## 1. Lecture 1 – What is this course

Commutative algebra is the study of commutative rings, and their associated structures. The goal of today's lecture is to remind ourselves what that means.

We'll never see noncommutative rings in this course, nor rings without multiplicative identities. So we will use the word **ring** for commutative rings with identity. Let's revise what that means.

**Definition.** A **ring** is a set $A$ equipped with two binary operations. For $a, b \in A$, we have the operations of *addition*, denoted $a + b$, and *multiplication* denoted $ab$. These must satisfy axioms:

(1) $(A, +)$ is an abelian group, with identity element denoted $0 \in A$.
(2) Multiplication is associative: $(ab)c = a(bc)$.
(3) Multiplication is commutative: $ab = ba$.
(4) Given $a, b, c \in A$, we have
$$(a + b)c = ac + bc.$$
(5) There exists an element $1 \in A$, such that for all $a \in A$, we have
$$1a = a.$$

The algebraic rules we use to manipulate ordinary numbers mostly work arbitrary rings, in particular, for $a, b \in A$, we have

$$(-a)(-b) = ab, (-a)b = -ab \text{ and } 0a = 0$$

**Example.** The **0 ring** has one element 0, and addition and multiplication is defined in the only way it can be: $0 + 0 = 0 = 00$.

**Example.** Most things we call numbers form rings: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are rings with the standard addition and multiplication operations.

**Example.** The set of all functions $f \colon \mathbb{R} \to \mathbb{R}$ forms a ring with the usual operations of addition and multiplication of functions.

More generally, if $X$ is a set and $A$ a ring, the set of functions $f \colon X \to A$ form a ring by defining $(f + g)(x) = f(x) +_A g(x)$ for all $x \in X$.

**Example.** Given a ring $A$, the **ring of polynomials** (in one variable) over $A$ is denoted $A[x]$. Its elements are formal polynomials, that is expressions like

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0, \qquad a_i \in A,$$

and the operations of addition and multiplication in $A[x]$ are defined in a straightforward way (e.g. think of how you add and multiply polynomials with real coefficients, then do the same thing except using the operations on the coefficients in $A$ instead).

**Example.** More generally, given a ring $A$ and an $n \geq 1$, we can defined $A[x_1, \ldots, x_n]$. This is the ring of polynomials in $n$ variables. Its elements are expressions of the form

$$\sum_{i_1, \ldots, i_n \geq 0} a_{i_1 i_2 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n}, \qquad a_{i_1 \ldots i_n} \in A$$

Again the ring operations are defined in a natural way which we won't write down.

We often write $A[x, y]$ instead of $A[x_1, x_2]$ and $A[x, y, z]$ instead of $A[x_1, x_2, x_3]$.

**Example.** In the ring $A[x, y]$, with chosen elements $a, b, c \in A$, say, we can compute

$$(1 + axy^2)(b + cxy) = 1b + 1cx + axy^2 b + axy^2 cx = b + cx + abxy^2 + acx^2 y^2$$

### 1.1. **Homomorphisms.**

**Definition.** Let $A$ and $B$ be rings. A map $\phi\colon A \to B$ is a **homomorphism** if it satisfies

1. $\phi(1_A) = 1_B$
2. For all $a, a' \in A$, we have
$$\phi(aa') = \phi(a)\phi(a').$$
3. For all $a, a' \in A$, we have
$$\phi(a + a') = \phi(a) + \phi(a')$$

If $\phi$ is moreover bijective, then we say $\phi$ is an **isomorphism** and write $A \cong B$.

**Example.** The inclusion maps $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$ preserve the identity element and both binary structures, so are homomorphisms.

**Example.** Let $a \in A$ be an element, then there is a **evaluation homomorphism** $\phi_a\colon A[x] \to A$ defined by (replace $x$ with $a$ everywhere!)
$$\phi(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) = a_n a^n + a_{n-1}a^{n-1} + \cdots + a_0$$

### 1.2. **Ideals.**

**Definition.** Let $A$ be a ring. A subset $\mathfrak{a} \subset A$ is an **ideal** if it satisfies two conditions:

1. $\mathfrak{a}$ forms a subgroup of $(R, +)$
2. For every $x \in A$ and $a \in \mathfrak{a}$, we have $xa \in \mathfrak{a}$.

