Notes on Commutative Algebra

Eric Liu

Contents

Chapter 1

Definitions

1.1 Definition of Rings

The precise meaning of the term **ring** varies across different books, depending on the context and purpose. In this note, the multiplication of a ring is always associative and commutative, and have an identity. The additive identity is denoted by 0. From the axioms, we can straightforwardly show that $x \cdot 0 = 0$ for all x. Consequently, the multiplicative and additive identities are always distinct unless the ring contained only one element, called **zero** in this case.

An **ideal** of a ring R is an additive subgroup I such that $ar \in I$ for all $a \in I, r \in R$, or equivalently, the kernel of some **ring homomorphism**[1]. To see the equivalency, one simply construct the **quotient ring**[2] R/I, under which the quotient map $\pi : R \to R/I$ is a surjective ring homomorphism whose kernel is the ideal I. Remarkably, the mapping defined by

$$\text{Ideal } J \text{ of } R \text{ that contains } I \mapsto \{[x] \in R/I : x \in J\}$$

forms a bijection between the collection of the ideals of R containing I and the collection of the ideals of R/I. This fact is commonly referred to as the **correspondence theorem** for rings.

A **unit** is an element that has a multiplicative inverse. Under our initial requirement that rings are commutative, for a non-zero ring R to be a **field**, we only need all non-zero elements of R to be units, or equivalently, the only ideals of R to be $\{0\}$ or R itself.

[1] Ring homomorphisms are mapping between two rings that respects addition, multiplication and multiplicative identity.

[2] Consider the equivalence relation on R defined by $x \sim y \overset{\triangle}{\iff} x - y \in I$

We use the term **proper** to describe strict set inclusion. By a **maximal ideal**, we mean a proper ideal I contained by no other proper ideals, or equivalently[3], a proper ideal I such that R/I is a field.

A **zero-divisor** is an element x that has some non-zero element y such that $xy = 0$. Again, under our initial requirement that rings are commutative, for a non-zero ring R to be an **integral domain**, we only need all non-zero elements to be zero-divisors. By a **prime ideal**, we mean a proper ideal I such that the product of two elements belongs to I only if one of them belong to I, or equivalently, a proper ideal I such that R/I is an integral domain.

There are many binary operations defined for ideals. Given two ideals I and S, we define their **sum** $I + S$ to be the set of all $x + y$ where $x \in I$ and $y \in S$, and define their **product** IS to be the set of all finite sums $\sum x_i y_i$ where $x_i \in I$ and $y_i \in S$. Note that the ideal multiplications are indeed distributive over addition, and they are both associative, so it make sense to write something like $I_1 + I_2 + I_3$ or $I_1 I_2 I_3$. Obviously, the intersection of ideals is still ideal, while the union of ideals generally are not. Moreover, we define their **quotient** $(I : S)$ to be the set of elements x of R such that $xy \in I$ for all $y \in S$. To simplify matters, we write $(I : x)$ instead of $(I : \langle x \rangle)$.

For all subsets S of some ring R, we may **generate** an ideal by setting it to be the set of all finite sum $\sum rs$ such that $r \in R$ and $s \in S$, or equivalently, the smallest ideal of R containing S. An ideal is called **principal** and denoted by $\langle x \rangle$ if it can be generated by a single element x.

An element x is called **nilpotent** if $x^n = 0$ for some $n \in \mathbb{N}$. The set of all nilpotent elements obviously form an ideal, which we call **nilradical** and denote by $\mathrm{Nil}(R)$. Here, we give a nice description of the nilradical.

Theorem 1.1.1. (Equivalent Definition for Nilradical) We use the term **spectrum** of R and the notation $\mathrm{spec}(R)$ to denote the set of prime ideals of R. We have

$$\mathrm{Nil}(R) = \bigcap \mathrm{spec}(R)$$

Proof. $\mathrm{Nil}(R) \subseteq \bigcap \mathrm{Spec}(R)$ is obvious. Suppose $x \in \bigcap \mathrm{Spec}(R) \setminus \mathrm{Nil}(R)$. Let Σ be the set of ideals I such that $x^n \notin I$ for all $n > 0$. Because unions of chains in Σ belong to Σ and $0 \in \Sigma$, by Zorn's Lemma, there exists some maximal element $I \in \Sigma$. Because $x \notin I$, to close out the proof, we only have to show I is prime.

[3]By the Correspondence Theorem for Rings.

Let $yz \in I$. Assume for a contradiction that $y \notin I$ and $z \notin I$. By maximality of I, both ideal $I+\langle y\rangle$ and ideal $I+\langle z\rangle$ do not belong to Σ. This implies $x^n \in I+\langle y\rangle$ and $x^m \in I+\langle z\rangle$ for some $n, m > 0$, which cause a contradiction to $I \in \Sigma$, since $x^{n+m} \in I + \langle yz\rangle = I$. ■

Let I be an ideal of the ring R. By the term **radical** of I, we mean $\sqrt{I} \triangleq \{x \in R : x^n \in I \text{ for some } n > 0\}$, which is equivalent to the preimage of $\mathrm{Nil}(R/I)$ under the quotient map and equivalent[4] to the intersection of all prime ideals of R that contain I.

It should be noted that there is a "less is more" philosophy in our wording and notations for product, quotient and radical of ideals. For any ideal I, Q, we have

$$IQ \subseteq I \subseteq \sqrt{I} \text{ and } I \subseteq (I : Q)$$

For ease in the section on fraction of rings and modules, we close this section by introducing two concept. Let $f : A \to B$ be some ring homomorphism. If E is a subset of A, we call the ideal in B generated by $f(E)$ the **extension** of E, which we denote by E^e. If E is a subset of B, we call the ideal in A generated by $f^{-1}(E)$ the **contraction** of E, which we denote by E^c. Clearly, if E is an ideal in B, then $E^c = f^{-1}(E)$.

[4]This follows from the fact that the correspondence between the ideals of R and the ideals of R/I can be restricted to a bijection between $\mathrm{Spec}(R)$ and $\mathrm{Spec}(R/I)$.

1.2 Definition of Modules and Algebra

Let A be some ring. By an A-**module**, we mean an abelian group M together with a A-scalar multiplication. Given another A-module N, we use the notation $\mathrm{Hom}(M, N)$ to denote the space of A-**module homomorphism** from M to N. It is clear that the obvious assignment of A-scalar multiplication and addition makes $\mathrm{Hom}(M, N)$ a A-module.

Let M be an A-module, and let N be a subset of M. We say N is a A-**submodule** if N forms an additive subgroup and is closed under A-scalar multiplication. Just like how ideals is proved to always be the kernel of some ring homomorphism, to see submodules is always the kernel of some A-module homomorphism, we simply construct the **quotient module** M/N, and get the quotient map $\pi : M \to M/N$ that is a A-module homomorphism with kernel N, and get also the bijection

$$A\text{-submodule } S \text{ of } M \text{ that contains } N \mapsto \{[x] \in M/N : x \in S\}$$

between the collection of the A-submodules of M that contains N and the collection of the A-submodule of M/N. This is called the **correspondence theorem** for modules.

Again similar to the other algebraic structure, we have the **third isomorphism theorem** for modules. Let $N \subseteq M \subseteq L$ be three modules. It is obvious that M/N is a subset of L/N, and moreover, M/N forms a submodule of L/N. We have an isomorphism $\phi : (L/N)/(M/N) \to L/M$ defined by $(l+N)+(M/N) \mapsto l+M$. To simplify matters, from now on we use the term "module" in place of "A-module" until the end of this section.

Let $\{M_i : i \in I\}$ be a collection of modules. If we give the Cartesian product $\prod M_i$ the obvious addition and multiplication, then we say it is the **direct product**. It is clear that

$$\left\{(x_i)_{i\in I} \in \prod_{i\in I} M_i : x_i \neq 0 \text{ for finitely many } i.\right\}$$

forms a submodule of the direct product. We denote this submodule by $\bigoplus M_i$, and call it the **direct sum**. Obviously, if the index set I is finite, then the direct product and direct sum are identical.

Given a subset E of M, clearly its **span**, the set of finite sum $\sum rx$ where $x \in E$, forms a submodule. Interestingly, depending on the view one wish to take, there are multiple common notation for spans of E. To view modules as generalization of vector spaces, one may write $\mathrm{span}(E)$, to view module as generalizations of rings, one may write $\langle E \rangle$, and to adapt the algebraic convention, one may also write $\sum_{x\in E} Ax$.

We say M is **finitely generated** if M can be spanned by some finite set $\{x_1, \ldots, x_n\} \subseteq M$. Clearly, $(a_1, \ldots, a_n) \mapsto \sum a_i x_i$ forms a surjective homomorphism from A^n to M, which implies M is isomorphic to some quotient of A^n. This behavior, albeit seems unimportant for now, will later prove to be useful for it guarantees that finitely generated module over rings of some certain properties carry the same property.[5]

By the **Jacobson radical** $\mathrm{Jacob}(A)$ of A, we mean the intersection of all maximal ideals of A. Given an ideal $\mathfrak{a}$ of A, some module M and some submodule N of M, the **product $\mathfrak{a}N$ of the submodule N by the ideal $\mathfrak{a}$** is the submodule of M consisting of finite sum $\sum a_i x_i$ where $a_i \in \mathfrak{a}$ and $x_i \in N$. We may now state Nakyama's Lemma.

Lemma 1.2.1. (Nakayama) Let M be a finitely generate A-module, and $\mathfrak{a}$ an ideal of A contained by the Jacobson radical of A. If $\mathfrak{a}M = M$, then $M = 0$.

Proof. Assume for a contradiction that $M \neq 0$. Let $u_1, \ldots, u_n$ be a minimal set of generators of M. Write $u_n = a_1 u_1 + \cdots + a_n u_n$ where $a_i \in \mathfrak{a}$. This give us

$$(1 - a_n)u_n = a_1 u_1 + \cdots + a_{n-1} u_{n-1} \tag{1.1}$$

We know that $1 - a_n$ must be a unit, otherwise by Zorn's Lemma[6] there exists a maximal ideal $\mathfrak{m}$ containing $1 - a_n$, which is impossible since $a_n \in \mathrm{Jacob}(A)$ would have implies $1 \in \mathfrak{m}$. Because $1 - a_n$ is a unit, by Equation 1.1, u_n can be generated by $\{u_1, \ldots, u_{n-1}\}$, a contradiction to the minimality of $\{u_1, \ldots, u_n\}$.

