1. Rings and homomorphisms

Definition. A ring $A$ is a set equipped with two binary operations, usually denoted $+$ (addition) and $\cdot$ (multiplication), such that:

1. $(A, +)$ is an abelian group with identity denoted by $0$ (if $x \in A$ then the inverse of $x$ is denoted $-x$);
2. $(A, \cdot)$ is a monoid; that is $\cdot$ is associative and has a unit denoted $1$;
3. addition distributes over multiplication; that is $x.(y + z) = x.y + x.z$ and $(y + z).x = y.x + z.x$.

As expected given the title, in this course we will only consider rings which are commutative; that is such that $xy = yx$ for every pair of elements $x, y \in A$. In fact, we are going to use ring to mean commutative ring for this reason. Note this doesn’t mean the lecturer believes all rings are commutative just that he is too lazy to write commutative every time he writes ring in this course.

Examples. Some of the most important examples are:

1. Fields such as the rationals $\mathbb{Q}$, the reals $\mathbb{R}$, the complex numbers $\mathbb{C}$ and algebraic number fields; that is algebraic extensions of $\mathbb{Q}$.
2. The integers $\mathbb{Z}$ with their usual operations or indeed the ring of integers $\mathcal{O}$ of any algebraic number field.
3. Polynomial rings in $n$ variables over a field $k$ written $k[x_1, \ldots, x_n]$.
4. Continuous functions from a topological space to $\mathbb{R}$ or $\mathbb{C}$ with pointwise addition and multiplication;
5. Smooth functions from a manifold to $\mathbb{R}$; and so on.

Definition. A subset $S$ of a ring $A$ is called a subring if it is a subgroup under addition, closed under multiplication and contains the 1.

Remarks. Note that:

- Some people don’t insist that rings have a multiplicative identity and would call our rings ‘rings with a 1’.
- We don’t insist the elements 0 and 1 are different. If not, then $A$ must be the zero ring consisting of just one element.

Definitions. Suppose that $x$ is an element of a ring $A$:

- $x$ is called a unit if there is an element $y$ of $A$ such that $xy = 1$ — such a $y$ is then unique and is usually written $x^{-1}$;
- $x$ is called a zero-divisor if there is a non-zero element $y$ of $A$ such that $xy = 0$;
- $x$ is called nilpotent if $x^n = 0$ for some positive integer $n$.

A non-zero ring $A$ is called an integral domain if it has no non-zero zero-divisors.
Examples.

(1) In a field every non-zero element is a unit; so every field is an integral domain.

(2) In the ring of integers modulo 12, 6 is nilpotent, 3 and 2 are non-nilpotent zero-divisors, and 5 is a unit.

(3) The ring of integers \(\mathbb{Z}\) and the polynomial rings \(k[x_1, \ldots, x_n]\) with \(k\) a field are integral domains.

After rings probably the most important notion in commutative algebra is the notion of a ring homomorphism.

**Definition.** If \(A\) and \(B\) are two rings then a function \(f : A \rightarrow B\) is a ring homomorphism if it respects addition, multiplication and the 1; that is:

1. \(f(x + y) = f(x) + f(y)\);
2. \(f(xy) = f(x)f(y)\);
3. \(f(1) = 1\).

It follows that if \(S\) is a subring of a ring \(A\) then the inclusion map \(i : S \rightarrow A\) is a ring homomorphism.

Notice that if \(f : A \rightarrow B\) and \(g : B \rightarrow C\) are ring homomorphisms then their composite \(g \circ f : A \rightarrow C\) is also a ring homomorphism.

**Remark.** For those doing category theory this means that rings and ring homomorphisms form a category.

**Exercise.** For every ring \(A\), there is a unique ring homomorphism from \(\mathbb{Z}\) to \(A\) and a unique ring homomorphism from \(A\) to the zero ring.

1.2. **Ideals.**

**Definition.** Given a ring \(A\), an ideal \(I\) of \(A\) is a non-empty subset of \(A\) that is
(a) closed under addition and
(b) closed under multiplication by elements of \(A\); i.e. if \(a \in A\) and \(x \in I\) then \(ax \in I\).

**Examples.**

(1) Every ideal of a field \(K\) is either 0 or \(K\).

(2) The ideals of \(\mathbb{Z}\) are all sets of the form \((n) = \{na | a \in \mathbb{Z}\}\).

(3) If \(A\) is a ring of functions on a space \(X\) and \(Y\) is a subset of \(X\) then the subset of \(A\) consisting of functions that vanish on \(Y\) is an ideal.

**Definitions.** As in example (2), in any ring \(A\), we’ll write \((x) = \{xa | a \in A\}\) for each \(x\) in \(A\). Such an ideal is called a principal ideal.

Given any subset \(S\) of \(A\), we will write \((S)\) for the smallest ideal containing \(S\). We say \((S)\) is the ideal generated by \(S\). It is easy to see that

\[
(S) = \left\{ \sum_{i=1}^{n} a_is_i | a_i \in A \text{ and } s_i \in S \right\}
\]

Given two ideals \(I\) and \(J\) in \(A\), we write \(I + J\) for the set \(\{a + b | a \in I, b \in J\}\), again it is easy to see that this is the smallest ideal containing \(I\) and \(J\).
Definition. Given a ring $A$ and an ideal $I$ the additive quotient group $A/I$ may be made into a ring by defining $(x + I)(y + I) = xy + I$. We call this the quotient ring or the residue-class ring $A/I$. There is a natural surjective ring homomorphism $\pi: A \to A/I$.

