Introduction to Commutative Algebra

Amal M

January 4, 2021

Abstract

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 florished 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.

Chapter 1

Introduction: What is Algebraic Geometry?

1.1 Some historical problems

1.1.1 27 lines

1.1.2 Bezout's Theorem

1.1.3 Brief History of Algebraic Geometry

1.2 What is geometry?

1.3 What is algebra?

Chapter 2

Hilbert's Nullstellensatz

2.1 Basics ideas in ring theory

2.2 The Nullstellensatz

Chapter 3

Rings and Ideals

3.1 Basic Definitions

Definition 3.1.1. *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. *Multipicatio 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 3.1.2. *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 3.1.3. *A subset S of a ring A is a subring of A if S is closed under addition and multiplication and contains th identity element of A.*

3.2 Ideals and Quotients

Definition 3.2.1. *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 3.2.2. *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 $\phi : A \to A/\mathfrak{a}$ which maps each $x \in A$ to its coset $x + \mathfrak{a}$ is a surjective ring homomorphism.*

Proposition 3.2.3. *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 $\mathfrak{b} = \phi^{-1}(\bar{\mathfrak{b}})$.*

3.3 Zero-Divisors, Nilpotent Elements, Units

Definition 3.3.1. *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 3.3.2. *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 3.3.3. *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 3.3.4. *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.*

3.4 Prime and Maximal Ideals

Definition 3.4.1. *An ideal $\mathfrak{p}$ in A is prime if $\mathfrak{p} \neq (1)$ and if $xy \in \mathfrak{p} \implies x \in \mathfrak{p} or y \in \mathfrak{p}$. 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:*

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

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

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

1. *If $f : A \to B$ 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 3.4.2. *Every commutative ring A (with identity) $\neq 0$ has at least one maximal ideal.*

Corollary 3.4.2.1. *Every non-unit of A is contained in a maximal ideal.*

Definition 3.4.3. *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.*

Proposition 3.4.4.
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 3.4.5. *$A = k[x_1, \cdots, x_n], k$ is a field. Let $f \in A$ be an irreducible polynomial. By unique factorization, the ideal (f) is prime.*

Example 3.4.6. *$A = Z$. Every ideal in Z is of the form (m) for some $m \geq 0$. The ideal (m) is prime $\Leftrightarrow \mathfrak{m} = 0$ or a prime number. All the ideals (p), where $\mathfrak{p}$ is a prime number are maximal: $Z/(p)$ is a field of p elements.*

3.5 Nilradical and Jacobson Radical

Proposition 3.5.1. *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 3.5.2. *The ideal $\mathfrak{N}$ is called the nilradical of A. The following proposition gives an alternative definition of $\mathfrak{N}$:*

Proposition 3.5.3. *The nilradical of A is the intersection of all the prime ideals of A.*

Definition 3.5.4. *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 3.5.5. *$x \in \mathfrak{R} \Leftrightarrow 1 - xy$ is a unit in A for all $y \in A$.*

3.6 Some properties of ideals

Definition 3.6.1. *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 $Ann(\mathfrak{b})$.*

Definition 3.6.2. *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 $\phi : A \to A/\mathfrak{a}$ 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 3.6.3. *1. $r(\mathfrak{a}) \supseteq \mathfrak{a}$*

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

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

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

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

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

Proposition 3.6.4. *The radical of an ideal $\mathfrak{a}$ is the intersection of the prime ideals which contain $\mathfrak{a}$.*

Proposition 3.6.5. *D = set of zero-divisors of $A = \bigcup_{x \neq 0} r(Ann(x))$.*

Proposition 3.6.6. *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.*

Chapter 4

Modules

4.1 Modules and Module homomorphisms

Definition 4.1.1. *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, μ) is called a module

4.2 Submodules and Quotient Modules

Definition 4.2.1. *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 4.2.2. *If $f : M \to N$ A-module homomorphism then,*

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

Proposition 4.2.3. *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 4.2.4. *(Induced homomorphism) If $M' \subseteq Ker(f)$. Define $\bar{f} : M/M' \to N$ as $\bar{f}(\bar{x}) = f(x)$. Then it is a homomorphism and it is said to be induced by f. Specially we have, $Ker(\bar{f}) = Ker(f)/M'$.*

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

Proposition 4.2.5. *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

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

4.2.1 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, $Ann(M) = (0, M) = \{a \in A : aM = 0\}$*
4. *An A-module is called *faithful* if $Ann(M) = 0$.*
5. *If $a \subseteq Ann(M)$ 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 indepenent of the choice of the representative of $\bar{x}$.*
6. *If $Ann(M) = a$, then M is faithful as an $A/a-$module.*

4.3 Direct Sum and Product

Definition 4.3.1. *(Direct Sum) Given two A-moduels 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,*

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

$$a.(x, y) = (ax, ay)$$

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 4.3.2. *(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.*

4.4 Finitely Generated Module

Definition 4.4.1. *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.*

4.4.1 Free Module

Definition 4.4.2. *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 $\oplus_{i \in I} M_i$, where M_i are A-modules isomorphic to A. * A^0 is the zero module denoted by 0.*

Proposition 4.4.3. *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 4.4.4. *Let M be a finitely generated A-module and $a \subseteq A$ be an ideal of M. If ϕ is an endomorphism of M such that $\phi(M) \subseteq aM$ then ϕ satisfies a polynomial equation in ϕ,*

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

for some $a_i \in a$.

Corollary 4.4.4.1. *If M is a finitely generated module such that for an ideal $a \subseteq A$, $aM = M$ then there exists an $x \equiv 1 (mod\ a)$ such that $xM = 0$.*

Proposition 4.4.5. *(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 4.4.6. *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 4.4.7. *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.*

4.5 Exact Sequence

Definition 4.5.1. *A sequence of A-modules and A-homomorphisms,*

$$\cdots \to M_{i-1} \to^{f_i} M_i \to^{f_{i+1}} M_{i+1} \to \cdots$$

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

1. $0 \to M' \to^f M$ *is exact* $\Leftrightarrow$ f *is inective.*

2. $M \to^g M'' \to 0$ *is exact* $\Leftrightarrow$ g *is surjective.*

3. $0 \to M' \to^f M \to^g M'' \to 0$ *is exact* $\Leftrightarrow$ f *is injective and* g *is surjective. But also* $Coker(f) = M/f(M')$ *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* $N_i = Im(f_i) = Ker(f_{i+1})$ *we have the short exact sequence* $0 \to N_i \to M_i \to N_{i+1} \to 0$ *for each* i*.*

4.6 Tensor Product of Modules

Definition 4.6.1. *(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* $M \times N \to P$ *and the* A*-linear map* $M \otimes N \to P$*. But this is not important nor useful at this stage. Whatever it is is ultimately exactly equivalent to the definition above.*

Chapter 5

Rings and Modules of Fractions

Chapter 6

Integral Dependence

Bibliography