

# Introductory Lecture on Commutative Algebra

May 24, 2009

## 1 Rings

We will review some commutative algebra that is needed for the lecture series Algebraic Geometry by James D. Lewis. We will start with the definition of a ring.

Ring  $R$  = Elements + Addition + Multiplication + Certain Properties

### Properties:

1. With respect to addition  $R$  must be an abelian group. This will guarantee that  $R$  has a zero element, every element has an additive inverse (hence we will be able to do subtraction as well) and the order of the addition is not important.
2. Multiplication must be associative, i.e.  $(xy)z = x(yz)$ . So we do not need to worry about the order we multiply.
3. Multiplication must be distributive over addition, i.e.  $x(y + z) = xy + xz$ ,  $(y + z)x = yx + zx$ . So we do not have to worry if we add first or multiply first.

**Example 1**  $\mathbb{Z}_+ = \{0, 1, 2, 3, \dots\}$  with the usual addition and multiplication, is not a ring since the first property fails because of not having additive inverses. By adding additive inverse of each element to this set we get the ring  $\mathbb{Z}$ .

We will be working with commutative rings with identity. For this our ring  $R$  must satisfy two additional properties

- (i) For all  $x, y \in R$  we must have  $xy = yx$  (commutativity)
- (ii) There exists  $1 \in R$ , identity element such that for all  $x \in R$ ,  $x1 = 1x = x$ . The identity element is unique.  
(Let  $1, 1'$  be two identity elements of  $R$ , then  $1 \times 1' = 1 \Rightarrow 1 \times 1' + (-1) = 1 + (-1) = 0 \Rightarrow 1 \times 1' + 1(-1) = 0 \Rightarrow 1(1' + (-1)) = 0 \Rightarrow 1' = -(-1) = 1$ )

**Remark 2** 1. If  $R$  is a ring with identity then the distributive law forces  $R$  to be abelian group with respect to addition. (This can be shown by applying distributive condition to  $(1 + 1)(a + b)$  for any  $a, b \in R$ )

2. The zero ring,  $0$ , is a commutative ring with identity as taking  $1 = 0$ . This is the only ring with this property. If you want to exclude the zero ring then make the assumption  $1 \neq 0$ .

Let us see more examples:

**Example 3** (a) Let  $M(\mathbb{R})_{n \times n}$  = set of all  $n \times n$  real matrices. Then  $M(\mathbb{R})_{n \times n}$  with the usual matrix addition and multiplication is a non-commutative ring with identity. ( $AB \neq BA, 1 = I, 0 = 0$ )

(b) In fact, one of the first non-commutative rings was discovered by Sir William Rowan Hamilton in 1843, the (real) Hamilton Quaternions. This is a non-commutative ring with identity and denoted by  $\mathbb{H} = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j\}$ . Addition is the componentwise addition and multiplication is by expansion. [DF, pg:224]

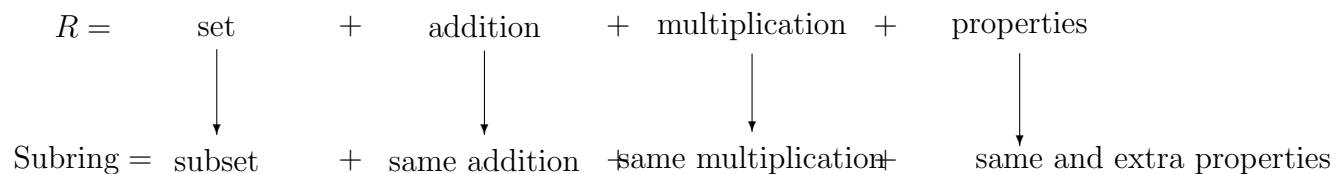
(c)  $2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \dots\}$  with the usual addition and multiplication is a commutative ring without identity

(d)  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  with the usual addition and multiplication is a commutative ring with identity

(e)  $\mathbb{C}[x] = \{f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 | a_i \in \mathbb{C}, n \in \mathbb{Z}_+\}$  with the usual polynomial addition and multiplication is a commutative ring with identity.

