Advanced ALgebra

Rasmus Curt Raschke

October 22, 2025

Contents

1 Introduction **2**
1.1 Ring Theory 2
1.1.1 Lecture 15.10.25 2
1.1.2 Lecture 17.10.25 2
1.2 Modules 4
1.2.1 Lecture 22.10.25 5

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 $\operatorname{im}\varphi$ are submodules.

1.2.1 Lecture 22.10.25

Definition 1.12 (Center)**.** Let R be a ring. The **center** of R is defined as

$$Z(R) := \{x \in R \mid \forall r \in R : xr = rx\}.$$

Exercise. Let M be an R-module and $r \in Z(R)$, then

$$rM := \{r \cdot m \mid m \in M\}$$

is a submodule. If $\mathcal{I} \subseteq R$ is any left ideal of R, then $\mathcal{I}M$ is a submodule of M.

Proposition 1.13 (Submodules are normal)**.** Let $N \subseteq M$ be a submodule. Then, N is a normal subgrup of M viewed as abelian groups.

Remark. This tells us that M/N is an abelian group. We want to give it some R-mod structure as follows: Consider the canonical projection $\pi : M \to M/N$ with $\pi(m) = m + N$. We have

$$r \cdot (m + N) = r \cdot \pi(m) = \pi(r \cdot m) = r \cdot m + N,$$

hence we define $r \cdot (m + N) = r \cdot m + N$. This is closed under addition.

Proposition 1.14 (Quotient Submodule)**.** Let M be an R-module and $N \subseteq M$ be a submodule. Then, M/N is also an R-module.

Proposition 1.15 (Quotient Ideal)**.** Suppose $\mathcal{I} \subseteq R$ is a two-sided ideal. Then, $\mathcal{I}$, R and $R/\mathcal{I}$ are all R-modules.

Theorem 1.16 (Universal Property of Quotient Modules)**.** Let M be an R-module and $N \subseteq M$ be a submodule. Then for every R-module homomorphism

$$\varphi : M \to P$$

such that $N \subseteq \ker \varphi$, there exists a unique R-mod homomorphism $\widetilde{\varphi}$ that makes the following diagram commute:

$$\begin{tikzcd} M \arrow[r, "\pi"] \arrow[d, "\varphi"'] & M/N \arrow[dl, dashed, "\exists!\widetilde{\varphi}"] \\ P & \end{tikzcd}$$

Proof. Define

$$\widetilde{\varphi} : M/N \to P$$

by $\widetilde{\varphi}(m+N) := \varphi(m)$. We have to check that it is a R-mod homomorphism, well-defined and unique. □

Theorem 1.17 (Homomorphism Theorem for Rings)**.** Every R-module homomorphism $\varphi : M \to P$ can be decomposed as

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\pi"] & P \\ M/\ker(\varphi) \arrow[r, "\overline{\varphi}"] & \mathrm{im}(\varphi) \arrow[u, hook, "\iota"] \end{tikzcd}$$

where $\overline{\varphi}$ is an isomorphism induced by the universal property.

Proof. $\widetilde{\varphi}$ with $\mathrm{im}(\varphi)$ as target and $\ker(\varphi)$ as the quotient, show it is iso. □

Corollary 1.18. Suppose $\varphi : M \to P$ is a surjective R-module homomorphism. Then

$$P \cong M/\ker(\varphi).$$

Left-Right Confusion

We denote left R-modules by ${}_RM$ and right modules by M_R.

Remark. Every right R-module M_R can be considered as a left R^{op}-module ${}_{R^{\mathrm{op}}}M$ by the opposite multiplication

$$\mu^{\mathrm{op}} : R^{\mathrm{op}} \times M \to M$$

with $\mu^{\mathrm{op}}(r, m) = m \cdot r$. Equivalently, ${}_RM \cong M_{R^{\mathrm{op}}}$.

Lemma 1.19. Let R be a commutative ring. Then every left module is natrually a right module, and vice versa.

Definition 1.20 (Bimodule)**.** Let R, S be not necessarily distinct rings. An $R - S$ bimodule ${}_RM_S$ is an abelian group M that is a left R-module and a right S module such that

$$\forall r \in R, s \in S, m \in M : (r \cdot m) \cdot s = r \cdot (m \cdot s).$$

Definition 1.21 (Generated Submodule)**.** Let M be an R-module and $A \subseteq M$ be a subset. Then

$$\langle A \rangle := \left\{ \sum_{i \in I} r_i a_i \mid r_i \in R, a_i \in A, \text{ only finitely many } a_i r_i \neq 0 \right\}$$

denotes the submodule generated by A.