■

[5] For example, this shows that finitely generated module over Noetherian ring is Noetherian. See Section 4.1

[6] Note that union of proper ideals is always proper because otherwise one of them would have contain 1.

1.3 Localization

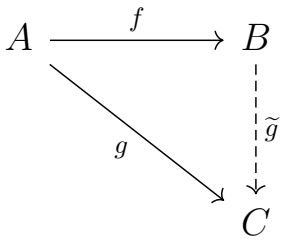
Let A be a ring. We say $S \subseteq A$ is a **multiplicatively closed subset** of A if S contains 1 and is closed under multiplication. We say a ring B and a homomorphism $f : A \to B$ satisfies the **universal property of localization of A by S** if

(a) $f(S) \subseteq B^\times$.

(b) $f(a) = 0 \implies as = 0$ for some $s \in S$.

(c) $B = \{f(a)f(s)^{-1} : a \in A \text{ and } s \in S\}$

Suppose $A \xrightarrow{f} B$ satisfies the universal property of localization of A by S. A routine check shows that for any ring homomorphism $g : A \to C$ that maps S into $C^\times$, the ring homomorphism $\widetilde{g} : B \to C$ well-defined by $\widetilde{g}(f(a)f(s)^{-1}) \triangleq g(a)g(s)^{-1}$ is the unique ring homomorphism such that the diagram



commutes. Just like the universal properties for other mathematical objects, one many check[7] that if $A \xrightarrow{f'} B'$ also satisfies the universal property of localization of A by S, then $B \cong B'$. Immediately, we need to ask: Does there really exists some $A \xrightarrow{f} B$ that satisfies the universal property of localization of A by S? The answer if of course affirmative: Define an equivalence relation on $A \times S$ by

$$(a, s) \sim (b, t) \overset{\triangle}{\iff} (at - bs)u = 0 \text{ for some } u \in S$$

Denoting the set of equivalence classes by $S^{-1}A$ and denoting the equivalence class of (a, s) by $\frac{a}{s}$, we have a ring structure on $S^{-1}A$ from defining

$$\frac{a}{s} + \frac{b}{t} \triangleq \frac{at + bs}{st} \text{ and } \frac{a}{s} \cdot \frac{b}{t} \triangleq \frac{ab}{st}$$

Clearly, the **canonical** ring homomorphism $A \longrightarrow S^{-1}A; a \mapsto \frac{a}{1}$ satisfies the universal property of localization of A by S, and just as out notation and intuition suggest, $S^{-1}A = 0$ if $0 \in S$.

[7] The proof is exactly the same as the ones for other mathematical objects.

If P is a prime ideal of A, we often just call $A_P \triangleq (A \setminus P)^{-1}A$ the **localization of A at P**. A nonzero ring is said to be a **local ring** if it has only one maximal ideal. One may check that a ring A is local if and only if it is the localization of some ring B at some prime ideal P of B[8], thus the naming of "local ring".

Let $I \subseteq A$ be some ideal, clearly its extension is the **localization of I by S** defined by $S^{-1}I = \{\frac{i}{s} \in S^{-1}A : i \in I\}$. We use the notation $S(I)$ to denote the contraction of $S^{-1}I$. For the section on uniqueness of primary decomposition, we first prove some basic properties of localization of ideals.

Theorem 1.3.1. (Properties of localization of ideals) Let A be a ring, and let S be some multiplicatively closed subset of A.

(a) If I is an ideal in A, then

$$S(I) = \bigcup_{s \in S} (I : s)$$

(b) If I is an ideal in A, then

$$\sqrt{S^{-1}I} = S^{-1}\sqrt{I}$$

(c) If $I_1, \ldots, I_n$ are ideals in A, then

$$S^{-1}(I_1 \cap \cdots \cap I_n) = S^{-1}I_1 \cap \cdots \cap S^{-1}I_n$$

Proof. We first prove part (a). Let $t \in (I : s)$ for some s. Because $\frac{t}{1} = \frac{st}{s} \in S^{-1}I$, we see $t \in I^{ec}$. Let $t \in I^{ec}$, so $\frac{t}{1} = \frac{i}{s}$ for some $i \in I, s \in S$. Observe $tss' = is' \in I$ for some s' to conclude $t \in (I : ss')$, and we are done. We now prove part (b). It is clear that $S^{-1}\sqrt{I} \subseteq \sqrt{S^{-1}I}$. Let $\frac{a}{s} \in \sqrt{S^{-1}I}$, so $\frac{a^n}{s^n} = \frac{i}{s'} \in S^{-1}I$ for some n, i, s'. Let s'' satisfies $a^n s' s'' = is^n s'' \in I$. Observations of $\frac{a}{s} = \frac{as's''}{ss's''}$ and $as's'' \in \sqrt{I}$ finish the proof. We now prove part (c). It is clear that $S^{-1}(I_1 \cap \cdots \cap I_n) \subseteq S^{-1}I_1 \cap \cdots S^{-1}I_n$. Let $\frac{a}{s} \in S^{-1}I_1 \cap \cdots \cap S^{-1}I_n$. For each $j \in \{1, \ldots, n\}$, we may find $s_j, s_j' \in S, i_j \in I$ such that $as_j s_j' = si_j s_j' \in I_j$. Writing

$$\frac{a}{s} = \frac{as_1s_1's_2s_2' \cdots s_ns_n'}{ss_1s_1's_2s_2' \cdots s_ns_n'} \in S^{-1}(I_1 \cap \cdots \cap I_n)$$

and we are done. ∎

[8]If A is local, then it is the localization of itself at its unique maximal ideal. If $A = B_P$, then the set of non-units $\{\frac{p}{s} \in B_P : p \in P\}$ is clearly the only maximal ideal of A.

1.4 Integral Dependence

Let A be a subring of some ring B. We say $x \in B$ is **integral over** A if x is a root of some monic polynomial with coefficients in A.

Theorem 1.4.1. (Cayley-Hamilton Theorem for finitely generated module) Suppose $\mathfrak{a} \subseteq A$ is an ideal, and M is a finitely generated A-module. If $\phi \in \mathrm{End}(M)$ satisfies $\mathrm{Im}\,\phi \subseteq \mathfrak{a}M$, then there exists some $a_0, \ldots, a_{n-1} \in \mathfrak{a}$ such that

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

Proof. Let $\{m_1, \ldots, m_n\}$ generate M. Because $\mathrm{Im}(\phi) \subseteq \mathfrak{a}M$, we may write

$$\phi(m_i) = \sum_{j=1}^{n} a_{ij} m_j, \quad \text{where } a_{ij} \in \mathfrak{a}$$

Clearly, for each i, we have

$$\sum_{j=1}^{n} (\delta_{ij}\phi - a_{ij}\mathbf{1}) m_i = 0,$$

where $\mathbf{1} \in \mathrm{End}(M)$ is the identity operator and δ_{ij} is the Kronecker delta. Defining $R \triangleq A[\phi] \subseteq \mathrm{End}(M)$, we may now view $\delta_{ij}\phi - a_{ij}\mathbf{1}$ as an $n \times n$ matrix, whose entries are elements of ring R. Because R is a commutative unital ring, there exist R-matrix X **adjugate** to $(\delta_{ij}\phi - a_{ij}\mathbf{1})$, i.e., $X(\delta_{ij}\phi - a_{ij}\mathbf{1}) = \det(\delta_{ij}\phi - a_{ij}\mathbf{1})I$, where I is the identity R-matrix. This implies that

$$\det(\delta_{ij}\phi - a_{ij}\mathbf{1}) m_k = 0, \quad \text{for all } k \in \{1, \ldots, n\}$$

Noting that $\mathrm{der}(\delta_{ij}\phi - a_{ij}\mathbf{1})$ is an $\mathfrak{a}$-polynomial in ϕ and $M = \langle m_1, \ldots, m_n \rangle$, our proof is done. ■

Cayley-Hamilton Theorem for finitely generated module allow us to give the following equivalent definitions of integral dependence, which are the keys for defining integral closure.

Theorem 1.4.2. (Equivalent Definitions for integral dependence) Let A be a subring of B, and let $x \in B$. The following are equivalent:

(i) $x \in B$ is integral over A.

(ii) $A[x]$ is a finitely generated A-module.

(iii) $A[x]$ is contained in a subring C of B such that C as the obvious A-module is finitely generated.

Proof. (i) $\implies$ (ii) $\implies$ (iii) is clear. We now prove (iii) $\implies$ (i). Define an A-module endomorphism $\phi : C \to C$ by $c \mapsto xc$. By Cayley-Hamilton Theorem for finitely generated module, $\phi^n + a_{n-1}\phi^{n-1} + \cdots + a_0 = 0$. In other words, $(x^n + a_{n-1}x^{n-1} + \cdots + a_0)c = 0$ for all $c \in C$. Consider the case when $c = 1$, and we are done. ■

Corollary 1.4.3. (Definition of Integral Closure) If A is a subring of B, then the set of elements of B which are integral over A forms a subring of B containing A.

Proof. Let $x, y \in B$ be integral over A. We are required to prove $x \pm y, xy$ are also integral over A. The first step of the proof is to observe that $A[x + y], A[x - y], A[xy]$ are both contained by the ring $A[x, y]$, which is a subring of C. Therefore, we only have to show $A[x, y]$ as an A-module is finitely generated.

Now, note that $A[x, y] = (A[x])[y]$. Clearly y is integral over $A[x]$, so we know $A[x, y] = (A[x])[y]$ is a finitely generated $A[x]$-module. Moreover, because x is integral over A, we also know $A[x]$ is a finitely generated A-module. Let $A[x, y]$ as an $A[x]$-module be generated by $\{z_1, \ldots, z_n\}$, and let $A[x]$ as an A-module be generated by $\{v_1, \ldots, v_k\}$. It is easy to check that, indeed, $A[x, y]$ as an A-module is generated by $\{z_i v_j \in A[x, y] : 1 \leq i \leq n, 1 \leq j \leq k\}$. ■

Let A be a subring of B. Because of Corollary 1.4.3, when we talk about the **integral closure of A in B**, the set of elements of B integral over A, we know we are indeed talking about a ring. If B itself is the integral closure of A in B, we say A is **integrally closed** in B.

For the proof of Corollary 1.4.4, note that induction and argument similar to the second paragraph of the proof of Corollary 1.4.3 shows that if $x_1, \ldots, x_n$ are all integral over A, then $A[x_1, \ldots, x_n]$ as an A-module is finitely generated.

