\}$. Obviously, $\operatorname{ht}(I) + \dim(R/I) \leqslant \dim(R)$.

Definition (Catenary)**.** A ring R is called catenary if for any two prime ideals $p \subseteq q$, there exists a chain of prime ideals $p = p_0 \subsetneq p_1 \subsetneq \cdots \subsetneq p_n = q$ which cannot be refined any further, and every such chain has the same length.

Remark. It is, in fact, extremely hard to find rings which are not catenary.

Remark (Remark 6.2)**.** Suppose R is a local catenary domain. Then for any every ideal I, $\operatorname{ht}(I) + \dim(R/I) = \dim(R)$.

Hilbert's Nullstellensatz

Proposition (Proposition 6.3)**.** Suppose k is a field, $k \subseteq K$ a field extension, $\alpha_1, \ldots, \alpha_n \in K$ are algebraic over k. Then $k(\alpha_1, \ldots, \alpha_n) = k[\alpha_1, \ldots, \alpha_n] \cong k[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$. Furthermore, $f_i \in k[X_1, \ldots, X_n]$ are monic in X_i.

Proof. We will prove this via induction on n. For $n = 1$, we have $k[\alpha] = k[X]/I$, where I is an ideal and $I \neq 0$. Also $k[\alpha] \subseteq K$, so I is a prime ideal, hence I is a maximal ideal. So $k[\alpha] \cong k[X]/I$ is a field, hence $k[\alpha] = \operatorname{Quot}(k[\alpha]) = k(\alpha)$. Notice $I = (f)$ for some nonzero polynomial,

which we can assume is monic. Thus, the first step is complete. By the induction hypothesis, $k(\alpha_1, \ldots, \alpha_{n-1}) = k[\alpha_1, \ldots, \alpha_{n-1}] \cong k[X_1, \ldots, X_{n-1}]/(f_1, \ldots, f_{n-1})$, with f_i monic. Call this field k_0. By the result for $n = 1$, $k_0(\alpha_n) = k[\alpha_n] \cong k_0[X_n]/(g)$, g a monic polynomial. Now we have natural surjections $k[X_1, \ldots, X_{n-1}][X_n] \twoheadrightarrow k_0[X_n]$ via projection. Let $f_n \in k[X_1, \ldots, X_{n-1}][X_n]$ be monic and the preimage of g. Now $k(\alpha_1, \ldots, \alpha_n) = k_0(\alpha_n) = k_0[\alpha_n] = k[\alpha_1, \ldots, \alpha_{n-1}, \alpha_n] \cong k_0[\alpha_n] \cong (k[X_1, \ldots, X_{n-1}]/(f_1, \ldots, f_{n-1}))[X_n]/g \cong k[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$. **Q.E.D**

Theorem (Theorem 6.4)**.** $k \subseteq T \subseteq R$ rings, k Noetherian, R is a finite T-module. If R is a finitely generated k-algebra, then so is T.

Proof. We'll construct a finitely generated k-algebra, call it k_0 with $k_0 \subseteq T$ such that R is a finite k_0-module. Then k_0 is a Noetherian ring (Corollary 3.19), hence R is a Noetherian k_0-module (Corollary 3.6), hence its k_0-submodule T is finitely generated as a k_0-module (Proposition 3.2). Hence, T is a finitely generated k-algebra. To obtain k_0, write $R = k[\alpha_1, \ldots, \alpha_n] = T\beta_1 + \cdots + T\beta_m$, where we may assume $\beta_1 = 1$. We have that for all i, j $\alpha_i\beta_j = \sum_{k=1}^{m} \alpha_{i_{j_k}}\beta_k$ with $\{\alpha_{i_{j_k}}\}$ a finite subset of T. Now $k_0 = k[\{\alpha_{i_{j_k}}\}] \subseteq T$, which is a finitely generated k-algebra in T. So we need to establish R is a finite k_0-module, because $R = k_0\beta_1 + \cdots + k_0\beta_m$, where $k[\alpha_1, \ldots, \alpha_n] = R$. We show this by induction on the degree that monomials in $\alpha_1, \ldots, \alpha_n$ are in the right hand side. **Q.E.D**

Theorem (Theorem 6.5)**.** Suppose k ia field, R a finitely generated k-algebra that is a field. Then $k \subseteq R$ is algebraic.

Proof. Suppose not. Then there is a purely transcendental extension $k \subseteq T = k(Y_1, \ldots, Y_k)$ inside R, and $t > 0$, so that $T \subseteq R$ is algebraic. Notice R is a finite T-module, since $T \subseteq R$ is algebraic and finitely generated field extension. So by the prior theorem T is a finitely generated k-algebra. Now $T = k(Y_1, \ldots, Y_k) = \text{Quot}(k[Y_1, \ldots, Y_k])$ with $t > 0$ and $Y_1, \ldots, Y_k$ indeterminates is finitely generated as a k-algebra. Hence, $T = k[\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n}]$ and not all of the g_i are in k. Let $h = \prod_{i=1}^{n} g_i + 1$. Then h is not a constant, $h \notin k$. Then $\frac{1}{h} \in k[\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n}]$ and hence in $k[Y_1, \ldots, Y_k]$ we have that h divides a product of the powers of $g_1, \ldots, g_n$. This is impossible, because h is not a unit, and furthermore $\gcd(h, g_i) \sim 1$. **Q.E.D**

Remark. Using Proposition 6.3 and Theorem 6.5 we can show that if $k \subseteq K$ a finitely generated field extension, then $k \subseteq K$ algebraic if and only if K is a finitely generated k-algebra.

Theorem (Theorem 6.6 (Hilbert's Nullstellensatz (Part 1)))**.** Suppose k is a field, and $m \in m\text{-Spec}(k[X_1, \ldots, X_n)$. Since $k \hookrightarrow k[X_1, \ldots, X_n]/m$ is an algebraically closed, then we get $k = k[X_1, \ldots, X_n]/m$. Furthermore, $m = (x_1 - a_1, \ldots, x_n - a_n)$ where $a_i \in k$.

