Advanced ALgebra

Rasmus Curt Raschke

October 17, 2025

Contents

Chapter 1

Introduction

1.1 Ring Theory

1.1.1 Lecture 15.10.25

1.1.2 Lecture 17.10.25

Important Ring Homomorphisms

Theorem 1.1 (Initial Ring)**.** The ring of integers $\mathbb{Z}$ is initial in `Ring`, i.e. for every unital ring R, there is a unique ring homomorphism $f : \mathbb{Z} \to \mathbb{R}$ and f is determined by $f(1) = 1_R$.

The last statement works by using the homomorphism property

$$f(\sum 1) = \sum f(1).$$

Theorem 1.2 (Terminal Ring)**.** The *null ring* is terminal in `Ring`, i.e. for every ring there is a unique ring homomorphism $f : R \to \{0\}$.

Example. Let $(A, +)$ be an abelian group and denote by $\mathrm{End}(A)$ the endomorphisms $A \to A$. Given any $f, g \in End(A)$, we define

$$(f + g)(x) := f(x) + g(x)$$

and

$$(f \cdot g)(x) := f(g(x))$$

for any $x \in A$. This makes $\mathrm{End}(A)$ an abelian group. The identity map $1 \in \mathrm{End}(A)$ turns $\mathrm{End}(A)$ into a ring. ◇

Exercise. What happens if A is not abelian?

There are several standard constructions of rings:

Definition 1.3 (Opposite Ring)**.** Let $(R, +, \cdot)$ be a ring. The **opposite ring** R^{op} is the same abelian group $(R, +)$ together with the inverted multiplication

$$(r, s) \mapsto s \cdot r.$$

Definition 1.4 (Polynomial Ring)**.** Given any ring R, define the **polynomial ring** of polynomials in x with coefficients in R by

$$R[x] := \left\{ \sum_i a_i x^i \mid a_i \in R,\ a_i = 0 \text{ for } i \text{ suff. large} \right\}.$$

Addition, multiplication and identity are inherited from R.

We construct higher polynomial rings $R[x_1, \ldots, x_n] := R[x_1, \ldots, x_{n-1}][x_n]$ inductively. For $p(x) \in \mathbb{F}[x]$, the degree is the highest non-zero power of x appearing in $p(x)$. We have

$$\deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x)).$$

This is not well-defined unless R is an integral domain: $\mathbb{R}[x]$ to $\mathbb{Z}/6\mathbb{Z}[x]$ shows this.

Example. The ring of *Laurent polynomials* is given by $R[x, x^{-1}]$. ◇

Example. The **ring of power series** in x is given by

$$R[\![x]\!] := \left\{ \sum_{i \geq 0} a_i x^i \mid a_i \in R \right\},$$

so we allow infinite sums. If one considers $1 - x \in \mathbb{R}[x]$, it does not have an inverse in $\mathbb{R}[\![x]\!]]$. However, in $\mathbb{R}[\![x]\!]$ one has the (formal) geometric series

$$\frac{1}{1-x} = \sum_{i \geq 0} x^i$$

as an inverse. ◇

Definition 1.5 (Principal Ideal)**.** A (left/right/two-sided) **principal ideal** of a ring R is a subset $Ra/aR/RaR$ for some $a \in R$ defined by

$$Ra := \{ra \mid r \in R\}.$$

Exercise. Principal ideals are ideals.

Remark. If R is commutative, all these notions collapse to one and one writes $\langle a \rangle$ for the ideal generated by a.

Example. We already know many principal ideals, e.g. $\langle 2 \rangle$ in $2\mathbb{Z}$ or $\langle n \rangle$ in $n\mathbb{Z}$. In $\mathbb{Z}$, every ideal is principal. For any ring, $\langle 0 \rangle$ and $\langle 1 \rangle$ are principal ideals. In polynomial rings, we always have principal ideals in the form of powers of x, e.g. $\langle x \rangle$, $\langle x^2 \rangle$, or $\langle x^2 + 1 \rangle$. In $R[x, y]$, $\langle x, y \rangle$ is a principal ideal. ◇

1.2 Modules

The idea is to generalize the idea of vector spaces, which are over fields, to something defined over rings.

Definition 1.6 (Module)**.** A **left R-module** (module over R) is an abelian group M together with a map

$$\begin{aligned} R \times M &\to M \\ (r, m) &\mapsto r \cdot m \end{aligned}$$

satisfying

1. $r(m+n) = rm + rn$
2. $(r+s)m = rm + sm$
3. $(rs)m = r(sm)$
4. $1_R \cdot m = m$

Right modules are defined analogously.

Exercise. There are several statements easy to prove:

- $\forall m \in M : 0 \cdot m = 0_M$
- $(-1) \cdot m = -m$

Theorem 1.7 (Abelian groups as module)**.** Every abelian group is a $\mathbb{Z}$-module in exactly one way.

Proof. $\mathbb{Z}$ is initial, so there is a unique homomorphism $\mathbb{Z} \to R$ for all unital R. □

This shows that abelian groups are nothing but $\mathbb{Z}$-modules (or, abstractly, $\mathbb{Z}$-vector spaces). End(`AGrp`) is a ring and we have an action of $\mathbb{Z}$ on any abelian groups by endomorphisms.

Example. Every ring R is a (left) R-module over itself. Furthermore, every (left) ideal $\mathcal{I} \subseteq R$ is a (left) R-module. Of course, there is also the trivial module $M = \{0\}$. ◇

If $\mathcal{I} \subseteq R$ is a left ideal, R/I is not a ring.

Exercise. If $\mathbb{I} \subseteq R$ is a left ideal, R/I is a left module.

Submodules

Definition 1.8 (Submodule)**.** A **submodule** N of a left R-module M is a subgroup preserved by the action of R, i.e.

$$\forall r \in R \forall n \in N : rn \in N.$$

Note. The (left) ideals of R are the left submodules of R viewing R as a module over itself.

Definition 1.9 (Simple Module)**.** A module M is **simple** if its only submodules are M and $\{0\}$.

Module Homomorphisms

Definition 1.10 (Module Homomorphism)**.** An **R-module homomorphism** is a homomorphism of abelian groups compatible with the R-module structure: If M, N are R-modules and $\varphi : M \to N$ is a homomorphism, then

1. $\forall m_1, m_2 \in M : \ \varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$
2. $\forall r \in R, \forall m \in M : \ \varphi(rm) = r\varphi(m)$.

Theorem 1.11 (Kernel and Image are Subs)**.** Let φ be an R-mod homomorphism. Both $\ker \varphi$ and φ are submodules.