Corollary 1.4.4. (Transitivity of Integral Closure) Let B be a subring of C, and A a subring of B. If A is integrally closed in B and B is integrally closed in C, then A is integrally closed in C.

Proof. Let $x \in C$. Because B is integrally closed in C, we know

$$x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0, \quad \text{for some } b_0, \ldots, b_{n-1} \in B$$

By Theorem 1.4.2, we are only required to show $A[b_0, \ldots, b_{n-1}, x]$ as an A-module is finitely generated. Clearly, x is integral over the subring $A[b_0, \ldots, b_{n-1}]$, so by Theorem 1.4.2, we know $A[b_0, \ldots, b_{n-1}, x]$ as an $A[b_0, \ldots, b_{n-1}]$-module is finitely generated. The proof then follows from noting $A[b_0, \ldots, b_{n-1}]$ is finitely generated as an A-module since all $b_0, \ldots, b_{n-1}$ are all integral over A. ■

1.5 The Nonsense Lemmas

Let R be some ring. Given a sequence of R-modules and R-modules homomorphism

$$\cdots \longrightarrow M_{k-1} \xrightarrow{f} M_k \xrightarrow{g} M_{k+1} \longrightarrow \cdots$$

we say the sequence is **exact** at M_k if $\mathrm{Im}(f) = \mathrm{Ker}(g)$, and we say a sequence is **exact** if it is exact at each of its module. By a **short** exact sequence, we mean exact sequence of the form

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

Lemma 1.5.1. (Five Lemma) Given a commutative diagram in the category of R-module:

$$\begin{array}{ccccccccc}
A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{j} & E \\
\downarrow{\scriptstyle l} & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle q} \\
A' & \xrightarrow{r} & B' & \xrightarrow{s} & C' & \xrightarrow{t} & D' & \xrightarrow{u} & E'
\end{array}$$

If the two rows are exact, m, p are isomorphism, l is surjective and q is injective, then n is also an isomorphism. The proof of Five Lemma follows immediately from the two Four Lemma, and their proof are both just diagram chasing. For demonstration, we present a proof for the first four lemma.

Lemma 1.5.2. (First Four Lemma) Given a commutative diagram in the category of R-module:

$$\begin{array}{ccccccc}
A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D \\
\downarrow{\scriptstyle l} & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle p} \\
A' & \xrightarrow{r} & B' & \xrightarrow{s} & C' & \xrightarrow{t} & D'
\end{array}$$

If the two rows are exact, m, p are injective, l is surjective, then n is injective.

Proof. Let $c \in C$ such that $n(c) = 0$. We are required to show $c = 0$. Using the hypothesis, we may deduce

$$n(c) = 0 \implies t \circ n(c) = 0 \implies p \circ h(c) = 0 \implies h(c) = 0 \implies c = g(b)$$

for some $b \in B$. Observing that $s(m(b)) = n \circ g(b) = n(c) = 0$, we see $m(b) = r(a')$ for some $a' \in A'$. Because l is surjective, $a' = l(a)$ for some $a \in A$. Now, because

$$m \circ f(a) = r \circ l(a) = r(a') = m(b)$$

by injectivity of m, we may deduce $b = f(a)$. This together with first row being exact shows that

$$c = g(b) = g \circ f(a) = 0$$

■

Lemma 1.5.3. (Second Four Lemma) Given a commutative diagram in the category of R-modules:

$$\begin{array}{ccccccc} B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{j} & E \\ \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle q} \\ B' & \xrightarrow{s} & C' & \xrightarrow{t} & D' & \xrightarrow{u} & E' \end{array}$$

If the two rows are exact, m, p are surjective, q is injective, then n is surjective. As a special case of the Five Lemma, we now have the Short Five Lemma.

Lemma 1.5.4. (Short Five Lemma) Given a commutative diagram in the category of R-modules:

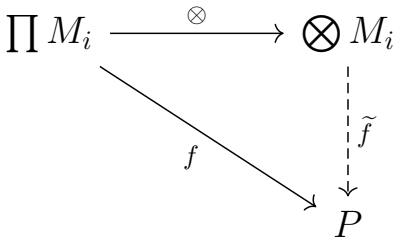
$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & C & \longrightarrow & D & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle p} & & \\ 0 & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & D' & \longrightarrow & 0 \end{array}$$

If the two rows are exact and m, p are isomorphisms, then n is an isomorphism.

1.6 Tensor Product of Modules

By **free modules**, we mean modules of the form $\bigoplus_{i\in I} M_i$ where $M_i \cong R$. We denote the free module $\bigoplus_{i\in I} M_i$ by $R^{(I)}$.

Let R be some ring. Given a finite collection $\{M_1, \ldots, M_n\}$ of R-modules, by the term **tensor product space**, we mean a R-module denoted by $\bigotimes M_i$ and a R-multilinear map $\otimes : \prod M_i \to \bigotimes M_i$ that satisfies the **universal property**: For each multilinear map $f : \prod M_i \to P$, there exists unique linear map $\widetilde{f} : \bigotimes M_i \to P$ such that the diagram



commutes. This definition is unique up to isomorphism: If $\bigotimes' M_i$ is also a tensor product, then there exists some module isomorphism from $\bigotimes M_i$ to $\bigotimes' M_i$ that sends $m_1 \otimes \cdots \otimes m_n$ to $m_1 \otimes' \cdots \otimes' m_n$. One common construction of the tensor product space is to quotient the free module $R^{(\prod M_i)}$ with the submodule spanned by the set:

$$\bigcup_{i=1}^{n}\Big[\Big\{(x_1, \ldots, rx_i, \ldots, x_n) - r(x_1, \ldots, x_n)\Big\} \cup \Big\{(x_1, \ldots, x_i + x_i', \ldots, x_n) - (x_1, \ldots, x_i, \ldots, x_n) - (x_1, \ldots, x_i', \ldots, x_n)\Big\}\Big]$$

Denoting this spanned submodule by D, our tensor product space $\bigotimes M_i$ is now $R^{(\prod M_i)} \big/ D$, and because of the forms of the generators of D, the tensor product map $\otimes : \prod M_i \to \bigotimes M_i$ defined by

$$x_1 \otimes \cdots \otimes x_n \triangleq [(x_1, \ldots, x_n)]$$

is clearly multilinear. Because free module $R^{(\prod M_i)}$ is a direct sum, it is clear that $\bigotimes M_i$ is generated by the **basic elements**[9], and because of such, for every multilinear map $f : \prod M_i \to P$, the induced map $\widetilde{f} : \bigotimes M_i \to P$ must be unique. To actually induce $\widetilde{f}$, one first extend f to the whole free module $\overline{f} : R^{(\prod M_i)} \to P$ by setting $\overline{f}(\sum r(x_1, \ldots, x_n)) \triangleq \sum rf(x_1, \ldots, x_n)$, and see that because $\overline{f}$ vanishes on the generators of D, we may induce some mapping from $\bigotimes M_i$ to P that clearly has the desired action of $\widetilde{f}$ on the basic elements.

[9] Elements of the form $x_1 \otimes \cdots \otimes x_n$

Note that the **tensor-horn adjunction** isomorphism

$$\mathrm{Hom}(M \otimes N, P) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, P))$$

maps $f \in \mathrm{Hom}(M \otimes N, P)$ to $\widetilde{f} \in \mathrm{Hom}(M, \mathrm{Hom}(N, P))$ with the action

$$\widetilde{f}(m)n \triangleq f(m \otimes n)$$

1.7 Chain Condition

Given some collection Σ of sets, we say Σ satisfies the **ascending chain condition, a.c.c.**, if for each chain $x_1 \subseteq x_2 \subseteq \cdots$ there exists n such that $x_n = x_{n+1} = \cdots$, and we say Σ satisfies the **descending chain condition, d.c.c.**, if for each chain $x_1 \supseteq x_2 \supseteq \cdots$ there exists n such that $x_n = x_{n+1} = \cdots$. Let M be some module. We say M is **Noetherian** if the collection of submodules of M satisfies a.c.c., and we say M is **Artinian** if the collection of submodules satisfies d.c.c. Thanks to axiom of choice, module M is Noetherian if and only if every nonempty collection of submodules of M has a maximal element if and only if every submodule of M is finitely generated.

Given a finite **chain** of submodules

$$M_0 \subset M_1 \subset \cdots \subset M_n$$

we say this chain is of **length** n. Under the obvious assignment of order on the collection of all finite chains of submodules of M, by a **composition series** of M, we mean a maximal finite chain. Clearly, a finite chain

$$0 = M_0 \subset \cdots \subset M_n = M$$

is maximal if and only if M_k/M_{k-1} are simple.

Theorem 1.7.1. (Length of modules is well defined) Every composition series of a module M have the same length.

Proof. Suppose M has a composition series, and let $l(M)$ denote the least length of a composition series of M. We wish to show every chain has length smaller than $l(M)$. Before such, we first prove

$$N \subset M \implies l(N) < l(M) \tag{1.2}$$

Let $M_0 \subset \cdots \subset M_n = M$ be a composition series of least length. Define $N_k \triangleq N \cap M_k$ for all $k \in \{0, \ldots, n\}$. Consider the obvious homomorphism $N_k/N_{k-1} \to M_k/M_{k-1}$. We see that either $N_k/N_{k-1} \cong M_k/M_{k-1}$ or $N_k = N_{k-1}$. This implies that the chain $N_0 \subset \cdots \subset N_n$ will be a composition series of N after the unnecessary terms are removed. It remains to show there are unnecessary terms in $N_0 \subset \cdots \subset N_n$. Assume not for a contradiction. Because $N_1 \subseteq M_1$ and $N_1/\{0\} \cong M_1/\{0\}$, we have $N_1 = M_1$. Repeating the same argument, we have $N = N_n = M_n = M$, a contradiction. We have proved statement 1.2.

Now, let $M'_0 \subset \cdots \subset M'_r$ be some composition series of M. The proof then follows from using statement 1.2 to deduce

$$l(M) = l(M'_r) > \cdots > l(M'_0) = 0 \implies r \leq l(M)$$

■

Because of Theorem 1.7.1, we may well define the **length** $l(M)$ of module. For obvious reason, if module M has no composition series, we say M has infinite length and write $l(M) = \infty$. Clearly, if M is of finite length, then M is both Noetherian and Artinian. Conversely, if M is both Noetherian and Artinian, then by the maximal element definition of Noetherian, there exists a decreasing sequence $M = M_0 \supset M_1 \supset M_2 \supset \cdots$, which by d.c.c. must be finite.

