Commutative Algebra

Yankı Lekili

■ Statement of a convention used throughout the text.
► Little facts that can be checked but we don't bother to check explicitly. If you don't find what's stated intuitive, you should stop and think about how to prove it. If you can't, then consult a book and if that doesn't help either, please come ask me. I will assume that you know how to prove these.
◁ Exercise. Try it!
□ Marks the end of a proof.

When something is defined for the first time, I make it **bold** and when I want to emphasise something I underline it.

```
Code snippets in Macaulay2 are inserted with this font.
I won't ask you any coding problems in the exam but you should install Macaulay2
on your computer and have fun with it as you learn commutative algebra.
Macaulay2 is available at
```

https://macaulay2.com/.

```
It is available for basically all platforms.
I run it on a GNU/Linux machine where you just type M2 to run it on the command line.
```

$:=$ denotes a definition. $\simeq$ denotes an isomorphism. I very often make a mistake and use $=$ where I really meant to use $:=$ or $\simeq$.

Lecture 1. Prelude; rings and ideals

---

1 Prelude

Commutative Algebra has its roots in Algebraic Number Theory and forms the foundation of the modern theory of Algebraic Geometry.

In this course, the students will learn about Noetherian rings and modules, Hilbert basis theorem, Hilbert polynomials, Gröbner bases and Buchberger's algorithm, integral dependence, Noether normalisation, the Nullstellensatz, Spectrum of rings and Zariski topology, Krull dimension,

localisation, Artin rings, Krull's principal ideal theorem, Cohen-Seidenberg lying over/going up theorem, (Discrete) Valuation Rings, Artin-Rees lemma, Krull intersection theorem, Completion, Hensel's lemma.

1.1 Algebraic Geometry

Algebraic Geometry is the study of algebraic varieties - spaces cut out by polynomial equations in several variables. An example of an algebraic variety is the subspace of k^2 cut out by the equation $X^2 = Y^3$ where k is a field. The algebraic functions on these spaces form commutative algebras isomorphic to quotients of polynomial rings in several variables. For example, the functions on the space cut out by $X^2 = Y^3$ are given by the quotient ring $k[X, Y]/(X^2 - Y^3)$. Hilbert's Nullstellensatz, one of the main themes in this course, gives a dictionary between the geometry of algebraic varieties and the algebra of functions on these spaces. In a sense, there is a complete correspondence: problems of algebra can be turned into geometry and vice versa.

1.2 Algebraic Number Theory

Algebraic Number Theory is a subject which was developed with the main goal of solving Fermat's Last Theorem which states that there are no solutions in positive integers to $X^n + Y^n = Z^n$ for $n > 2$. An early approach to this question was by making use of the factorisation

$$Y^n = \prod_{i=0}^{n-1} (Z - \xi^i X) \text{ with } \xi \text{ a primitive } n^{th} \text{ root of unity}$$

in the commutative ring $\mathbb{Z}[\xi]$. If one knows that every element of $\mathbb{Z}[\xi]$ can be factorised into primes (like the case of $\mathbb{Z}$) by using elementary methods in divisibility one arrives at a contradiction. Thus, it is of importance to understand whether such unique factorisation property holds. (It turns out this depends on the value of n. For example, $\mathbb{Z}[\xi]$ does not have this property for $n = 23$). Algebraic number theory brings in methods of commutative algebra to approach this problem by studying "number rings" like $\mathbb{Z}[\xi]$ (and often inspired by analogous geometric results valid for co-ordinate rings of algebraic varieties.)

1.3 Logic: Constructive vs. Non-constructive

"Das ist nicht Mathematik, das ist Theologie."[1] is a famous quote attributed to Paul Gordan, a well-known algebraist in the 19^{th} century, about young Hilbert who vastly generalised Gordan's work by proving what is now known as the Hilbert basis theorem and the Nullstellensatz. The proof that Hilbert gave was non-constructive. In modern language, his arguments proved existence results based on axiomatic methods without actually giving an algorithm to construct the desired structure. Hilbert's ideas were revolutionary. The axiomatic method favours abstract, non-constructive arguments. They tend to be considerably shorter and more elegant. Emmy Noether, a student of Gordan developed this approach significantly and developed what's known as the Noetherian induction. In essence, the non-constructive methods of Hilbert and Noether

[1] "This is not mathematics, it is theology."

rely on the law of excluded middle and, often, on a version of the Axiom of Choice or equivalently Zorn's lemma. Most of modern commutative algebra textbooks accept these and build the theory that way. In more recent years, the advent of computers prompted a renewed interest in constructive methods. The computers vastly increased the scope of computations. The crux of constructive methods is the theory of Gröbner bases and Buchberger's algorithm which simultaneously generalise Gaussian elimination in linear algebra and Euclid's division algorithm in the theory of polynomials in one variable to the case of polynomials in several variables. In this course, we will favour constructive methods when this doesn't take us too far afield. Notably, we will give a proof of Hilbert's Nullstellensatz that is constructive. We will also make use of non-constructive methods when either this is illuminating or else the corresponding constructive argument is much harder. We will not define what constructive or non-constructive means precisely. However, we will specify whenever an argument is non-constructive in the hope that the reader will build an intuitive understanding of these concepts.[2]

2 Rings, Ideals and Modules

This section is mostly basic definitions that lay out the protagonists of our topic. Please bear with it as we need these. The fun starts in the next section.

