Commutative Algebra

Seminar Note

Liyve

2025-06-25

Abstract

Note about [1, Introduction to Commutative Algebra].

## 1 Rings and Ideals

### 1.1 Rings and Ring Homomorphisms

**Definition 1 (Ring)** A ring is a set with two binary operations, usually called addition and multiplication, such that:

1. is an abelian group,
2. is a semigroup,
3. Multiplication is distributive over addition: for all , and .
4. Multiplication is commutative: for all , .
5. There exists a multiplicative identity such that for all , .

**Definition 2 (Ring Homomorphism)** A ring homomorphism is a mapping between rings and such that for all :

1. ,
2. ,
3. .

### 1.2 Ideals and Quotient Rings

**Definition 3 (Ideal)** An ideal of a ring is a subset such that:

1. is a subgroup of ,
2. For all and , both and are in (i.e., is closed under multiplication by elements of ).

**Definition 4 (Quotient Ring)** The quotient ring is defined as follows: Let be a ring and an ideal of . The set of cosets

forms a ring with operations defined by

The natural projection given by is a surjective ring homomorphism with kernel .

**Proposition 1 (Correspondence of Ideals)** Let be a ring and an ideal. There is a bijective correspondence between the set of ideals of containing and the set of ideals of the quotient ring .

Explicitly, for each ideal of with , the image is an ideal of . Conversely, for each ideal of , its preimage under the natural projection is an ideal of containing .

This correspondence preserves inclusion, sums, intersections, and properties such as being prime or maximal (with suitable conditions).

**Definition 5 (Kernel)** Let be a ring homomorphism. The kernel of , denoted , is the set

where is the additive identity in . The kernel is an ideal of .

**Definition 6 (Image)** Let be a ring homomorphism. The image of , denoted , is the set

which is a subring of .

### 1.3 Zero-Divisors, Nilpotent Elements and Units

**Definition 7 (Zero Divisor)** Let be a ring. An element , , is called a **zero-divisor** if there exists a nonzero such that or .

**Definition 8 (Integral Domain)** A ring is called an **integral domain** if and has no zero-divisors; that is, for all , if , then either or .

**Definition 9 (Nilpotent)** Let be a ring. An element is called **nilpotent** if there exists a positive integer such that .

**Definition 10 (Unit)** An element of a ring is called a **unit** if there exists such that , where is the multiplicative identity in . The set of all units in is denoted by .

**Definition 11 (Principal Ideal)** An ideal of a ring is called a **principal ideal** if there exists an element such that

That is, is generated by a single element .

**Proposition 2** Let , then TFAE:

1. A is a field
2. the only ideals in are and .
3. is injective.

*Proof*.

:

Let . If , then is a unit ,

:

The kernel is either or . If , then is the zero map, so , contradicting . Thus, , so is injective.

:

Let be not a unit. . Let , .

### 1.4 Prime Ideals and Maximal Ideals

**Definition 12 (Prime Ideal)** An ideal in is prime if and if .

**Definition 13 (Maximal Ideal)** An ideal in is maximal if and there is no ideal s.t. .

**Proposition 3**

1. is prime ideal is integral domain.
2. is maximal ideal is field. Hence maximal ideals are prime.
3. Let is ring homomorphism. is a prime ideal in , then is prime in .

*Proof*.

:

Omitted. cf.[2, Ch. 3, Sec.4, p.110, thm.7, thm.8]

:

You can consider the preimage . If , then . Since is prime, or , so or .

In particular, you can consider .

*Remark*. Note that if is maximal, then is a maximal ideal of if is surjective. In general, the preimage of a maximal ideal under a ring homomorphism need not be maximal unless the map is surjective.

Let be the natural embedding, . is a field, is maximal, but its preimage in is properly contained in , for any .

**Lemma 1 (Zorn’s lemma)** Let be a non-empty partially ordered set such that every chain (i.e., totally ordered subset) in has an upper bound in . Then contains at least one maximal element; that is, there exists such that if for some , then .

**Theorem 1 (Existence of Maximal Ideals)** Every nonzero ring with has at least one maximal ideal.

*Proof*. Let be the set of all proper ideals of , partially ordered by inclusion. is nonempty since is a proper ideal (as ). Any chain of ideals in has an upper bound given by the union of the chain, which is again a proper ideal. By Zorn’s Lemma, has a maximal element, which is a maximal ideal of .

