

# Introduction to Commutative Algebra

Amal M

January 4, 2021

## Abstract

iendthebibliography

The motivation for the study of algebraic geometry is how algebraic objects (rings of rational functions) are associated with varieties (zeros of polynomials). This subject flourished during the second half of the twentieth century. Algebraic geometry allows us to study the geometry arising from algebraic objects. Core to the deeper understanding of this subject is an understanding of the subject of commutative algebra which studies commutative rings and their ideals and modules. The purpose of the present project is to gain an understanding of commutative algebra through solving exercises from Atiyah-MacDonald's book, *Introduction to Commutative Algebra*. The reading project comprised of the study of the theory of rings and modules, their tensor product and exact sequences of rings and modules. The project concluded with a proof of the Going-Up Theorem.

# Contents

<b>1</b>	<b>What is Algebraic Geometry?</b>	<b>2</b>
1.1	Hilbert's Nullstellensatz . . . . .	2
<b>2</b>	<b>Rings and Ideals</b>	<b>3</b>
2.1	Basic Definitions . . . . .	3
2.2	Ideals and Quotients . . . . .	3
2.3	Zero-Divisors, Nilpotent Elements, Units . . . . .	4
2.4	Prime and Maximal Ideals . . . . .	4
2.5	Nilradical and Jacobson Radical . . . . .	5
2.6	Some properties of ideals . . . . .	5
<b>3</b>	<b>Modules</b>	<b>10</b>
3.1	Modules and Module homomorphisms . . . . .	10
3.2	Submodules and Quotient Modules . . . . .	10
3.2.1	Some important notes . . . . .	11
3.3	Direct Sum and Product . . . . .	11
3.4	Finitely Generated Module . . . . .	11
3.4.1	Free Module . . . . .	12
3.5	Exact Sequence . . . . .	12
3.6	Tensor Product of Modules . . . . .	13
3.7	Restriction and extension of scalars . . . . .	13
3.8	Exactness Properties of the Tensor Product . . . . .	14
<b>4</b>	<b>Rings and Modules of Fractions</b>	<b>16</b>
4.1	Ring of Fractions . . . . .	16
4.2	Localization . . . . .	16
4.3	Ring of fraction of Modules . . . . .	17
4.4	Some examples of local properties . . . . .	18
<b>5</b>	<b>Integral Dependence and the Going-Up Theorem</b>	<b>21</b>
5.1	Integral Dependence . . . . .	21
5.2	The Going-up Theorem . . . . .	22

# Chapter 1

## What is Algebraic Geometry?

Algebraic Geometry is the study of curves. Specifically the study of the solution set of polynomial cuves which are called *varieties*. For example a major branch of algebraic geometry is concerned with the study of special curves called *elliptical curves*. For example, a curve defined by the polynomial equation

$$y^2 = x^3 + ax + b$$

Which is one example of a variety, specifically *a projective variety*.

There are different types of such varieties and algebraic geometry provides a toolbox to study such problems where the solution set of cuves are considered as surfaces and rational functions on such a surfaces form a ring which suprisingly is seen to be, if interpreted correctly, equivalent to the surface which is being described.

So in modern algebraic geometry to every ring  $A$ , we associated a set  $X$  which is the set of all prime ideals of  $A$ . We find that this set called  $\text{Spec}(A)$  or the *spectrum* of the ring, has a topology on it which turns the set into a topological space.

So algebraic geometry uses quite a lot of algebraic machinery. That is it uses a lot of important results from Commutative Algebra.

### 1.1 Hilbert's Nullstellensatz

**Theorem 1.1.1.** (Hilbert's Nullstellensatz). Suppose  $\bar{k} = k$ . Then, the following statements are both true and equivalent:

1. Given an ideal  $J \subset \mathbb{A}_k^n$ , we have  $\sqrt{J} = I(V(J))$ ,
2. Given an ideal  $J \subset \mathbb{A}_k^n$ , we have the implication  $(V(J)) = \emptyset \implies J = \bar{k}[x_1, \dots, x_n]$ ,
3. The maximal ideals of  $k[x_1, \dots, x_n]$  are exactly  $J = (x_1 - a, \dots, x_n - a_n), (a_1, \dots, a_n) \in k^n$ , with  $\bar{k}[x_1, \dots, x_n]/J \cong \bar{k}$

## Chapter 2

# Rings and Ideals

### 2.1 Basic Definitions

**Definition 2.1.1.** A ring  $A$  is a set with two binary operations (addition and multiplication) such that

1.  $A$  is an abelian group with respect to addition
2. Multiplication is associative  $((xy)z = x(yz))$  and distributive over addition  $(x(y+z) = xy + xz, (y+z)x = yx + zx)$ .
3.  $xy = yx$  for all  $x, y \in A$ . (for our purpose we consider only rings that commute)
4.  $\exists 1 \in A$  such that  $x1 = 1x = x$  for all  $x \in A$ . The identity element is unique.  
If  $1 = 0$  then for any  $x \in A$  we have  $x = x1 = x0 = 0$  so  $A$  has only one element  $0$ .

**Definition 2.1.2.** A ring homomorphism is a mapping  $f$  of a ring  $A$  into a ring  $B$  such that

1.  $f(x+y) = f(x) + f(y)$  so that  $f$  is a homomorphism of abelian groups.
2.  $f(xy) = f(x)f(y)$ ,
3.  $f(1) = 1$

**Definition 2.1.3.** A subset  $S$  of a ring  $A$  is a subring of  $A$  if  $S$  is closed under addition and multiplication and contains the identity element of  $A$ .

### 2.2 Ideals and Quotients

**Definition 2.2.1.** An ideal  $\mathfrak{a}$  of a ring  $A$  is a subset of  $A$  which is an additive subgroup and is such that  $A\mathfrak{a} \subseteq \mathfrak{a}$ .

**Definition 2.2.2.** The quotient group  $A/\mathfrak{a}$  inherits a uniquely defined multiplication from  $A$  which makes it into a ring. Called the quotient ring  $A/\mathfrak{a}$ . The elements of  $A/\mathfrak{a}$  are the cosets of  $\mathfrak{a}$  in  $A$ , and the mapping  $\phi : A \rightarrow A/\mathfrak{a}$  which maps each  $x \in A$  to its coset  $x + \mathfrak{a}$  is a surjective ring homomorphism.

**Proposition 2.2.3.** There is a one-to-one order-preserving correspondence between the ideals  $\mathfrak{b}$  of  $A$  which contain  $\mathfrak{a}$  and the ideals  $\bar{\mathfrak{b}}$  of  $A/\mathfrak{a}$ , given by  $\bar{\mathfrak{b}} = \phi^{-1}(\mathfrak{b})$ .

## 2.3 Zero-Divisors, Nilpotent Elements, Units

**Definition 2.3.1.** A zero-divisor in a ring  $A$  is an element  $x$  for which there exists  $y \neq 0$  in  $A$  such that  $xy = 0$ . A ring with no zero-divisors  $\neq 0$  is called an *\*integral domain\**.

**Definition 2.3.2.** An element  $x \in A$  is nilpotent if  $x^n = 0$  for some  $n > 0$ . A nilpotent element is a zero-divisor. A *\*unit\** in  $A$  is an element  $x$  such that  $xy = 1$  for some  $y \in A$ . The element  $y$  is then uniquely determined by  $x$  and is written  $x^{-1}$ . The units in  $A$  form a multiplicative abelian group.

**Definition 2.3.3.** The multiples  $ax$  of an element  $x \in A$  form a principal ideal, denoted by  $(x)$  or  $Ax$ .  $x$  is a unit  $\Leftrightarrow (x) = A = (1)$ . The zero ideal  $(0)$  is usually denoted by  $0$ . A *\*field\** is a ring  $A$  in which  $1 \neq 0$  and every non-zero element is a unit. Every field is an integral domain.

**Proposition 2.3.4.** Let  $A$  be a ring  $\neq 0$ . Then the following are equivalent:

1.  $A$  is a field
2. the only ideals in  $A$  are  $0$  and  $(1)$ .
3. every homomorphism of  $A$  into a non-zero ring  $B$  is injective.