Chapter 2

IDK where u belong

2.1 Valuation Rings

Let A be a ring, and let $S \subseteq A$ be a multiplicatively closed subset that contains no zero-divisors. Clearly, in $S^{-1}A$,

$$\frac{a}{s} = \frac{b}{t} \text{ if and only if } at = bs.$$

This implies that the canonical ring homomorphism $A \to S^{-1}A$ is injective, and it thus make sense for us to identify A as a subring of $S^{-1}A$. In particular, if D is an integral domain, then we consider D to be a subring of its **field of fraction** $(D^*)^{-1}D$. Let K be a field and D a subring of K. If for all $x \in K$, either $x \in D$ or $x^{-1} \in D$, then the mapping $F \longrightarrow \text{Frac}(D)$ defined by

$$x \mapsto \begin{cases} \frac{x}{1} & \text{if } x \in D \\ \frac{1}{x^{-1}} & \text{if } x \notin D \end{cases}$$

forms a field isomorphism. Because of this identification, for each integral domain D, it make sense to say D is a **valuation ring (of some field)** whenever $x \in \text{Frac}(D) \implies x \in D$ or $x^{-1} \in D$.

Given a field K and an totally ordered abelian group Γ, we say $\nu : K \to \Gamma \cup \{\infty\}$ is a **valuation** if it satisfies:

(a) $\nu^{-1}(\infty) = \{0\}$.

(b) $\nu(xy) = \nu(x) + \nu(y)$.

(c) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$, with the equality holds true if $\nu(x) \neq \nu(y)$.

Let D be an integral domain. We say D is a **valuation ring** if for each $x \in \mathrm{Frac}(D)$, either $x \in D$ or $x^{-1} \in D$.

Theorem 2.1.1. (Equivalent Definitions of valuation rings) Let D be an integral domain. The following are equivalent

(i) D is a valuation ring.

(ii) The principal ideals of D are totally ordered by inclusion.

(iii) The ideals of D are totally ordered by inclusion.

(iv) There is a totally ordered abelian group Γ and a valuation $\nu : \mathrm{Frac}(D) \to \Gamma \cup \{\infty\}$ such that $D = \{x \in \mathrm{Frac}(D) : \nu(x) \geq 0 \in \Gamma\}$.

(v) D is a local Bezout Domain.

Proof. It is easy to prove (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (i). For (i) $\implies$ (iv), let $D^\times$ be the set of units of D. Clearly, $D^\times$ is a normal subgroup of $(\mathrm{Frac}\, D)^*$. Because D is a valuation ring, we may well define a total order on $\Gamma \triangleq (\mathrm{Frac}\, D)^* / D^\times$ by

$$[x] \geq [y] \overset{\triangle}{\iff} xy^{-1} \in D$$

It is routine to check that $\nu : \mathrm{Frac}(D) \to \Gamma \cup \{\infty\}$ defined by

$$\nu(x) \triangleq \begin{cases} [x] & \text{if } x \neq 0 \\ \infty & \text{if } x = 0 \end{cases}$$

is a valuation such that $D = \{x \in \mathrm{Frac}(D) : \nu(x) \geq 0 \in \Gamma\}$. j ■

Because of ideals of valuation ring are totally ordered by inclusion, clearly valuation rings are always local rings.

2.2 Discrete Valuation Rings

Let K be a field. A **discrete valuation** $\nu : K \to \Gamma \cup \{\infty\}$ is a valuation such that $\Gamma = \mathbb{Z}$. Clearly, the set of $x \in K$ such that $\nu(x) \geq 0$ forms a ring[1], called the **discrete valuation ring** of ν, since indeed it is a valuation ring.

[1] $\nu(1) = \nu(-1) = 0$.

2.3 Fractional "Ideal"

Notably, if S contains 0, then $S^{-1}A$ is zero ring, so when we talk about the **filed of fraction** K of an integral domain A, we mean $(A \setminus 0)^{-1}A$. Given an A-submodule M of K, if $xM \subseteq A$ for some $x \neq 0 \in A$, unfortunately we say M is a **fractional ideal** of A even though M needs not to be a subset of A. However, if I is an ideal of A, then clearly I is also a fractional ideal of A.

If $M \subseteq K$ is a finitely generated A-submodule, then M is a fractional ideal of A, since if $M = \langle \frac{b_1}{a_1}, \ldots, \frac{b_n}{a_n} \rangle$, then $(a_1 \cdots a_n)M \subseteq A$. We say an A-submodule $M \subseteq K$ is **invertible** if there exists some A-submodule $N \subseteq \mathbb{F}$ such that $MN = A$ where $MN \triangleq \{m_1n_1 + \cdots + m_kn_k \in \mathbb{F} : m_i \in M, n_i \in N\}$.

2.4 Local Property

If we say a module property X is a **local property**, we mean that for every A-module M and prime ideal $P \subseteq A$, M satisfies X if and only if M_P satisfies X, and if we say a ring property X is a **local property**, we mean that for every ring A and prime ideal $P \subseteq A$, A satisfies X if and only if A_P satisfies X.

Chapter 3

Some Theorems

3.1 Uniqueness of Primary Decomposition

Let A be a ring. We say a proper ideal Q is **primary** if for each $xy \in Q$, either $x \in Q$ or $y^n \in Q$ for some $n > 0$. Equivalently, a proper ideal I is primary if and only if every zero-divisors in A/Q is nilpotent. Clearly, the radical $P = \sqrt{Q}$ of a primary ideal Q is prime. In such case, we say Q is **P-primary**. A **primary decomposition** of an ideal I is an expression of I as a finite intersection of primary ideals

$$I = \bigcap_{i=1}^{n} Q_i$$

Such primary decomposition is said to be **irredundant** if $\sqrt{Q_i}$ are all distinct and no Q_i is unnecessary in the sense that

$$\bigcap_{j \neq i} Q_j \not\subseteq Q_i \text{ for all } i.$$

An ideal I is said to be **decomposable** if there exists some primary decomposition of I. Because finite intersection of P-primary ideals is again P-primary, every decomposable ideal has an irredundant primary decomposition.

Theorem 3.1.1. (First uniqueness theorem for irredundant primary decomposition) Given some irredundant primary decomposition $I = \bigcap_{i=1}^{n} Q_i$, we have

$$\left\{\sqrt{Q_i a} : 1 \leq i \leq n\right\} = \operatorname{Spec}(R) \cap \left\{\sqrt{(I : x)} \subseteq R : x \in R\right\} \tag{3.1}$$

Proof. Before showing that both sides of equation 3.1 are subsets of each other, we first make the following observation. For all $x \in R$, clearly

$$(I : x) = \left(\bigcap Q_i : x\right) = \bigcap (Q_i : x)$$

Therefore,

$$\sqrt{(I:x)} = \bigcap \sqrt{(Q_i:x)} = \bigcap_{k:x\notin Q_k} \sqrt{Q_k} \tag{3.2}$$

where the last equality is justified by

$$x \in Q_i \implies (Q_i:x) = R, \quad \text{and } x \notin Q_i \implies \sqrt{(Q_i:x)} = \sqrt{Q_i}$$

We now prove that the left hand side of equation 3.1 is a subset of the right hand side. Fix i. By irredundancy of the decomposition, there exists some $x \in R$ such that x belongs to all Q_j except Q_i. This x by equation 3.2 must satisfies

$$\sqrt{Q_i} = \sqrt{(I:x)}$$

Noting that $\sqrt{Q_i}$ must be prime due to Q_i being primary, we have shown the left hand side of Equation 5.1 is a indeed a subset of the right hand side.

Now, suppose for some $x \in R$ that $\sqrt{(I:x)}$ is prime. Because prime ideal must be proper, we know there must exists some k such that $x \notin Q_k$. By equation 3.2, to finish the proof, we only need to show $\sqrt{Q_k} \subseteq \sqrt{(I:x)}$ for some k such that $x \notin Q_k$. Assume not for a contradiction. Then for all k such that $x \notin Q_k$, there exists $y_k \in \sqrt{Q_k}$ such that $y_k \notin \sqrt{(I:x)}$. The product of these y_k is an element of $\bigcap \sqrt{Q_k}$, thus an element of $\sqrt{(I:x)}$. This with $\sqrt{(I:x)}$ being prime shows that $y_k \in \sqrt{(I:x)}$ for some k, a contradiction. ■

Because of the first uniqueness theorem, we may well define the **inner spectrum** of decomposable ideal I, independent of choice of irredundant decomposition, to be

$$\left\{\sqrt{Q_1}, \ldots, \sqrt{Q_n}\right\}$$

where

$$I = \bigcap_{i=1}^{n} Q_i \text{ is some irredundant primary decomposition.}$$

Given such irredundant primary decomposition, we say Q_i is an **isolated primary component** if $\sqrt{Q_i}$ is minimal in the inner spectrum.

Lemma 3.1.2. (preparation lemma for second uniqueness theorem) Let S be a multiplicatively closed subset of A, and let Q be a P-primary ideal. If S and P are disjoint, then $S^{-1}Q$ is $S^{-1}P$-primary and $S(Q) = Q$. If S and P meet, then $S^{-1}Q = S^{-1}A$.

Proof. Suppose S and P are disjoint. Clearly we have $Q \subseteq S(Q)$, so to show $S(Q) = Q$, we only have to show $S(Q) \subseteq Q$. Let $a \in S(Q)$. The first part of Theorem 1.3.1 states that $a \in (Q : s)$ for some $s \in S$. Because $Q \subseteq P$, this implies $a \in Q$. We have shown $S(Q) = Q$. Note that the second part of Theorem 1.3.1 states that

$$\sqrt{S^{-1}Q} = S^{-1}\sqrt{Q} = S^{-1}P$$

so for the case when S and P are disjoint, it only remains to prove $S^{-1}Q$ is indeed primary, which is routine and even unnecessary for the Second uniqueness theorem below.

Suppose $s \in S \cap P$. Let $s^n \in Q$. The fact that $S^{-1}Q = S^{-1}A$ follows from the fact $\frac{s^n}{1}$ is a unit with inverse $\frac{1}{s^n}$. ■

Theorem 3.1.3. (Second uniqueness theorem for isolated primary component) The isolated primary components of a decomposable ideal I is uniquely determined by I, independent of the irredundant decomposition.