It is easy to check that $\pi$ induces an order preserving bijection between the ideals of $A$ containing $I$ and the ideals of $A/I$.

Definition. If $f: A \to B$ is any ring homomorphism then the kernel of $f$ is the set $f^{-1}(0)$ and the image of $f$ is the set $f(A)$.

Examples.

1) $\mathbb{Z}/(n)$ is the ring of integers modulo $n$.

2) If $X$ is a topological space with subset $Y$, $A$ is the ring of continuous functions from $X$ to $\mathbb{R}$ and $I$ is the set of functions that vanish on $Y$ then $A/I$ is isomorphic to a subring of the set of continuous functions on $Y$ with the subspace topology.

Exercise (The first isomorphism theorem for rings). If $f: A \to B$ is a ring homomorphism then the kernel of $f$ is an ideal of $A$ and the image of $f$ is a subring of $B$. Moreover, $f$ induces a ring homomorphism $A/\ker f \cong \text{Im} f$.

Proposition. Let $A$ be a non-zero ring. The following are equivalent:

i) $A$ is a field;

ii) the only ideals in $A$ are $0$ and $A$;

iii) every homomorphism of $A$ into a non-zero ring $B$ is an injection.

Proof. (Exercise) \qed

Exercise. Show that the set of nilpotent elements in a ring $A$ is an ideal $N(A)$. Show moreover that $A/N(A)$ has no non-zero nilpotent elements.

We call $N(A)$ the nilradical of $A$.

2. Modules

2.1. Definitions and Examples. Suppose that $A$ is a ring.

Definition. An $A$-module is an abelian group $(M, +)$ with a linear $A$-action i.e. there is a function $A \times M \to M$ such that the image of $(a, m)$ is written $am$ and

1) $a(x + y) = ax + ay$

2) $(a + b)x = ax + bx$

3) $(ab)x = a(bx)$

4) $1x = x$

for $a, b \in A$ and $x, y \in M$.

Remarks.

- We may equivalently define an $A$-module $M$ to be an abelian group along with a ring homomorphism from $A$ to the (non-commutative) ring of group homomorphisms from $M$ to $M$ under pointwise addition and composition.
Examples.

(1) As mentioned above, if \( k \) is a field then a \( k \)-module is the same as a \( k \)-vector space.

(2) If \( A \) is any ring then the set \( A^n \) which consists of \( n \)-tuples of elements of \( A \) is an \( A \)-module under coordinatewise addition and multiplication.

(3) A \( \mathbb{Z} \)-module is just an abelian group.

(4) An ideal of \( A \) is an \( A \)-module under the usual ring multiplication.

(5) If \( A = k[x] \) for \( k \) a field then to define an \( A \)-module is to define a \( k \)-vector space \( M \) along with a \( k \)-linear endomorphism of \( M \): \( x: M \to M \).

(6) If \( A \) is the ring of \( C \)-valued continuous functions on a topological space \( X \) and \( \pi: E \to X \) is a vector-bundle then the set of sections of \( \pi \) is an \( A \)-module.

We also want a notion of an \( A \)-module homomorphism.

Definition. If \( M \) and \( N \) are \( A \)-modules a function \( f: M \to N \) is an \( A \)-module homomorphism if

\[
\text{• } f \text{ is a group homomorphism}
\]
\[
\text{• } f(am) = a.f(m).
\]

for each \( a \in A \) and \( m \in M \).

Examples.

(1) If \( k \) is a field, a \( k \)-module map is just a \( k \)-linear map.

(2) A \( \mathbb{Z} \)-module map is just a group homomorphism.

(3) If \( A = k[x] \) then an \( A \)-module map is a linear map that commutes with the action of \( x \).

As we might expect, the composition of two \( A \)-module maps is an \( A \)-module map (and so we have a category of \( A \)-modules).

Moreover, it is easy to check that we may turn the set of \( A \)-module maps into an abelian group under pointwise addition. Not only that, but we may also turn it into an \( A \)-module under pointwise multiplication; i.e., \( (af)(m) = a.(f(m)) \).

Notation. We write \( \operatorname{Hom}_A(M, N) \) for the \( A \)-module of all \( A \)-module maps between the \( A \)-modules \( M \) and \( N \).

Warning. The fact that \( \operatorname{Hom}_A(M, N) \) is an \( A \)-module depends strongly on the fact that \( A \) is a commutative ring. It is still an abelian group without this assumption.

Definitions.

- A submodule \( N \) of an \( A \)-module \( M \) is an subgroup that is closed under multiplication by elements of \( A \).
- If \( N \) is a submodule of \( M \), the quotient \( M/N \) is the abelian group \( M/N \) with \( A \)-action given by \( a.(m + N) = am + N \).
- If \( f: M \to N \) is an \( A \)-module map then the kernel of \( f \) is the \( A \)-submodule of \( M \) given by \( f^{-1}(0) \). The image of \( f \) is the \( A \)-submodule of \( N \) given by \( f(M) \), and the cokernel of \( f \) is the quotient module of \( N \) given by \( N/f(M) \).

Exercise. Formulate and prove a first isomorphism theorem for \( A \)-modules. [Hint: compare with the ring version]