## 2.4 Prime and Maximal Ideals

**Definition 2.4.1.** An ideal  $\mathfrak{p}$  in  $A$  is prime if  $\mathfrak{p} \neq (1)$  and if  $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$  or  $y \in \mathfrak{p}$ . An ideal  $\mathfrak{m}$  in  $A$  is maximal if  $\mathfrak{m} \neq (1)$  and if there is no ideal  $\mathfrak{a}$  such that  $\mathfrak{m} \subset \mathfrak{a} \subset (1)$ . Equivalently:

$\mathfrak{p}$  is prime  $\Leftrightarrow A/\mathfrak{p}$  is an integral domain

$\mathfrak{m}$  is maximal  $\Leftrightarrow A/\mathfrak{p}$  is a field

Hence a maximal ideal is prime. But the converse is not true in general.

1. If  $f : A \rightarrow B$  is a ring homomorphism and  $\mathfrak{q}$  is a prime ideal in  $B$ , then  $f^{-1}(\mathfrak{q})$  is a prime ideal in  $A$ , for  $A/f^{-1}(\mathfrak{q})$  is isomorphic to a subring of  $B/\mathfrak{q}$  and hence has no zero-divisor  $\neq 0$ .

**Theorem 2.4.2.** Every commutative ring  $A$  (with identity)  $\neq 0$  has at least one maximal ideal.

**Corollary 2.4.2.1.** Every non-unit of  $A$  is contained in a maximal ideal.

**Definition 2.4.3.** A ring  $A$  with exactly one maximal ideal  $\mathfrak{m}$  is called a local ring. The field  $k = A/\mathfrak{m}$  is called the residue field of  $A$ .

**Exercise 2.4.4.** A local ring contains no idempotent  $\neq 0, 1$ . (Ex 12)

**Proposition 2.4.5.** 1. Let  $A$  be a ring and  $\mathfrak{m} \neq (1)$  an ideal of  $A$  such that every  $x \in A - \mathfrak{m}$  is a unit in  $A$ . Then  $A$  is a local ring and  $\mathfrak{m}$  its maximal ideal.

2. Let  $A$  be a ring and  $\mathfrak{m}$  a maximal ideal of  $A$ , such that every element of  $1 + \mathfrak{m}$  (every  $1 + x$  where  $x \in \mathfrak{m}$ ) is a unit in  $A$ . Then  $A$  is a local ring.

**Example 2.4.6.**  $A = k[x_1, \dots, x_n]$ ,  $k$  is a field. Let  $f \in A$  be an irreducible polynomial. By unique factorization, the ideal  $(f)$  is prime.

**Example 2.4.7.**  $A = \mathbb{Z}$ . Every ideal in  $\mathbb{Z}$  is of the form  $(m)$  for some  $m \geq 0$ . The ideal  $(m)$  is prime  $\Leftrightarrow m = 0$  or a prime number. All the ideals  $(p)$ , where  $p$  is a prime number are maximal:  $\mathbb{Z}/(p)$  is a field of  $p$  elements.

## 2.5 Nilradical and Jacobson Radical

**Proposition 2.5.1.** The set  $\mathfrak{N}$  of all nilpotent elements in a ring  $A$  is an ideal and  $A/\mathfrak{N}$  has no nilpotent element  $\neq 0$ .

**Definition 2.5.2.** The ideal  $\mathfrak{N}$  is called the nilradical of  $A$ . The following proposition gives an alternative definition of  $\mathfrak{N}$ :

**Proposition 2.5.3.** The nilradical of  $A$  is the intersection of all the prime ideals of  $A$ .

**Definition 2.5.4.** The Jacobson radical of  $\mathfrak{R}$  of  $A$  is defined to be the intersection of all the maximal ideals of  $A$ . It can be characterized as follows:

**Proposition 2.5.5.**  $x \in \mathfrak{R} \Leftrightarrow 1 - xy$  is a unit in  $A$  for all  $y \in A$ .

**Exercise 2.5.6.** Let  $x$  be a nilpotent element of a ring  $A$ . Show that  $1 + x$  is a unit of  $A$ . Deduce that the sum of a nilpotent element and a unit is a unit. (Ex 1)

**Exercise 2.5.7.** Let  $A$  be a ring in which every element  $x$  satisfies  $x^n = x$  for some  $n > 1$  (depending on  $x$ ). Show that every prime ideal in  $A$  is maximal.

## 2.6 Some properties of ideals

**Definition 2.6.1.** If  $\mathfrak{a}, \mathfrak{b}$  are ideals in a ring  $A$ , their *ideal quotient* is

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A : x\mathfrak{b} \subseteq \mathfrak{a}\}$$

which is an ideal. In particular,  $(0 : \mathfrak{b})$  is called the *annihilator* of  $\mathfrak{b}$  and is also denoted by  $\text{Ann}(\mathfrak{b})$ .

**Definition 2.6.2.** If  $\mathfrak{a}$  is any ideal of  $A$ , the radical of  $\mathfrak{a}$  is

$$r(\mathfrak{a}) = \{x \in A : x^n \in \mathfrak{a} \text{ for some } n > 0\}$$

If  $\phi : A \rightarrow A/\mathfrak{a}$  is the standard homomorphism, then  $r(\mathfrak{a}) = \phi^{-1}(\mathfrak{N}_{A/\mathfrak{a}})$  and hence  $r(\mathfrak{a})$  is an ideal by (1.7).

**Exercise 2.6.3.** 1.  $r(\mathfrak{a}) \supseteq \mathfrak{a}$

$$2. \ r(r(\mathfrak{a})) = r(\mathfrak{a})$$

$$3. \ r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$$

$$4. \ r(\mathfrak{a}\mathfrak{b}) = (1) \Leftrightarrow \mathfrak{a} = (1)$$

$$5. r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$$

$$6. \text{ If } \mathfrak{p} \text{ is prime, } r(\mathfrak{p}^n) = \mathfrak{p} \text{ for all } n > 0.$$

**Proposition 2.6.4.** *The radical of an ideal  $\mathfrak{a}$  is the intersection of the prime ideals which contain  $\mathfrak{a}$ .*

**Proposition 2.6.5.**  *$D = \text{set of zero-divisors of } A = \bigcup_{x \neq 0} r(\text{Ann}(x))$ .*

**Proposition 2.6.6.** *Let  $\mathfrak{a}, \mathfrak{b}$  be ideals in a ring  $A$  such that  $r(\mathfrak{a}), r(\mathfrak{b})$  are coprime. Then  $\mathfrak{a}, \mathfrak{b}$  are coprime.*

**Exercise 2.6.7.** *Let  $\mathfrak{a}$  be an ideal  $\neq (1)$  in a ring  $A$ . Show that  $\mathfrak{a} = r(\mathfrak{a}) \Leftrightarrow \mathfrak{a}$  is an intersection of prime ideals. (Ex 9)*

**Exercise 2.6.8.** *Let  $A$  be a ring and let  $X$  be the set of all prime ideals of  $A$ . For each subset  $E$  of  $A$ , let  $V(E)$  denote the set of all prime ideals of  $A$  which contain  $E$ . Prove that*

$$1. \text{ if } \mathfrak{a} \text{ is the ideal generated by } E, \text{ then } V(E) = V(\mathfrak{a}) = V(r(\mathfrak{a})).$$

$$2. V(0) = X, V(1) = \emptyset.$$

$$3. \text{ if } (E_i)_{i \in I} \text{ is an family of subsets of } A, \text{ then}$$

$$V\left(\bigcup_{i \in I} E_i\right) = \bigcap_{i \in I} V(E_i)$$

$$4. V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b}) \text{ for any ideals } \mathfrak{a}, \mathfrak{b} \text{ of } A.$$

*These results show that the sets  $V(E)$  satisfy the axioms for closed sets in a topological space. The resulting topology is called the Zariski Topology. The topological space  $X$  is called the prime spectrum of  $A$ , and is written  $\text{Spec}(A)$ . (Ex 15)*

**Exercise 2.6.9.** *Draw pictures of  $\text{Spec}(\mathbb{Z}), \text{Spec}(\mathbb{R}), \text{Spec}(\mathbb{C}[x]), \text{Spec}(\mathbb{R}[x]), \text{Spec}(\mathbb{Z}[x])$ . (Ex 16)*