Proof. Let P be a minimal element of the inner spectrum of I, and let $I = \bigcap_{i=1}^{n} Q_i$ be an arbitrary irredundant primary decomposition, where $\sqrt{Q_1} = P$. Clearly $S \triangleq A \setminus P$ is multiplicatively closed. Because the definition of S is independent of the choice of the primary decomposition, we are only required to prove the goal

$$Q_1 = S(I)$$

Because S and P are disjoint, we may apply Lemma 3.1.2 to reduces this goal into

$$S^{-1}Q_1 = S^{-1}I$$

Noting that $\sqrt{Q_i}$ meets $S = A \setminus \sqrt{Q_1}$ for every $i > 1$ due to the minimality of $\sqrt{Q_1}$, we conclude our proof using Lemma 3.1.2 and the third part of Theorem 1.3.1:

$$S^{-1}I = \bigcap_{i=1}^{n} S^{-1}Q_i = S^{-1}Q_1$$

■

3.2 Existence of Primary Decomposition in Noetherian ring

Let A be a ring, and let $I \subseteq A$ be some ideal. We say I is **irreducible** if whenever I is expressed as an intersection of two ideals, I equals to one of them. Clearly, to show every ideal in Noetherian ring is decomposable, we only need to show the following two lemmas.

Lemma 3.2.1. In Noetherian ring A, every ideal is a finite intersection of irreducible ideals.

Proof. Assume not for a contradiction. Let I be a maximal element of the collection Σ of all ideals that can not be expressed as finite intersections of irreducible ideals. Clearly, I must be reducible, so there exists some $I = J_1 \cap J_2$ such that $I \subset J_1$ and $I \subset J_2$. Because $J_1, J_2 \notin \Sigma$, we may express them both as finite intersection of irreducible ideals. This implies that we may express I as a finite intersection of irreducible ideals, a contradiction. ■

Lemma 3.2.2. In Noetherian ring A, every irreducible ideal is primary.

Proof. Let $I \subseteq A$ be irreducible. Clearly, the zero ideal in A/I is irreducible, and if the zero ideal in A/I is primary, then I is also primary. Because of such, we may WLOG suppose I is zero. Let $xy = 0$ and $y \neq 0$. We are required to show $x^n = 0$. Clearly we have the chain $\text{Ann}(x) \subseteq \text{Ann}(x^2) \subseteq \cdots$, and by a.c.c., there exists some n such that $\text{Ann}(x^n) = \text{Ann}(x^{n+1}) = \cdots$. We now show

$$\langle x^n \rangle \cap \langle y \rangle = 0 \tag{3.3}$$

Let $a \in \langle x^n \rangle \cap \langle y \rangle$. Because $a \in \langle y \rangle$ and $xy = 0$, we know $ax = 0$. Writing $a = bx^n$, we now see $b \in \text{Ann}(x^{n+1}) = \text{Ann}(x^n)$. This implies $a = bx^n = 0$. We have shown Equation 3.3.

Finally, because the zero ideal is irreducible, we must have $\langle x^n \rangle = 0$ or $\langle y \rangle = 0$. Because $y \neq 0$, we may conclude $x^n = 0$. ■

3.3 Equivalent Definitions of DVR

3.4 Unique factorization Theorem for ideals in Noetherian domain of Krull dimension 1

Before the main course, we first develop some basic notion. We say two ideals are **coprime** if their sum equals to the whole ring. Note that two prime ideals need not be coprime. If K is a field, then $\langle x\rangle, \langle y\rangle$ are not coprime in $K[x, y]$.

Proposition 3.4.1. (Product of coprime ideals is the intersection) Let I_k be a finite collection of pairwise coprime ideals. We have $\prod I_k = \bigcap I_k$.

Proof. The proof relies on induction of total number of the pairwise coprime ideals. The base case is when there are only two, says, I and J. Clearly $IJ \subseteq I \cap J$. To prove the converse, observe for $c \in I \cap J$, there exists $1 = i + j$ so that $c = ci + cj$, where $ci, cj \in I \cap J$. ■

Chapter 4

Big Theorems

4.1 Hilbert's Basis Theorem

Before we prove the Hilbert's Basis Theorem, we must first show that finitely generated modules over Noetherian rings is also Noetherian.

Proposition 4.1.1. (Formal properties of Noetherian modules) Given a short exact sequence of A-modules:

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

M is Noetherian if and only if M' and M'' are both Noetherian.

Proof. Consider the ascending chain condition definition. For the "if" part, let L_n be an ascending chain of submodules of M, and use short five lemma on

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \alpha^{-1}(L_n) & \xrightarrow{\alpha} & L_n & \xrightarrow{\beta} & \beta(L_n) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \alpha^{-1}(L_{n+1}) & \xrightarrow{\alpha} & L_{n+1} & \xrightarrow{\beta} & \beta(L_{n+1}) & \longrightarrow & 0
\end{array}$$

to conclude that L_n must stop at some point. ■

Suppose A is a Noetherian ring. Applying Proposition 4.1.1 inductively to

$$0 \longrightarrow A \longrightarrow A^n \longrightarrow A^{n-1} \longrightarrow 0$$

we see the module A^n is also Noetherian, and so any finitely generated module over A, isomorphic to some quotient of A^n, is also Noetherian. We may now give a simple proof to Hilbert's Basis Theorem.

Theorem 4.1.2. (Hilbert's Basis Theorem) If A is Noetherian, than the polynomial ring $A[x]$ is also Noetherian.

Proof. Let X be an ideal in $A[x]$. We are required to show that X is finitely generated. Let I be the ideal in A that contains exactly the leading coefficients of elements of X. Because A is Noetherian, we may let $I = \langle a_1, \ldots, a_n \rangle$ and let $f_1, \ldots, f_n \in X$ have leading coefficients $a_1, \ldots, a_n$. Let $X' \triangleq \langle f_1, \ldots, f_n \rangle \subseteq X$ and let $r \triangleq \max\{\deg(f_1), \ldots, \deg(f_n)\}$.

We first show

$$X = \left(X \cap \langle 1, x, \ldots, x^{r-1} \rangle\right) + X' \tag{4.1}$$

Let $f \in X$ with $\deg(f) = m$ and leading coefficients a. We wish to show $f \in (X \cap \langle 1, x, \ldots, x^{r-1} \rangle) + X'$. Because $a \in I$, we may find some $u_i \in A$ such that $a = \sum u_i a_i$. Clearly, these u_i satisfy

$$f - \sum u_i f_i x^{m-\deg(f_i)} \in X, \quad \text{and} \quad \sum u_i f_i x^{m-\deg(f_i)} \in X'$$

and satisfy

$$\deg\left(f - \sum u_i f_i x^{m-\deg(f_i)}\right) < m$$

Proceeding this way, we end up with $f - g = h$ where $g \in X'$ and $h \in X \cap \langle 1, x, \ldots, x^{r-1} \rangle$. We have proved Equation 4.1. Now, because X' is finitely generated, to show X is finitely generated, it only remains to show the ideal $X \cap \langle 1, x, \ldots, x^{r-1} \rangle$ is finitely generated, which follows immediately from noting $\langle 1, x, \ldots, x^{r-1} \rangle$ as a module is Noetherian. ■

We close this section by giving a cute corollary of Hilbert's Basis Theorem in classical algebraic geometry. Suppose $E \subseteq R[x_0, \ldots, x_{n-1}]$ is an infinite collection of polynomials. Let V be the set of common roots of these polynomials, i.e.,

$$V \triangleq \{x \in R^n : f(x) = 0 \text{ for all } f \in E\}$$

Clearly,

$$V = \{x \in R^n : f(x) = 0 \text{ for all } f \in \langle E \rangle\}$$

Induction with Hilbert's Basis Theorem shows that $R[x_0, \ldots, x_{n-1}]$ is Noetherian, so $\langle E \rangle$ is finitely generated. This allow us to write $\langle E \rangle = \langle f_1, \ldots, f_n \rangle$ for some finite set of polynomials $f_1, \ldots, f_n \in R[x_0, \ldots, x_{n-1}]$. We now see that the locus V of an infinite collection of polynomials can always be written as a locus of some finite collection of polynomials.

4.2 Nullstellensatz

Theorem 4.2.1. (Hilbert's Nullstellensatz) Let K be an algebraically closed field, and let I be an ideal of $K[t_1, \ldots, t_n]$. Define

$$V \triangleq \{x \in K^n : f(x) = 0 \text{ for all } f \in I\}$$

If we let X be the ideal

$$X \triangleq \{g \in K[t_1, \ldots, t_n] : g(x) = 0 \text{ for all } x \in V\}$$

then $X = \sqrt{I}$.

Proof. ■

Chapter 5

Scripts

5.1 Script 3

A **primary decomposition** of an ideal I is an expression of I as a finite intersection of primary ideals

$$I = \bigcap_{i=1}^{n} Q_i$$

Moreover, if $\sqrt{Q_i}$ are all distinct and

$$\bigcap_{j \neq i} Q_j \not\subseteq Q_i \text{ for all } i$$

then we say the primary decomposition is **irredundant**.

Theorem 5.1.1. (First uniqueness theorem for irredundant primary decomposition) Given some irredundant primary decomposition $I = \bigcap_{i=1}^{n} Q_i$, we have

$$\left\{ \sqrt{Q_i} : 1 \leq i \leq n \right\} = \operatorname{Spec}(R) \cap \left\{ \sqrt{(I : x)} \subseteq R : x \in R \right\} \tag{5.1}$$

Proof. Before showing that both sides of Equation 5.1 are subsets of each other, we first make the following observation. For all $x \in R$, clearly

$$(I : x) = \left(\bigcap Q_i : x \right) = \bigcap (Q_i : x)$$

Therefore,

$$\sqrt{(I : x)} = \bigcap \sqrt{(Q_i : x)} = \bigcap_{k : x \notin Q_k} \sqrt{Q_k} \tag{5.2}$$

where the last equality is justified by

$$x \in Q_i \implies (Q_i : x) = R, \quad \text{and } x \notin Q_i \implies \sqrt{(Q_i : x)} = \sqrt{Q_i}$$

We now prove that the left hand side of Equation 5.1 is a subset of the right hand side. Fix i. By irredundancy of the decomposition, there exists some $x \in R$ such that x belongs to all Q_j except Q_i. This x by Equation 5.2 must satisfies

$$\sqrt{Q_i} = \sqrt{(I : x)}$$

Noting that $\sqrt{Q_i}$ must be prime due to Q_i being primary, we have shown the left hand side of Equation 5.1 is a indeed a subset of the right hand side.

