# M4P55 Commutative Algebra

Lectured by Prof Alexei Skorobogatov
Typed by David Kurniadi Angdinata

Autumn 2019

**Syllabus**

# Contents

# 0 Introduction

Lecture 1
Thursday
03/10/19

The prerequisites are

- groups,
- rings,
- fields, and
- a solid linear algebra.

This course is good for

- algebraic geometry, and
- algebraic number theory.

The following are books.

- M Reid, Undergraduate commutative algebra, 1995
- M F Atiyah and I G Macdonald, Introduction to commutative algebra, 1969

The following is the structure of the course.

- Generalities on rings, such as ideals, and examples.
- Localisation of rings between a ring $R$ and the fraction field $K$ of $R$, such as $\mathbb{Z}$ and $\mathbb{Q}$.
- Finiteness conditions of Noetherian rings and Artinian rings.
- Integral closure and normal rings, such as $\mathbb{Z}[i] \subset \mathbb{Q}(i)$ and $\mathbb{Z}\left[\sqrt{-3}\right] \subset \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \subset \mathbb{Q}\left(\sqrt{-3}\right)$.
- Discrete valuation rings.
- Completion of rings with topology.

# 1 Rings and ideals

**Definition 1.1.** A **commutative ring** is a set $(A, +, \cdot, 0, 1)$ such that

1. $(A, +, 0)$ is an abelian group,
2. for all $x, y, z \in A$,
   - $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
   - $x \cdot y = y \cdot x$,
   - $x \cdot (y + z) = x \cdot y + x \cdot z$, and
3. for all $x \in A$, $x \cdot 1 = 1 \cdot x = x$.

**Remark 1.2.**

- One is uniquely determined by 3, since $1' = 1' \cdot 1 = 1$.
- If $1 = 0$, then $0 = x \cdot 0 = x \cdot 1 = x$, since

$$x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0,$$

  so $x \cdot 0 = 0$. So every element is zero. Hence $R = \{0\}$.

**Definition 1.3.** A **homomorphism of rings** $f : A \to B$ is a map such that for all $x, y \in A$,

$$f(x + y) = f(x) + f(y), \qquad f(xy) = f(x) f(y), \qquad f(1) = 1.$$

**Example.** If $A \subset B$ is closed under $+$ and $\cdot$, and $1 \in A$, then

$$\begin{array}{ccc} A & \longrightarrow & B \\ x & \longmapsto & x \end{array}$$

is a homomorphism.

**Remark 1.4.**

- A composition of homomorphisms is a homomorphism.
- An **isomorphism** is a bijective homomorphism.

**Definition 1.5.** A subset $I$ of a ring $A$ is an **ideal** if $I$ is a subgroup of the additive group $(A, +)$ which is closed under multiplication by elements of $A$, so $xI \subset I$ for any $x \in A$. Sometimes this is written as $I \triangleleft A$. In this case the **quotient group** $A/I$ is naturally a ring, where $(x + I)(y + I)$ is defined as $xy + I$.

**Proposition 1.6.** *Let $I$ be an ideal of a commutative ring $A$. Then there is a natural bijection between the ideals $J \subset A$ such that $I \subset J$ and the ideals of $A/I$.*

*Proof.* Let

$$\begin{array}{ccc} A & \longrightarrow & A/I \\ x & \longmapsto & x + I \end{array}$$

be the natural surjective map. Send $J$ to its image under this map. □

**Definition 1.7.** If $f : A \to B$ is a homomorphism, then

$$\operatorname{Ker} f = \{x \in A \mid f(x) = 0\}$$

is an ideal in $A$, and

$$\operatorname{Im} f = f(A) \cong A/\operatorname{Ker} f \subset B.$$

## 2 Polynomials and formal power series

Lecture 2
Tuesday
08/10/19

**Definition 2.1.** Let $R$ be a ring. The **polynomial ring** with coefficients in $R$ is

$$R[x] = \{a_0 + \cdots + a_n x^n \mid a_i \in R,\ n \in \mathbb{Z}_{\geq 0}\}.$$