Proof. We use Theorem 6.5 and Proposition 6.3. If k is algebraically closed, then $k = k[X_1, \ldots, X_n]/m$, hence for all i, there exists $a_i \in k$ so that $x_i \equiv a_i \pmod{m}$. Hence $(x_1 - a_1, \ldots, x_n - a_n) \subseteq m$, but both are max ideals, and so they must be equal. **Q.E.D**

Theorem (Theorem 6.7 (Hilbert's Nullstellensatz (Part 2)))**.** Suppose k is a field, R is a finitely generated k-algebra, I an R-ideal. Then

$$\sqrt{I} = \bigcap_{\substack{I \subseteq m \\ m \in m\text{-Spec}(R)}} m.$$

Proof. Use Theorem 6.5 and Proposition 6.3. Assume $I = 0$ via replacing R by R/I. Then we just need to show that $\sqrt{0} = \text{Rad}(R)$. Let $f \in R$, $f \notin \sqrt{0}$. We need to show $f \notin \text{Rad}(R)$. So we must show that there exists a $m \in m\text{-Spec}(R)$ with $f \notin m$. Since $f \notin \sqrt{0}$, we know R_f, which is $S^{-1}R, S = \{1, f, f^2, \ldots\}$, is not equal to 0. Then we can see R_f has a maximal ideal, n. Let $m = n^c$. We know that $f \notin m$, and m is prime. Now $k \subseteq R/m = R/n^c \subseteq R_f/n$. Now $R_f = \varphi(R)[\frac{1}{f}]$ is a finitely generated k-algebra. Therefore, R_f/n is still finitely generated, and it's a field. Then R/m is algebraic, and so ti is a field by Proposition 6.3. So m is a maximal ideal in R, and we're done. **Q.E.D**

Remark. Let k be any field, $R = k[X_1, \ldots, X_n]$, $\mathbb{A}_k^n = k^n$. Suppose $A \subseteq R$ a subset, then $V(A) = \{(a_1, \ldots, a_n) \in \mathbb{A}_k^n : \varphi(a_1, \ldots, a_n) = 0 \forall f \in A\}$. This is obviously a subset of $\mathbb{A}_k^n$. Conversely, $X \subseteq \mathbb{A}_k^n$ a subset, then $I(X) = \{f \in R : f(a_1, \ldots, a_n) = 0 \forall a_i \in X\}$. This is, in fact, an ideal of R. We call $X \subseteq \mathbb{A}_k^n$ is algebraic if $X = V(A)$ for some $A \subseteq R$.

Remark (Remark 6.8)**.** Suppose $A \subseteq R$, $X \subseteq \mathbb{A}_k^n$ subsets.

(a) $V(a) = V(RA) = V(Rf_1 + \cdots + Rf_m) = V(\{f_1, \ldots, f_m\} = \cap_{i=1}^m V(f_i)$. (Every algebraic set is a finite intersection of hypersurfaces.)

(b) $A \subseteq I(V(A))$ and $X \subseteq V(I(X))$; furthermore, I and V are order reversing (or inclusion reversing).

(c) $V() = V(I(V(A)))$ and $I(X) = I(V(I(X)))$, like in Galois theory. In particular, for every algebraic set X, we have $V(I(X)) = X$.

Theorem (Theorem 6.9 (Hilbert's Nullstellensatz))**.** Suppose k is an algebraically closed field, $R = k[X_1, \ldots, X_n]$, and I is an ideal. Then $I(V(I)) = \sqrt{I}$.

Remark. Notice this gives us a one-to-one correspondence.

Proof. Let $J = I(V(I))$. By Remark 6.8 (c), we know $V(J) = V(I)$. Notice that $V(I) = V(\sqrt{I})$. This then gives us $I(V(I)) = I(V(\sqrt{I}))$, which contains $\sqrt{I}$, and so we have $\sqrt{I} \subseteq J$. For the converse, recall $V(J) = V(I) \subseteq \mathbb{A}_k^n$. This says a point is in $V(J)$ if and only if it's in $V(I)$. This is equivalent to $J \subseteq (x_1 - a_1, \ldots, x_n - a_n)$ and this means $I \subseteq (x_1 - a_1, \ldots, x_n - a_n)$. This then gives us $\{(x_1 - a_1, \ldots, x_n - a_n) : J \subseteq (x_1 - a_1, \ldots, x_n - a_n)\} = \{(x_1 - a_1, \ldots, x_n - a_n) : I \subseteq (x_1 - a_1, \ldots, x_n - a_n)\}$. Therefore, by Theorem 6.6 (Hilbert's Nullstellensatz (Part 1)), $\{m \in m\text{-Spec}(R) : J \subseteq m\} = \{m \in m\text{Spec}(R) : I \subseteq m\}$. This gives us that the intersections are the same, and so moreover by Theorem 6.7 (Hilbert's Nullstellensatz (Part 2)) we have $\sqrt{I} = \sqrt{J}$ and so $J \subseteq \sqrt{I}$. This then gives us the result. **Q.E.D**

Definition (Affine Coordinate Ring of X)**.** Suppose $X \subseteq \mathbb{A}_k^n$ is an algebraic set. Then $A(x) = \{f : x \to k : f \text{ a polynomial}\} = R/I(X)$. This is called the affine coordinate ring of X.

Definition (Local Ring of X at p)**.** Suppose you had a point $p \in X$, then $p = (a_1, \ldots, a_n)$. Then there is a maximal ideal corresponding to it via $I(p) = (x_1 - a_1, \ldots, x_n - a_n) = m \in m\text{-Spec}(R)$. Hence, $I(x) \subseteq I(p)$. So $\bar{m} = I(p)/I(x) \subseteq I(a)$ is a maximal ideal. Then we can localize $A(x)_{\bar{m}} = \mathcal{O}_p(x)$. This is called the local ring of X at p. The element in $\mathcal{O}_p(x) = \{\frac{f}{g} : f, g \text{ polynomials}, g \notin \bar{m}\} = \{\text{rational functions defined at p}\}$.

Definition (Transcendence Degree of a Field)**.** Suppose k is a field, and R is a domain which is finitely generated as a k-algebra, $K = \text{Quot}(R)$. Then K is a finitely generated field extension of K. Hence, $k \subseteq k(Y_1, \ldots, Y_n) \subseteq K$ with $k \subseteq k(Y_1, \ldots, Y_n)$ purely transcendental, and $k(Y_1, \ldots, Y_n) \subseteq K$ is algebraic, and n does not depend on any choice. Set $\text{trdeg}_R(K) = r$.

Theorem (Theorem 6.10)**.** The Krull dimension $\dim(R) = \text{trdeg}_k(R)$, where R is a domain and a finitely generated k-algebra.

Proof. We omit the proof for now, and will return in Chapter 7. **Q.E.D**

Corollary (Corollary 6.11)**.** Let k be a field. Then $\dim(k[X_1, \ldots, X_n]) = n$.

Proof. Proof omitted. Will return in Chapter 7. Corollary 7.21 **Q.E.D**

Definition (Forster Number of M)**.** Suppose R is any ring, and M is a finitely generated module. We define

$$b(M) = \begin{cases} 0 \text{ if } M = 0 \\ \sup\{\mu_{R_p}(M_p) + \dim(R/p) : p \in \text{Supp}_R(M)\} \text{ if } M \neq 0 \end{cases}.$$

We call this number the Forster number of M.