**Example.** In a ring $A$, the subsets $A$ and $\{0\}$ are ideals.

**Definition.** Let $x \in A$. The **principal ideal** generated by $x$, denoted $(x) \subset A$, is defined as
$$\{ax \mid a \in A\} \subseteq A$$

**Example.** In any ring $A$, we have $\{0\} = (0)$ and $A = (1)$, so these are principal ideals.

**Example.** The ideals of $\mathbb{Z}$ are all principal, so are given by $(n) \subseteq \mathbb{Z}$ for $n \geq 0$.

### 1.3. **Quotient rings.**

**Definition.** If $\mathfrak{a} \subset A$ is an ideal, then we may form the **quotient ring** $A/\mathfrak{a}$, whose elements are the additive cosets of $\mathfrak{a}$ in $A$, with addition and multiplication defined by
$$(x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}$$
and
$$(x + \mathfrak{a})(y + \mathfrak{a}) = xy + \mathfrak{a}.$$
The **quotient homomorphism** $\phi\colon A \to A/\mathfrak{a}$ is given by, for $x \in A$,
$$\phi(x) = x + \mathfrak{a}.$$

**Example.** The ring $A/A$ has one element, $A$, and so is (isomorphic to) the zero ring.

**Example.** Let $n \geq 1$, then the ring $\mathbb{Z}/(n)$ is the **ring of integers modulo** $n$, and has $n$ elements
$$\mathbb{Z}/(n) = \{0 + (n), 1 + (n), \ldots, n - 1 + (n)\}.$$

**Example** (A purely motivational example)**.** Let $f = \sum a_{ij}x^i y^j \in \mathbb{C}[x,y]$. The vanishing locus of $f$ is the set of $(a,b) \in \mathbb{C}^2$ such that $f(a,b) = 0$, and a set of points defined in this way is what is called an algebraic curve. The ring

$$\mathbb{C}[x,y]/(f)$$

is interpreted as the ring of "algebraic functions" on the curve. In algebraic geometry, we study the geometry of this curve via the algebra of its ring of functions.

**Definition.** Let $\phi\colon A \to B$ be a homomorphism. The **kernel of** $\phi$ is given by

$$\ker\phi = \{x \in A \mid \phi(x) = 0\}.$$

**Theorem.** *Let $\phi\colon A \to B$ be a homomorphism. The kernel of $\phi$ is an ideal of $A$.*

**Theorem** (The fundamental homomorphism theorem)**.**

- *The image of $\phi$, denoted $\phi(A) \subset B$, is a subring of $B$, and we have*

$$A/\ker\phi \cong \phi(A)$$

- *The homomorphism $\phi$ is injective if and only if* $\ker\phi = \{0\}$.

1.4. **The relation between ideals of a ring and a quotient ring.** Let $\mathfrak{a} \subset A$ be an ideal in a ring, and $\phi\colon A \to A/\mathfrak{a}$ the quotient homomorphism.

**Theorem.** *There is a bijective correspondence*

$$\{\textit{Ideals of } A/\mathfrak{a}\} \leftrightarrow \{\textit{Ideals of } A \textit{ containing } \mathfrak{a}\},$$

*given by*

$$\mathfrak{b} \subset A/\mathfrak{a} \mapsto \phi^{-1}(\mathfrak{b})$$

*and the other way by*

$$\mathfrak{a} \subseteq \mathfrak{b} \subset A \mapsto \phi(\mathfrak{b})$$

*Sketch proof.* First check $\phi^{-1}$ is well-defined, i.e. that if $\mathfrak{b} \subseteq A/\mathfrak{a}$ is an ideal, then $\phi^{-1}(\mathfrak{b})$ is an ideal containing $\mathfrak{a}$. Then check $\phi$ is well-defined, i.e. that if $\mathfrak{b} \subseteq A$ is an ideal containing $\mathfrak{a}$, then $\phi(\mathfrak{b})$ is an ideal of $A/\mathfrak{a}$. Finally check that $\phi(\phi^{-1}(\mathfrak{b})) = \mathfrak{b}$ and $\phi^{-1}(\phi(\mathfrak{b}) = \mathfrak{b}$ if $\mathfrak{b}$ contains $\mathfrak{a}$, so that $\phi$ and $\phi^{-1}$ are inverse operations. □

**Definition.** Let $A$ be a ring.

- An element $x \in A$ is a **unit** if there exists a $y$ such that $xy = 1$.[1]
- An element $0 \neq x \in A$ is a **zero-divisor** if there exists a $y \neq 0$ such that $xy = 0$.
- A ring is an **integral domain** if it has no zero-divisors
- A ring is a **field** if all its non-zero elements are units

**Proposition.** *Let $x \in A$. Then $x$ is a unit* $\Leftrightarrow$ $(x) = (1) = A$.

*Proof.* If $x$ is a unit, there exists a $y \in A$ such that $xy = 1$, hence for every $z \in A$, we have $(zy)x = z(yx) = z1 = z \in (x)$, so $(x) = A$.

Conversely, if $(x) = A$, then there exists a $y$ such that $yx = 1$. □

[1] Prove that the units of $A$ form a group under multiplication.

**Key concepts Lecture 1**

- Rings
- Polynomial ring of a base ring
- Homomorphism
- Isomorphism
- Evaluation homomorphism
- Ideal
- Principal ideal
- Ideals of $\mathbb{Z}$
- Quotient rings
- Integers modulo $n$, $\mathbb{Z}_n$
- Kernel of a homomorphism
- Kernels are ideals
- The fundamental homomorphism theorem
- Relation between ideals of $A$ and of $A/\mathfrak{a}$
- Unit
- Zero-divisor
- Integral domain
- Field