The addition is coefficient-wise, and the multiplication is given by the formula

$$\left(\sum_{i\geq 0} a_i x^i\right)\left(\sum_{j\geq 0} b_j x^j\right) = \sum_{i\geq 0}\left(\sum_{j+k=i,\ j\geq 0,\ k\geq 0} a_j b_k\right) x^i,$$

where all but finitely many coefficients are zero. Define

$$R[x_1,\ldots,x_n] = R[x_1]\ldots[x_n] = \left\{ \sum_{i_1,\ldots,i_n\geq 0} a_{i_1,\ldots,i_n} x_1^{i_1}\ldots x_n^{i_n} \;\middle|\; a_{i_1,\ldots,i_n} \in R \right\},$$

where all but finitely many coefficients $a_{i_1,\ldots,i_n}$ are equal to zero.

**Definition 2.2.** The **ring of formal power series** with coefficients in $R$ is

$$R[[t]] = \{a_0 + a_1 t + \ldots \mid a_i \in R\}.$$

The addition is coefficient-wise, and the multiplication is given by the formula

$$\left(\sum_{i\geq 0} a_i t^i\right)\left(\sum_{j\geq 0} b_j t^j\right) = \sum_{i\geq 0}\left(\sum_{j+k=i,\ j\geq 0,\ k\geq 0} a_j b_k\right) x^i.$$

Define

$$R[[t_1,\ldots,t_n]] = R[[t_1]]\ldots[[t_n]].$$

In $R[[t]]$ many products equal one unlike in $R[t]$, for example $(1-t)(1+t+\ldots) = 1$.

## 3 Zero-divisors, nilpotents, units

**Definition 3.1.** Let $A$ be a ring. An element $x \in A$ is a **zero-divisor** if $x \neq 0$ but $xy = 0$ for some $y \neq 0$ in $A$. A ring without zero-divisors is called an **integral domain**. An element $x \in A$ is **nilpotent** if $x^n = 0$ for some $n \in \mathbb{Z}_{>0}$. A **unit** $x \in A$ is an element such that $xy = 1$ for some $y \in A$. The units of $A$ form a group under multiplication, denoted by $A^*$, or $A^\times$.

**Definition 3.2.** Let $x \in A$. Then the set

$$\langle x\rangle = \{xy \mid y \in A\}$$

is an ideal. Such ideals are called **principal ideals**.

**Remark.** $x \in A^*$ if and only if $\langle x\rangle = A$, and $R$ is a field if and only if $R^* = R \setminus \{0\}$.

**Proposition 3.3.** *Let $A$ be a non-zero ring. Then the following are equivalent.*

1. *$A$ is a field.*
2. *There are no ideals in $A$ other than $\langle 0\rangle$ and $A$.*
3. *Every non-zero homomorphism $f : A \to B$ is injective.*

*Proof.*

$1 \implies 2$ Clear.

$2 \implies 3$ $\operatorname{Ker} f \subset A$ is an ideal. Since $f \neq 0$, $\operatorname{Ker} f \neq A$. Hence $\operatorname{Ker} f = 0$.

$3 \implies 1$ Take any $x \neq 0$ in $A$. Look at $\langle x\rangle$. Define $B = A/\langle x\rangle$. Then take $f : A \to B$ to be the natural surjective map. If $f$ is not identically zero, we get a contradiction with 3.

□

# 4 Prime ideals and maximal ideals

**Definition 4.1.** An ideal $I \subset A$ is called **prime** if $I \neq A$ and if whenever $xy \in I$, then $x \in I$ or $y \in I$. An ideal $J \subset A$ is called **maximal** if there is no ideal $J'$ such that $J \subsetneq J' \subsetneq A$.

**Notation.** The set of prime ideals of $A$ is called the **spectrum** of $A$ and is denoted by $\operatorname{Spec} A$.