Definition (Basic)**.** Suppose R is any ring, M a finite R-module, $p \in \text{Supp}_R(M)$, $x \in M$. The following are equivalent.

(i.) x is basic at p.

(ii.) $\mu_{R_p}(M/R_p x) < \mu(M_p)$.

(iii.) $\dim(k(p) \otimes_R M/k(p)(1 \otimes_R \bar{x})) < \dim(k(p) \otimes_R M)$.

(iv.) $\bar{0} \neq x \in k(p) \otimes_R M$.

(v.) x is part of a minimal generating set of M_p.

Lemma (Lemma 6.13)**.** Suppose M is a finite R-module, $\{p_1, \ldots, p_n\}$ a finite subset of $\text{Supp}_R(M)$. Then there exists an $x \in M$ that is basic at $p_1, \ldots, p_n$.

Proof. It follows by induction on n. For the case $n = 1$, $p = p_1 \in \text{Supp}_R(M)$, hence $M_p \neq 0$. By Theorem 2.2 (Nakayama's Lemma), we get $0 \neq M_p/pM_p \cong k(p) \otimes_R M$. So there exists an element $x \in M$ so that $\bar{x} \neq \bar{0} \in k(p) \otimes_R M$. Now assume it holds for $n-1$. After rearranging, we may assume p_n is minimal in $\{p_1, \ldots, p_n\}$. Hence, $p_i \subsetneq p_n$ for all $1 \leqslant i \leqslant n-1$. Since p_n is prime, it follows that $p_1 \cdots p_{n-1} \subsetneq p_n$. So there exists an $x \in p_1 \cdots p_{n-1}$ such that $x \notin p_n$. By induction, there exists an $x' \in M$ that is basic at $p_1, \ldots, p_{n-1}$. If x' is basic at p_n, then we win. Otherwise, notice $\bar{x}' \in k(p_n) \otimes_R M$ such that $\bar{x}' = \bar{0}$. By the case $n = 1$, we know there exists a $y \in M$ with $\bar{y} = 1 \otimes_R y \in k(p_n) \otimes_R M$, where $\bar{y} \neq \bar{0}$. Now take $x = x' + ay \in M$. If $1 \leqslant i \leqslant n-1$, $\bar{x} = 1 \otimes_R x \in k(p_i) \otimes_R M$, then $\bar{x} = \bar{x}' + \bar{a}\bar{y} = \bar{x}' \neq \bar{0}$. If $i = n$, then $\bar{x} = 1 \otimes_R x \in k(p_n) \otimes_R M$ gives $\bar{x}' + \bar{a}\bar{y}$, but remember $\bar{x}' = 0$, so $\bar{x} = \bar{a}\bar{y} \neq \bar{0}$, because $\bar{y} \neq \bar{0}$ and $\bar{a} \neq \bar{0}$ in $k(p_n)$. **Q.E.D**

Example. If M is a finite module over a semilocal ring R, and $\mu_{R_m}(M_m) \leqslant n$ for all $m \in m\text{-Spec}(R)$, then M can be generated by n elements.

Proof. We induct on n. If $N = 0$, this result trivially follows. Otherwise, assume it holds for $n-1$. Since $m\text{-Spec}(R) \cap \text{Supp}_R(M) = \{m_1, \ldots, m_n\}$ is finite. By Lemma 6.13, there exists an $x \in M$ which is basic simultaneously at all of the ideals. So $\mu((M/Rx)_m) \leqslant \mu(M_m) - 1 \leqslant n-1$. Hence, by induction, M/Rx can be generated by $n-1$ elements, hence M can be generated by n elements. **Q.E.D**

Theorem (Theorem 6.14 (Forster's Theorem))**.** Let R be a Noetherian ring, and M a finite R-module. Then M can be generated by $b(M)$ elements.

Proof. Proof omitted. **Q.E.D**

Example (Applications (Determining if a Module is Free))**.** Suppose R is a domain, $K = \text{Quot}(R)$, M a finite module. Then $\text{rank}(M) = \dim(J) \otimes M$. Generally, the rank is a lower bound for $\mu(M)$. If equality holds, then the module is free.

Corollary (Corollary 6.15)**.** Suppose R is a Noetherian domain of dimension d, M a finite projective module of rank Γ. Then M can be generated by $d + r$ elements.

Proof. For all $p \in \text{Supp}_R(M)$, we know that if we localize M_p then we get a projective module (since M is projective, and localizing preserves projectiveness). Hence M_p is a free R_p module by Theorem 2.15, since R_p is local. This means $M_p \cong R_p^s$. So $K \otimes M_p \cong K^s$. On the left hand side, we can rewrite this as $K \otimes_{R_p} (R_p \otimes_R M) \cong (K \otimes_{R_p} R_p) \otimes_R M \cong K \otimes_R M \cong K^r$. Hence, we have $K^r \cong_{\bar{K}} K^s$, so this tells us that $s = r$. So $\mu(M_p) = r = \text{rank}(M)$. Hence $b(M) \leqslant r + d$. By Theorem 6.14 (Forster's Theorem), we get the result. **Q.E.D**

Corollary (Corollary 6.16)**.** Suppose R is a Noetherian ring, and $I \subsetneq R$ an ideal. Then $n = \sup\{\mu_{R_p}(I_P) + \dim(R_p) : p \in V(I)\}$, and let $d = \dim(R)$. Then I can be generated by $\max\{n, d+1\}$ elements.

Proof. If $p \in \text{Spec}(R) \backslash V(I)$, then $\mu_{R_p}(I_p) = \mu_{R_p}(R_p) = 1$. Therefore, $V(I) \leqslant \max\{n, d+1\}$. **Q.E.D**

Corollary (Corollary 6.17)**.** In a Dedekind domain, every ideal can be generated by at most 2 elements.

Proof. Follows from Corollary 6.16, since $n \leqslant 1$ and $d \leqslant 1$. **Q.E.D**

Chapter 7: Integral Extensions

Definition (Integral)**.** Let $R \subseteq S$ be an extension of fields, $x \in S$. We say x is integral over R if there exists a monic polynomial expression with coefficients in R so that if you evaluate this polynomial at x, you get 0.

Proposition (Proposition 7.1)**.** Suppose $R \subseteq S$, and $x \in S$, then the following are equivalent.

(a) We have that x is integral over R.

(b) $R[x]$ is a finitely generated R-module.

(c) $R[x] \subseteq T \subseteq S$, T a ring and a finite R-module.

(d) There exists a $R[x]$-module M which is faithful as an $R[x]$-module, and is finite as an R-module.