**Exercise 2.6.10.** *For each  $f \in A$ , let  $X_f$  denote the complement of  $V(f)$  in  $X = \text{Spec}(A)$ . The sets  $X_f$  are open. Show that they form a basis of open sets for the Zariski topology, and that*

$$1. X_f \cap X_g = X_{fg}$$

$$2. X_f = \emptyset \Leftrightarrow f \text{ is nilpotent.}$$

$$3. X_f = X \Leftrightarrow f \text{ is a unit.}$$

$$4. X_f = X_g \Leftrightarrow r((f)) = r((g)).$$

$$5. X \text{ is a quasi-compact (that is, every open covering of } X \text{ has a finite subcovering).}$$

$$6. \text{ More generally, each } X_f \text{ is quasi-compact.}$$

$$7. \text{ An open subset of } X \text{ is quasi-compact if and only if it is a finite union of sets } X_f.$$

*The sets  $X_f$  are called basic open sets of  $X = \text{Spec}(A)$ . (Ex 17)*



**Exercise 2.6.11.** For psychological reasons it's sometimes convenient to denote a prime ideal of  $A$  by a letter such as  $x$  or  $y$  when thinking of it as a point of  $X = \text{Spec}(A)$ . When thinking of  $x$  as a prime ideal of  $A$ , we denote it by  $\mathfrak{p}_x$  (logically, of course, it is the same thing). Show that

1. the set  $\{x\}$  is closed (we say that  $x$  is a "closed point") in  $\text{Spec}(A) \Leftrightarrow \mathfrak{p}_x$  is maximal.
2.  $\bar{\{x\}} = V(\mathfrak{p}_x)$ .
3.  $y \in \bar{\{x\}} \Leftrightarrow \mathfrak{p}_x \subseteq \mathfrak{p}_y$ .
4.  $X$  is a  $T_0$ -space (this means that if  $x, y$  are distinct points of  $X$ , then either there is a neighborhood of  $y$  which does not contain  $x$ ).

(Ex 18)

**Exercise 2.6.12.** A topological space  $X$  is said to be irreducible if  $X \neq \emptyset$  and if every pair of non-empty open sets in  $X$  intersect, or equivalently if every non-empty open set is dense in  $X$ . Show that  $\text{Spec}(A)$  is irreducible if and only if the nilradical of  $A$  is a prime ideal. (Ex 19)

**Exercise 2.6.13.** Let  $X$  be a topological space.

1. If  $Y$  is an irreducible (Ex 19) subspace of  $X$ , then the closure  $\bar{Y}$  of  $Y$  in  $X$  is irreducible.
2. Every irreducible subspace of  $X$  is contained in a maximal irreducible subspace.
3. The maximal irreducible subspaces of  $X$  are closed and cover  $X$ . They are called the irreducible components of  $X$ . What are the irreducible components of a Hausdorff space?
4. If  $A$  is a ring and  $X = \text{Spec}(A)$ , then the irreducible components of  $X$  are the closed sets  $V(\mathfrak{p})$ , where  $\mathfrak{p}$  is a maximal prime ideal of  $A$ . (Ex 8)

(Ex 20)

**Exercise 2.6.14.** Let  $\phi : A \rightarrow B$  be a ring homomorphism. Let  $X = \text{Spec}(A)$  and  $Y = \text{Spec}(B)$ . If  $\mathfrak{q} \in Y$ , then  $\phi^{-1}(\mathfrak{q})$  is a prime ideal of  $A$ , i.e., a point of  $X$ . Hence  $\phi$  induces a mapping  $\phi^* : Y \rightarrow X$ . Show that

1. If  $f \in A$  then  $\phi^{*-1}(X_f) = Y_{\phi(f)}$ , and hence that  $\phi^*$  is continuous.
2. If  $\mathfrak{a}$  is an ideal of  $A$ , then  $\phi^{*-1}(V(\mathfrak{a})) = V(\mathfrak{a}^e)$ .
3. If  $\mathfrak{b}$  is an ideal of  $B$ , then  $\phi^*(\bar{V}(\mathfrak{b})) = V(\mathfrak{b}^e)$ .
4. If  $\phi$  is surjective, then  $\phi^*$  is a homeomorphism of  $Y$  onto the closed subset  $V(\text{Ker}(\phi))$  of  $X$ . (In particular,  $\text{Spec}(A)$  and  $\text{Spec}(A/\mathfrak{N})$  (where  $\mathfrak{N}$  is the nilradical of  $A$ ) are naturally homeomorphic.)
5. If  $\phi$  is injective, then  $\phi^*(Y)$  is dense in  $X$ . More precisely,  $\phi^*(Y)$  is dense in  $X \Leftrightarrow \text{Ker}(\phi) \subseteq \mathfrak{N}$ .
6. Let  $\psi : B \rightarrow C$  be another ring homomorphism. Then  $(\psi \circ \phi)^* = \phi^* \circ \psi^*$ .

7. Let  $A$  be an integral domain with just one non-zero prime ideal  $\mathfrak{p}$ , and let  $K$  be the field of fractions of  $A$ . Let  $B = (A/\mathfrak{p}) \times K$ . Define  $\phi : A \rightarrow B$  by  $\phi(x) = (\bar{x}, x)$ , where  $\bar{x}$  is the image of  $x$  in  $A/\mathfrak{p}$ . Show that  $\phi^*$  is bijective but not a homeomorphism.

(Ex 21)

**Exercise 2.6.15.** Let  $A$  be a ring. The subspace of  $\text{Spec}(A)$  consisting of the maximal ideals of  $A$ , with the induced topology, is called the maximal spectrum of  $A$  and is denoted by  $\text{Max}(A)$ . For arbitrary commutative rings it does not have the nice functorial properties of  $\text{Spec}(A)$  (see Ex 21), because the inverse image of a maximal ideal under a ring homomorphism need not be maximal. Let  $X$  be a compact Hausdorff space and let  $C(X)$  denote the ring of all real-valued continuous functions on  $X$  (add and multiply functions by adding and multiplying their values). For each  $x \in X$ , let  $\mathfrak{m}_x$  be maximal, because it is the kernel of the (surjective) homomorphism  $C(X) \rightarrow \mathbb{R}$  which takes  $f$  to  $f(x)$ . If  $\hat{X}$  denotes  $\text{Max}(C(X))$ , we have therefore defined a mapping  $\mu : X \rightarrow \hat{X}$ , namely  $x \mapsto \mathfrak{m}_x$ . We shall show that  $\mu$  is a homeomorphism of  $X$  onto  $\hat{X}$ .

1. Let  $\mathfrak{m}$  be any maximal ideal of  $C(X)$ , and let  $V = V(\mathfrak{m})$  be the set of common zeros of the functions in  $\mathfrak{m}$ : that is,

$$V = \{x \in X : f(x) = 0 \text{ for all } f \in \mathfrak{m}\}.$$

Suppose that  $V$  is empty. Then for each  $x \in X$  there exists  $f_x \in \mathfrak{m}$  such that  $f_x(x) \neq 0$ . Since  $f_x$  is continuous, there is an open neighborhood  $U_x$  of  $x$  in  $X$  on which  $f_x$  does not vanish. By compactness a finite number of the neighborhoods, say  $U_{x_1}, \dots, U_{x_n}$  cover  $X$ . Let

$$f = f_{x_1}^2 + \dots + f_{x_n}^2.$$

Then  $f$  does not vanish at any point of  $X$ , hence is a unit in  $C(X)$ . But this contradicts  $f \in \mathfrak{m}$ , hence  $V$  is not empty. Let  $x$  be a point of  $V$ . Then  $\mathfrak{m} \subseteq \mathfrak{m}_x$ , hence  $\mathfrak{m} = \mathfrak{m}_x$  because  $\mathfrak{m}$  is maximal. Hence  $\mu$  is surjective.

2. By Urysohn's lemma (this is the only non-trivial fact required in the argument) the continuous functions separate the points of  $X$ . Hence  $x \neq y \Rightarrow \mathfrak{m}_x \neq \mathfrak{m}_y$ , and therefore  $\mu$  is injective.

3. Let  $f \in C(X)$ ; let

$$U_f = \{x \in X : f(x) \neq 0\}$$

and let

$$\hat{U}_f = \{\mathfrak{m} \in \hat{X} : f \notin \mathfrak{m}\}$$

Show that  $\mu(U_f) = \hat{U}_f$ . The open sets  $U_f$  (resp.  $\hat{U}_f$ ) form a basis of the topology of  $X$  (resp.  $\hat{X}$ ) and therefore  $\mu$  is a homeomorphism. Thus  $X$  can be reconstructed from the ring of functions  $C(X)$ .