**Corollary 1 (Every Ideal is Contained in a Maximal Ideal)** If be a proper ideal of , then is maximal, s.t. .

*Proof*. Let be a proper ideal of (i.e., ). Consider the quotient ring . By the existence of maximal ideals, has a maximal ideal . The preimage under the natural projection is a maximal ideal of containing .

**Corollary 2 (Every Non-Unit is Contained in a Maximal Ideal)** Every non-unit element of is contained in some maximal ideal of . Let be a non-unit. Then the ideal generated by is a proper ideal, i.e., . By the previous corollary, there exists a maximal ideal such that . Thus, .

*Proof*. Let be the set of all proper ideals of , partially ordered by inclusion. is nonempty since is a proper ideal (as ). Any chain of ideals in has an upper bound given by the union of the chain, which is again a proper ideal. By Zorn’s Lemma, has a maximal element, which is a maximal ideal of .

**Definition 14 (Local Ring)** A ring is called a **local ring** if it has a unique maximal ideal . That is, there exists exactly one maximal ideal in .

**Definition 15 (Residue Field)** Let be a local ring with unique maximal ideal . The **residue field** of is the quotient ring

which is a field. The natural projection is called the **residue map**.

**Proposition 4**

1. Let be a ring and , s.t. is a unit. Then is a local ring, and is maximal.
2. Let be a ring and maximal ideal of , s.t. is a unit of . Then is a local ring.

*Proof*.

:

Every non-unit is contained in . Hence is the only maximal ideal.

:

. If , take . . is a unit. Then . Contradiction!

**Definition 16 (Semi-local Ring)** A ring is called **semi-local** if has only finitely many maximal ideals.

**Definition 17 (PID)** An integral domain is called a **principal ideal domain (PID)** if every ideal of is principal; that is, for every ideal , there exists such that .

**Proposition 5** In PID, is prime is maximal.

*Proof*. If is prime. Let . Then s.t. . $

### 1.5 Nilradical and Jacobson Radical

**Proposition 6**

1. The set of all nilpotent elements of is an ideal.
2. And has no non-zero nilpotent element.

*Proof*.

:

If , then . , then

:

If , .

**Definition 18 (Nilradical)** The set is called **Nilradical** of .

**Proposition 7** The nilradical of a ring is equal to the intersection of all prime ideals of

That is, an element is nilpotent if and only if belongs to every prime ideal of .

Let

We need to show

*Proof*.

:

If , then for any . It implies for any .

:

Suppose , . Let

Let be a totally ordered chain in . Consider . We claim that .

* is an ideal: Since is a chain, the union of the ideals in is again an ideal.
* For all , if , then for some , contradicting the definition of .

Thus, every chain in has an upper bound, so by Zorn’s Lemma, has a maximal element, say . We claim that is a prime ideal.

Suppose . Then the ideals and strictly contain , so by maximality, there exist such that and . Thus,

for some , . Then

Expanding and using that is an ideal, all terms except are in , so

Thus, , so by maximality, for some , but by construction, so .

Therefore, is a prime ideal not containing any power of , contradicting . Thus, .

**Definition 19 (Jacobson Radical)** Let be the intersection of all maximal ideals of :

This ideal is called the **Jacobson radical** of .

**Proposition 8** is a unit in for all

*Proof*. : Suppose , but is not a unit for some . Then the ideal is proper, so it is contained in some maximal ideal . Thus, . But , so , hence , which is impossible since is proper. Therefore, must be a unit for all .

:

Suppose for some maximal ideal . Then the ideal generated by and is the whole ring: . This means there exist and such that , or equivalently, . Since is maximal, is not a unit only if it lies in some maximal ideal, but by assumption , so cannot be non-invertible. Therefore, if is a unit for all , then must be contained in every maximal ideal, i.e., .

### 1.6 Operations on Arbitrary Families of Ideals

Let be a family of ideals in a ring .

**Definition 20 (Sum of Ideals)** The **sum** is defined as:

**Definition 21 (Intersection of Ideals)** The **product** is defined as:

(For infinite families, the product is usually defined only for finite subfamilies.)

**Definition 22 (Product of Ideals)** The **intersection** is defined as:

1. Distributive law:
2. Modular law:

* In general, we have . Clearly,, hence provided .