**Lemma 4.2.** *An ideal $I \subset A$ is prime if and only if $A/I$ is an integral domain.*

*Proof.* Obvious. □

**Lemma 4.3.** *An ideal $J \subset A$ is maximal if and only if $A/J$ is a field.*

*Proof.* Obvious. □

**Proposition 4.4.** *If $f : A \to B$ is a ring homomorphism and $I \subset B$ is a prime ideal, then $f^{-1}(I)$ is a prime ideal of $A$.*

*Proof.* It is easy to see that $f^{-1}(I)$ is an ideal in $A$. Suppose $xy \in f^{-1}(I)$ for some $x, y \in A$. Then $f(x) f(y) = f(xy) \in I$. Since $I$ is prime, $f(x) \in I$ or $f(y) \in I$, so $x \in f^{-1}(I)$ or $y \in f^{-1}(I)$. □

So we get a canonical map

$$\begin{array}{rccc} f^* & : & \operatorname{Spec} B & \longrightarrow & \operatorname{Spec} A \\ & & I \subset B & \longmapsto & f^{-1}(I) \subset A \end{array}.$$

Lecture 3
Wednesday
09/10/19

**Remark 4.5.** If $f : A \to B$ is a ring homomorphism, then $f^{-1}(\mathfrak{p})$, where $\mathfrak{p} \subset B$ is a prime ideal, is a prime ideal. But this is false for maximal ideals. Let $A = \mathbb{Z}$, let $B = \mathbb{Q}$, and let $f(x) = x$. Then $\langle 0 \rangle \subset \mathbb{Q}$ is a maximal ideal and $f^{-1}(\langle 0 \rangle) = \langle 0 \rangle \subset \mathbb{Z}$ is not a maximal ideal. For example, $\langle 0 \rangle \subsetneq \langle 2 \rangle \subsetneq \mathbb{Z}$.

**Theorem 4.6.** *Let $A$ be a non-zero ring. Then $A$ has at least one maximal ideal. In particular,* $\operatorname{Spec} A$ *is not empty.*

The proof is based on Zorn's lemma. Let $S$ be a set. Then a **partial order** is a binary relation $\leq$ such that

- $x \leq x$ for all $x \in S$,
- $x \leq y \leq z$ implies that $x \leq z$, and
- $x \leq y$ and $y \leq x$ imply that $x = y$,

where not all pairs are comparable. A **chain** $T \subset S$ is a subset in which every two elements are comparable.

**Lemma 4.7** (Zorn)**.** *Suppose that $S$ is a partially ordered set such that every chain $T \subset S$ has an upper bound, that is an element $t \in S$ such that $x \leq t$ for all $x \in T$. Then $S$ has a maximal element, that is there exists $s \in S$ such that if $x \in S$ and $x \geq s$, then $x = s$.*

Zorn's lemma is equivalent to the axiom of choice.

*Proof of Theorem 4.6.* Let $\Sigma$ be the set of all ideals of $A$ which are not equal to $A$. Then $\langle 0 \rangle \in \Sigma$, so $\Sigma \neq \emptyset$. Equip $\Sigma$ with partial order given by inclusion. Enough to check the assumption of Zorn's lemma. Suppose $T$ is a chain of ideals, so it is a collection of ideals $J_i$ for $i \in T$. Consider instead

$$I = \bigcup_{i \in T} J_i.$$

Claim that $T$ is a chain implies that $I$ is an ideal. Then $x \in I$ implies that $x \in J_i$ for some $i$. Take any $x, y \in I$. Then $x \in J_i$ and $y \in J_k$ for some $i, k \in T$, so $T$ is a chain, hence $i \leq k$ or $k \leq i$, so $J_i \subset J_k$ or $J_k \subset J_i$. Without loss of generality assume $J_i \subset J_k$. Then $x, y \in J_k$, so $x + y \in J_k \subset I$. Clearly, $I$ is an upper bound. □

**Corollary 4.8.** *Any ideal of $A$ is contained in a maximal ideal of $A$.*

*Proof.* If $I \subset A$ is an ideal, apply Theorem 4.6 to $A/I$. □

**Corollary 4.9.** *Any non-unit of $A$ is contained in a maximal ideal.*

*Proof.* Apply Corollary 4.8 to $\langle a \rangle$. □

**Example.** The maximal ideals of $\mathbb{Z}$ are $\langle p \rangle$, where $p$ is prime.

**Definition 4.10.** A ring $A$ is **local** if $A$ has exactly one maximal ideal.

**Example.** Any field is a local ring. If $k$ is a field, then $k[[t]]$ is a local ring.

**Lemma 4.11** (Prime avoidance)**.** *Let $A$ be a ring and let $\mathfrak{p} \subset A$ be a prime ideal. Suppose that $I_1, \ldots, I_n$ are ideals in $A$ such that $\bigcap_{j=1}^{n} I_j \subset \mathfrak{p}$. Then $I_j \subset \mathfrak{p}$ for some $j$. If, moreover, $\bigcap_{j=1}^{k} I_j = \mathfrak{p}$, then $I_j = \mathfrak{p}$ for some $j$.*