Proof. We show that (a) implies (b). It follows since $x^n + a_{n-1}x^{n-1} + \cdots + a_n = 0$, for some $a_i \in R$. So $r[x] = R + Rx + Rx^2 + \cdots + Rx^{n-1}$.

Notice that (b) implies (c) is clear, since we can just take $T = R[x]$.

For (c) implies (d), we can just take $M = T$.

Finally, we show (d) implies (a). WE have that $M = Ra_1 + \cdots + Ra_n$ and $xM \subseteq M$. So there exists an $n \times n$ matrix A with coefficients in R such that $\begin{pmatrix} xa_1 \\ \vdots \\ xa_n \end{pmatrix} = A \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$. So $(x1_{n\times n} - A) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Hence, by Lemma 2.1, we know that $\det(x1_{n\times n} - A) - a_i = 0$ for all i. So therefore $\det(x1_{n\times n} - A) \in \mathrm{Ann}_{R[x]}(M) = 0$. So we get that $\det(x1_{n\times n} - A) = 0$ in $R[x]$. Expanding this gives us a monic polynomial expression in x with coefficients in R. **Q.E.D**

Definition (Integral Closure)**.** Suppose we have an extension of rings $R \subseteq S$. Then we denote by $\bar{R} = \bar{R}^S = \{x \in S : \exists f \in R[x], f(x) = 0\}$ the integral closure of a ring R.

Corollary (Corollary 7.2)**.** $\bar{R}$ is a subring of S containing R.

Proof. Let $x, y \in \bar{R}$. If we show $R[x, y] \subseteq \bar{R}$, then we're done. By Proposition 7.1, we know that $R[x]$ is a finite R-module, and we also know that $R[x][y] = R[x, y]$ is a finite $R[x]$ module. So clearly $R[x, y]$ is a finite R module, since both steps are finite. By Proposition 7.1, we get $R[x, y] \subseteq \bar{R}$. **Q.E.D**

Definition (Integrally Closed)**.** Suppose $R \subseteq S$ is an extension of rings. We say R is integrally closed if $R = \bar{R}$.

Proposition (Proposition 7.3)**.** Suppose $R \subseteq S \subseteq T$ are rings, where T is integral over S and S is integral over R. Then T is integral over R.

Proof. Proof omitted. It is an easy result to derive. **Q.E.D**

Corollary (Corollary 7.4)**.** The integral closure is integrally closed.

Proof. Proof omitted. It is an easy result to derive. **Q.E.D**

Proposition (Proposition 7.5)**.** Suppose $R \subseteq S$ are rings, $W \subseteq R$ is a mutliplicatively closed subset, then in $W^{-1}S$, $W^{-1}(\bar{R}) = \bar{W^{-1}R}$.

Proof. For the inclusion, we need to show that $x \in \bar{R}$ localized is in $\bar{W^{-1}R}$. We have $x^n + a_1X^{n_1} + \cdots + a_n = 0$ for some $a_i \in R$. Let $w \in W$. Divide our equation by w^n. This gives us $(x/w)^n + a_1/w(x/w)^{n-1} + \cdots + a_n/w^n = 0$. This is our equation, and so we get that (x/w) is integral, and so it's in the right hand side. For the other relation, we have an element in $\bar{W^{-1}R}$. Take $x \in S$, and $w \in W$ so that $x/w \in \bar{W^{-1}R}$. This means $(x/w)^n + a_1/w(x/w)^{n-1} + \cdots + a_n/w^n = 0$. Let $v = w^n \prod_{i=1}^n w_i s$. Then we get $vx^n + v_1x^{n-1} + \cdots + v_n$, $v \in W$. Multiply by v^{n-1} to get a monic polynomial which satisfies our conditions, and so we get the other inclusion. Hence, we have equality. **Q.E.D**

Corollary (Corollary 7.6)**.** R is an integrally closed ring in S and $R \subseteq S$ if and only if it is so locally.

Proof. $R = \bar{R}$ if and only if $\bar{R}/R = 0$. But $\bar{R}/R = 0$ if and only if $(\bar{R}/R)_m = 0$ for all $m \in m\text{-Spec}(R)$. This was by Theorem 4.9 (Local to Global Principle). This is the same as $\bar{R}_m/R_m = 0$ for all $m \in m\text{-Spec}(R)$. This is the same as $(R\backslash m)^{-1}\bar{R}/R_m = 0$, and by Proposition 7.5 this is the same as $\bar{R}_m/R_m = 0$. **Q.E.D**

Definition (Normal Domain)**.** R is a normal domain if it is a domain and R is integrally closed in it's own quotient field.

Definition (Normal Ring)**.** Let R be a ring. The following are equivalent.

(a) R is a normal ring.

(b) R_m is a normal domain for all $m \in m\text{-Spec}(R)$.

(c) R_p is a normal domain for all $p \in \text{Spec}(R)$.

Proposition (Proposition 7.7)**.** Every UFD is a normal domain.

Proof. Let R be a UFD, $k = \text{Quot}(R)$. Take $x \in \bar{R}$. This means that $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, $a_i \in R$. We can write $x = a/b$, $a, b \in R$, $b \neq 0$, $\gcd(a, b) \sim 1$. Then multiply the above equation by b^n, and you see b/a^n but $\gcd(b, a^n) \sim 1$. But if b/a^n exists then $\gcd(b, a^n) \sim b$, which implies that b is a unit and we get $x \in R$. **Q.E.D**

Theorem. Let R be a normal domain, $K = \text{Quot}(R)$, $K \subseteq L$ an algebraic field extension, $\alpha \in L$. Then $(R\backslash 0)^{-1}\bar{R} = L$. In particular, $\text{Quot}(\bar{R}) = L$. Furthermore, $\alpha \in \bar{R}$ if and only if the minimal polynomial of α over K has all of its coefficients in R.

Proof. By Proposition 7.5, $(R\backslash 0)^{-1}\bar{R} = \overline{(R\backslash 0)R} = \bar{K} = L$. For the if and only if statement, notice that the converse is trivial. For the implication, we have that if $\alpha \in \bar{R}$ then the coefficients of the minimal polynomial are in R, denoted by $f(x) \in R[x]$. Replace L by the splitting field of f over L. Then $f = \prod_{i=1}^n (x - \alpha_i)$, where $\alpha_i \in L$, $\alpha_1 = \alpha$. Replace L by $K(\alpha_1, \ldots, \alpha_n)$. Then $K \subseteq L$ is finite and normal. Therefore, all of the α_i are conjugates, since f is irreducible. Now notice that α is integral over R by assumption, hence $\delta_i(\alpha)$ is integral over R, $\delta_i \in \text{Aut}_K(L)$, and hence all of the α_i are integral over R. But $f = \prod_{i=1}^n (x - \alpha_i) \in \bar{R}[x] \in (\bar{R} \cap K)[x] = (\bar{R})[x] = R[x]$, since R is normal. **Q.E.D**

Proposition (Proposition 7.9)**.** Let R be a UFD with $2 \in R^\times$, and suppose $a \in R$ is square free, $K = \text{Quot}(R)$, $K \subsetneq L = K(\sqrt{a})$ is a quadratic extension, and we examine $\bar{R}$. Then $\bar{R} = R[\sqrt{a}]$. Furthermore, $\bar{R} \cong R[x]/(x^2 - a)$ is a normal domain.