(Ex 26)

**Exercise 2.6.16.** Let  $k$  be an algebraically closed field and let

$$f_\alpha(t_1, \dots, t_n) = 0$$

be a set of polynomial equations in  $n$  variables with coefficients in  $k$ . The set  $X$  of all points  $x = (x_1, \dots, x_n) \in k^n$  which satisfy these equations is an affine algebraic variety.

Consider the set of all polynomials  $g \in k[t_1, \dots, t_n]$  with the property that  $g(x) = 0$  for all  $x \in X$ . This set is an ideal  $I(X)$  in the polynomial ring, and is called the ideal of the variety  $X$ . The quotient ring

$$P(X) = k[t_1, \dots, t_n]/I(X)$$

is the ring of polynomial functions on  $X$ , because two polynomials  $g, h$  define the same polynomial function on  $X$  if and only if  $g - h$  vanishes at every point of  $X$ , that is, if and only if  $g - h \in I(X)$ .

Let  $\xi_i$  be the image of  $t_i$  in  $P(X)$ . The  $\xi_i$  ( $1 \leq i \leq n$ ) are the coordinate functions on  $X$ : if  $x \in X$ , then  $\xi_i(x)$  is the  $i$ th coordinate of  $x$ .  $P(X)$  is generated as a  $k$ -algebra by the coordinate functions, and is called the coordinate ring (or affine algebra) of  $X$ .

As in Ex 26, for each  $x \in X$  let  $\mathfrak{m}_x$  be the ideal of all  $f \in P(X)$  such that  $f(x) = 0$ ; it is maximal ideal of  $P(X)$ . Hence, if  $\hat{X} = \text{Max}(P(X))$ , we have defined a mapping  $\mu : X \rightarrow \hat{X}$ , namely  $x \mapsto \mathfrak{m}_x$ .

It is easy to show that  $\mu$  is injective: if  $x \neq y$ , we must have  $x_i \neq y_i$  for some  $i$  ( $1 \leq i \leq n$ ), and hence  $\xi_i = x_i$  is in  $\mathfrak{m}_x$  but not in  $\mathfrak{m}_y$ , so that  $\mathfrak{m}_x \neq \mathfrak{m}_y$ . What is less obvious (but still true) is that  $\mu$  is surjective. This is one form of Hilbert's Nullstellensatz. (Ex 27)

**Exercise 2.6.17.** Let  $f_1, \dots, f_m$  be elements of  $k[t_1, \dots, t_n]$ . They determine a polynomial mapping  $\phi : k^n \rightarrow k^m$ : if  $x \in k^n$ , the coordinates of  $\phi(x)$  are  $f_1(x), \dots, f_m(x)$ .

Let  $X, Y$  be affine algebraic varieties in  $k^n, k^m$  respectively. A mapping  $\phi : X \rightarrow Y$  is said to be regular if  $\phi$  is the restriction to  $X$  of a polynomial mapping from  $k^n$  to  $k^m$ .

If  $\eta$  is a polynomial function on  $Y$ , then  $\eta \circ \phi$  is a polynomial function on  $X$ . Hence  $\phi$  induces a  $k$ -algebra homomorphism  $P(Y) \rightarrow P(X)$ , namely  $\eta \mapsto \eta \circ \phi$ .

Show that in this way we obtain a one-to-one correspondence between the regular mappings  $X \rightarrow Y$  and the  $k$ -algebra homomorphisms  $P(Y) \rightarrow P(X)$ . (Ex 28)

## Chapter 3

# Modules

### 3.1 Modules and Module homomorphisms

**Definition 3.1.1.** Let  $M$  be an abelian group and let  $A$  be a commutative ring that acts *\*linearly\** on  $M$ . If we denote  $\mu(a, x) = ax$ , where  $a \in A, x \in M$  and the following axioms are satisfied,

1.  $a(x + y) = ax + ay$
2.  $(a + b)x = ax + bx$
3.  $(ab)x = a(bx)$
4.  $1x = x, (\forall a, b \in A, \forall x, y \in M.)$

Then  $(M, \mu)$  is called a module

### 3.2 Submodules and Quotient Modules

**Definition 3.2.1.** A submodule  $M'$  of  $M$  is a subgroup that is closed under multiplication by elements of  $A$ . The quotient  $M/M'$  is also an  $A$ -module is the action of  $A$  on the quotient is  $a(x + M') = ax + M'$ .

**Definition 3.2.2.** If  $f : M \rightarrow N$   $A$ -module homomorphism then,

1.  $\text{Ker}(f) = \{x \in M : f(x) = 0\}$
2.  $\text{Im}(f) = f(M)$
3. The cokernel of  $f$  is denoted by,  $\text{Coker}(f) = N/\text{Im}(f)$

**Proposition 3.2.3.** There is a one-to-one order preserving correspondence between the submodules of  $M$  containing the submodule  $M'$  and the submodules of the quotient  $M/M'$ . The correspondence for ideals is a special case of this proposition.

**Definition 3.2.4.** (Induced homomorphism) If  $M' \subseteq \text{Ker}(f)$ . Define  $\bar{f} : M/M' \rightarrow N$  as  $\bar{f}(\bar{x}) = f(x)$ . Then it is a homomorphism and it is said to be induced by  $f$ . Specially we have,  $\text{Ker}(\bar{f}) = \text{Ker}(f)/M'$ .

If we take  $\text{Ker}(f) = M'$  we have that  $M/\text{Ker}(f) \cong \text{Im}(f)$ .

**Proposition 3.2.5.** 1. If  $L \supseteq M \supseteq N$  are  $A$ -modules, then

$$\frac{L/N}{M/N} = L/M.$$

2. If  $M_1, M_2$  are submodules of  $M$ , then

$$(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2).$$

### 3.2.1 Some important notes

1. The product  $aM$  where  $a$  is an ideal is the set of all finite sums  $\sum a_i x_i$  with  $a_i \in a, x_i \in M$ .
2. If  $N, P$  are submodules of  $M$  then  $(N : P) = \{a \in A : aP \subseteq N\}$ .
3. The annihilator,  $\text{Ann}(M) = (0, M) = \{a \in A : aM = 0\}$
4. An  $A$ -module is called \*faithful\* if  $\text{Ann}(M) = 0$ .
5. If  $a \subseteq \text{Ann}(M)$  we can define  $M$  as an  $A/a$ -module by setting  $\bar{x}m = xm$ ,  $\bar{x} \in A/a, m \in M$ . This is true as  $x, y \in \bar{x}$  then  $x - y \in a$  hence  $(x - y)m = 0 \implies xm = ym$ . So it's independent of the choice of the representative of  $\bar{x}$ .
6. If  $\text{Ann}(M) = a$ , then  $M$  is faithful as an  $A/a$ -module.

## 3.3 Direct Sum and Product

**Definition 3.3.1.** (Direct Sum) Given two  $A$ -modules  $M$  and  $N$  their direct product denoted by  $M \oplus N$  is defined as the set of all pair  $(x, y)$  such that  $x \in M$  and  $y \in N$  and is an  $A$ -module by,

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

$$a \cdot (x, y) = (ax, ay)$$

If  $(M_i)_{i \in I}$  is a family of  $A$ -modules then the direct sum  $\oplus_{i \in I} M_i$  is the set of all  $(x_i)_{i \in I}$  such that all but finitely many  $x_i$  are zero.

**Definition 3.3.2.** (Direct Product) The direct product of a family of  $A$ -modules denoted by  $\prod_{i \in I} M_i$ , is exactly the same as the direct sum if  $I$  is finite. Otherwise the only difference is that  $(x_i)_{i \in I}$  does not have the condition that  $x_i$  must be zero for all but finitely many  $x_i$ .

## 3.4 Finitely Generated Module

**Definition 3.4.1.** A module  $M$  is said to be finitely generated if it can be expressed as  $M = \sum_{i \in I} Ax_i$ . That is each  $m \in M$  can be expressed as a finite linear combination of elements in  $A$  with  $x_i$ . If the number of  $x_i$  is finite then the module is said to be a finitely generated  $A$ -module.