*Proof.* Suppose that $I_j$ is not a subset of $\mathfrak{p}$ for any $j$. Then there exists $x_j \in I_j$ such that $x_j \notin \mathfrak{p}$. Hence

$$x_1, \ldots, x_n \in I_1 \ldots I_n \subset \bigcap_{j=1}^{n} I_j \subset \mathfrak{p},$$

so $x_1 (x_2 \ldots x_n) \in \mathfrak{p}$. Then $x_1 \notin \mathfrak{p}$ implies that $x_2 \ldots x_n \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime we get a contradiction. For the second claim, we know that some $I_j \subset \mathfrak{p}$. But $\mathfrak{p} = \bigcap_{j=1}^{k} I_j \subset I_k$ for all $k$. Hence $\mathfrak{p} = I_j$. □

# 5 Nilradical and the Jacobson radical

Lecture 4
Thursday
10/10/19

**Proposition 5.1.** *The set $\mathcal{N}(A)$ consisting of all nilpotents of the ring $A$ and zero is an ideal. Then $\mathcal{N}(A)$ is called the **nilradical** of $A$. The quotient $A/\mathcal{N}(A)$ has no nilpotents.*

*Proof.* Suppose $x \in A$ is nilpotent, so $x^n = 0$. For any $a \in A$, $(ax)^n = a^n x^n = 0$. Let $x$ and $y$ be nilpotents. Say $x^n = y^m = 0$. Then

$$(x+y)^{n+m} = \sum_{i,j \geq 0,\ i+j=n+m} a_{ij} x^i y^j, \qquad a_{ij} \in A.$$

Clearly, either $i \geq n$ or $j \geq m$. Then $a_{ij} x^i y^j = 0$. Therefore, $(x+y)^{n+m} = 0$, hence $x + y \in \mathcal{N}(A)$. If $x + \mathcal{N}(A)$ is nilpotent in $A/\mathcal{N}(A)$, then $x^n + \mathcal{N}(A) = \mathcal{N}(A)$ is the trivial coset. Hence $x^n \in \mathcal{N}(A)$. Thus $(x^n)^m = 0$ for some $m$. □

**Definition 5.2.** A ring $A$ such that $\mathcal{N}(A) = 0$ is called a **reduced ring**.

**Proposition 5.3.** *$\mathcal{N}(A)$ is the intersection of all prime ideals of $A$.*

*Proof.*

- $\subset$ Let $I$ be the intersection of all prime ideals of $A$. Let $f \in A$ be such that $f^n = 0$. Take any prime ideal $\mathfrak{p} \subset A$. We know that $f^n = 0 \in \mathfrak{p}$. Then $f(f \ldots f) \in \mathfrak{p}$ and $\mathfrak{p}$ prime implies that $f \in \mathfrak{p}$, so $f \in I$.

- $\supset$ Let us prove the converse. Suppose $f$ is not nilpotent, so $f^n \neq 0$ for all $n \geq 1$. We will show that there exists a prime ideal $\mathfrak{p} \subset A$ that does not contain $f$. Let us consider all ideals of $A$ that do not contain $f^m$, where $m \in \mathbb{Z}_{>0}$. Let $\Sigma$ be the set of ideals $J \subset A$ such that