(f)  $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}, i = \sqrt{-1}\}$  (introduced by Gauss around 1800s [DF]) with the usual complex addition and multiplication is a commutative ring with identity.

From now on ring will mean commutative ring with identity.



The extra property of a subring is being closed under addition and multiplication with the ring's identity. (That is when we add or multiply two elements we want the result to stay inside the subset and this subset be a ring by itself.)

**Example 4** 1. If  $S$  is a subring of  $R$  then  $S[x]$  is a subring of  $R[x]$ , hence  $\mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}[x]$  are all subrings of  $\mathbb{C}[x]$ .

2. The ring of all continuous functions from  $\mathbb{R}$  to  $\mathbb{R}$  is a subring of all functions from  $\mathbb{R}$  to  $\mathbb{R}$ .

Now the next step is relating two rings to each other. How we will do this?

Ring homomorphism is a tool that can be used for relating two rings

ring homomorphism = a map that respects the properties of a ring

**Definition 5** Let  $R$  and  $S$  be two rings.  $f : R \longrightarrow S$  is called a ring homomorphism if

$$(a) \ f(x + y) = f(x) + f(y) \text{ for all } x, y \in R$$

$$(b) \ f(xy) = f(x)f(y) \text{ for all } x, y \in R$$

$$(c) \ f(1) = 1$$

**Remark 6** One can show  $f(0) = 0$  and  $f(-x) = -f(x)$  for all  $x \in R$ .

$$(f(0 + 0) = f(0) + f(0) \Rightarrow f(0) = f(0) + f(0) \Rightarrow f(0) = 0,$$

$$f(x + (-x)) = f(x) + f(-x) \Rightarrow f(0) = f(x) + f(-x) \Rightarrow 0 = f(x) + f(-x) \Rightarrow f(-x) = -f(x))$$

**Example 7** 1.  $S$  be a subring of  $R$ , then  $\text{id} : S \hookrightarrow R$  is an injective ring homomorphism

2.  $\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}, n \longrightarrow n \pmod{2}$  is a surjective ring homomorphism

3.  $\mathbb{R}^2 \longrightarrow \mathbb{C}, (x, y) \longrightarrow x + iy$  is a bijective ring homomorphism (= isomorphism) with the multiplication  $(x, y)(z, w) = (xz - yw, xw + yz)$

We can take composition of ring homomorphisms let  $f : A \longrightarrow B$   $g : B \longrightarrow C$  be ring homomorphisms, then  $g \circ f : A \longrightarrow C$  is also a ring homomorphism.

**Proof.** Take any  $a_1, a_2 \in A$ , and consider  $(g \circ f)(a_1 + a_2) = g(f(a_1 + a_2)) = g(f(a_1) + f(a_2)) = g(f(a_1) + f(a_2)) = gf(a_1) + gf(a_2)$ .

Then consider  $(g \circ f)(a_1 a_2) = g(f(a_1 a_2)) = g(f(a_1)f(a_2)) = gf(a_1)gf(a_2)$ .

$$(g \circ f)(1) = g(f(1)) = g(1) = 1 \quad \blacksquare$$

## 2 Ideals

We saw

$$\begin{array}{lcl} \text{set} & + & \text{properties} = \text{Ring} \\ \text{subset} & + & \text{properties} = \text{Subring} \end{array}$$

Now we will see a new object subset + new properties = Ideal.

**Definition 8**  $a \subseteq R$  is called ideal of  $R$  if  $a$  is an additive subgroup (i.e. for  $x, y \in a$ ,  $x + y \in a$ ,  $0 \in a$ ,  $-x \in a$ ) and is such that  $Ra \subseteq a$  (i.e.  $\forall r \in R, \forall x \in a, rx = xr \in a$ ).

So right ideal=left ideal=ideal, as our ring is commutative. Ideals will play an important role in the lectures Algebraic Geometry.

**Remark 9** We can choose an element  $x \in R$  and then the set  $\{rx | r \in R\}$  will be an ideal. This ideal is denoted by  $xR$  or  $(x)$  and called the ideal generated by  $x$ .