Proof. Proof omitted. **Q.E.D**

Proposition (Proposition 7.10)**.** Suppose $R \subseteq S$ domains, and suppose S is integral over R. Then R is a field if and only if S is a field.

Proof. Proof omitted. **Q.E.D**

Corollary (Corollary 7.11)**.** Suppose $R \subseteq S$ rings so that S is integral over R. Let $q \in S$ be a prime ideal, and let $p = q \cap R$. Then p is a maximal ideal of R if and only if q is a maximal ideal of S.

Proof. Notice that the extension of domains $R/p \hookrightarrow S/q$ is integral, and then apply Proposition 7.10. **Q.E.D**

Definition (Lying Over)**.** Suppose we have $\varphi : R \to S$ a homomorphism of rings, then we have an induced map $\varphi^* : \text{Spec}(S) \to \text{Spec}(R)$. We say that φ satisfies lying over if, for all $p \in \text{Spec}(R)$, there exists a $q \in \text{Spec}(S)$ with $p = q^c$.

Definition (Going Up)**.** Suppose we have $\varphi : R \to S$ a homomorphism of rings, then we have an induced map $\varphi^* : \text{Spec}(S) \to \text{Spec}(R)$. We say that φ satisfies going up if, for every chain of prime ideals in R, $p_0 \subseteq p_1 \subseteq \cdots \subseteq p_n$, and every $q_0 \in \text{Spec}(S)$, $q_0^c = p_0$. There also exists a chain of prime ideals $q_0 q_1 \subseteq \cdots \subseteq q_n$ such that $q_i^c = p_i$ for all i.

Definition (Going Down)**.** Suppose we have $\varphi : R \to S$ a homomorphism of rings, then we have an induced map $\varphi^* : \text{Spec}(S) \to \text{Spec}(R)$. We say that φ satisfies going down if for every chain of prime ideals $p_n \subseteq \cdots \subseteq p_0$ in R and every $q_0 \in \text{Spec}(S)$ lying over o_0, there exists a chain of prime ideals $q_n \cdots \subseteq q_0$ in S so that $q_i^c = p_i$ for all i.

Theorem (Theorem 7.12)**.** Let $R \subseteq S$ be an integral extension of rings. Then we have the following.

(a) $R \subseteq S$ satisfies lying over.

(b) If $q_0 \subseteq q_1$ are in $\text{Spec}(S)$ and $q_0^c = q_1^c$, then $q_0 = q_1$.

(c) $R \subseteq S$ satisfies going up.

Proof. Proof omitted. **Q.E.D**

Corollary (Corollary 7.13)**.** Suppose $R \subseteq S$ is an integral extension of rings. Then $\dim(R) = \dim(S)$.

Proof. This readily follows from Theorem 7.12. **Q.E.D**

Lemma (Lemma 7.14)**.** Suppose $\varphi : R \to S$ is a homomorphism of rings, $p \in \text{Spec}(R)$. Then there exists a $q \in \text{Spec}(S)$ with $q^c = p$ if and only if $p^{ec} = p$.

Proof. Proof omitted. **Q.E.D**

Lemma (Lemma 7.15)**.** Suppose $R \subseteq S$ is an integral extension of domains, where R is normal, let $K = \text{Quot}(R)$, let $p \in R$, $\alpha \in p^e = pS$, and let $f(x)$ be the minimal polynomial of α over K. Then all coefficients of f, except for the leading coefficients, are in p.

Proof. Proof omitted. **Q.E.D**

Theorem (Theorem 7.16)**.** Suppose $R \subseteq S$ is an integral extension of domains, where R is normal. Then going down holds.

Proof. Proof omitted. **Q.E.D**

Theorem (Theorem 7.17)**.** Suppose R is a normal domain, $K = \text{Quot}(R)$, $K \subseteq L$ is a finite separable field extension, and $S \subseteq L$ a subring so that S is integral over R. Then there exists a K-basis of L so that $S \subseteq Rx_1 \oplus \cdots \oplus Rx_n$. In particular, if R is Noetherian, then S is finitely generated as an R-module. Thus, S is a Noetherian ring.

Proof. Proof omitted. **Q.E.D**

Theorem (Theorem 7.18 (Noether Normalization))**.** Let k be a field, and R a finitely generated K-algebra, $I_1 \subseteq \cdots \subseteq I_n \subsetneq R$ a finite chain of R ideals, then there exists a polynomial ring $k[y_1, \ldots, y_d] \subseteq R$ o that R is integral over $k[y_1, \ldots, y_d]$ and $I_j \cap k[y_1, \ldots, y_d] = k(y_1, \ldots, y_{h_{(j)}})$.

Proof. Proof omitted. **Q.E.D**

Corollary (Corollary 7.19)**.** We have that $\dim(k[X_1, \ldots, X_d]) = d$.

Proof. Proof omitted. **Q.E.D**

Corollary (Corollary 7.20)**.** If R is a domain (Theorem 7.18 (Noether Normalization)), then $h(j)$ is simply the height of the ideal I. Furthermore, $\dim(R) = \text{ht}(I_i) + \dim(R/I_j)$.

Proof. Proof omitted. **Q.E.D**

Corollary (Corollary 7.21)**.** Let k be a field, and R a finitely generated k-algebra. Then R is integral over the polynomial ring in d variables, where d is the Krull dimension of R. If R is a domain, then $\dim(R) = \text{trdeg}_k(R)$.

Proof. This follows readily from Theorem 7.18 (Noether Normalization), Corollary 7.13, and Corollary 7.19 **Q.E.D**

Corollary (Corollary 7.22)**.** Let k be a field and let R be a finitely generated k-algebra. Then the following are equivalent.

(a) If R is a domain and I is an R-ideal, then $\text{ht}(I) + \dim(R/I) = \dim(R)$.

(b) R is catenary.

Proof. Proof omitted. **Q.E.D**

Chapter 8: DVR and Dedekind Domains

Definition (Discrete Valuation)**.** Let K be a field. A discrete valuation on K is a surjective map $v : K^\times \twoheadrightarrow \mathbb{Z}$ with the following.

