250B: Commutative Algebra

Nir Elber

Spring 2022

Contents

Theme 1: Introduction

1.1 January 18

So it begins.

1.1.1 Unique Factorization

Warning 1. I am missing approximately the first third of class, so the remaining notes will likely be scattered as well.

We have the following definition.

Irreducible, prime

Definition 2 (Irreducible, prime)**.** Fix R a ring and $r \in R$ an element.

- We say that $r \in R$ is *irreducible* if and only if $r = ab$ for $a, b \in R$ implies that one of a or b is a unit.
- We say that $r \in R$ is *prime* if and only if r is not a unit, not zero, and (r) is a prie ideal: $r \mid ab$ implies $r \mid a$ or $r \mid b$.

This gives rise to the following important definition.

Unique factorization domain

Definition 3 (Unique factorization domain)**.** Fix R an integral domain. Then R is a *unique factorization domain* if and only if all nonzero elements of R have a unique factorization into irreducible elements.

Example 4. The ring $\mathbb{Z}$ is a unique factorization domain.

Note there are two things to check: that the factorization exists and that it exists.

Example 5. Consider the subring $R := k\left[x^2, xy, y^2\right] \subseteq k[x, y]$. Here x^2, xy, y^2 are all irreducibles because there are no linear polynomials, so the only possible decompositions must include a degree-0 (i.e., unit) polynomial. However, they are not prime:

$$x^2 \mid xy \cdot xy$$

while x^2 does not divide xy.

The following condition will provide a more

Ascending chain condition

Definition 6 (Ascending chain condition)**.** Given a collection of sets $\mathcal{S}$, we say that $\mathcal{S}$ *has the ascendinc chain condition* (ACC) if and only every chain of sets in $\mathcal{S}$ must eventually stablize.

Example 7 (ACC for principal ideals)**.** A ring R has the ascending chain condition for principal ideals if and only if every ascending chain of principal ideals

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$$

has some N such that $(a_N) = (a_n)$ for $n \geq N$.

Now, the fact that $\mathbb{Z}$ is a unique factorization domain roughly comes from the fact that $\mathbb{Z}$ is a principal ideal domain.

Theorem 8. Fix R a ring. Then R is a principal ideal domain implies that R is a unique factorizatino domain.

Proof. We start by showing that R has the ascending chain for principal ideals. Indeed, suppose that we have some ascending chain of principal ideals

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots .$$

Then the key idea is to look at the union of all these ideals, which will be an ideal by following the chain condition. However, R is a principal ideal domain, so there exists $b \in R$ such that

$$\bigcup_{k=1}^{\infty} (a_k) = (b).$$

However, it follows $b \in (a_N)$ for some N, in which case $(a_n) = (a_N)$ for each $n \geq N$.

Next we show that all prime elements are irreducible elements. The main idea is that prime ideals correspond to maximal ideals correspond to "irreducible ideals." We will not write this out; we showed this last semester. ∎

1.1.2 Digression on Gaussian Integers

As an aside, the study of unique factorization came from Gauss's study of the Gaussian integers.

Gaussian integers

Definition 9 (Gaussian integers)**.** The *Gaussian integers* are the ring

$$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}.$$

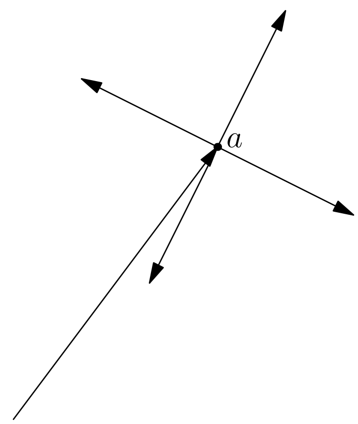
One can in fact check that $\mathbb{Z}[i]$ is a principal ideal domain, which implies that $\mathbb{Z}[i]$ is a unique factorization domain. The correct way to check that $\mathbb{Z}[i]$ is a principal ideal domain is to show that it is Euclidean.

Lemma 10. The ring $\mathbb{Z}[i]$ is Euclidean, where our norm is $\mathrm{N}(a + bi) := a^2 + b^2$. In other words, given $\alpha, \beta \in \mathbb{Z}[i]$, we need to show that there exists $q \in \mathbb{Z}[i]$ such that

$$a = bq + r$$

where $r = 0$ or $\mathrm{N}(r) < \mathrm{N}(\beta)$.

Proof. The main idea is to view $\mathbb{Z}[i] \subseteq \mathbb{C}$ geometrically as in $\mathbb{R}^2$. We may assume that $|\beta| \leq |\alpha|$, and then it suffices to show that in this case we may find q so that $a - bq$ has smaller norm than a. Well, for this it suffices to look at $a + b, a - b, a + ib, a - ib$; the proof that one of these works essentially boils down to the following image.



Note that at least one of the endpoints here has norm smaller than a. ■

What about the primes? Well, there is the following theorem which will classify.

