Algebra 3

Lectured by Alession Corti
Scribed by Yu Coughlin

Autumn 2025

Contents

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 $R^\times$.

1.2 Classical algebra and whatnot

You probably already know what an Euclidean domain, principal ideal domain, unique factorisation domain, and a Noetherian ring are.

There won't be a particularly rigorous discussion of the relationship, because I don't care. Look at any set of official notes for something of higher quality if you require it.

Proposition 1.2.1. An Euclidean domain is a principal ideal domain.

Proof. Let R be an Euclidean domain with degree function φ, and let $I \trianglelefteq R$, consider $\varphi(I)$, this must have a smallest element, call it a. Now for any $i \in I$, we can write $i = qa + r$ with $\phi(r) < \phi(a)$, but r must be in I so cannot have degree less than that of a, so $r = 0$. Therefore, $I = (a)$. □

Proposition 1.2.2. A ring is Noetherian iff all ideals are finitely generated.

Proof. Suppose an ideal $I \trianglelefteq R$ does not admit a finite generating set. Find $i_0 \in I$, and $i_1 \in I \setminus (i_0)$, and recursively find $i_n \in I \setminus (i_0, i_1, \ldots, i_{n-1})$, this produces an ascending chain:

$$(i_0) \subsetneq (i_0, i_1) \subsetneq (i_0, i_1, i_2) \subsetneq \cdots$$

Conversely, suppose every ideal in R is finitely generated, then for any ascending chain of ideals:

$$I_0 \subset I_1 \subset I_2 \subset \cdots$$

their union I is also an ideal, which is finitely generated with its elements living in some I_N, thus the chain stabilises at this ideal. □

Proposition 1.2.3. A principal ideal domain is a unique factorisation domain.

Proof. First we show that any $r \in R$ a PID can't be an infinite product of irreducibles. Suppose such and r exists, then as r irreducible we can find a nontrivial factorisation $r = r_1 s$, one of these must contain infinitely many irreducibles, let this be r_1. Repeat this process ad infinum to get a chain of ideals

$$(r) \subsetneq (r_1) \subsetneq (r_2) \subsetneq \cdots$$

as R is a PID it is also Noetherian, so this ascending never stabilising chain of ideals cannot exist.[1]

We now wish to show any such product of irreducibles

$$r_1 r_2 \cdots r_n = r = s_1 s_2 \cdots s_m$$

are equivalent. First note that in a PID an element is irreducible iff it is prime.[2] We can now see each r_i appears in the RHS, as we are living in an integral domain we can cancel and thus are done. □

1.3 Unique factorisation in polynomial rings

Definition 1.3.1. Let R be a UFD, if $f \in R[x]$ the **content** of f is the gcd of its nonzero coefficients, written $c(f)$.

Lemma 1.3.2. If $f, g \in R[x]$, then $c(fg) = c(f)c(g)$.[3]

This really follows easily from

Lemma 1.3.3. If $c(f) = c(g) = 1$ then $c(fg) = 1$.

Proof. Suppose $c(fg) \neq 1$, then there exists some prime p dividing all the coefficients. First observe that as R is an integral domain, so is $R[x]$. Now consider the projection mod p, as $c(f) = c(g) = 1$ there exists no prime dividing all elements so they are both nonzero in $R/(p)[X]$ which we know to be an ID, but supposedly their product is 0. This is clearly a contradiction. □

For our next step we need the following

Theorem 1.3.4 (Gauss lemma)**.** If R is a UFD, and $f \in R[x]$ splits completely in $\mathrm{Frac}(R)[x]$, then f splits completely in $R[x]$.

From these two statements you should apparently be able to deduce that if R is a UFD, so is $R[X]$???

1.4 Newton polytopes

1.5 Hilbert basis theorem

2 Matrix Lie groups

[1] This proof is clearly nonconstructive as we are choosing contably many irreducible factorisations all at once

[2] Given r irreducible, if $r \mid ab$ we can consider $c = \gcd(r, a)$ and observe $c \mid r$. I'm only really interested in R an ED, so lets assume that. We know $r = cd$ for some d, as r is irreducible either c is a unit, in which case we can write $xr + ya = c$ implying $xrb + yab = cb$, as $r = ab$ we have that $r \mid b$. If, instead, c is an associate of r, then $r \mid a$. The other direction is easier.

[3] As with lots of things in this course, this must be taken up to multiplication by a unit.