(i) We have $v(xy) = v(x) + v(y)$.

(ii) We have$v(x + y) \geqslant \min\{v(x), v(y)\}$.

Remark. Sometimes, one extends v to $v : K \to \mathbb{Z} \cup \{\infty\}$ by $v(0) = \infty$.

Remark. Given a discrete valuation v on l, one obtains an absolute value on k by $|\cdot| : k \to \mathbb{R}_{\geqslant 0}$ by $|x| = e^{-v(x)}$. This is an absolute value since

(i) $|xy| = e^{-v(xy)} = e^{-v(x)-v(y)} = e^{-v(x)}e^{-v(y)} = |x||y|$.

(ii) $|x + y| = e^{-v(x+y)} \leqslant \max\{e^{-v(x)}, e^{-v(y)}\} = \max\{|x|, |y|\}$.

This also gives you the triangle inequality. Notice $|x| = 0$ if and only if $x = 0$. If you replace e with p, you get the p-adic absolute value.

Definition. We define $R_v := \{x \in K : v(x) \geqslant 0\}$, $m_v := \{x \in K : v(x) > 0\}$, and $U_v = \{x \in K : v(x) = 0\}$.

Remark (Remark 8.2)**.** (a) R_v is a local domain with max ideal m_v and $R_v^\times = U_v$.

(b) Let x and y be elements in R_v. Then $x|y$ if and only if $v(x) \leqslant v(y)$; $x \sim y$ if and only if $v(x) = v(y)$. Either $x|y$ or $y|x$.
Note also that the group of units in the ring is the set of elements with $v(x) = 1$.

Definition (Uniformizing Parameter)**.** Notice that there exists a $\pi \in K$ such that $v(\pi) = 1$. This π is called the uniformizing parameter of R_v. This value is unique up to units.

Remark (Remark 8.3)**.** Every $x \in K^\times$ can be written uniquely as $x = u\pi^n$, where $u \in U_v$ and $n \in \mathbb{Z}_¿$ Depends on the choice of π, but once we know π exists then this representation is unique. In particular, this shows $K = \text{Quot}(R_v) = R_v[\frac{1}{\pi}]$.

Remark. Notice that R_v is a Euclidean domain.

Definition (DVR)**.** Suppose R is any ring. Then we say R is a DVR if R is R_v for some discrete valuation v on the field K. One can define valuation rings more generally by changing $\mathbb{Z}$ to any totally ordered abelian group.

Lemma (Lemma 8.4)**.** Suppose R is a Noetherian ring, $x \in \text{Rad}(R)$. Then $\cap_{n\in\mathbb{N}}(x^n) = 0$.

Proof. Let $y \in \cap_{n\in\mathbb{N}}(x^n)$. Now $(y) : (x^n)$ is a non-decreasing chain of ideals by the Noetherian property, the chain must stabilize. In particular, there exists $i > 0$ with $(y) : (x^{i-1}) = (y) : (x^i)$. Now $y \in \cap_{n\in\mathbb{N}}(x^n) \subseteq (x^i)$ so that $y = \lambda x^i = \lambda x x^{i-1}$. Notice $\lambda \in (y) : (x^i) = (y) : (x^{i-1})$. Hence $\lambda x^{i-1} \in (y)$, hence $\lambda x^{i-1} = \mu y$. So $y = \mu y x$, hence $(1 - \mu x)y = 0$. Hence $y = 0$, since $x \in \text{Rad}(()R)$ and so $1 - \mu x \in R^\times$. **Q.E.D**

Theorem (Theorem 8.5)**.** The following are equivalent for a ring R.

(i) R is a DVR.

(ii) R is a local PID which is not a field.

(iii) R is a Noetherian local ring with principal max ideal and $\dim(R) > 0$.

(iv) R is a Noetherian local normal ring with $\dim(R) = 1$.

Proof. We show (i) implies (ii). Every DVR is Euclidean, so it follows. Notice that (ii) implies (iii) is trivial, along with (ii) implies (iv). Remember that PID implies UFD implies Normal.

We show that (iii) implies (i). Let m be the maximal ideal. By assumption, m is principal, and so $m = (x)$. We first show that, for every nonzero $y \in m$, $y \sim x^n$ for some $n > 0$. By Lemma 8.4, we know there exists a maximal ideal $n \in \mathbb{N}_{>0}$ with $y \in (x^n)$. Thus $y = x^n$ for some u. If $u \in m = (x)$, then $y \in (x^{n+1})$, contradicting maximality of n. Thus, $U \in R - m = R^\times$. Therefore, $y \sim x^n$. We now show R is a domain. Take $y, x \in R$, so that they're non-zero. By what we've just shown $y \sim x^n$, $z \sim x^l$ for somen, l. Thus $yz \sim x^{n+l} \neq 0$, since otherwise $m = (x) \subseteq \sqrt{0}$, hence $\dim(R) = 0$. But since (iii) assumes $\dim(R) > 0$, this is a contradiction. Hence, R is a domain, $x \neq 0$, $x \nsim 1$. Let $K = \text{Quot}(R)$. Now every $0 \neq y \in K$ can be written uniquely as $y = ux^n, u \in R^\times, n \in \mathbb{Z}$. Set $v(y) = n$. Then $v : K^\times \to \mathbb{Z}$ is a discrete valuation on K with $R_v = R$.

We now show that (iv) implies (iii). Essentially, we just need to show the maximal ideal is principal. First, notice R is a domain, since R is normal and local. Let M be the maximal ideal of R. We show M is principal. Since R is Noetherian, and $m \neq 0$, $m \neq m^2$ by Theorem 2.2 (Nakayama's Lemma). Let $x \in m \backslash m^2$. We will show $m = (x)$. Write $m^{-1} = R : m = \{z \in K : mz \subseteq R\}$, and $K = \text{Quot}(R)$. Now notice $R \subseteq m^{-1}$. Multiplying both sides by m gives us $m \subseteq mm^{-1} \subseteq R$. Hence $mm^{-1} = m$. So let $a \in m^{-1}$, then $am \subseteq m^{-1}m = m$. Hence $a^n m \subseteq m$ for all n. Hence, m is an $R[a]$-module, and m is finite as an R-module. Hence, a is integral over R (Proposition 7.1). But now R is normal, so $a \in R$, and therefore $m^{-1} \subseteq R$. Thus, $m^{-1} = R$ Now, $R = m^{-1} = R : m$. Multiplying both sides by x gives us $xR \subseteq xR : m \subseteq x(R : m) = xR : m = xR$. Thus, $xR : m = xR$. Hence, m is not an associated prime of (R/xR). But this is impossible, since m is an associated prime of R/xR, because R is a 1-dimensional Noetherian local ring (so $\text{Spec}(R) = \{0, m\}$) but $x \neq 0$. It must have one associated prime. Therefore, $mm^{-1} = R$. So now xm^{-1} is an R ideal. Suppose $xm^{-1} \subseteq m$. Then $x \in xR = xm^{-1}m \subseteq m^2$. This contradicts our choice of x (recall $x \notin m^2$). Thus $xm^{-1} = R$. Hence, $xR = xm^{-1}m = Rm = m$. **Q.E.D**

Definition (Fractional Ideal)**.** Let R be a domain, $K = \text{Quot}(R)$. I is a fractional ideal of R if I is an R submodule of K, $I \neq 0$, and $\exists x \in R \backslash 0$, such that $xI \subseteq R$.

