Notes on Commutative Algebra

Eric Liu

Contents

Chapter 1

Rings Theory

1.1 Definitions

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 $R \diagup I$ 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 $R \diagup I$ 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 $\text{Nil}(R)$. 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 $\text{spec}(R)$ to denote the set of prime ideals of R. We have

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

Proof. $\text{Nil}(R) \subseteq \bigcap \text{spec}(R)$ is obvious. Suppose $x \notin \text{Nil}(R)$. 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, 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

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

[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 Rings of Fraction

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. Given some multiplicatively closed subset S of A, we may 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 denote the equivalence class of (a, s) by $\frac{a}{s}$, we have a ring structure on $S^{-1}A$ by defining

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

The ring $S^{-1}A$ is called the **ring of fraction**, or the **localization of A by S**.

1.3 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 R/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 1.3.1. (First uniqueness theorem for irredundant primary decomposition) Given some irredundant primary decomposition $I = \bigcap_{i=1}^{n} Q_i$, we have

$$\left\{ \sqrt{Q_i} : 1 \leq i \leq n \right\} = \operatorname{Spec}(R) \cap \left\{ \sqrt{(I : x)} \subseteq R : x \in R \right\} \tag{1.1}$$

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,

$$\sqrt{(I : x)} = \bigcap \sqrt{(Q_i : x)} = \bigcap_{k : x \notin Q_k} \sqrt{Q_k} \tag{1.2}$$

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 3.1 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 Theorem 3.1.1, 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 a **minimal** prime ideal belonging to I.

Chapter 2

Modules

2.1 Modules

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

Let M be a R-module, and let N be a subset of M. We say N is a R-**submodule** if N is closed under both addition and R-scalar multiplication, or equivalently, if N is the kernel of some R-module homomorphism. Just like how ideal is proved to be kernel of some ring homomorphism, to see submodule is the kernel of some R-module homomorphism, we simply construct the **quotient module** M/N, and get the quotient map $\pi : M \to M/N$ that is a R-module homomorphism with kernel N, and get also the bijection

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

between the collection of the R-submodules of M that contains N and the collection of the R-submodule of $M \setminus N$, 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 R-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 all modules and submodules are over R in this section.

Given a subset E of M, clearly its **span**, the set of finite sum $\sum rx$ where $x \in E$, forms a submodule. We say M is **finitely generated** if M can be spanned by a finite set.

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.

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 $R^{(I)}$.

Given an ideal $\mathfrak{a}$ of R, some R-module M and some R-submodule N of M, the **product of the R-submodule N by the ideal $\mathfrak{a}$** is the set of finite sum $\sum a_i x_i$ where $a_i \in \mathfrak{a}$ and $x_i \in N$. We denote such set by $\mathfrak{a}N$, and $\mathfrak{a}N$ clearly forms a R-submodule of M.

2.2 Tensor Product of Modules

Let R be some ring. Given a finite collection $\{M_1, \dots, M_n\}$ 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

$$\begin{tikzcd} \prod M_i \arrow[r, "\otimes"] \arrow[dr, "f"'] & \bigotimes M_i \arrow[d, dashed, "\widetilde{f}"] \\ & P \end{tikzcd}$$

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:

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

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

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

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**[1], 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 $\overline{f}(\sum r(x_1, \dots, x_n)) \triangleq \sum rf(x_1, \dots, x_n)$, 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.

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

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

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

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

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

2.3 Rings and Modules of Fraction

2.4 Primary Decomposition Theorem

Chapter 3

Scripts

3.1 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 3.1.1. (First uniqueness theorem for irredundant primary decomposition) Given some irredundant primary decomposition $I = \bigcap_{i=1}^{n} Q_i$, we have

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

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 3.1 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 Theorem 3.1.1, we may well define the following notions. Given some decomposable ideal I, we say the prime ideals $\{\sqrt{Q_1}, \dots, \sqrt{Q_n}\}$ **belong** to I, and if $\sqrt{Q_i}$ is a minimal element of $\{\sqrt{Q_1}, \dots, \sqrt{Q_n}\}$, then we say $\sqrt{Q_i}$ is a **minimal** prime ideal belonging to I.

Theorem 3.1.2. (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

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

Proof. Clearly,

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

This together with Equation 3.2 shows that D is a subset of the union of all prime ideals belonging to $\{0\}$. The converse follows directly from Theorem 3.1.1. ∎

We may generalize Theorem 3.1.2 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 3.1.2 implies

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

which implies

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

Theorem 3.1.3. (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

$$Q^{ec} = Q \tag{3.3}$$

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 3.3. 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. ■

3.2 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 $n_1, \dots, n_k$ generate N over B, and suppose $b_1, \dots, b_m$ 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 $\{m_1, \dots, m_n\}$ generates M over A. We claim $\{1_B \otimes m_i\}$ generate all the basic elements. Consider

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

■

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

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \tag{3.4}$$

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 $1 \in \text{End}(N)$ 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

$$\text{Coker}(f \otimes 1) \xrightarrow{\tilde{g}} M'' \otimes N$$

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

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

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

$$\begin{aligned} g(g^{-1}(am'') - ag^{-1}(m'')) &= 0 \\ g(g^{-1}(m''_1 + m''_2) - g^{-1}(m''_1) - g^{-1}(m''_2)) &= 0 \end{aligned}$$

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

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

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

Note that the exaction of tensor product holds only for sequence of the form 3.4. 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

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

is not exact, because

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

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

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

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

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

By (b), the short sequence

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

is also exact. This implies

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

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 $M'' \triangleq \operatorname{Coker}(f)$ and let $M \to M''$ be the quotient map. From (c) to (b) follows from right exaction and

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

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

Fix

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

Let M_0' be the submodule of M' generated by $\{x_1, \dots, x_n\}$, 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 $\{x_1, \dots, x_n\}$ generates M_0' and M_0 contains $\{f(x_1), \dots, f(x_n)\}$, 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

$$\begin{tikzcd}
M_0' \times N \arrow[r] \arrow[dr] & M_0' \otimes N \arrow[d, dashed, "\phi"'] \\
& M' \otimes N
\end{tikzcd}$$

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.

∎

3.3 Script 1

I proved and gathered the propositions in my paragraphs.

Theorem 3.3.1. (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 3.3.2. (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 3.3.3. (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 3.3.4. (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 3.3.5. (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 3.3.6. (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 3.3.7. (Description of radical) Let I be an ideal of R.

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

3.4 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

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0 \tag{3.5}$$

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

$$0 \longrightarrow \text{Hom}(M'', N) \xrightarrow{\overline{v}} \text{Hom}(M, N) \xrightarrow{\overline{u}} \text{Hom}(M', N) \tag{3.6}$$

is exact.

Proof. Suppose for every module N the sequence 3.6 is exact. To show sequence 3.5 is also exact, we are required to show v is surjective and $\text{Im}(u) = \text{Ker}(v)$. To see v is surjective, let $N \triangleq \text{Coker}(v)$, and use the injectivity of $\overline{v}$ to show that the quotient map $\pi : M'' \to N$ is indeed zero.

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

Now, suppose sequence 3.5 is exact and let N be some module. To show sequence 3.6 is exact, we are required to show $\overline{v}$ is injective and $\text{Im}(\overline{v}) = \text{Ker}(\overline{u})$. 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.

3.5 Mail Draft

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

$$I = \bigcap_{i=1}^{n} Q_i \tag{3.7}$$

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 3.7 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