Now, suppose for some $x \in R$ that $\sqrt{(I : x)}$ is prime. Because prime ideal must be proper, we know there must exists some k such that $x \notin Q_k$. By Equation 5.2, to finish the proof, we only need to show $\sqrt{Q_k} \subseteq \sqrt{(I : x)}$ for some k such that $x \notin Q_k$. Assume not for a contradiction. Then for all k such that $x \notin Q_k$, there exists $y_k \in \sqrt{Q_k}$ such that $y_k \notin \sqrt{(I : x)}$. The product of these y_k is an element of $\bigcap \sqrt{Q_k}$, thus an element of $\sqrt{(I : x)}$. This with $\sqrt{(I : x)}$ being prime shows that $y_k \in \sqrt{(I : x)}$ for some k, a contradiction. ■

Because of Theorem 5.1.1, we may well define the following notions. Given some decomposable ideal I, we say the prime ideals $\{\sqrt{Q_1}, \ldots, \sqrt{Q_n}\}$ **belong** to I, and if $\sqrt{Q_i}$ is a minimal element of $\{\sqrt{Q_1}, \ldots, \sqrt{Q_n}\}$, then we say $\sqrt{Q_i}$ is an **isolated** prime ideal belonging to I.

Theorem 5.1.2. (Proposition 4.6) Let I be a decomposable ideal. Any prime ideal $P \supseteq I$ contains an isolated prime ideal belonging to I.

Proof. Let

$$\bigcap_{i=1}^{n} Q_i = I \subseteq P$$

We have

$$\bigcap_{i=1}^{n} \sqrt{Q_i} = \sqrt{\bigcap_{i=1}^{n} Q_i} \subseteq \sqrt{P} = P$$

Because P is prime, we see that there must exists some $i \in \{1, \ldots, n\}$ such that $\sqrt{Q_i} \subseteq P$, otherwise, we may construct some $\prod x_i \in \bigcap \sqrt{Q_i} \setminus P$ by selecting $x_i \in \sqrt{Q_i} \setminus P$. If $\sqrt{Q_i}$ is isolated, we are done. If not, then there exists some isolated ideal $\sqrt{Q_j}$ such that $\sqrt{Q_j} \subseteq \sqrt{Q_i}$ and we are done. ■

The second remark gives an example of two distinct irredundant primary decomposition of an ideal. Let $\langle x^2, xy\rangle \subseteq \mathbb{F}[x,y]$. We have

$$\langle x^2, xy\rangle = \langle x\rangle \cap \langle x, y\rangle^2 = \langle x\rangle \cap \langle x^2, y\rangle$$

where

$$y \notin \langle x, y\rangle^2$$

Also, note from Theorem 5.1.2 that

$$\mathrm{Nil}(R) = \bigcap \text{ all minimal primes ideal belonging to } \{0\}$$

Theorem 5.1.3. (Set of zero-divisors is the union of all prime ideals belonging to $\{0\}$) If we let D be set of zero-divisors of R, then

$$D = \bigcup \{I \in \mathrm{Spec}(R) : I \text{ belongs to } \{0\}\}$$

Proof. Clearly,

$$D = \bigcup_{x\neq 0} \sqrt{(\{0\} : x)}$$

This together with Equation 5.2 shows that D is a subset of the union of all prime ideals belonging to $\{0\}$. The converse follows directly from Theorem 5.1.1. ■

We may generalize Theorem 5.1.3 as following. Let $I = \bigcap Q_i$ be an irredundant primary decomposition. Let $\pi : R \to R/I$ be the quotient map. Clearly $\{[0]\} = \bigcap \pi(Q_i)$ forms an irredundant primary decomposition. Therefore, Theorem 5.1.3 implies

$$\bigcup \sqrt{\pi(Q_i)} = \Big\{[x] \in R/I : xy \in I \text{ for some } y \neq 0\Big\}$$

which implies

$$\bigcup \sqrt{Q_i} = \Big\{x \in R : (I : x) \neq I\Big\}$$

Theorem 5.1.4. (Proposition 4.8) Let S be a multiplicatively closed subset of A, and let Q be a P-primary ideal.

$$S \cap P \neq \varnothing \implies S^{-1}Q = S^{-1}A$$

and

$$S \cap P = \varnothing \implies S^{-1}Q \text{ is } P\text{-primary and its contraction in } A \text{ is } Q$$

Proof. If $s \in S \cap P$, then $s^n \in Q$ for some $n > 0$, and $\frac{s^n}{1} \in S^{-1}Q$. Note that

$$\frac{s^n}{1} \cdot \frac{1}{s^n} = \frac{s^n}{s^n} = 1$$

Suppose $S \cap P = \varnothing$. Note that $S^{-1}Q = Q^e$, so to show the contraction of $S^{-1}Q$ is Q, we only have to show

$$Q^{ec} = Q \tag{5.3}$$

Obviously $Q \subseteq Q^{ec}$. We show the opposite. The second part of proposition 3.11 states that

$$Q^{ec} = \bigcup_{s \in S} (Q : s)$$

Because $Q \subseteq P$, if $as \in Q$, then $a \in Q$. Therefore, $a \in (Q : s) \implies a \in Q$. We have shown goal 5.3. Note that the fifth part of proposition 3.11 states that

$$\sqrt{S^{-1}Q} = S^{-1}\sqrt{Q} = S^{-1}P$$

It remains to show $S^{-1}Q$ is indeed primary. Let $\frac{ab}{ss'} = \frac{q}{s''} \in S^{-1}Q$. This implies $(abs'' - qss')t = 0$ for some $t \in S$, which implies $ab(s''t) \in Q$. Because S is closed under multiplication and $S \cap P = \varnothing$, we know $(s''t)^n \notin Q$ for all $n > 0$. This implies $ab \in Q$, which implies $a \in Q$ or some powers of b is an element of Q. We have shown either $\frac{a}{s} \in S^{-1}Q$ or some power of $\frac{b}{s''}$ belongs to $S^{-1}Q$. We have shown $S^{-1}Q$ is indeed primary. ■

5.2 Script 2

Let A and B be two rings. Let M be an A-module, and let N be a (A, B)-**bimodule**. By N being a (A, B)-bimodule, we mean that N not only have both structure of A-module and B-module, but also satisfy $a(bx) = b(ax)$. Consider the tensor product $M \otimes_A N$. For any $b \in B$, we may define a A-bilinear map $M \times N \to M \otimes_A N$ by

$$(m, n) \mapsto m \otimes bn$$

Therefore, by universal property, there exists some unique A-linear map $\widetilde{b} : M \otimes_A N \to M \otimes_A N$. Doing this procedure for each $b \in B$, to claim $M \otimes_A N$ forms a (A, B)-bimodule, it remains to check that

(a) $b(x + y) = bx + by$.

(b) $(b_1 + b_2)x = b_1x + b_2x$.

(c) $(b_1b_2)x = b_1(b_2x)$.

(d) $1_Bx = x$.

(e) $a(bx) = b(ax)$.

Question 1: Exercise 2.15

Let P be a B-module. Find an (A, B)-bimodule isomorphism between

$$(M \otimes_A N) \otimes_B P \text{ and } M \otimes_A (N \otimes_B P)$$

Proof. For each $p \in P$, the A-bilinear map from $M \times N$ to $M \otimes_A (N \otimes_B P)$ defined by $(m, n) \mapsto m \otimes (n \otimes p)$ induce a unique A-linear map $f_p : M \otimes_A N \to M \otimes_A (N \otimes_B P)$ that sends $m \otimes n$ to $m \otimes (n \otimes p)$. By expressing elements of $M \otimes_A N$ as finite sum of basic elements, one can see that f_p is also B-linear. Therefore, if we define $f : (M \otimes_A N) \times P \to M \otimes_A (N \otimes_B P)$ by

$$f(x, p) \triangleq f_p(x)$$

we see that f is B-linear in $M \otimes_A N$. Again, by expressing elements of $M \otimes_A N$ as finite sum of basic elements, one can see that f is also B-linear in P. Therefore, by universal property, there exists some B-linear mapping $\widetilde{f} : (M \otimes_A N) \otimes_B P \to M \otimes_A (N \otimes_B P)$ with action:

$$(m \otimes n) \otimes p \mapsto f_p(m \otimes n) = m \otimes (n \otimes p)$$

Tedious computation by expressing elements of $(M \otimes_A N) \otimes_B P$ into finite sum of basic elements shows that $\widetilde{f}$ is also A-linear. We have shown $\widetilde{f}$ is an (A, B)-bimodule homomorphism.

To finish the proof, one first use similar argument to construct some (A, B)-bimodule homomorphism $\widetilde{g} : M \otimes_A (N \otimes_B P) \to (M \otimes_A N) \otimes_B P$ with action:

$$m \otimes (n \otimes p) \mapsto (m \otimes n) \otimes p$$

And then, see that $\widetilde{g} \circ \widetilde{f} \in \mathrm{End}_{(A,B)}[(M \otimes_A N) \otimes_B P]$ have the identity action on basic elements $x \otimes p$[1] to conclude by universal property that $\widetilde{g} \circ \widetilde{f}$ is the identity function. ■

Let $f : A \to B$ be a ring homomorphism. If N is a B-module, then the A-module structure on N defined by $an \triangleq f(a)n$ is called **restriction of scalars**. If M is an A-module, then the B-module structure on $B \otimes_A M$[a] defined by

$$b(b' \otimes m) \triangleq bb' \otimes m$$

is called **extension of scalars**.

[a] B is given an A-module structure by restriction of scalar.

Question 2: Proposition 2.16

Let A, B be two rings, and let B be an A-module, so we have a ring homomorphism $f : A \to B$ defined by $f(a) \triangleq a1_B$. Let N be a B-module, and give N an A-module structure using restriction of scalars with respect to f.

Show that if N is finitely generated as a B-module and if B is finitely generated as an A-module, then N is finitely generated as an A-module.

Proof. Suppose $n_1, \ldots, n_k$ generate N over B, and suppose $b_1, \ldots, b_m$ generate B over A. We claim $\{b_j n_i\}$ generates N over A. Let

$$b'_i = \sum_{j=1}^{m} a_{i,j} b_j$$

[1] Again, by expressing x as basic element $x = \sum m_i \otimes n_i$.