**Definition 10** Let  $X$  be a subset of a ring  $R$ . Let  $\{a_i | i \in I\}$  be the family of all ideals of  $R$  which contains  $X$ . Then  $\cap_{i \in I} a_i = (X)$  is called the ideal generated by  $X$ . The elements of  $X$  are called the generators of the ideal  $(X)$ . If  $X = \{x_1, \dots, x_n\}$ , then  $(X) = (x_1, \dots, x_n) = \{\sum_{i=1}^n r_i x_i | r_i \in R\}$  is said to be finitely generated.

**Example 11** 1.  $\mathbb{Z}$  is a ring,  $2\mathbb{Z}$  is an ideal of  $\mathbb{Z}$ . In fact ideals of  $\mathbb{Z}$  are of the form  $d\mathbb{Z}$  where  $d$  is an integer.

2.  $\mathbb{C}[x]$  is a ring, then  $(x^3 + 2)\mathbb{C}[x]$  and  $(x^2 + 1, 2x^3 + 5)\mathbb{C}[x] = \{(x^2 + 1)f(x) + (2x^3 + 5)g(x) | f(x), g(x) \in \mathbb{C}[x]\}$  are ideals of  $\mathbb{C}[x]$ .

3. If  $f : R \rightarrow S$  is any ring homomorphism then the  $\ker(f)$  is an ideal of  $R$ , but the  $\text{im}(f)$  need not be an ideal of  $S$  (e.g. in the case  $f$  is not surjective), it is only a subring of  $S$ .

**Remark 12** Different than subring, an ideal do not need to have the identity element of the ring. In fact, if the ideal has the identity element than that ideal is the whole ring.  $[1 \in a \Rightarrow r1 \in a \forall r \in R \Rightarrow R \subseteq a, a \subseteq R \Rightarrow a = R]$ . We sometimes denote  $R = (1)$ , i.e.  $R$  can be viewed as an ideal that is generated by the element 1.

The finitely generated ideals will be important for us. In fact for the Algebraic Geometry lecture, you will be working with the ring  $\mathbb{C}[x_1, \dots, x_n]$  and the ideals you will deal with will be always finitely generated. (comes from the Noetherian property of  $\mathbb{C}[x_1, \dots, x_n]$ ).

The ideals we will mostly work with will be prime and maximal ideals. Now let us see the definition of those.

$$\text{prime ideal} \leftrightarrow \text{Prime numbers}$$

Recall that if  $p$  is a prime number then  $p \neq 1$  and  $p|ab \Rightarrow p|a$  or  $p|b$ .

We say  $p \subset R$  is a prime ideal if  $p \neq (1)$  and  $xy \in p \Rightarrow x \in p$  or  $y \in p$ . In fact, prime numbers is generalized to prime ideals by Dedekind in 1871.

Importance:

- We will use them to define algebraic varieties = solution set of polynomials in a prime ideal
- They can be used to form integral domains from rings. (definition is coming)

**Example 13** 1. For  $\mathbb{Z}$ ,  $(p)$  is a prime ideal if and only if  $p$  is 0 or a prime number.

2. For  $\mathbb{C}[x]$ ,  $(f(x))$  is a prime ideal if and only if  $f(x)$  is an irreducible polynomial.

3.  $\text{Spec}(R) = \text{all prime ideals of } R$ ;  $\text{Spec}(\mathbb{Z}) = \{(0), (p) | p \text{ is a prime number}\}$ ,  $\text{Spec}(k) = \{(0)\}$  for  $k$  a field. This spectrum of a ring will be related to algebraic varieties.

maximal ideal  $\leftrightarrow$  Maximum of something, kind of an upper bound

$m \subset R$  is called a maximal ideal if  $m \neq (1)$  and there is no ideal  $a$  such that  $m \subset a \subset (1) = R$ .

**Example 14** In  $\mathbb{Z}$  consider  $(3) \subset (d) \subset (1)$ .  $(3) \subset (d)$  implies  $3 = dr$  for some  $r \in \mathbb{Z}$ . This means  $d|3 \Rightarrow d = 3$  or  $d = 1$ . Hence  $(3)$  is a maximal ideal.

**Remark 15**  $m$  is not unique, there might be many maximal ideals. In fact rings with only one maximal ideal are special, they are called local rings.