Assume I is a fractional ideal. We define $I^{-1} = \{x \in K : xI \subseteq R\} = R : I$ is again a fractional ideal. Notice $I \subseteq (I^{-1})^{-1}$ and II^{-1} is an R-ideal.

Definition (Invertible Ideal)**.** We say that I is invertible if $II^{-1} = R$.

Theorem (Theorem 8.6)**.** Let R be a domain, and I a fractional ideal of R. Then the following are equivalent.

(a) I is invertible.

(b) I is projective (as an R-module).

(c) I is finitely generated with I_m principle for all $m \in m\text{-Spec}(R)$.

Proof. We show (a) implies (b). We have $II^{-1} = R$, so $\sum_{i=1}^n a_i b_i = 1$ for some $a_i \in I$, $b_i \in I^{-1}$. Now $\varphi : R^n \to I$ with $\varphi(r_1, \ldots, r_n) = \sum_{i=1}^n r_i a_i \in I$. This map is R-linear, and we define $\psi : I \to R^n$ with $\psi(t) = (tb_1, \ldots, tb_n) \in R^n$ is also R-linear. Furthermore, $9\varphi \circ \psi)(t) = (\sum_{i=1}^n a_i b_i)t = t$. So by $(\varphi \circ \psi) = \mathrm{id}_I$. Thus I is a direct summand of R^n. This is equivalent to being projective.

We show (b) implies (c). We first show I is finitely generated. Let $F = \oplus_{i \in I} Re_i$ be a free module. We have $\varphi : F \to I$ and $\psi : I \to F$ with $\varphi \circ \psi = \mathrm{Id}_I$. Let $K = \mathrm{Quot}(R)$. Now $\psi \otimes K : I \otimes K \cong IK = K \to F \otimes K = \oplus_{i \in I} Ke_i$. Since $I \otimes K$ is a finite K-module, we have $\mathrm{im}(\psi \otimes K) \subseteq Ke_{i_1} \oplus \cdots \oplus Ke_{i_n}$. Hence $\mathrm{im}(\psi) \subseteq \oplus_{i \in I} Re_i \cap (Ke_{i_1} \oplus \cdots \oplus Ke_{i_n}) = Re_{i_1} \oplus \cdots \oplus Re_{i_n} = 0$. Hence $\varphi|_G \circ \psi = \mathrm{id}_I$, so $\varphi|_G$ is surjective. So G is surjective onto I, G is finitely generated, hence I is finitely generated. Now I_m is a finite projective module over the local ring R_m, and so I_m is R_m-free (Theorem 2.15).

We finally show (c) implies (a). Since I is finitely generated, $I_m^{-1} = (R : I)_m = R_m : I_m = (I_m)^{-1}$. So inverting commutes with localization. So $0 \neq I_m$ is principle, hence invertible, hence $R_m = I_m \cdot I_m^{-1} = I_m (I^{-1})_m = (II^{-1})_m$ for all $m \in m\text{-Spec}(R)$. Hence $II^{-1} = R$ by the local-to-global principle. **Q.E.D**

Theorem (Theorem 8.7)**.** Let R be a Noetherian domain, p a nonzero prime ideal. If p is invertible, then $\mathrm{ht}(p) = 1$ and R_p is a DVR.

Proof. By Theorem 8.6, pR_p is a principal ideal. Also R_p is Noetherian, local, and $\dim(R_p) > 0$, with principal maximal ideal, pR_p. So R_p is a DVR (Theorem 8.5), hence $\dim(R_p) = 1$, i.e. $\mathrm{ht}(p) = 1$. **Q.E.D**

Theorem (Theorem 8.8)**.** Let R be a Noetherian normal domain. Then

(a) $0 \neq x \notin R^\times$, $p \in \mathrm{Ass}_R(R/(x))$ then $\mathrm{ht}(p) = 1$.

(b) $R = \cap_{\mathrm{ht}(p)=1} R_p$, and furthermore the R_p are DVR's.

Proof. We show (a). Localizing at p, we may assume R is a normal, Noetherian, local domain (Corollary 7.6) with maximal ideal m. We may now assume $m \in \mathrm{Ass}_R(R/(x))$, $0 \neq x \in R^\times$. Notice R is now R_p. We need to show that $\dim(R) = 1$. To do so, we show that m is invertible (we are then done by the previous theorem). Now $m \subseteq mm^{-1}$. By definition, $mm^{-1} \subseteq R$. If m is not invertible, $m = mm^{-1}$, since M is maximal. If we have such an equation, every element in m^{-1} is integral. As in the proof of Theorem 8.5, this tells us that $m^{-1} = R$. Now $(Rx :_R m) \subseteq (Rx :_K m) = x(R :_K m) = xm^{-1} = (x)$. So $(Rx :_R m) = (x)$. So m cannot be an associated prime. This gives us a contradiction.

We show (b). We have $R \subseteq \cap_{\mathrm{ht}(p)=1} R_p$ trivially. Take $\frac{y}{x} \in R_p$ for every $p \in \mathrm{Spec}(R)$ with $\mathrm{ht}(p) = 1$. This means that $y \in xR_p$ if and only if $(yR)_p \subseteq (xR)_p$ for all $p \in \mathrm{Spec}(R)$ with $\mathrm{ht}(p) = 1$. By (a), we get that all $p \in \mathrm{Ass}_R(R/Rx)$. Then it follows $yR \subseteq xR$ by Homework 6.3. Then $\frac{y}{x} \in R$. Finally, R_p is a DVR for any such p by Theorem 8.5. **Q.E.D**

Corollary (Corollary 8.9)**.** Suppose R is a Noetherian domain. Then the following are equivalent.

(i) R is normal.

(ii) (a) (Serre's Condition on R_1) R_p is a DVR for all $p \in \mathrm{Spec}(R)$, $\mathrm{ht}(p) = 1$.