Compute

$$\begin{aligned}\sum_{i=1}^{k} b_i' n_i &= \sum_{i=1}^{k} \Big(\sum_{j=1}^{m} a_{i,j} b_j \Big) n_i \\ &= \sum_{i=1}^{k} \sum_{j=1}^{m} (a_{i,j} b_j) n_i \\ &= \sum_{i,j} (a_{i,j} b_j) n_i \\ &= \sum_{i,j} a_{i,j} (b_j n_i)\end{aligned}$$

For justification of last equality, compute

$$a(bn) = f(a)(bn) = (f(a)b)n = (ab)n$$

Remark: similar routine computation shows that N is in fact an (A, B)-bimodule. ■

Question 3: Proposition 2.17

Let $f : A \to B$ be a ring homomorphism, and let M be a finitely generated A-module, show that its extension of scalar $B \otimes_A M$ is finitely generated as a B-module.

Proof. Let $\{m_1, \ldots, m_n\}$ generates M over A. We claim $\{1_B \otimes m_i\}$ generate all the basic elements. Consider

$$\begin{aligned}b \otimes \sum a_i m_i &= \sum b \otimes a_i m_i \\ &= \sum b(1_B \otimes a_i m_i) \\ &= \sum b(a_i 1_B \otimes m_i) \quad (\because \ B \text{ is regarded as an } A\text{-module when we write } B \otimes_A M) \\ &= \sum b(f(a_i) \otimes m_i) \\ &= \sum bf(a_i)(1 \otimes m_i)\end{aligned}$$

■

Let $M \xrightarrow{f} M'$ and $N \xrightarrow{g} N'$ be in the category of A-module. The function $h : M \times N \to M' \otimes N'$ defined by

$$h(x, y) \triangleq f(x) \otimes g(y)$$

is clearly A-bilinear. Therefore, we may induce some unique A-linear map $f \otimes g$:

$M \otimes N \to M' \otimes N'$ such that

$$(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$$

Note that for each $M' \xrightarrow{f'} M''$ and $N' \xrightarrow{g'} N''$, we have

$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$$

because they agree on the basic elements.

Question 4: Proposition 2.18 (Exaction of Tensor Product)

If

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \tag{5.4}$$

is an exact sequence of A-modules and homomorphism, then for any A-module N, the sequence

$$M' \otimes N \xrightarrow{f\otimes 1} M \otimes N \xrightarrow{g\otimes 1} M'' \otimes N \to 0$$

is also exact, where $1 \in \mathrm{End}(N)$ is the identity mapping.

Proof. Because g is surjective, we may construct an **right inverse** $g^{-1} : M'' \to M$. That is, $g \circ g^{-1}(m'') = m''$ for all $m'' \in M''$. To see $g \otimes 1$ is surjective, just observe

$$\sum m_i'' \otimes n_i = (g \otimes 1)\Big(\sum g^{-1}(m_i'') \otimes n_i\Big)$$

After computing

$$(g \otimes 1) \circ (f \otimes 1) = (g \circ f) \otimes (1 \circ 1) = 0$$

we may reduce the problem into proving the factored map

$$\mathrm{Coker}(f \otimes 1) \xrightarrow{\widetilde{g}} M'' \otimes N$$

is injective. Consider the map $h : M'' \times N \to \mathrm{Coker}(f \otimes 1)$ defined by

$$h(m'', n) \triangleq [g^{-1}(m'') \otimes n]$$

Clearly, h is linear in n. Using the fact $\mathrm{Im}(f) = \mathrm{Ker}(g)$ and computation

$$g(g^{-1}(am'') - ag^{-1}(m'')) = 0$$
$$g(g^{-1}(m_1'' + m_2'') - g^{-1}(m_1'') - g^{-1}(m_2'')) = 0$$

we may conclude that h is also linear in M''. Now, because h is bilinear, we may induce some linear $\widetilde{h} : M'' \otimes N \to \mathrm{Coker}(f \otimes 1)$ with action

$$\widetilde{h}(m'' \otimes n) = [g^{-1}(m'') \otimes n]$$

Using universal property, it is east to check that $\widetilde{h} \circ \widetilde{g} \in \mathrm{End}(\mathrm{Coker}(f \otimes 1))$ is identity mapping. We have shown $\widetilde{g}$ is injective. ■

Note that the exaction of tensor product holds only for sequence of the form 5.4. One can't delete the zero space at the end and still reach the same conclusion. Consider

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f(x)=2x} \mathbb{Z}$$

where the underlying ring is $\mathbb{Z}$. The sequence

$$0 \longrightarrow \mathbb{Z} \otimes \mathrm{Coker}(f) \xrightarrow{f\otimes 1} \mathbb{Z} \otimes \mathrm{Coker}(f)$$

is not exact, because

$$(f \otimes 1)(x \otimes [y]) = 2x \otimes [y] = x \otimes [2y] = 0$$

implies $\mathrm{Ker}(f \otimes 1) = \mathbb{Z} \otimes \mathrm{Coker}(f)$, while

$$\mathbb{Z} \otimes \mathrm{Coker}(f) \cong \mathrm{Coker}(f) \neq 0$$

An A-module N is said to be **flat** if for any exact sequence

$$\cdots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \to \cdots$$

in the category of A-modules, the sequence

$$\cdots \to M_{i-1} \otimes N \xrightarrow{f_{i-1}\otimes 1} M_i \otimes N \xrightarrow{f_i\otimes 1} M_{i+1} \otimes N \to \cdots$$

is also exact.

Question 5

Show that for an A-module N, the following are equivalents

(a) N is flat.

(b) If $0 \to M' \longrightarrow M \longrightarrow M'' \to 0$ is exact, then $0 \to M' \otimes N \longrightarrow M \otimes N \longrightarrow M'' \otimes N \to 0$ is also exact.

(c) If $f : M' \to M$ is injective, then $f \otimes 1 : M' \otimes N \to M \otimes N$ is injective.

(d) If $f : M' \to N$ is injective and M, M' are finitely generated, then $f \otimes 1 : M' \otimes N \to M \otimes N$ is injective.

Proof. From (a) to (b) is definition. We now prove from (b) to (a). Consider the exact sequence

$$\cdots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \to \cdots$$

We may split this into a short exact sequence

$$0 \longrightarrow \mathrm{Im}(f_{i-1}) \hookrightarrow M_i \xrightarrow{f_i} \mathrm{Im}(f_i) \longrightarrow 0$$

By (b), the short sequence

$$0 \longrightarrow \mathrm{Im}(f_{i-1}) \otimes N \hookrightarrow M_i \otimes N \xrightarrow{f_i \otimes 1} \mathrm{Im}(f_i) \otimes N \longrightarrow 0$$

is also exact. This implies

$$\mathrm{Ker}(f_i \otimes 1) = \mathrm{Im}(f_{i-1}) \otimes N = \mathrm{Im}(f_{i-1} \otimes 1)$$

We have shown

$$\cdots \to M_{i-1} \otimes N \xrightarrow{f_{i-1} \otimes 1} M_i \otimes N \xrightarrow{f_i \otimes 1} M_{i+1} \otimes N \to \cdots$$

is also exact, thus proving (a). From (b) to (c), we simply let $M'' \triangleq \mathrm{Coker}(f)$ and let $M \to M''$ be the quotient map. From (c) to (b) follows from right exaction and

$$\mathrm{Im}(f \otimes 1) = \mathrm{Im}(f) \otimes N = \mathrm{Ker}(g) \otimes N = \mathrm{Ker}(g \otimes 1)$$

From (c) to (d) is clear. It only remains to show from (d) to (c).

Fix

$$u = \sum_{i=1}^{n} x_i \otimes y_i \in \mathrm{Ker}(f \otimes 1)$$

Let M'_0 be the submodule of M' generated by $\{x_1, \ldots, x_n\}$, and let $u'_0 \in M'_0 \otimes N$ be the element

$$u'_0 \triangleq \sum_{i=1}^{n} x_i \otimes y_i \in M'_0 \otimes N$$

By Corollary 2.13, there exists some finitely generated submodule M_0 of M such that $u_0 \in M_0 \otimes N$ defined by

$$u_0 \triangleq \sum_{i=1}^{n} f(x_i) \otimes y_i \in M_0 \otimes N$$

equals to 0. Note that because $\{x_1, \ldots, x_n\}$ generates M_0' and M_0 contains $\{f(x_1), \ldots, f(x_n)\}$, so M_0 contains $f(M_0')$, and obviously

$$f|_{M_0'} : M_0' \to M_0 \text{ is injective.}$$

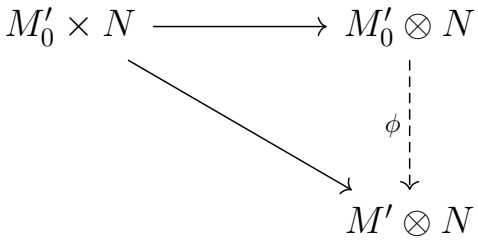
We now see from (d) that

$$f|_{M_0'} \otimes 1 : M_0' \otimes N \to M_0 \otimes N \text{ is injective.}$$

Compute

$$(f|_{M_0'} \otimes 1)(u_0') = \sum_{i=1}^{n} f(x_i) \otimes y_i = u_0 = 0$$

We see $u_0' = \sum_{i=1}^{n} x_i \otimes y_i \in M_0' \otimes N$ is zero. Now consider the universal property



We may see $u = \phi(u_0')$ is zero. Finishing the proof. ■

Question 6: Exercise 2.20

Let ring B be an (A, B)-bimodule, and let M be a flat A-module. Show that the extension of scalar $B \otimes_A M$ is a flat B-module.

Proof. Let $g : P' \to P$ be an injective B-module homomorphism. We are required to show

$$P' \otimes_B (B \otimes_A M) \xrightarrow{g \otimes 1} P \otimes_B (B \otimes_A M)$$

is also injective. We have the isomorphism

$$P' \otimes_B (B \otimes_A M) \cong (P' \otimes_B B) \otimes_A M \cong P' \otimes_A M$$

It now follows from M being flat that $g \otimes 1$ is injective.

■

5.3 Script 1

I proved and gathered the propositions in my paragraphs.

Theorem 5.3.1. (Ideal Quotients are well defined) If we define for each pair I, S of ideals of R their **ideal quotient** by

$$(I : S) \triangleq \{x \in R : xy \in I \text{ for all } y \in S\}$$

Then $(I : S)$ forms an ideal.

