Rings and Modules

Chao Ren

February 7, 2026

Contents

Chapter 1

Rings: Definition and Examples

Definition 1. A ring is a datum $(R, +, \times, 0, 1)$ where R is a set, $1, 0, \in \mathbb{R}$ and $+, \times$ are binary operations on R such that

- R is an abelian group under $+$ with identity element 0
- The binary operation $\times$ is associative and $1 \times x = x \times 1 = x$ for all $x \in \mathbb{R}$.
- Multiplication distributes over addition:

$$x \times (y + z) = (x \times y) + (x \times z),$$
$$(x + y) \times z = (x \times z) + (y \times z), \forall x, y, z \in \mathbb{R}.$$

Example. Common rings:

- The integers $\mathbb{Z}$ are the fundamental example of a ring. Much of the course will be about finding an interesting class of rings which behave a lot like $\mathbb{Z}$.
- $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} : a, b \in \mathbb{Z}\}$ is a ring. It is known as the *Gaussian integers*.
- Any field is a ring. The only difference between the axioms for a field and for a ring is that a ring does not require multiplicative inverses, and that for fields one assumes $1 \neq 0$. Also fields must have commutative multiplication, but we assume it for rings in this course.

Lemma 1. (Subring criterion) Let R be a ring and S a subset of R, then S is a subring if and only if $1 \in S$ and for all $s_1, s_2 \in S$ we have $s_1 s_2, s_1 - s_2 \in S$.

Chapter 2

Basic Properties

2.1 Integral Domains

Definition 2. Let R be a ring. The subset

$$R^\times = \{r \in R : \exists s \in R, rs = 1\}$$

is called the group of *units* in R, i.e. $(R, \times, 1_R)$ is a group. Intuitively these are the invertible elements.

Proposition 1. Let K be a field and let $\theta : R \to K$ be an embedding (injective homomorphism). Then there is a unique injective homomorphism $\tilde{\theta} : F(R) \to K$ extending θ, in the sense that $\tilde{\theta}_{|R} = \theta$ where we view R as a subring of $F(R)$ via the above embedding.

Remark. If $u \in I$ where $u \in R^\times$, then $uu^{-1} \in I$, then $1_R \in I$, then $I = R$.

Chapter 3

Ideals and Quotients

Definition 3. $x \in R$ non-zero, not a unit is irreducible if whenever $a|x$ we have $a \sim 1$ or $a \sim x$.

Definition 4. If every ideal in integral domain R is principal, we say R is a Principal Ideal Domain (PID).

Example. $\mathbb{Z}, \mathbb{F}[t]$

If we're asked to show a quotient is isomorphic to something, a good way to do it is to produce a SURJECTION onto the something whose kernel is the thing we're quotienting out by and using the isomorphism theorem.

Proposition 2. If the only ideals in commutative ring R are $\{0\}$ and R, then R is a field.