### 3.4.1 Free Module

**Definition 3.4.2.** A finitely generated free  $A$ -module is a module that's isomorphic to  $A \oplus \cdots \oplus A$  denoted as  $A^{(n)}$  ( $n$  summands). If we remove the restriction of being finite a free  $A$ -module is isomorphic to a module of the form  $\bigoplus_{i \in I} M_i$ , where  $M_i$  are  $A$ -modules isomorphic to  $A$ .  ${}^*A^0$  is the zero module denoted by  $0$ .

**Proposition 3.4.3.**  $M$  is a finitely generated  $A$ -module if and only if  $M$  is isomorphic to a quotient of  $A^n$  for some  $n > 1$ .

**Definition 3.4.4.** Let  $M$  be a finitely generated  $A$ -module and  $a \subseteq A$  be an ideal of  $M$ . If  $\phi$  is an endomorphism of  $M$  such that  $\phi(M) \subseteq aM$  then  $\phi$  satisfies a polynomial equation in  $\phi$ ,

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0,$$

for some  $a_i \in a$ .

**Corollary 3.4.4.1.** If  $M$  is a finitely generated module such that for an ideal  $a \subseteq A$ ,  $aM = M$  then there exists an  $x \equiv 1 \pmod{a}$  such that  $xM = 0$ .

**Proposition 3.4.5.** (Nakayama's lemma) If  $M$  is a finitely generated module and  $a \subseteq A$  is an ideal of  $A$  contained in the Jacobson radical of  $A$  then  $aM = M$  implies that  $M = 0$ .

**Proposition 3.4.6.** Suppose  $M$  is finitely generated  $A$ -module and  $a$  is an ideal contained in the Jacobson radical of  $A$  then  $aM = M + N$  implies that  $M = N$  for any submodule  $N$  of  $M$ .

**Proposition 3.4.7.** Let  $x_i$  be element of  $M$  whose image in  $M/mM$  are the basis of this vector space. Then the  $x_i$  generate  $M$ .

## 3.5 Exact Sequence

**Definition 3.5.1.** A sequence of  $A$ -modules and  $A$ -homomorphisms,

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

is said to be exact at  $M_i$  if,  $\text{Ker}(f_{i+1}) = \text{Im}(f_i)$ . The sequence is exact if it is exact at each  $M_i$ .

1.  $0 \rightarrow M' \xrightarrow{f} M$  is exact  $\Leftrightarrow f$  is injective.
2.  $M \xrightarrow{g} M'' \rightarrow 0$  is exact  $\Leftrightarrow g$  is surjective.
3.  $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$  is exact  $\Leftrightarrow f$  is injective and  $g$  is surjective. But also  $\text{Coker}(f) = M/f(M')$  is isomorphic to  $M''$ .
4. This type of exact sequence is also called a short exact sequence. Any exact sequence can be split up into a collection of short exact sequences. If  $N_i = \text{Im}(f_i) = \text{Ker}(f_{i+1})$  we have the short exact sequence  $0 \rightarrow N_i \rightarrow M_i \rightarrow N_{i+1} \rightarrow 0$  for each  $i$ .

### 3.6 Tensor Product of Modules

**Definition 3.6.1.** (*Tensor product*) The tensor product of two  $A$ -modules  $M$  and  $N$  is the  $A$ -module  $M \otimes N$  of all linear combination of the pair  $x \otimes y$  with coefficients in  $A$  along with the following properties,

1.  $(x + x') \otimes y = x \otimes y + x' \otimes y$
2.  $x \otimes (y + y') = x \otimes y + x \otimes y'$
3.  $a.x \otimes y = x \otimes a.y = a(x \otimes y)$

Properties:

1.  $0 \otimes x = 0$
2. If  $x_i$  generates  $M$  and  $y_i$  generates  $N$  then  $x_i \otimes y_i$  generates  $M \otimes N$ .
3. Let  $x \in M$  and  $y \in N$  if  $M' \subseteq M$  and  $N' \subseteq N$  are submodules then  $x \otimes y \in M \otimes N$  is not the same as  $x \otimes y \in M' \otimes N'$
4. To be specific the tensor product of  $A$ -modules is denoted by  $M \otimes_A N$  but if the context is clear we can write  $M \otimes N$ .

**Note:** The correct definition of a tensor product is by a universal property that there's a one to one correspondence between the bilinear maps  $M \times N \rightarrow P$  and the  $A$ -linear map  $M \otimes N \rightarrow P$ . But this is not important nor useful at this stage. Whatever it is is ultimately exactly equivalent to the definition above.

The following isomorphisms are considered canonical.

**Proposition 3.6.2.** Let  $M, N, P$  be  $A$ -modules. Then there exists unique isomorphism

1.  $M \otimes N \rightarrow N \otimes M$ , (given by  $x \otimes y \mapsto y \otimes x$ )
2.  $(M \otimes N) \otimes P \rightarrow M \otimes (N \otimes P) \rightarrow M \otimes N \otimes P$ , (given by  $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z) \mapsto x \otimes y \otimes z$ )
3.  $(M \oplus N) \otimes P \rightarrow (M \otimes P) \oplus (N \otimes P)$ , given by  $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$
4.  $A \otimes M \rightarrow M$ , given by  $a \otimes x \mapsto ax$ .

### 3.7 Restriction and extension of scalars

**Definition 3.7.1.** Let  $f : A \rightarrow B$  be a ring homomorphism and  $N$  be a  $B$ -module then the  $A$ -module defined by the action  $f(a)x$  where  $a \in A$  and  $x \in N$  is called the  $A$ -module obtained by *restriction of scalars*. The homomorphism induces an  $A$ -module structure on  $N$ . Then the module  $M_B = B \otimes M$  where  $B$  is considered as an  $A$ -module is said to be obtained from  $M$  by the extension of scalars.  $M_B$  also has a  $B$ -module structure as well by  $b(b' \otimes x) = bb' \otimes x$ .

**Proposition 3.7.2.** Let  $N$  be a finitely generated  $B$ -modules and  $B$  be a finitely generated  $A$ -module then  $N$  is a finitely generated as an  $A$ -module.

**Proposition 3.7.3.** If  $M$  is finitely generated as an  $A$ -module then  $M_B$  is finitely generated as a  $B$ -module!

### 3.8 Exactness Properties of the Tensor Product

The set  $S$  of  $A$ -bilinear mappings  $M \times N \rightarrow P$  is in natural 1-1 correspondence with  $\text{Hom}(M, \text{Hom}(N, P))$  but by the definition of the Tensor product  $S$  is in 1-1 correspondence with the  $A$ -linear maps  $M \otimes N \rightarrow P$ . There fore we have,

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

For a  $A$ -module  $N$  let  $T(M) = M \otimes N$  be a functor that takes modules to modules and let  $U(P) = \text{Hom}(N, P)$ . Then by the correspondence formula above we have,

$$\text{Hom}(T(M), P) = \text{Hom}(M, U(P))$$

This condition means exactly in the language of category theory that  $T$  is the left-adjoint of  $U$  and that  $U$  is the right-adjoint of  $T$ .

**Note:** The following proposition says that any functor which is left adjoint is right exact and any functor which is right adjoint is left exact.

**Proposition 3.8.1.** *If,  $M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$  is an exact sequence of  $A$ -modules and homomorphisms then for any  $A$ -module  $N$ ,*

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

*is an exact sequence as well where 1 denotes the identity map taking  $N$  to  $N$ .*

In general tensoring with an  $A$ -module does not turn an exact sequence into another exact sequence. But

**Definition 3.8.2.** (Flat Modules) *Let  $N$  be an  $A$ -moduels and let  $T_N : M \mapsto M \otimes N$  be a functor. If  $T_N$  is exact, that is tensoring with  $N$  turns all exact sequences into exact sequences, then  $N$  is called a flat module.*

**Proposition 3.8.3.** *The following statements are equivalent, for an  $A$ -module  $N$ :*

1.  $N$  is flat
2. *If  $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$  is any exact sequences of  $A$ -moduels, the tensored sequence  $0 \rightarrow M' \otimes N \rightarrow M \otimes N \rightarrow M'' \otimes N \rightarrow 0$  is exact.*
3. *If  $f : M' \rightarrow M$  is injective, then  $f \otimes 1 : M' \otimes N \rightarrow M \otimes N$  is injective.*
4. *If  $f : M' \rightarrow M$  is injective and  $M, M'$  are finitely generated, then  $f \otimes 1 : M' \otimes N \rightarrow M \otimes N$  is injective.*

**Exercise 3.8.4.** *A partially ordered set  $I$  is said to be a directed set if for each pair  $i, j$  in  $I$  there exists  $k \in I$  such that  $i \leq k$  and  $j \leq k$ .*

*Let  $A$  be a ring, let  $I$  be a directed set and let  $(M_i)_{i \in I}$  be a family of  $A$ -modules indexed by  $I$ . For each pair  $i, j$  in  $I$  such that  $i \leq j$ , let  $\mu_{ij} : M_i \rightarrow M_j$  be an  $A$ -homomorphism, and suppose that the following axioms are satisfied:*

1.  $\mu_{ii}$  is the identity mapping of  $M_i$ , for all  $i \in I$ .
2.  $\mu_{ik} = \mu_{jk} \circ \mu_{ij}$  whenever  $i \leq j \leq k$ .