**Example 16** 1. In  $\mathbb{Z}$ , prime ideals are also maximal ideals, hence  $\{(2), (3), (5), \dots\}$  are maximal ideals of  $\mathbb{Z}$ .

2. This comes from [DF] Chapter 8, Proposition 7: Every non-zero prime ideal in a Principal Ideal Domain is a maximal ideal.

Importance:

- Maximal ideals correspond to points in algebraic varieties.
- They can be used to form fields from rings.

Roughly

prime ideals  $\leftrightarrow$  algebraic varieties  
 maximal ideals  $\leftrightarrow$  points in algebraic varieties

**Theorem 17** ([Atiyah-MacDonald], 1.3) Every ring  $R \neq 0$  has at least one maximal ideal.

**Proof.** Let  $\Sigma$  be the set of all ideals of  $R$  different from  $(1)$ . We will show that every chain in this set has an upper bound and use the Zorn's lemma. First let us recall what chain is:

$S$  be a non-empty partially ordered set, i.e. we have a reflexive and transitive relation  $\leq$  on  $S$  such that  $x \leq y$  and  $y \leq x$  implies  $x = y$  for all  $x, y \in S$ . A subset  $T \subseteq S$  is called a chain if either  $x \leq y$  or  $y \leq x$  for every pair  $x, y \in T$ .

Next let us recall Zorn's Lemma: If every chain  $T$  in  $S$  has an upper bound in  $S$  then  $S$  has at least one maximal element.

So we will put a relation on  $\Sigma$  by inclusion.  $\Sigma \neq \emptyset$  as  $0 \in \Sigma$ . Then consider  $\{a_i\}$  a chain of ideals from  $\Sigma$ . Let  $a = \cup a_i$ , note that  $a$  is also an ideal and  $1 \notin a$  as  $1 \notin a_i$  so  $a \in \Sigma$  and  $a_i \subset a$  for each  $i$ . That is  $a$  is an upper bound for the chain  $\{a_i\}$ . As the chain is arbitrary, Zorn's lemma implies  $R$  has at least one maximal ideal. ■

**Corollary 18** If  $a \neq 1$  is an ideal of  $R$ , then there exists a maximal ideal of  $R$  that contains  $a$ .

**Proof.** Let  $\sum$  to be the set of all ideals of  $R$  that contain  $a$ . Then apply the proof of theorem 17 to  $\sum$ . ■

**Corollary 19** *Every non-unit of  $R$  is contained in a maximal ideal*

**Proof.** Let  $x \in R$  be a non-unit then  $(x) \neq 1$  is an ideal of  $R$ . Now corollary 18 gives the result. ■

Hence if  $R$  is a local ring, then elements that are not in its maximal ideals will be units.

I mentioned that prime ideals can be used to form integral domains from rings and maximal ideals can be used to form fields from rings. Now let us see how this can be done and also recall the definition of integral domain and field. For our purpose we will consider the quotient of a ring by an ideal.

**Definition 20** *Let  $R$  be a ring and  $a \subset R$  be an ideal. The quotient group  $R/a$  becomes a ring with the induced multiplication of  $R$ ,  $\overline{xy} = \overline{x} \overline{y}$ . This new ring is called the quotient ring. The elements of  $R/a$  are called the cosets of  $a$  and the map  $\phi : R \longrightarrow R/a, x \longrightarrow x + a$  is a surjective ring homomorphism.*

**Example 21** 1.  $\mathbb{Z}$  is a ring. We have  $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$  and ideal of  $\mathbb{Z}$  then  $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$  is the quotient formed by taking the quotient of  $\mathbb{Z}$  by  $n\mathbb{Z}$ .

Now what we did is from a ring we formed another ring called quotient ring. There are some special elements in a ring and these will help to form new type of rings.

**Definition 22** 1. A zero-divisor in a ring  $R$  is an element  $x$  which divides 0, i.e. there exists a  $y \in R$  such that  $xy = 0$ .

2. A ring with no zero divisors  $\neq 0$  is called an integral domain.

3. An integral domain is called a principal integral domain if every ideal is principal that is generated by one element.