**Definition 23 (Coprime)** Let be ideals of . We call are coprime, when .

**Definition 24 (Direct Product of Rings)** Let be a family of rings. The **direct product** is defined as

with addition and multiplication defined componentwise:

for all .

Let be rings, and let be the projection onto the -th component, defined by .

**Definition 25 (Chinese Remainder Map)** Let be a family of ideals of . Define the canonical ring homomorphism

where each component is the natural projection , .

This map is a ring homomorphism, called the **Chinese Remainder map** associated to the family .

**Proposition 9** Let be a family of ideals of .

1. , are coprime, then .
2. is surjective are coprime.
3. is injective .

*Proof*. Omitted. cf.[1, Ch. 1, sec.6, p.7, prop.1.10].

**Theorem 2 (Chinese Remainder Theorem)** Let be a ring and be ideals of such that for all (i.e., the ideals are pairwise coprime). Then the canonical map

is surjective, and its kernel is . Thus,

as rings.

In particular, if and the with for , then

*Proof*. Let be the canonical map, .

* **Kernel:** , since iff for all .
* **Surjectivity:** For any , we want such that for all .

Since the ideals are pairwise coprime, for each there exists such that and for . (This follows from the Chinese Remainder construction: for each , let , then , so with , ; set .)

Then set . For each , , since and for .

Thus, is surjective.

* **Isomorphism:** By the First Isomorphism Theorem, .

Therefore,

*Remark*. The union of ideals is not necessarily an ideal unless one contain the others.

In general, the union fails to be closed under addition. For example, in , the ideals and have union , but and , yet .

**Proposition 10**

1. Let be prime ideals and let be an ideal contained in . Then for some .
2. Let be ideals and let be a prime ideal containing . Then for some . If , then for some .

*Proof*. Omitted. cf.[1, Ch. 1, sec.6, p.8, prop.1.11].

**Definition 26 (Quotion of Ideals)** The set is **quotien** of and . This set is an ideal of .

If is a principal ideal of , then is denoted by .

**Definition 27 (Annihilator)** The set is called the **annihilator** of . It is denoted by .

**Proposition 11 (Zero-Divisors)** The set of zero-divisors of a ring is the set

This set is not necessarily an ideal, but it is a union of ideals of .

Moreover, it is a union of prime ideals of .

where the union is taken over all prime ideals of .

In particular, every zero-divisor lies in some prime ideal.

**Definition 28 (Radical of an Ideal)** Let be an ideal of a ring . The **radical** of , denoted or , is defined as

That is, is in the radical of if some power of lies in . The radical is itself an ideal of .

If , then is the set of all nilpotent elements, i.e., the nilradical of .

**Proposition 12**

1. .
2. .
3. .
4. .
5. .
6. If is prime, for all .

*Proof*. Left to the reader. (Easy to check)

**Proposition 13**

.

**Hint:** Consider nilradical of the quotient ring , and the corresponding of ideals.

*Proof* (Proof.1). Let be the canonical projection. By the Correspondence Theorem, there is a bijection between the set of prime ideals of containing and the set of prime ideals of .

The nilradical of , denoted , is the intersection of all prime ideals of :

The preimage of this intersection under is the intersection of all prime ideals of containing :

On the other hand, consists of all elements such that for some , i.e., . Thus,

Therefore,

*Proof* (Proof.2). Let . Then for some . For any prime ideal , since is prime and , it follows that . Thus, is in every prime ideal containing , so .

Conversely, suppose . Then for all . Consider the quotient ring and the image of . Then for all . By the proof of the nilradical as intersection of primes, there exists a prime ideal of not containing any power of . The preimage of under the projection is a prime ideal of containing but not . Thus, .

Therefore, .

**Definition 29 (Radical of a Subset)** More general, let be any subset of a ring . The **radical** of , denoted or , is defined as the intersection of all prime ideals of containing :

**Proposition 14**

### 1.7 Extension and Contraction of Ideals

Let be a ring homomorphism.

**Definition 30 (Extension)** Given an ideal , the **extension** of to is the ideal

That is, is the ideal of generated by the image of .