Then the module  $M_i$  and homomorphism  $\mu_{ij}$  are said to form a directed system  $M = (M_i, \mu_{ij})$  over the directed set  $I$ .

We shall construct an  $A$ -module  $M$  called the direct limit of the direct system  $M$ . Let  $C$  be the direct sum of the  $M_i$ , and identify each module  $M_i$  with its canonical image in  $C$ . Let  $D$  be the submodule of  $C$  generated by all elements of the form  $x_i - \mu_{ij}(x_j)$  where  $i \leq j$  and  $x_j \in M_j$ . Let  $M = C/D$ , let  $\mu : C \rightarrow M$  be the projection and let  $\mu_j$  be the restriction of  $\mu$  to  $M_j$ .

The module  $M$ , or more correctly the pair consisting of  $M$  and the family of homomorphisms  $\mu_i : M_i \rightarrow M$ , is called the direct limit of the direct system  $M$ , and is written  $\varinjlim M_i$ . From the construction it is clear that  $\mu_i = \mu_j \circ \mu_{ij}$  whenever  $i \leq j$ . (Ex 14)

**Exercise 3.8.5.** Show that the direct limit is characterized (up to isomorphism) by the following property. Let  $N$  be an  $A$ -module and for each  $i \in I$  let  $\alpha_i : M_i \rightarrow N$  be an  $A$ -module homomorphism such that  $\alpha_i = \alpha_j \circ \mu_{ij}$  whenever  $i \leq j$ . Then there exists a unique homomorphism  $\alpha : M \rightarrow N$  such that  $\alpha_i = \alpha \circ \mu_i$  for all  $i \in I$ . (Ex 16)

## Chapter 4

# Rings and Modules of Fractions

### 4.1 Ring of Fractions

The standard rings of fraction of a ring  $A$  can only be defined when  $A$  is an integral domain. But we can generalise the notion to arbitrary rings. Let  $A$  be a commutative ring and  $S$  be a \*multiplicative subset\* of  $A$ . That is  $1 \in S$  and for every  $x, y \in S$ ,  $xy \in S$ . Define the equivalence relation  $\sim$  on  $A \times S$  to be:

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

**Definition 4.1.1.** Define the fraction  $a/s$  to be the equivalence class of  $(a, s)$  and let  $S^{-1}A$  denote the set of these equivalence classes. Then  $S^{-1}A$  is a ring with addition and multiplication defined by,

$$(a/s) + (b/t) = (at + bs)/st,$$

$$(a/s)(b/t) = ab/st.$$

$S^{-1}A$  is called the ring of fraction of  $A$  with respect to  $S$ . By  $f$  we mean the ring homomorphism  $f : A \rightarrow S^{-1}A$  defined by  $f(x) = x/1$ .

**Exercise 4.1.2.** Verify that these definitions are independent of the choices of representatives  $(a, s)$  and  $(b, t)$ , and that  $S^{-1}A$  satisfies the axioms of a commutative ring with identity.

The ring  $S^{-1}A$  and the homomorphism  $f : A \rightarrow S^{-1}A$  have the following property:

1.  $s \in S \implies f(s)$  is a unit in  $S^{-1}A$ .
2.  $f(a) = 0 \implies as = 0$  for some  $s \in S$ .
3. Every element of  $S^{-1}A$  is of the form  $f(a)f(s)^{-1}$  for some  $a \in A$  and some  $s \in S$ .

### 4.2 Localization

$S = A - \mathfrak{p}$ , is a multiplicative subset of  $A \Leftrightarrow \mathfrak{p}$  is prime. In this case write  $A_{\mathfrak{p}}$  instead of  $S^{-1}A$ . \*\*The process of passing from  $A$  to  $A_{\mathfrak{p}}$  is called localisation at  $\mathfrak{p}$ .\*\*

1.  $A_p$  is a local ring. To see this we construct an ideal  $\mathfrak{m}$  in  $A_p$  as the set of elements  $a/s \in A_p$  such that  $a \in \mathfrak{p}$ .  $\mathfrak{m}$  has the property that if  $b/s \notin \mathfrak{m}$  then  $b \notin \mathfrak{p}$  and hence  $b \in S$  which makes  $b/s$  a unit. So if  $A_p$  contains an ideal not in  $\mathfrak{m}$  then it must contain a unit and so it's the whole ring. Therefore  $\mathfrak{m}$  is the only maximal ideal of  $A_p$ .
2.  $S^{-1}A$  is the zero ring if and only if  $0 \in S$ .
3. Let  $f \in A$  and let  $S = \{f^n\}_{n \geq 0}$ . We denote by  $A_f$ , the ring of fractions  $S^{-1}A$ .
4. **Example:** If  $\mathfrak{a}$  is an ideal in  $A$  then  $S = 1 + \mathfrak{a}$  is multiplicatively closed.
5. Local ring of  $k^n$  along the variety  $V$ : Let  $A = k[t_1, \dots, t_n]$  where  $k$  is a field.  $A_p$  is the set of all rational functions  $f/g$  where  $g \notin \mathfrak{p}$ . If  $V = V(\mathfrak{p})$  is a variety then  $A_p$  can be identified with the ring of all rational function on  $k^n$  that are defined at almost all points in  $V$ .

### 4.3 Ring of fraction of Modules

$S^{-1}M$  is an  $S^{-1}A$ -module when  $M$  is an  $A$ -module. When  $S = A - \mathfrak{p}$  we denote the ring of fractions by  $M_p$ .

If  $u : M \rightarrow N$  is an  $A$ -module homomorphism. Then it gives rise to an  $S^{-1}A$ -module homomorphism  $S^{-1}u : S^{-1}M \rightarrow S^{-1}N$ , namely  $S^{-1}u$  maps  $m/s$  to  $u(m)/s$ . We have  $S^{-1}(v \circ u) = (S^{-1}v) \circ (S^{-1}u)$

**Proposition 4.3.1.**  $S^{-1}$  is exact. If  $M' \rightarrow_f M \rightarrow_g M''$  is exact at  $M$  then  $S^{-1}M \rightarrow_{S^{-1}f} S^{-1}M \rightarrow_{S^{-1}g} S^{-1}M''$  is exact at  $S^{-1}M$ .

If  $M'$  is a submodule of  $M$  then  $S^{-1}M' \rightarrow S^{-1}M$  is injective and  $S^{-1}M'$  is a submodule of  $S^{-1}M$ .

**Corollary 4.3.1.1.** Formation of fractions commutes with formation of finite sums, finite intersections and quotients. Precisely, if  $N, P$  are submodules of an  $A$ -module  $M$ , then,

1.  $S^{-1}(N + P) = S^{-1}(N) + S^{-1}(P)$
2.  $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$
3.  $S^{-1}(M/N)$  and  $S^{-1}M/S^{-1}N$  are isomorphic.