  $$J \cap \{f^m \mid m \geq 1\} = \emptyset.$$

  The zero ideal $\langle 0 \rangle$ is in $\Sigma$. So $\Sigma \neq \emptyset$. Equip $\Sigma$ with a partial order given by inclusion. Applying Zorn's lemma we obtain that $\Sigma$ contains a maximal element. Call it $\mathfrak{p}$. By construction, $\mathfrak{p} \cap \{f^m \mid m \geq 1\} = \emptyset$, so $f \notin \mathfrak{p}$. It remains to prove that $\mathfrak{p}$ is prime. Enough to prove that if $x \notin \mathfrak{p}$ and $y \notin \mathfrak{p}$, then $xy \notin \mathfrak{p}$. Consider the ideal $\mathfrak{p} + \langle x \rangle \supsetneq \mathfrak{p}$. Since $\mathfrak{p}$ is maximal in $\Sigma$, thus $\mathfrak{p} + \langle x \rangle$ is not in $\Sigma$. By definition of $\Sigma$ there exists $n \geq 1$ such that $f^n \in \mathfrak{p} + \langle x \rangle$. Similarly, there exists $m \geq 1$ such that $f^m \in \mathfrak{p} + \langle y \rangle$. Then $(\mathfrak{p} + \langle x \rangle)(\mathfrak{p} + \langle y \rangle) \subset \mathfrak{p} + \langle xy \rangle$. In particular, $f^{n+m} = f^n \cdot f^m \in \mathfrak{p} + \langle xy \rangle$. If $xy \in \mathfrak{p}$, then $f^{n+m} \in \mathfrak{p}$, which is not possible. Therefore, $xy \notin \mathfrak{p}$. So $\mathfrak{p}$ is a prime ideal that does not contain $f$.

□

**Definition 5.4.** The **Jacobson radical** $\mathcal{J}(A)$ is the intersection of all maximal ideals of $A$.

**Proposition 5.5.** *$x \in \mathcal{J}(A)$ if and only if $1 - xy \in A^*$ for all $y \in A$.*

*Proof.*

$\Longrightarrow$ Let $x \in \mathcal{J}(A)$. Suppose there exists $y \in A$ such that $1 - xy$ is not a unit. By Corollary 4.9 every non-unit is contained in a maximal ideal. Say $M \subset A$ is a maximal ideal and $1 - xy \in M$. But $x \in \mathcal{J}(A) \subset M$. Then $1 = (1 - xy) + xy \in M$, but then $M \neq A$. A contradiction.

$\Longleftarrow$ Given $x \in A$ such that $1 - xy \in A^*$ for all $y \in A$, we must have $x \in \mathcal{J}(A)$. If $x \notin \mathcal{J}(A)$, then there exists a maximal ideal $M \subset A$ such that $x \notin M$. Then $M + \langle x \rangle = A \ni 1$. Thus $1 = m + xy$, where $y \in A$. But by assumption $1 - xy \in A^*$, so $m \in A^*$. But then $M = A$. A contradiction.

□

**Definition 5.6.** Let $I$ be an ideal of $A$. The **radical** of $I$ is the set

$$\operatorname{rad} I = \{x \in A \mid \exists n \geq 1,\ x^n \in I\}.$$

**Proposition 5.7.** *The radical of $I$ is the intersection of all prime ideals of $A$ that contain $I$.*

*Proof.* Apply Proposition 5.3 to $A/I$. □

Lecture 5
Tuesday
15/10/19

**Definition 5.8.** Let $I$ be an indexing set. For each $i \in I$ we are given a ring $R_i$. Consider the product set $\prod_{i \in I} R_i$. This is $(x_i)_{i \in I}$ for $x_i \in R_i$. Define

$$0 = (0)_{i \in I} \in \prod_{i \in I} R_i, \qquad 1 = (1)_{i \in I} \in \prod_{i \in I} R_i.$$

Define addition and multiplication coordinate-wise, so

$$(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i + b_i)_{i \in I}, \qquad (a_i)_{i \in I} \cdot (b_i)_{i \in I} = (a_i \cdot b_i)_{i \in I}, \qquad (a_i)_{i \in I}, (b_i)_{i \in I} \in \prod_{i \in I} R_i.$$

Then $\prod_{i \in I} R_i$ is a ring, the **product of rings**.

A warning is if $I$ has at least two elements, then $\prod_{i \in I} R_i$ has zero-divisors.

**Example.** $R_1 \times R_2$ has $(1, 0) \cdot (0, 1) = (0, 0) = 0$.

If $h_i : R \to R_i$ is a ring homomorphism for $i \in I$, then $(h_i)_{i \in I}$ is a ring homomorphism $R \to \prod_{i \in I} R_i$.

