Notes on Commutative Algebra

Eric Liu

Contents

Chapter 1

Untitled

1.1 Rings and Ideals

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 $y \in S$.

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.

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

1.2 Script 1

I proved and gathered the propositions in my paragraphs.

Theorem 1.2.1. (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 1.2.2. (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 1.2.3. (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 1.2.4. (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 1

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 $x \sum v_\alpha = \sum x v_\alpha \in I$ because $x v_\alpha \in I$. ■

Theorem 1.2.5. (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 1.2.6. (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 2

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

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

1.3 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[5], we may apply **Zorn's Lemma** to show that a **maximal ideal**[6] always exists. Equivalently, we may define a proper ideal I to be maximal if and only if R/I is a field.

[5] No proper ideals contain 1.

[6] By a maximal ideal, we mean a proper ideal contained by no other proper ideal.