**Proposition 4.3.2.** Let  $M$  be an  $A$ -module. Then  $S^{-1}M$  is isomorphic to  $S^{-1}A \otimes_A M$ . That is there exists a unique isomorphism  $f : S^{-1}A \otimes_A M \rightarrow S^{-1}M$  given by,

$$f((a/s) \otimes m) = am/s \text{ for all } a \in A, m \in M \text{ and } s \in S$$

**Corollary 4.3.2.1.**  $S^{-1}A$  is a flat  $A$ -module.

**Proposition 4.3.3.** If  $M, N$  are  $A$ -modules then there is a unique isomorphism,  $f : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \rightarrow S^{-1}(M \otimes_A N)$  given by,

$$f((m/s) \otimes (n/t)) = (m \otimes n)/st$$

If  $\mathfrak{p}$  is any prime ideal then

$$M_p \otimes_{A_p} N_p \cong (M \otimes_A N)_p$$

## 4.4 Some examples of local properties

**Proposition 4.4.1.** *Let  $M$  be an  $A$ -module. Then the following are equivalent:*

1.  $M = 0$
2.  $M_{\mathfrak{p}} = 0$  for all prime ideals  $\mathfrak{p}$  of  $A$
3.  $M_{\mathfrak{m}} = 0$  for all maximal ideals  $\mathfrak{m}$  of  $A$

**Proposition 4.4.2.** *Let  $\phi : M \rightarrow N$  be an  $A$ -module homomorphism. Then the following are equivalent:*

1.  $\phi$  is injective
2.  $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$  is injective for each prime ideal  $\mathfrak{p}$ .
3.  $\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \rightarrow N_{\mathfrak{m}}$  is injective for each maximal ideal  $\mathfrak{m}$ . Similarly with "injective" replaced by "surjective" throughout.

**Note:** Flatness is a local property.

**Proposition 4.4.3.** *For any  $A$ -module  $M$ , the following statements are equivalent:*

1.  $M$  is a flat  $A$ -module
2.  $M_{\mathfrak{p}}$  is a flat  $A_{\mathfrak{p}}$ -module for each prime ideal  $\mathfrak{p}$ .
3.  $M_{\mathfrak{m}}$  is a flat  $A_{\mathfrak{m}}$ -module for each maximal ideal  $\mathfrak{m}$

**Exercise 4.4.4.** 1. Let  $A$  be a ring.  $S$  is a multiplicatively closed subset of  $A$ , and  $\phi : A \rightarrow S^{-1}A$  the canonical homomorphism. Show that  $\phi^* : \text{Spec}(S^{-1}A) \rightarrow \text{Spec}(A)$  is a homomorphism of  $\text{Spec}(S^{-1}A)$  onto its image in  $X = \text{Spec}(A)$ . Let this image be denoted by  $S^{-1}X$ . In particular, if  $f \in A$ , the image of  $\text{Spec}(A_f)$  in  $X$  is the basic open set  $X_f$ .

2. Let  $f : A \rightarrow B$  be a ring homomorphism. Let  $X = \text{Spec}(A)$  and  $Y = \text{Spec}(B)$ , and let  $f^* : Y \rightarrow X$  be the mapping associated with  $f$ . Identifying  $\text{Spec}(S^{-1}A)$  with its canonical image  $S^{-1}X$  in  $X$ , and  $\text{Spec}(S^{-1}B) (= \text{Spec}(f(S)^{-1}B))$  with its canonical image  $S^{-1}Y$  in  $Y$ , show that  $S^{-1}f^* : \text{Spec}(S^{-1}B) \rightarrow \text{Spec}(S^{-1}A)$  is the restriction of  $f^*$  to  $S^{-1}Y$ , and that  $S^{-1}Y = f^{*-1}(S^{-1}X)$ .

3. Let  $\mathfrak{a}$  be an ideal of  $A$  and let  $\mathfrak{b} = \mathfrak{b}^e$  be its extension in  $B$ . Let  $\bar{f} : A/\mathfrak{a} \rightarrow B/\mathfrak{b}$  be the homomorphism induced by  $f$ . If  $\text{Spec}(A/\mathfrak{a})$  is identified with its canonical image  $V(\mathfrak{a})$  in  $X$ , and  $\text{Spec}(B/\mathfrak{b})$  with its image  $V(\mathfrak{b})$  in  $Y$ , show that  $\bar{f}^*$  is the restriction of  $f^*$  to  $V(\mathfrak{b})$ .

4. Let  $\mathfrak{p}$  be a prime ideal of  $A$ . Take  $S = A - \mathfrak{p}$  in 2) and then reduce mod  $S^{-1}\mathfrak{p}$  as in 3). Deduce that the subspace  $f^{*-1}(\emptyset)$  of  $Y$  is naturally homeomorphic to  $\text{Spec}(B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}) = \text{Spec}(k(\mathfrak{p}) \otimes_A B)$ , where  $k(\mathfrak{p})$  is the residue field of the local ring  $A_{\mathfrak{p}}$ .

$\text{Spec}(k(\mathfrak{p}) \otimes_A B)$  is called the fiber of  $f^*$  over  $\mathfrak{p}$ .

(Ex 21)

**Exercise 4.4.5.** Let  $A$  be a ring and  $\mathfrak{p}$  a prime ideal of  $A$ . Then the canonical image of  $\text{Spec}(A_{\mathfrak{p}})$  in  $\text{Spec}(A)$  is equal to the intersection of all the open neighborhoods of  $\mathfrak{p}$  in  $\text{Spec}(A)$ . (Ex 22)

**Exercise 4.4.6.** Let  $A$  be a ring, let  $X = \text{Spec}(A)$  and let  $U$  be a basic open set in  $X$  (i.e.  $U = X_f$ , for some  $f \in A$ : Chapter 1, Ex 17)

1. If  $U = X_f$ , show that the ring  $A(U) = A_f$  depends only on  $U$  and not on  $f$ .
2. Let  $U' = X$ , be another basic open set such that  $U' \subseteq U$ . Show that there is an equation of the form  $g^n = u f$  for some integer  $n > 0$  and some  $u \in A$  and use this to define a homomorphism  $\rho : A(U) \rightarrow A(U')$  (i.e.  $A_f \rightarrow A_g$ ) by mapping  $a/f^m$  to  $au^m/g^{mn}$ . Show that  $\rho$  depends only on  $U$  and  $U'$ . This homomorphism is called the restriction homomorphism.
3. If  $U = U'$ , then  $\rho$  is the identity map.
4. If  $U \supseteq U' \supseteq U''$  are basic open sets in  $X$ , show that the diagram

$$\begin{array}{ccc} A(U) & \xrightarrow{\quad} & A(U'') \\ & \searrow & \nearrow \\ & A(U') & \end{array}$$

(in which the arrows are restriction homomorphisms) is commutative.

5. Let  $x(=\mathfrak{p})$  be a point of  $X$ . Show that

$$\varinjlim_{U \ni x} A(U) \cong A_{\mathfrak{p}}$$

The assignment of the ring  $A(U)$  to each basic open set  $U$  of  $X$ , and the restriction homomorphism  $\rho$ , satisfying the conditions 3) and 4) above, constitutes a presheaf of rings on the basis of open sets  $(X_f)_{f \in A}$ . 5) says that the stalk of this presheaf at  $x \in X$  is the corresponding local ring  $A_{\mathfrak{p}}$ . (Ex 23)

**Exercise 4.4.7.** Show that the presheaf of Ex 23 has the following property. Let  $(U_i)_{i \in I}$  be a covering of  $X$  by basic open sets. For each  $i \in I$  let  $s_i \in A(U_i)$  be such that, for each pair of indices  $i, j$ , the images of  $s_i$  and  $s_j$  in  $A(U_i \cap U_j)$  are equal. Then there exists a unique  $s \in A(=A(X))$  whose image in  $A(U_i)$  is  $s_i$ , for all  $i \in I$ . (This essentially implies that the presheaf is a sheaf.) (Ex 24)

**Exercise 4.4.8.** 1. Let  $f_{\alpha} : A \rightarrow B_{\alpha}$  be any family of  $A$ -algebras and let  $f : A \rightarrow B$  be their tensor product over  $A$  (Chap 2, Ex 23). Then

$$f^*(\text{Spec}(B)) = \bigcap_{\alpha} f_{\alpha}^*(\text{Spec}(B_{\alpha})).$$

2. Let  $f_{\alpha} : A \rightarrow B_{\alpha}$  be any finite family of  $A$ -algebras and let  $B = \prod_{\alpha} B_{\alpha}$ . Define  $f : A \rightarrow B$  by  $f(x) = (f_{\alpha}(x))$ . Then  $f^*(\text{Spec}(B)) = \bigcup_{\alpha} f_{\alpha}^*(\text{Spec}(B_{\alpha}))$ .