(b) (Serre's Condition S_2) For every $0 \neq x \notin R^\times$, $\mathrm{ht}(p) = 1$ for all $p \in \mathrm{Ass}_R(R/xR)$.

Proof. (i) implies (ii) follows from Theorem 8.8. We show (ii) implies (i). By the proof of Theorem 8.8, $R = \cap_{\mathrm{ht}(p)=1} R_p$, by (b). By condition (a), R_p is a DVR, and hence it's normal. Therefore, R must be normal, since it's an intersection of normal domains. **Q.E.D**

Definition (Dedekind Domain)**.** R is a Dedekind domain if R is a Noetherian domain, not a field, and R_p is a DVR for all $p \in \mathrm{Spec}(R)$.

Theorem (Theorem 8.10)**.** Let R be a domain, not a field. Then the following are equivalent.

(i) R is a Dedekind domain.

(ii) R is Noetherian and locally a DVR.

(iii) R is Noetherian, normal, and $\dim(R) = 1$.

(iv) Every ideal is invertible, so long as it's not 0.

(v) Every ideal is projective.

(vi) R is Noetherian, and every ideal not equal to R is the product of prime ideals.

Proof. Proof omitted. **Q.E.D**

Remark (Remark 8.11)**.** Let R be a Dedekind domain. Then the prime factorization in Theorem 8.10 (vi) is unique (up to order of the factors).

Proof. Suppose $0 \neq I \neq R$, and $I = p_1^{e_1} \cdots p_n^{e_n}$, p_i prime, and actually piecewise maximal, and $e_i > 0$. Now $I_{p_i} = p_i^{e_i} R_{p_i} = (p_i R_{p_i})^{e_i}$. Notice that e_i is uniquely determined, so it determines it in the extension as well. **Q.E.D**

Theorem (Theorem 8.12)**.** Suppose R is a Noetherian domain, $\dim(R) = 1$, $K = \mathrm{Quot}(R)$, $K \subseteq L$ finite field extensions (not necessarily separable). Then $\bar{R}$ is a Dedekind domain.

Proof. Proof omitted. **Q.E.D**

Theorem (Theorem 8.13 (Krull - Akizuki))**.** Let R be a Noetherian domain, $K = \mathrm{Quot}(R)$, $\dim(R) = 1$, $K \subseteq L$ a finite field extension, S is any ring $R \subseteq S \subseteq L$. Then

(i) S is a Noetherian ring.

(ii) $\dim(S) \leqslant 1$.

(iii) $l_R(S/J) < \infty$ for all ideals $J \neq 0$ in S.

Proof. Proof omitted. **Q.E.D**

Lemma (Lemma 8.14)**.** R is a Noetherian domain, $\dim(R) = 1$, M a torsion free R-module of finite rank, suppose we have $0 \neq a \in R$. Then $l_R(M/aM) \leqslant \mathrm{rank}(M) \cdot l_R(R/aR) < \infty$.

Proof. Proof omitted. **Q.E.D**

Index

$\mu(M)$, 15
$l_R(M)$, 32

Abelian Group, 3
Affine Coordinate Ring of X, 49
Algebra, 20
Annihilator, 13
Artinian Module, 28
Ascending Chain Condition, 28
Associated Prime, 42

Basic, 50
Bimodules, 18
Binary Operation, 3

Catenary, 47
Chinese Remainder Theorem, 11
Cokernel, 21
Comaximal, 10
Comaximality Property, 10
Commutative Group, 3
Complex Sequence, 21
Composition Series, 31
Contraction of an Ideal, 38
Contravariant Functor, 41

Dedekind Domain, 59
Descending Chain Condition, 28
Dimension of a Prime, 47
Discrete Valuation, 56
DVR, 56

Eakin's Theorem, 34
Epimorphism, 4
Equivalence Relation, 4
Exact Sequence, 21
Extension of an Ideal, 38

Factor Ring, 5
Faithful Module, 13
Finitely Generated Modules, 14
Flat Module, 25
Fractional Ideal, 57
Free Modules, 14
Fundamental Theorem on Homomorphisms, 4

Going Down, 54
Going Up, 54

Height of a Prime, 47
Height of an Ideal, 47
Hilbert's Basis Theorem, 33
Hilbert's Nullstellensatz, 49
Hilbert's Nullstellensatz (Part 1), 48
Hilbert's Nullstellensatz (Part 2)), 48
Hom, 22
Homomorphism, 5
Homomorphism of Modules, 13

Ideal, 5
Ideal Quotient, 13
Injective Module, 25
Integral, 52
Integral Closure, 52
Integral Domain, 6
Integrally Closed, 52
Inverse of a Module, 36
Invertible Ideal, 57
Irreducible Submodule, 44

Jacobson Radical, 10

Krull Dimension, 47
Krull-Akizuki, 59

Length of Composition Series, 32
Local, 7
Local Ring of X at p, 49
Local To Global Principle, 37
localization, 35
Localization at a Prime, 35
Localization at an Element, 35
Lying Over, 54

Magma, 3
Maximal Ideal, 6
Minimal Generating Set, 14
Minimal Number of Generators, 15
Module, 13

Monoid, 3
Monomorphism, 4
Multiplicative Subset, 8

Nakayama's Lemma, 14
Natural Projection, 5
Nilpotent Element, 9
Nilradical, 9
Noether Normalization, 55
Noetherian Module, 28
Noetherian/Artinian Ring, 28
Normal Domain, 53
Normal Ring, 53

Operation on Modules, 13
Operations on Ideals, 8

P-Primary Submodule of M, 44
Power Series Ring, 4
Primary Decomposition, 45
Primary Ideal, 38
Primary Submodule, 44
Prime Avoidance, 12
Prime Ideal, 6
Principal Ideal, 6
Principle Ideal Domain, 6
Product Comaximality, 11
Projective Module, 25

Quotient Field, 35
Quotient Module, 13
Quotient Ring, 35
quotientfield, 35

Radical Ideal, 9
Reduced, 9
Reduced Ring, 10
Reducible Submodule, 44
Residue Field, 7
Ring, 5
Ring of Fractions, 35

Saturated, 40
Saturation, 40
Semigroup, 3
Semilocal, 7
Short Exact Sequence, 21
Snake Lemma, 21
Spectrum of Rings, 39
Split Exact Sequences, 25
Submodule, 13
Subring, 5
Support of a Module, 41

Tensor Product, 16
Total Ring of Quotients, 35
Transcendence Degree of a Field, 50

Uniformizing Parameter, 56
Unit, 6

Zariski Topology, 40
Zero Divisor, 6
Zorn's Lemma, 3