2.1 Rings

Rings are things where you can do addition and multiplication in a compatible way modeled on the ring of integers $\mathbb{Z}$. A general ring does not have to be commutative. For example, the set of 2-by-2 matrices $M_2(\mathbb{Z})$ is a ring under the familiar addition and multiplication rules but it is not commutative. There are matrices such that $A \cdot B \neq B \cdot A$.

The crucial assumption in this lecture course is the assumption of commutativity of the multiplication.

A **commutative ring with identity** is a set $(R, +, \cdot, 0, 1)$ such that

$$\begin{aligned}
(R, +, 0) &\text{ is an abelian group.} \\
a \cdot (b \cdot c) &= (a \cdot b) \cdot c \\
a \cdot (b + c) &= a \cdot b + a \cdot c. \\
a \cdot b &= b \cdot a \\
a \cdot 1 &= 1 \cdot a = a.
\end{aligned}$$

Note that a **field** is a commutative ring with $1 \neq 0$ where every non-zero element a is invertible; i.e., has a multiplicative inverse b such that $ab = 1$. Therefore, any field is a commutative ring. Recall also that an **integral domain** is a subring of a field.

► Let $R \neq \{0\}$ be a ring in which there is no zero divisor, that is, for all $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$. This is equivalent to R being an integral domain. Indeed, every such ring can

[2] Personally, I do not object to nonconstructive proofs depending on Axiom of Choice however I feel that theorems which do not depend on them are more fundamental.

be embedded in a field Frac(R) called the **field of fractions** of R consisting only of elements a/b with $a, b \in R$ and $b \neq 0$, which is unique up to isomorphism.

Those elements of a commutative ring R which are invertible are called **units** of the ring R.

■ In this course, a ring will always mean a commutative ring with identity.

A **homomorphism** of rings $f : R \to S$ is a map satisfying

$$\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(ab) &= f(a)f(b) \\ f(1) &= 1 \end{aligned}$$

An integral domain is a **unique factorisation domain (UFD)** if every non-zero element a factors as a product of irreducible elements p_i and a unit u: $a = up_1p_2 \dots p_n$ and this representation is unique up to reordering the p_i and multiplying them by units.

An integral domain R is a **Euclidean domain** if it has a norm $|\cdot| : R \to \mathbb{N}$ such that given a, b with $b \neq 0$, we can find r, q such that $a = bq + r$ and $|r| < |b|$.

2.2 Ideals

Unique factorisation domain property does not hold in other rings of integers, such as $\mathbb{Z}[\sqrt{-5}]$, the extension ring obtained by adjoining $\sqrt{-5}$ to $\mathbb{Z}$. We have

$$21 = 3 \times 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

Theory of ideals ("ideal numbers") was motivated by a desire to restore the property of unique factorisation in number fields. Indeed, towards the end of the course, when we study Dedekind domains, we will see that in $\mathbb{Z}[\sqrt{-5}]$ every non-zero ideal factors uniquely as a product of prime ideals. The theory of ideals is also motivated via Algebraic Geometry: We will see later that the set $I(S)$ of polynomials in $\mathbb{C}[X_1, X_2, \dots, X_n]$ vanishing along a subset S of the affine space $\mathbb{C}^n$ is an ideal.

Ideal of a ring R is a kernel of a homomorphism $f : R \to S$. Equivalently, an **ideal** is a subset of R that can be characterized by the following properties

$$0 \in I, \quad a \pm b \in I, \text{ for } a, b \in I$$

$$ar \in I, \text{ for } a \in I, r \in R$$

Given an ideal $I \subset R$, we can produce a ring R/I with the multiplication $(x + I)(y + I)$ defined to be $xy + I$. There is a natural surjective homomorphism $f : R \to R/I$ sending x to $x + I$ such that $I = \text{Ker}(f)$.

▶ There is a natural bijection between the ideals $J \subset R$ such that $I \subset J$ and the ideals of R/I. Just send J to $f(J)$.

▶ An ideal I in a commutative ring R itself is a commutative ring but without an identity!

Given a subset S of R, the ideal generated by S is the subset

$$(S) = \{r_1 s_1 + \ldots + r_t s_t | r_i \in R, s_i \in S, t \in \mathbb{N}\}.$$

We write $(f_1, f_2, \ldots, f_t)$ for the ideal generated by a finite set of elements $f_1, \ldots, f_t \in R$.

■ R itself is the ideal (1) of R. To exclude this ideal, we say that I is a **proper** ideal if I is an ideal of R but not equal to (1).

An ideal is **principal** if it is generated by a single element. An integral domain is a **principal ideal domain (PID)** if every ideal is principal.

▶ Euclidean domain implies PID.
▶ PID implies UFD (this uses the Axiom of Dependent Choice, a countable version of the Axiom of Choice).

A ring is called **Noetherian** if all of its ideals are finitely generated. We will study this condition in detail later on. In particular, we will see that most rings of interest in this course are Noetherian, but not all!

◁ Show that the ring of differentiable functions on $\mathbb{R}^n$ is not Noetherian. For the geometry of manifolds, Commutative Algebra is not enough; you need Calculus.