Remark. We also have

$$\langle A \rangle = \bigcap_{U_i \subseteq M} U_i.$$

where each U_i is a submodule containing A, so $\langle A \rangle$ is the smallest submodule containing A.

Definition 1.22 (Generators and Cyclicity)**.** Let M be an R-module and $A \subseteq M$.

- If $M = \langle A \rangle$, A is the **generating set** of M.
- If A generates M and is finite, M is called **finitely generated**.
- A module M is **cyclic** if it admits a generating set with a single element.

Exercise. Show that the cyclic groups are all cyclic $\mathbb{Z}$-modules.

Definition 1.23 (Annihilator)**.** Let M be an R-module. The **annihilator** of a subset $U \subseteq M$ is given by

$$\operatorname{Ann}_R(U) := \{r \in R \mid \forall u \in U : r \cdot u = 0\}.$$

If M is a left R-module, the annihilator of some $U \subseteq M$ is a left ideal of R. For a single $x \in M$, we write

$$\operatorname{Ann}_R(x) := \{r \in R \mid r \cdot x = 0\}.$$

Corollary 1.24. There is a isomorphism of left R-modules

$$R/\operatorname{Ann}(x) \to Rx.$$

Proposition 1.25. If $U \subseteq M$ is a submodule, then $\operatorname{Ann}(U)$ is a two-sided ideal of R.

Algebras

Definition 1.26 (Associative Algebra)**.** Let R be a commutative ring. An **associative R-algebra** is an R-module A with the structure of an associative *but not necessarily unital* ring, such that ring addition agrees with module addition

$$\underbrace{a_1 + a_2}_{\text{algebra}} := \underbrace{a_1 + a_2}_{\text{module}}$$

and satisfies

$$\lambda(m \cdot n) = (\lambda m) \cdot n = m \cdot (\lambda n)$$

for $\lambda \in R$ and $m, n \in A$. If there is a unit, we call A **unital**.

Definition 1.27 (Group Ring)**.** Let G be a group and K be a commutative ring. The **group ring** $K[G]$ is the abelian group of maps

$$f : G \to K$$

that vanish on all but finitly many elements of G.

Note. Elements of $K[G]$ can be expressed uniquely as linear combinations

$$f = \sum_{g \in G} f_g \delta_g,$$

where $f_g \in K$ and δ_g is the map $g \mapsto 1 \in K$. This is often written as $f = \sum_g f(g)g$ for $f(g) \in K$. The multiplication is given by convolution:

$$\left(\sum_g a_g g\right) * \left(\sum_h b_h h\right) = \sum_{x \in G} \left(\sum_{g,h \in G, g \cdot h = x} a_g b_h\right) x.$$

We obtain the identity $\delta_g * \delta_h = \delta_{gh}$.

Exercise. Let $G = \mathbb{Z}_3$ represented by $\langle a \mid a^3 = 1 \rangle$. Choose $K = \mathbb{C}$. $\mathbb{C}[\mathbb{Z}_3]$ has elements

$$p = z_0 1 + z_1 a + z_2 a^2.$$

Show that

$$\mathbb{C}[\mathbb{Z}_3] = \mathbb{C}[a]/\langle a^3 - 1 \rangle.$$

Definition 1.28 (Representation)**.** A **representation** of a group G is a pair (V, ρ) where V is a $\mathbb{K}$-vector space, and ρ is a group homomorphism

$$\rho : G \to \mathrm{GL}(V) := \{\varphi \in \mathrm{End}(V) \mid \varphi \, \text{invertible}\}\,.$$

Remark. Given a G-representation (V, ρ) then the map

$$\begin{aligned} G \times V &\to V \\ (g, v) &\mapsto \rho(g)v \end{aligned}$$

defines a module action for the ring $K[G]$.
Given (V, ρ), can one find a $K[G]$-module? Yes, since we can define

$$\sum_g (\lambda_g \delta_g) v := \sum \lambda_g \rho(g)(v),$$

which is a $K[G]$-module structure on V, given a representation. We have

$$\{G - \text{representations}\} \cong \{K[G] - \text{modules}\}.$$