Algebra 3

Lectured by Alession Corti
Scribed by Yu Coughlin

Autumn 2025

Contents

1 Rings and modules **1**
1.1 Monoid rings 1

2 Matrix Lie groups **2**

1 Rings and modules

1.1 Monoid rings

Definition 1.1.1. A **ring** is an abelian group $(R, +, 0)$ which is also a monoid $(R, \cdot, 1)$ such that $\cdot$ distributes over $+$. We may also require $0 \neq 1$.

Some classical examples are:

- $\mathbb{Z}$, the ring of integers;
- any field like $\mathbb{F}_{p^n}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$;
- $M_n(R)$ the ring of $n \times n$ matrices with entries in R, the first noncommutative example here;
- R-valued functions out of any set have a pointwise ring structure;
- the first Weyl algebra is roughly "the ring of polynomial valued differential operators", defined as

  $$A_1 := \mathbb{C}[x, \partial]/(\partial x - x\partial = 1)$$

  you should think of this acting of $f \in \mathbb{C}[x]$, generated by the product rule:

  $$\partial x f - x\partial f = f\frac{d}{dx}xf - x\frac{d}{dx}f = f.$$

Definition 1.1.2. For a monoid P and a ring R the **monoid ring** is the set of finite R-linear sums:

$$\sum_{p \in P} r_p p.$$

The addition and multiplication come from the independent inclusions $R, P \subset R[P]$ by $r \mapsto r1_p$ and $p \mapsto 1_R p$ respectively.

Obviously, every group is a monoid, but here are some other examples:

- $\mathbb{N}$ is a semiring, so a monoid under addition;
- given a set X, both $\cup$ and $\cap$ make $\mathcal{P}(X)$ a monoid with $\emptyset, X$ the respective identities;
- the set of endomorphisms of an object in a category is always a monoid;

- let $C \subseteq \mathbb{R}^n$ be a convex cone, i.e. $\mathbb{R}_{\geq 0}C = C$ and $C + C = C$, then $P = C \cap \mathbb{Z}^n$ is a monoid under addition, if $C = \langle (1,0), (-1,2) \rangle$ is generated by poitns in $\mathbb{Z}$ we may not necessarily have P generated as a monoid by these same elements (in this case $(0,1) \in P$ but cannot be realised as a $\mathbb{Z}$-linear combination of $(1,0)$ and $(-1,2)$).

Most of the canonical examples of rings missed out earlier was because they can be realised as monoid rings:

- $R[x_1, \ldots, x_n]$ the ring of polynomials in n variables, is just the monoid ring $R[\mathbb{N}^n]$;
- $R[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$ the ring of Laurent polynomials in n varialbes, is the monoid ring $R[\mathbb{Z}^n]$;
- we will see that a lot of ring homomorphisms are induced by monoid homomorphisms they are rings over, a first example of this is the isomorphism $\mathbb{C}[\mathbb{Z}/n\mathbb{Z}] \cong \mathbb{C}[x]/(x^n - 1)$;
- we can define the quaternions $\mathbb{H}$ as a quotient of $\mathbb{R}[Q_8]$, where Q_8 is the quaternionic group $\{\pm 1, \pm i, \pm j, \pm k\}$, by the ideal $(1 + (-1), i + (-i), j + (-j), k + (-k))$;
- $\mathbb{R}[P]$ from earlier is a subring of $\mathbb{R}[x, y]$ which, as P isn't generated by $\{(1,0), (-1,2)\}$, is actually $\mathbb{R}[x, y, y^2/x]$.

Definition 1.1.3. For two rings S, R a **ring homomorphism** is a function $f : R \to S$ such that f is a homomorphism of the additive groups and multiplicative monoids.

Constructing ring is in general very hard, it is a lot of data.

Definition 1.1.4. If R is a ring and $f : P \to Q$ is a monoid homomorphism then there is an **induced homomorphism** $f_* : R[P] \to R[Q]$ given by:

$$\sum_{p \in P} r_p p \mapsto \sum_{p \in P} r_p f(p).$$

This makes a lot of interesting ring homomorphisms, anything more interesting belongs to the land of algebraic geometry, we will not discuss that here.
The **image** and **kernel** of a ring homomorphism are inhereted from the additive group homomorphism.

Definition 1.1.5. An additive subgroup $I \leq R$ is a **left ideal** if $RI \subseteq I$. Right ideals and two-sided ideals are defined obviously.

The kernel of a ring homomrophism is certainly a two-sided ideal. Conversely, to any ideal I there is a unique ring structure on R/I that makes $\varphi : R \to R/I$ a ring homomorphism.

Definition 1.1.6. A **left unit** in R is an element $u \in R$ such that there exists some $v \in R$ with $uv = 1$.

Are left units always right units? We know this to be true in commutative rings and $M_{n \times n}(k)$, but if we consider $GL(\mathbb{R}^{\mathbb{N}})$, with the basis $\{e_1, e_2, \ldots\}$, then the linear map which sends each e_i to e_{i+1} is injective and has a left inverse, but is not surjective so has no right inverse. But, if u has both a right inverse **and** a left inverse, then these will always be the same. The group of two-sided units is called $R^\times$.

2 Matrix Lie groups