4. An element  $x \in R$  is called nilpotent if  $x^n = 0$  for some  $n > 0$ .

5. An element  $x \in R$  is called a unit if there exists  $y \in R$  such that  $xy = 1$ . The units of  $R$  form a multiplicative abelian group.

6. A field is a ring in which  $1 \neq 0$  and every element is a unit.

**Example 23** 1. In  $\mathbb{Z}/6\mathbb{Z}$ , 2, 3 are zero-divisors as  $2 \times 3 = 0$ , 5 is a unit as  $5 \times 5 = 1$ .

2. In  $\mathbb{Z}/4\mathbb{Z}$  2 is a nilpotent element as  $2^2 = 0$ .

3. A nilpotent element is a zero divisor, but not conversely.

4.  $\mathbb{Z}/p\mathbb{Z}$  is a field for  $p$  a prime number.

5. For  $f : R \longrightarrow S$  ring homomorphism  $\ker(f)$  is a prime ideal of  $R$  for  $S$  an integral domain.

**Proposition 24** ([Atiyah-MacDonald],1.1) There is a one-to-one order preserving correspondence between the ideals  $b$  of  $R$  that contain  $a$ , and the ideals  $\bar{b}$  of  $R/a$ , given by  $b = \phi^{-1}(\bar{b})$ .

**Proposition 25** ([Atiyah-MacDonald],1.2) let  $R \neq 0$  be a ring. TFAE:

- (a)  $R$  is a field
- (b) the only ideals in  $R$  are  $(0)$  and  $(1)$
- (c) every homomorphism of  $R$  into a non-zero ring  $S$  is injective

Importance:

- In a principal integral domain every non-zero prime ideal is maximal.
- $p$  is prime ideal  $\Leftrightarrow R/p$  is an integral domain
- $m$  is maximal ideal  $\Leftrightarrow R/m$  is a field.
- $0$  ideal is prime  $\Leftrightarrow R$  is an integral domain

### 3 Modules

The property that formed the ideals is that they are subset of the ring and when we multiply an element of an ideal with an element of a ring, the result stays inside the ideal. Now we will introduce new objects that has the multiplication property as ideals but they do not need to be a subset of the ring. They can be thought as generalization of ideals.

**Definition 26** Let  $R$  be a ring,  $M$  is called a  $R$ -module if  $M$  is an abelian group with an  $R$ -linear action on it. That is there is a map  $\mu : R \times M \longrightarrow M$ ,  $\mu(r, x) = rx$  satisfying the following properties:

- (a)  $r(x + y) = rx + ry$  for all  $r \in R, x, y \in M$
- (b)  $(r + s)x = rx + sx$  for all  $r, s \in R, x \in M$
- (c)  $(rs)x = r(sx)$  for all  $r, s \in R, x \in M$
- (d)  $1x = x$  for all  $x \in M$

**Example 27** 1. Any ideal of  $R$  is a  $R$ -module

2. If  $R$  is a field then  $R$ -module =  $R$  vector space

3.  $\mathbb{Z}$ -module = abelian group

Relation between two modules is given by a module homomorphism

**Definition 28** Let  $M, N$  be  $R$ -modules, then a map  $f : M \longrightarrow N$  is called a  $R$ -module homomorphism if for all  $r \in R, x, y \in M$  the following holds

(a)  $f(x + y) = f(x) + f(y)$

(b)  $f(rx) = rf(x)$

**Example 29** 1. If  $f : M \longrightarrow N, g : N \longrightarrow K$  are  $R$ -module homomorphisms, then  $g \circ f : M \longrightarrow K$  is a  $R$ -module homomorphism

2.  $\text{Hom}_R(M, N) = \{f | f : M \longrightarrow N \text{ } R\text{-module homomorphism}\}$  is an  $R$ -module.

3.  $\text{Hom}_R(R, M) \cong M$



## References

- [Atiyah-MacDonald] Atiyah, M.F., MacDonald, I.G., *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, Inc., 1969.
- [DF] Dummit, S. David, Foote M. Richard, *Abstract Algebra*, John Wiley Sons, Inc., 2004.