**Remark 5.9.** Let $\mathfrak{p}_i$ for $i \in I$ be all prime ideals of $R$. Let $h_i : R \to R/\mathfrak{p}_i$. Then

$$h = (h_i)_{i \in I} : R \to \prod_{i \in I} R/\mathfrak{p}_i$$

is a homomorphism, and

$$\operatorname{Ker} h = \bigcap_{i \in I} \operatorname{Ker} h_i = \bigcap_{i \in I} \mathfrak{p}_i = \mathcal{N}(R).$$

So there is an injective map

$$R/\mathcal{N}(R) \hookrightarrow \prod_{i \in I} R/\mathfrak{p}_i,$$

a product of integral domains. Now take $f_j : R \to R/M_j$, so if we take the indexing set $J$ to be the set of all maximal ideals of $R$, then we obtain an injective map

$$R/\mathcal{J}(R) \hookrightarrow \prod_{j \in J} R/M_j,$$

a product of fields.

# 6 Localisation of rings

**Example.** Fix a prime $p$. Then

$$\mathbb{Z} \subset \left\{ \frac{m}{p^k} \;\middle|\; m \in \mathbb{Z},\ k \in \mathbb{Z}_{\geq 0} \right\} \subset \mathbb{Q}.$$

**Definition 6.1.** A subset $S$ of a ring $A$ is called a **multiplicative set** if $1 \in S$ and $0 \notin S$, and $S$ is closed under multiplication.

**Example 6.2.**

- Let $a \in A$ be a non-nilpotent. Then $\{1, a, \dots\}$ is a multiplicative set.
- Let $\mathfrak{p} \subsetneq A$ be a prime ideal. Then $A \setminus \mathfrak{p}$ is a multiplicative set. Indeed, if $x \notin \mathfrak{p}$ and $y \notin \mathfrak{p}$ then $xy \notin \mathfrak{p}$ by the definition of a prime ideal.
- If we have a family $\mathfrak{p}_i$ for $i \in I$ of prime ideals, then $A \setminus \bigcup_{i \in I} \mathfrak{p}_i$ is a multiplicative set.
- $A^*$ is a multiplicative set.
- All non-zero-divisors in $A$ form a multiplicative set.
- Let $I \subsetneq A$ be an ideal. Then $1 + I = \{1 + x \mid x \in I\}$ is a multiplicative set.

**Definition 6.3.** Consider $A \times S$ and the equivalence relation on $A \times S$ defined as

$$(a, s) \sim (b, t) \qquad \Longleftrightarrow \qquad \exists u \in S,\ u\,(at - bs) = 0.$$

Check that this is indeed an equivalence relation. [1] The following is some notation.

- The equivalence class of $(a, s)$ is written as $a/s$. For example, if $t \in S$, then $a/s = at/st$.
- The set of equivalence classes is denoted by $S^{-1}A$.

Define

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Need to check that these operations are well-defined. [2] Define $\frac{0}{1}$ as the zero of $S^{-1}A$, and $\frac{1}{1}$ as the one of $S^{-1}A$. Then $S^{-1}A$ is a ring, the **localisation of $A$ with respect to a multiplicative set $S$**.

**Lemma 6.4.** *There is a ring homomorphism*

$$\begin{array}{rccc} f & : & A & \longrightarrow & S^{-1}A \\ & & x & \longmapsto & \dfrac{x}{1} \end{array}.$$

*This $f$ is injective if and only if $S$ has no zero-divisors.*

*Proof.* If $S$ contains a zero-divisor, say $u$, then there exists $a \in A$ for $a \neq 0$ such that $ua = 0$. Then

$$f(a) = \frac{a}{1} = \frac{au}{u} = \frac{0}{u} = 0.$$

So $\operatorname{Ker} f$ contains $a$, hence $f$ is not injective. If $f$ has no zero-divisors, then $u \cdot a = u\,(a - 0) \neq 0$ if $a \neq 0$ and any $u \in S$. Hence $f(a) \neq 0$. □

[1] Exercise
[2] Exercise