**Definition 31 (Contraction)** Given an ideal , the **contraction** of to is the ideal

**Proposition 15**

1. The extension of an ideal is always an ideal; the contraction of an ideal is always an ideal.
2. If , then .
3. If , then .
4. The set , and , then , and .
5. There is a correspondence between ideals of and ideals of that are stable under extension and contraction, i.e., there is a bijective between and .
6. If is surjective, then every ideal of is the extension of its contraction.
7. The contraction of a prime ideal of is a prime ideal of .
8. The extension of a prime ideal of need not be prime in .

*Proof*. Left to the reader. (Easy to check) cf.[1] {{ch.1, sec.7, p.10, prop.1.17}}

### 1.8 Spectrum and Zariski Topology

**This section all of proofs will be omitted, since we have discussed in seminar**

**Definition 32 (Spectrum of a Ring)** The **spectrum** of a ring , denoted , is the set of all prime ideals of :

**Proposition 16 (Toplogy Structure of Spectum)** Let be a ring and let be the set of all prime ideals of . For each subset of , let . Then we have: - If is the ideal generated by , . - ; . - . - .

**Definition 33 (Zariski Topology)** The spectrum is equipped with the **Zariski topology**, where the closed sets are of the form

for some subset .

In particular, for an ideal , .

**Proposition 17 (Open set of Spectum)** For each , let denote complement of in . 0. The basic open sets are complements of for : . The basic open sets is a basis of Zariski topology.

1. .
2. is nilpotent.
3. is a unit.
4. .
5. Each is quasi-compact.
6. An open subset of is quasi-compact if and only if it is a finite union of basic open sets for some .

**Proposition 18 (Closures of Spectum)** Denote a prime ideal of by a letter or when thinking of it as a point of . When thinking of as a prime ideal of , we denote it by .

1. The set is closed in is maximal.
2. .
3. is a -space.

*Remark*. The Zariski topology is generally not Hausdorff; its closed sets are typically large. The points corresponding to maximal ideals are called **closed points**.

**Proposition 19 (Irreducible)** A topology space is said **irreducible** if and if every pair of non-empty open sets in intersect, or equivalently if every non-emtpy open set is dense in .

1. is irreducible if and only if the nilradical of is a prime ideal.
2. If is an irreducible subspace of , then the closure of in is irreducible.
3. Every irreducible subspace of is contained in a maximal irreducible subspace.
4. The maximal irreducible subspaces of are closed and cover . They are called the **irreducible components** of .
5. The irreducible components of are the closed sets , where is a minimal prime ideal of .

*Remark*. Let is ring. Then has the minimal prime ideal with respect to inclusion. (You can consider Zorn’s lemma to prove this remark)

**Definition 34 (Induced Map on Spectra)** The map induces a map on spectra:

where denotes the set of all prime ideals of .

### 1.9 Affine Algebraic Varieties

Let be a field. An **affine algebraic variety** over is a subset defined as the common zeros of a set of polynomials:

for some subset .

The set of all polynomials vanishing on is an ideal:

There is a correspondence between affine varieties and radical ideals of (Hilbert’s Nullstellensatz).

The coordinate ring of is defined as

which encodes the algebraic structure of .

## 2 Modules

### 2.1 Modules and Module Hom

**Definition 35 (Module)** Let be a ring. An **-module** is an abelian group together with an action , , such that for all and :

1. (if has )

**Definition 36 (Submodule)** A **submodule** of an -module is a subgroup such that for all , .

**Definition 37 (Module Homomorphism)** Let be -modules. A map is an **-module homomorphism** if for all and :

The set of all -module homomorphisms from to is denoted .

Moreover, the set forms an abelian group under pointwise addition:

for all and .

If is commutative, then is itself an -module, with scalar multiplication defined by

for , , and .

### 2.2 Submodules and Quotient Modules

**Definition 38 (Quotient Module)** If is a submodule, the **quotient module** is the abelian group of cosets with -action .

**Theorem 3 (Correspondence Theorem for Submodules)** Let be an -module and a submodule. There is a bijective correspondence between the set of submodules of containing and the set of submodules of the quotient module .

**Definition 39 (Kernel, Image and Cokernel)** Let be an -module homomorphism.

* The **kernel** is , a submodule of .
* The **image** is , a submodule of .
* The **cokernel** is .

**Proposition 20 (First Isomorphism Theorem)** Let be an -module homomorphism. Then

as -modules.

*Proof*. Define by . This map is well-defined, -linear, and bijective.