Proof. To see $(I : S)$ is closed under addition, let $x, z \in I, y \in S$, and observe

$$(x + z)y = xz + yz \in I$$

To see $(I : S)$ is a multiplicative black hole, let $u \in (I : S), v \in R, s \in S$ and observe

$$(uv)s = v(us) \in I \text{ because } us \in I$$

■

Theorem 5.3.2. (Description of annihilator) Given some ideal I of R, we use the notation $\text{Ann}(I)$ to denote its **annihilator** $(\{0\} : I)$. We have

$$\text{Ann}(I) = \{x \in R : xy = 0 \text{ for all } y \in I\}$$

Proof. Obvious. ■

Given a principal ideal $\langle x \rangle$, we shall always denote its annihilator simply by $\text{Ann}(x)$

Theorem 5.3.3. (Description of the set of zero-divisors) If we denote D the set of zero-divisors of R, we have

$$D = \bigcup_{x \neq 0 \in R} \text{Ann}(x)$$

Proof. If d is a zero-divisor, then $d \in \text{Ann}(s)$ for the $s \neq 0$ that divides 0 with d. If $x \neq 0$ and $y \in \text{Ann}(x)$, then $yx = 0$. ■

Theorem 5.3.4. (An example) Let $R \triangleq \mathbb{Z}, I \triangleq \langle m \rangle$ and $S \triangleq \langle n \rangle$. We have

$$(I : S) = \langle q \rangle$$

Where

$$q = \frac{m}{(m, n)} \text{ and } (m, n) \text{ is the highest common factor of } m \text{ and } n.$$

Proof. To show $\langle q \rangle \subseteq (I : S)$, we only have to show $q \in (I : S)$. Let p be arbitrary integer so pn is an arbitrary element of S. Note that

$$m \mid mp \cdot \frac{n}{(m,n)} = q(pn) \implies q(pn) \in I$$

Because pn is an arbitrary element of S, we have shown $q \in (I : S)$. To show $(I : S) \subseteq \langle q \rangle$, let $p \in (I : S)$. Because $p \in (I : S)$, we know $pn \in I$. That is,

$$m \mid pn$$

Dividing both side with (m, n), we see

$$q \mid p \cdot \frac{n}{(m,n)}$$

Because $q = \frac{m}{(m,n)}$ is by definition coprime with $\frac{n}{(m,n)}$, we can now deduce

$$q \mid p$$

as desired. ■

Question 7

Let I, S, T, V_α be ideals of ring R. Show

(a) $I \subseteq (I : S)$.

(b) $(I : S)S \subseteq I$.

(c) $((I : S) : T) = (I : ST) = ((I : T) : S)$.

(d) $(\bigcap V_\alpha : S) = \bigcap (V_\alpha : S)$.

(e) $(I : \sum V_\alpha) = \bigcap (I : V_\alpha)$.

Proof. Proposition (a) is obvious. Proposition (b) is also obvious once we reduce the problem into proving the single sum xy belongs to I where $x \in (I : S)$ and $y \in S$. For proposition (c), we first show

$$((I : S) : T) \subseteq (I : ST)$$

Because ideal is closed under addition, we only have to prove $xst \in I$ where $x \in ((I : S) : T), s \in S$ and $t \in T$, which follows from noting $xt \in (I : S)$. (done) . Note that

$$(I : ST) \subseteq ((I : T) : S)$$

is obvious. (done) . Lastly, we show

$$((I:T):S) \subseteq ((I:S):T)$$

Let $x \in ((I:T):S), t \in T$ and $s \in S$. We are required to show $xts \in I$, which is obvious since $xs \in (I:T)$. (done) . Proposition (d) is obvious. Let $x \in (I:\sum V_\alpha)$. Fix α and $r \in V_\alpha$. Because $r \in \sum V_\alpha$, we see $xr \in I$. Let x be in the intersection, it is clear that $x\sum v_\alpha = \sum xv_\alpha \in I$ because $xv_\alpha \in I$. ■

Theorem 5.3.5. (Radicals of ideals are well-defined) If I is an ideal of R, then the **radical** of I defined by

$$r(I) \triangleq \{x \in R : x^n \in I \text{ for some } n > 0\}$$

is also an ideal.

Proof. To see $r(I)$ is closed under addition, let $x^n, y^m \in I$, and observe $(x+y)^{n+m} \in I$. To see $r(I)$ is a multiplicative black hole, let $x^n \in I, v \in R$ and observe $(xv)^n = x^n v^n \in I$. ■

Theorem 5.3.6. (Description of Radicals) Let $\pi : R \to R/I$ be the quotient map. We have

$$r(I) = \pi^{-1}(\text{Nil}(R/I))$$

Proof. Obvious. ■

Question 8

(a) $I \subseteq r(I)$.

(b) $r(r(I)) = r(I)$.

(c) $r(IS) = r(I \cap S) = r(I) \cap r(S)$

(d) $r(I) = R \iff I = R$.

(e) $r(I+S) = r(r(I) + r(S))$.

(f) If I is prime, then $r(I^n) = I$ for all $n > 0$.

Proof. Proposition (a) and (b) are obvious. The proposition

$$r(IS) \subseteq r(I \cap S)$$

follows from $IS \subseteq I \cap S$. The propositions

$$r(I \cap S) \subseteq r(I) \cap r(S) \text{ and } r(I) \cap r(S) \subseteq r(IS)$$

are clear, thus proving proposition (c). The proposition

$$I = R \implies r(I) = R$$

is clear, and its converse follows from $1 \in r(I) \implies 1 = 1^n \in I$, thus proving proposition (d). The proposition

$$r(I + S) \subseteq r(r(I) + r(S))$$

is clear. Let $x^n = y + z$ where $y^m \in I$ and $z^p \in S$. We see $x^{n(m+p)} \in I + S$. We have shown

$$r(r(I) + r(S)) \subseteq r(I + S)$$

thus proving proposition (e). Let I be prime. We know $I \subseteq r(I)$. To see the converse, let $x^n \in I$. Because I is prime, either x or x^{n-1} belongs to I. If x does not belong to I, then x^{n-1} belongs to I, which implies either $x \in I$ or $x^{n-2} \in I$. Applying the same argument repeatedly, we see $x \in I$, thus proving $r(I) \subseteq I$. Because

$$I \supseteq I^2 \supseteq I^3 \supseteq I^4 \supseteq \cdots$$

we know

$$r(I) \supseteq r(I^2) \supseteq r(I^3) \supseteq r(I^4) \supseteq \cdots$$

Because

$$x^n \in I \implies x^{nk} \in I^k \text{ for all } k \in \mathbb{N}$$

We now also have

$$r(I) \subseteq r(I^k) \text{ for all } k \in \mathbb{N}$$

This proved proposition (e). ■

Theorem 5.3.7. (Description of radical) Let I be an ideal of R.

$$r(I) = \bigcap \{S \in \text{spec}(R) : I \subseteq S\}$$

5.4 archived

There are essentially two distinct substructures of a ring. A subset of a ring is called a **subring** if it is closed under addition and multiplication and contains the multiplicative identity.
Because the union of a chain of proper ideals is still a proper ideal[2], we may apply **Zorn's Lemma** to show that a **maximal ideal**[3] always exists. Equivalently, we may define a proper ideal I to be maximal if and only if R/I is a field.

Question 9

Show that the sequence

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0 \tag{5.5}$$

is exact if and only if for every module N the sequence

$$0 \longrightarrow \mathrm{Hom}(M'', N) \xrightarrow{\overline{v}} \mathrm{Hom}(M, N) \xrightarrow{\overline{u}} \mathrm{Hom}(M', N) \tag{5.6}$$

is exact.

Proof. Suppose for every module N the sequence 5.6 is exact. To show sequence 5.5 is also exact, we are required to show v is surjective and $\mathrm{Im}(u) = \mathrm{Ker}(v)$. To see v is surjective, let $N \triangleq \mathrm{Coker}(v)$, and use the injectivity of $\overline{v}$ to show that the quotient map $\pi : M'' \to N$ is indeed zero.

To see $\mathrm{Im}(u) \subseteq \mathrm{Ker}(v)$, let $N \triangleq M''$, consider the identity mapping $\mathbf{id}_{M''}$, and note that

$$\overline{u} \circ \overline{v}(\mathbf{id}_{M''}) = \mathbf{id}_{M''} \circ v \circ u = 0$$

To see $\mathrm{Ker}(v) \subseteq \mathrm{Im}(u)$, let $N \triangleq M/\mathrm{Im}(u)$, and let $\pi : M \to N$ be the quotient map. Obviously $\pi \in \mathrm{Ker}(\overline{u}) = \mathrm{Im}(\overline{v})$, so there exists some $\psi : M'' \to N$ such that $\pi = \psi \circ v$. This implies $\mathrm{Ker}(v) \subseteq \mathrm{Ker}(\pi) = \mathrm{Im}(u)$.

Now, suppose sequence 5.5 is exact and let N be some module. To show sequence 5.6 is exact, we are required to show $\overline{v}$ is injective and $\mathrm{Im}(\overline{v}) = \mathrm{Ker}(\overline{u})$. The fact $\overline{v}$ is injective follows from v is surjective.

■

[2] No proper ideals contain 1.
[3] By a maximal ideal, we mean a proper ideal contained by no other proper ideal.

5.5 Mail Draft

Sorry to bother you. At the bottom of page 51 and the top of page 52, Atiyah and Mac-Donald claim that for every primary decomposition

$$I = \bigcap_{i=1}^{n} Q_i \tag{5.7}$$

we may use their Lemma 4.3, which states

$$\sqrt{T_j} = P \text{ for all primary } T_j \in \{T_1, \ldots, T_m\} \implies \sqrt{\bigcap T_j} = P$$

to reduce the decomposition 5.7 into a new decomposition

$$I = \bigcap_{j=1}^{r} Q'_j$$

such that

$$\left\{\sqrt{Q'_1}, \ldots, \sqrt{Q'_r}\right\} \text{ are all distinct}$$

I am quite confused about this. Do they mean that if $\sqrt{Q_1} = \sqrt{Q_2}$, we may use $Q_1 \cap Q_2$ to replace Q_1 and Q_2? If so, they didn't show that $Q_1 \cap Q_2$ will be primary. Obviously, finite intersection of primary ideals need not be primary in general, and the minimal

5.6 Question