Theorem 11 (Primes in $\mathbb{Z}[i]$)**.** An element $\pi := a + bi \in \mathbb{Z}[i]$ is *prime* if and only if $\mathrm{N}(\pi)$ is a $1 \pmod 4$ prime, $(pi) = (1 + i)$, or $(\pi) = (p)$ for some prime $p \in \mathbb{Z}$ such that $p \equiv 3 \pmod 4$.

We will not fully prove this; it turns out to be quite hard, but we can say small things: for example, $3 \pmod 4$ primes p remain prime in $\mathbb{Z}[i]$ because it is then impossible to solve

$$p = a^2 + b^2$$

by checking $\pmod 4$.

Remark 12. This sort of analysis of "sums of squares" can be related to the much harder analysis of Fermat's last theorem, which asserts that the Diophantine equation

$$x^n + y^n = z^n$$

for $xyz \neq 0$ integers such that $n > 2$.

1.1.3 Noetherian Rings

We have the following definition.

Noetherian ring

Definition 13 (Noetherian ring)**.** A ring R is said to be *Noetherian* if its ideals have the ascending chain condition.

There are some equivalent conditions to this.

Proposition 14. Fix R a ring. The following conditions are equivalent.

- R is Noetherian.
- Every ideal of R is finitely generated.

Proof. We will show one direction, if R has an infinitely generated ideal

$$I := (a_1, a_2, a_3, \ldots),$$

then we have the non-stabilizing ascending chain

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots .$$

We leave the other direction as an exercise. ■

A large class of rings turn out to be Noetherian, and in fact oftentimes Noetherian rings can build more Noetherian rings.

Proposition 15. Fix R a Noetherian ring and $I \subseteq R$ an ideal. Then R/I is also Noetherian.

Proof. Any chain of ideals in R/I can be lifted to a chain in R by taking pre-images along $R \twoheadrightarrow R/I$. Then the chain must stabilize in R, so they will stabilize back down in R/I as well. ■

However, things are not always so nice. It is not true that $R_1 \subseteq R_2$ with R_2 Noetherian implies that R_1 is Noetherian.

example

Non-Example 16.

Here is another way to generate Noetherian rings.

Theorem 17 (Hilber basis)**.** If R is a Noetherian ring, then $R[x]$ is also a Noetherian ring.

Corollary 18. By induction, if R is Noetherian, then $R[x_1, x_2, \ldots, x_n]$ is Notherian for any finite n.

Warning 19. It is not true that $R[x_1, x_2, \ldots]$ is Noetherian: the ideal $(x_1, x_2, \ldots)$ is not finitely generated!

Proof of Theorem 17. The idea is to use the degree of polynomials to measure size. Fix $I \subseteq R[x]$ an ideal, and we apply the following inductive process.

- Pick up $f_1 \in I$ of minimal degree in I.
- If $I = (f_1)$ then stop. Otherwise find $f_2 \in I \setminus (f_1)$ of minimal degree.
- In general, if $I \neq (f_1, \ldots, f_n)$, then pick up $f_{n+1} \in I \setminus (f_1, \ldots, f_n)$ of minimal degree.

Importantly, we do not know that there are only finitely many $f_\bullet$ yet.

Now, look at the leading coefficients of the $f_\bullet$, which we name $a_\bullet$. However, the ideal

$$(a_1, a_2, \ldots) \subseteq R$$

must be finitely generated, so there is some finite N such that

$$(a_1, a_2, \ldots) = (a_1, a_2, \ldots, a_N).$$

To finish, we claim that

$$I \stackrel{?}{=} (f_1, f_2, \ldots, f_N).$$

Well, suppose for the sake of contradiction that we can find some $g \in I \setminus (f_1, f_2, \ldots, f_N)$ of least degree. We must have $\deg g \deg f_\bullet$ for each $f_\bullet$, or else we contradict the construction of $f_\bullet$ as being least degree.

why?

To finish, let a be the leading coefficient of g, which must be an element of $(a_1, a_2, \ldots)$, but then we can look at

$$g - \sum_{k=1}^{N} c_k a_k x^{(\deg g)-(\deg f_k)} f_k,$$

which will have degree smaller than g while not being in I either, which contradicts the minimality of the degree of g. ■

1.1.4 Modules

To review, we pick up the following definition.

Module

Definition 20 (Module)**.** Fix R a ring. Then M is an abelian group with an R-action. Explicitly, we have the following properties. Fix any $a, b \in R$ and $m, n \in M$.

- $1_R m = m$.
- $a(bm) = (ab)m$.
- $(a+b)m = am + bm$.
- $a(m+n) = am + an$.

Example 21. Any ideal $I \subseteq R$ is an R-module. In fact, ideals exactly correspond to the R-submodules of R.

Example 22. Given any two R-module M with a submodule $N \subseteq M$, we can form the quotient $N \subseteq M$.