3. Hence the subsets of  $X = \text{Spec}(A)$  of the form  $f^*(\text{Spec}(B))$ , where  $f : A \rightarrow B$  is a ring homomorphism, satisfy the axioms for closed sets in a topological space. The associated topology is the constructible topology on  $X$ . It is finer than the Zariski topology (i.e, there are more open sets, or equivalently more closed sets).
4. Let  $X_C$  denote the set  $X$  endowed with the constructible topology. Show that  $X_C$  is quasi-compact.  
(Ex 27)

**Exercise 4.4.9.** 1. For each  $g \in A$ , the set  $X_g$  (Chap 1, Ex 17) is both open and closed in the constructible topology.

2. Let  $C'$  denote the smallest topology on  $X$  for which the sets  $X_g$  are both open and closed, and let  $X_C$  denote the set  $X$  endowed with this topology. Show that  $X_C$  is Hausdorff.
3. Deduce that the identity mapping  $X_C \rightarrow X_{C'}$  is a homeomorphism. Hence a subset  $E$  of  $X$  is of the form  $f^*(\text{Spec}(B))$  for some  $f : A \rightarrow B$  if and only if it is closed in the topology of  $C'$ .
4. The topological space  $X_C$  is compact, Hausdorff and totally disconnected.  
(Ex 28)

**Exercise 4.4.10.** Let  $f : A \rightarrow B$  be a ring homomorphism. Show that  $f^* : \text{Spec}(B) \rightarrow \text{Spec}(A)$  is a continuous closed mapping (i.e., maps closed sets to closed sets) for the constructible topology. (Ex 29)

**Exercise 4.4.11.** Show that the Zariski topology and the constructible topology on  $\text{Spec}(A)$  are the same if and only if  $A/\mathfrak{N}$  is absolutely flat (where  $\mathfrak{N}$  is the nilradical of  $A$ ). (Ex 30)

**Exercise 4.4.12.** Let  $A$  be a ring. Prove that the following are equivalent:

1.  $A/\mathfrak{N}$  is absolutely flat ( $\mathfrak{N}$  being the nilradical of  $A$ ).
2. Every prime ideal of  $A$  is maximal.
3.  $\text{Spec}(A)$  is  $T_1$ -space (i.e., every subset consisting of a single point is closed).
4.  $\text{Spec}(A)$  is Hausdorff.

If these conditions are satisfied, show that  $\text{Spec}(A)$  is compact and totally disconnected (i.e., the only connected subsets of  $\text{Spec}(A)$  are those consisting of a single point). (Ex 11)

## Chapter 5

# Integral Dependence and the Going-Up Theorem

### 5.1 Integral Dependence

The going up and going down theorems are due to Cohen-Seidenberg.

**Definition 5.1.1.** (*Integral element*) Let  $B$  be a ring and  $A$  a subring of  $B$  with unity. An element  $x$  in  $B$  is said to be *integral* over  $A$  if  $x$  is a root of a *monic* polynomial with coefficients in  $A$ , i.e. if  $x$  satisfies an equation of the form

$$x^n + a_1x^{n-1} + \cdots + a_n = 0$$

where  $a_i \in A$ .

Every element of  $A$  is integral over  $A$ .

**Example 5.1.2.**  $A = \mathbb{Z}, B = \mathbb{Q}$ . If a rational number  $x = r/s$  is integral over  $\mathbb{Z}$ , where  $r, s$  have no common factor, we have,

$$r^n + a_1r^{n-1}s + \cdots + a_ns^n = 0$$

the  $a_i$  being rational integers. Hence  $s$  divides  $r^n$ , hence  $s = \pm 1$ , hence  $x \in \mathbb{Z}$ .

**Proposition 5.1.3.** The following are equivalent:

1.  $x \in B$  is integral over  $A$ .
2.  $A[x]$  is a finitely generated  $A$ -module.
3.  $A[x]$  is contained in a subring  $C$  of  $B$  such that  $C$  is a finitely generated  $A$ -module.
4. There exists a faithful  $A[x]$ -module  $M$  which is finitely generated as an  $A$ -module.

**Corollary 5.1.3.1.** Let  $x_i (1 \leq i \leq n)$  be elements of  $B$ , each integral over  $A$ . Then the ring  $A[x_1, \dots, x_n]$  is a finitely generated  $A$ -module.

**Corollary 5.1.3.2.** The set  $C$  of elements in  $B$  which are integral over  $A$  is a subring of  $B$  containing  $A$ .

**Definition 5.1.4.** (*Integral Closure*) The ring  $C$  in the above corollary is called the *\*integral closure\** of  $A$  in  $B$ . If  $C=A$ , then  $A$  is said to be *\*integrally closed\** in  $B$ . If  $C=B$ , the ring  $B$  is said to be *\*integral over\**  $A$ .

**Definition 5.1.5.** Let  $f : A \rightarrow B$  be a ring homomorphism, so that  $B$  is an  $A$ -algebra. Then  $f$  is said to be *\*integral\**, and  $B$  is said to be an *\*integral\**  $A$ -algebra, if  $B$  is integral over its subring  $f(A)$ . In this terminology, the above results show that,

$$\text{finite type} + \text{integral} = \text{finite}$$

**Corollary 5.1.5.1.** If  $A \subseteq B \subseteq C$  are rings and if  $B$  is integral over  $A$  and  $C$  is integral over  $B$ , then  $C$  is integral over  $A$  (transitivity of integral dependence).

**Corollary 5.1.5.2.** Let  $A \subseteq B$  be rings and let  $C$  be the integral closure of  $A$  in  $B$ . Then  $C$  is integrally closed in  $B$ .

We show that integral dependence is preserved on passing to quotients and to rings of fractions.

**Proposition 5.1.6.** Let  $A \subseteq B$  be rings,  $B$  integral over  $A$ .

1. If  $\mathfrak{b}$  is an ideal of  $B$  and  $\mathfrak{a} = \mathfrak{b}^c = A \cap \mathfrak{b}$ , then  $B/\mathfrak{b}$  is integral over  $A/\mathfrak{a}$ .
2. If  $S$  is a multiplicatively closed subset of  $A$ , then  $S^{-1}B$  is integral over  $S^{-1}A$ .

## 5.2 The Going-up Theorem

**Proposition 5.2.1.** Let  $A \subseteq B$  be integral domains,  $B$  integral over  $A$ . Then  $B$  is a field if and only if  $A$  is a field.

**Corollary 5.2.1.1.** Let  $A \subseteq B$  be rings,  $B$  integral over  $A$ ; let  $\mathfrak{q}$  be a prime ideal of  $B$  and let  $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap A$ . Then  $\mathfrak{q}$  is maximal if and only if  $\mathfrak{p}$  is maximal.

**Corollary 5.2.1.2.** Let  $A \subseteq B$  be rings.  $B$  integral over  $A$ ; let  $\mathfrak{q}, \mathfrak{q}'$  be prime ideals of  $B$  such that  $\mathfrak{q} \subseteq \mathfrak{q}'$  and  $\mathfrak{q}^c = \mathfrak{q}'^c = \mathfrak{p}$  say. Then  $\mathfrak{q} = \mathfrak{q}'$ .

**Theorem 5.2.2.** Let  $A \subseteq B$  be rings,  $B$  integral over  $A$ , and let  $\mathfrak{p}$  be a prime ideal of  $A$ . Then there exists a prime ideal  $\mathfrak{q}$  of  $B$  such that  $\mathfrak{q} \cap A = \mathfrak{p}$ .

**Theorem 5.2.3.** (*Going-up theorem*)\* Let  $A \subseteq B$  be rings,  $B$  integral over  $A$ ; let  $\mathfrak{p}_1 \subseteq \dots \subseteq \mathfrak{p}_n$  be a chain of prime ideals of  $A$  and  $\mathfrak{q} \subseteq \dots \subseteq \mathfrak{q}_m$  ( $m < n$ ) a chain of prime ideals of  $B$  such that  $\mathfrak{q}_i \cap A = \mathfrak{p}_i$  ( $1 \leq i \leq m$ ). Then the chain  $\mathfrak{q}_1 \subseteq \dots \subseteq \mathfrak{q}_m$  can be extended to a chain  $\mathfrak{q}_1 \subseteq \dots \subseteq \mathfrak{q}_n$  such that  $\mathfrak{q}_i \cap A = \mathfrak{p}_i$  for  $1 \leq i \leq n$ .