### 2.3 Operation of Submodule

Let be an -module, and let be a family of submodules of .

**Definition 40 (Sum of Submodules)** The **sum** of submodules is defined as:

This is the smallest submodule of containing all the .

**Definition 41 (Intersection of Submodules)** The **intersection** of submodules is:

This is the largest submodule contained in all the .

**Proposition 21 (Lattice Structure)** The set of submodules of forms a lattice under sum and intersection:

* is the least upper bound (join) of and .
* is the greatest lower bound (meet).

**Proposition 22 (Second Isomorphism Theorem)** Let be an -module, and let be submodules of . Then

as -modules.

*Proof*. Define the map by . This is an -module homomorphism with kernel , and it is surjective. By the First Isomorphism Theorem, .

**Proposition 23 (Third Isomorphism Theorem)** Let be an -module, and let be submodules. Then

as -modules.

*Proof*. Consider the natural map given by . This is a well-defined -module homomorphism with kernel . By the First Isomorphism Theorem, .

**Definition 42 (Submodule Generated by a Subset)** Given a subset , the submodule generated by is:

This is the smallest submodule of containing .

**Definition 43 (Product of Ideal and Submodule)** Let be a ring, an -module, an ideal, and a submodule. The **product** is defined as the submodule of generated by all products with , :

This is the smallest submodule of containing all elements with , .

**Definition 44 (Quotient of Submodules)** , then is an ideal of .

**Definition 45 (Annihilator of a Module)** Let be an -module. The **annihilator** of is

which is an ideal of .

**Proposition 24** If , then is also -module. The multiplication defined by , It’s easy to check well-defined.

**Definition 46** If , then -module is faithful.

If , then is faithful as a -module.

### 2.4 Direct Sum and Direct Product

**Definition 47 (Direct Sum and Direct Product of Modules)** Let be a family of -modules.

* The **direct product** is the set of all tuples with , with addition and scalar multiplication defined componentwise.
* The **direct sum** is the subset of the direct product consisting of tuples such that for all but finitely many .

Both and are -modules.

### 2.5 Finitely Generated Module

**Definition 48 (Finitely Generated Module)** An -module is **finitely generated** if there exist elements such that every can be written as

for some . In other words, .

**Definition 49 (Free Module)** Let be a ring and a set. The **free -module** on , denoted , is the set of all functions such that for all but finitely many . Equivalently, elements of are finite formal sums

where , , and is the function with .

is an -module with addition and scalar multiplication defined componentwise.

If is finite with elements, then as -modules.

A module is **free** if it is isomorphic to a free module on some set ; that is, for some .

**Proposition 25** An -module is finitely generated if and only if there exists an integer and a submodule such that .

*Proof* (Proof Sketch:). If is finitely generated by , define a surjective -module homomorphism by . Then . Conversely, any quotient of is finitely generated.

**Proposition 26** A quotient of a finitely generated module is finitely generated.

*Proof*. Hint: Let be generated by and . Then is generated by the images of in .

**Theorem 4 (Hamilton-Cayley Theorem)** Let be a finitely generated -module. Let , and let be an -module endomorphism such that . Then there exist (for some ) such that

as endomorphisms of .

*Proof*. Let be generated by . Since , for each ,

with . Let be the matrix over representing in this basis.

Consider the -module homomorphism given by , where is the identity. By the Cayley-Hamilton theorem for modules, the characteristic polynomial with annihilates :

as endomorphisms of .

**Corollary 3** Let be a finitely generated -module and such that . Then there exists with such that .

*Proof*. Take . There exists since [Theorem 4](#thm-hamilton-cayley), let .

**Theorem 5 (Nakayama’s lemma)** Let be a finitely generated -module and , if , then implies .

*Proof*. By [Corollary 3](#cor-hamilton-cayley), if and , then there exists with such that . That is, for some , and .

But is a unit in (since and [Proposition 8](#prp-jacobson)). Therefore, is invertible, so implies .

**Corollary 4** Let be a finitely generated -module, is a submodule of , , if , then implies .

*Proof*. Consider the quotient module . Since , we have

so . By [Theorem 5](#thm-nakayama-lemma), since and is finitely generated, it follows that , i.e., .

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*. CRC Press, 2018.

[2] 聂灵沼, *代数学引论*. 高等教育出版社, 2021.