Modules also have a notion of being Noetherian.

Noetherian module

Definition 23 (Noetherian module)**.** We say that an R-module M is *Noetherian* if and only if all R-submodules of M are finitely generated. Equivalently, the submodules of M have the ascending chain condition.

Modules have some interesting ways to create new Noetherian submodules. Here is one important way.

Proposition 24. Fix a short exact sequence

$$0 \to A \to B \to C \to 0$$

of R-modules. Then B is Noetherian if and only if A and C are both Noetherian.

Proof. We will not prove this here. The forwards direction is not too hard: A being a submodule of a Noetherian module implies that all of its submodules still must be finitely generated. Then for C, one considers the quotient in the same way we did for rings. ■

Because we like Noetherian rings, the following is a reassuring way to make Noetherian modules.

Proposition 25. Every finitely generated R-module over a Noetherian ring R is Noetherian.

Proof. If M is finitely generated, then there exists some $n \in \mathbb{N}$ and surjective morphism

$$\varphi : R^n \twoheadrightarrow M.$$

Now, because R is Noetherian, R^n will be Noetherian by an induction: the inductive step looks at the short exact sequence

$$0 \to R \to R^n \to R^{n-1} \to 0.$$

Thus, M is the quotient of a Noetherian ring R^n and hence Noetherian. ■

Here is the analogous result for algebras.

Algebra

Definition 26 (Algebra)**.** A ring S is an R-module if and only if there is an embedding $R \hookrightarrow S$.

Proposition 27. Fix R a Noetherian ring. Then any finitely generated R-algebra is Noetherian. Equivalently, we may think of an R-algebra as a ring with an R action.

Proof. Saying that S is a finitely generated R-algebra is the same as saying that there is a surjective morphism

$$\varphi : R[x_1, \ldots, x_n] \twoheadrightarrow S$$

for some $n \in \mathbb{N}$. But then S is the quotient of a $R[x_1, \ldots, x_n]$, which is Noetherian by Theorem 17, so S is Noetherian as well. ■

1.1.5 Invariant Theory

In our discussion, fix k a field of characteristic 0, and let G be a finite group or $\mathrm{GL}_n(k)$ (say). Now, suppose that we have a map

$$G \to \mathrm{GL}_n(k).$$

Then this gives $k[x_1, \ldots, x_n]$ a G-action by writing $gf(\vec{x}) := f(g^{-1}\vec{x})$. The central question of invariant theory is then as follows.

Question 28 (Invariant theory)**.** Fix everything as above. Then can we describe $k[x_1, \ldots, x_n]^G$?

By checking the group action, it is not difficult to verify that $k[x_1, \ldots, x_n]^G$ is a subring of $k[x_1, \ldots, x_n]$. For brevity, we will write $R := k[x_1, \ldots, x_n]$ and $S := R^G$.

Here is a result of Hilbert.

Theorem 29 (Hilbert)**.** Fix everything as above. Then the ring $k[x_1, \ldots, x_n]^G$ is Noetherian.

Proof. Please read this on your time; we skipped it in class. The main ingredient is the Hilbert basis theorem. ■

The main example here is as follows.

Example 30. Consider the action of S_n on $R = k[x_1, \ldots, x_n]$ by permuting the coordinates: $\sigma \in S_n$ acts by $\sigma \cdot x_m := x_{\sigma n}$. Then the polynomials in $S = R^G$ are the *homogeneous* polynomials. The fundamental theorem of symmetric polynomials tells us that

$$R^G = k[e_1, e_2, \ldots, e_n],$$

where the $e_\bullet$ are *elementary symmetric functions.* Explicitly,

$$e_m := \sum_{\substack{T \subseteq \{1,\ldots,n\} \\ \#S = m}} \prod_{t \in T} x_t.$$

Remark 31. Yes, I am in fact running out of letters. Thank you for asking.

Here is more esoteric example.

Example 32. Fix $R := k[x,y]$ and $G = \{1, g\} \cong \mathbb{Z}/2\mathbb{Z}$. Then we define our G-action by

$$g \cdot x = -x \qquad \text{and} \qquad g \cdot y = -y.$$

Then R^G consists of all polynomials $f(x,y)$ such that $f(x,y) = f(-x,-y)$; i.e., these are the polynomials in R that all have even degree. It follows after some pushing that

$$R^G = k\left[x^2, xy, y^2\right].$$

To see that this ring is Noetherian, we note that there is a surjection

$$\varphi : k[u,v,w] \to k\left[x^2, xy, y^2\right]$$

taking $u \mapsto x^2$ and $v \mapsto xy$ and $w \mapsto y^2$. Thus, R is the quotient of a Noetherian ring and hence Noetherian itself. In fact, we can check that $\ker \varphi = \left(uw - v^2\right)$.

Next class we will start talking about the Nullstellensatz, which has connections to algebraic geometry.