12 Factorization in Rings

12.1 Review

Last class, we began discussing factorization.

Definition 12.1
An element $a \in R$ is **irreducible** if it is not a unit, and if $a = bc$ then either b or c is a unit.

In other words, irreducible elements are ones which cannot be factored in a nontrivial way; so when attempting to factor in a ring, we want to factor our elements as a product of irreducibles.

In our discussion of factorization, we'll always assume R is an integral domain (meaning that if $ab = 0$, then either $a = 0$ or $b = 0$) — this allows us to perform cancellation.

When discussing unique factorization, we can always multiply the factors by units; so to make the notion of "essentially unique" (as mentioned last class) more precise, we use the following definition:

Definition 12.2
Two elements $a, b \in R$ are **associate** if $a = bu$ for a unit $u \in R$.

Then a domain R is a unique factorization domain (UFD) if every non-unit element can be written as a product of irreducible elements in a unique way, up to ordering and association.

Recall that a domain R is a principal ideal domain (PID) if every ideal in R is principal. As mentioned last class, we can generalize our proof that $F[x]$ is a UFD to work for any PID:

Theorem 12.3
Any PID is a UFD.

Sketch of Proof. We need to show that a factorization exists, and is unique.

To prove uniqueness, since R is a PID, we have that if $p \in R$ is irreducible, then (p) is maximal. So then $R/(p)$ is a field, and since fields have no zero divisors, it follows that if p divides ab, then p divides a or p divides b. This implies uniqueness — now given any two factorizations $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_m$, we can show that p_1 must appear on the right-hand side as well (up to association), and cancel it out from both sides.

We won't prove existence in general now (it requires a new idea, which we'll see later). But in the examples we'll deal with, existence is clear. We can start with any element of R and keep factoring it until we're stuck, at which point all factors must be irreducible. Then in our examples, this factorization process always "shrinks" the elements in some sense — in the case of integers, their size decreases, and in the case of polynomials, their degree decreases — so it must terminate. (We can't perform this argument in an abstract PID because it doesn't necessarily have a notion of size. We will later see a different way to show that the process terminates, using *Noetherian rings*.) □

Note 12.4
Elements with the property that if $p \mid ab$, then $p \mid a$ or $p \mid b$ (which we used in the proof of uniqueness) are called **prime**.

12.2 Euclidean Domains

Earlier, we saw that for a field F, the ring $F[x]$ is a PID. We can apply the argument used here to a somewhat more general class of rings.

Definition 12.5
A Euclidean domain is a domain R together with a size function $\sigma : R \setminus \{0\} \to \mathbb{Z}_{>0}$ such that for every $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that

$$a = bq + r,$$

and $\sigma(r) < \sigma(b)$ or $r = 0$.

In other words, a Euclidean domain is a domain where we can perform division with remainder, such that the remainder has smaller size than the element we're dividing by.

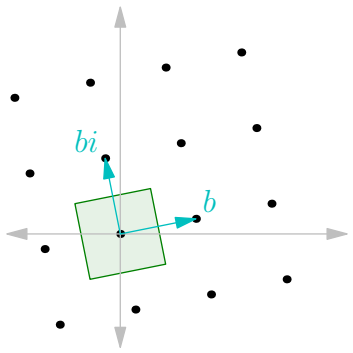
Proposition 12.6
A Euclidean domain is a PID, and therefore a UFD.

Example 12.7
The familiar ring $\mathbb{Z}$ is a Euclidean domain with size function $\sigma(a) = |a|$.

Example 12.8
For a field F, the polynomial ring $F[x]$ is a Euclidean domain with $\sigma(P) = \deg P$.

Example 12.9
The Gaussian integers $\mathbb{Z}[i]$ form a Euclidean domain with size function $\sigma(a + bi) = a^2 + b^2$.

Proof. We can prove that the division with remainder property holds by geometry. Given b, the multiples of b form a square lattice (generated as a lattice by b and bi).



So by subtracting multiples of b, we can guarantee that a lands in the small square centered at the origin — more precisely, we can guarantee that $r = \alpha b + \beta i b$ where $-\frac{1}{2} \leq \alpha, \beta \leq \frac{1}{2}$. Then we have $\sigma(r) \leq \frac{1}{2}\sigma(b) < \sigma(b)$, as desired. □

So the concept of a Euclidean domain is useful — there exist examples other than the ones we started thinking about. We can now prove that Euclidean domains are PIDs, in the same way as we did with polynomials.

Proof of Proposition 12.6. If $I \subset R$ is a nonzero ideal, then take an element $b \in I$ with minimal $\sigma(b)$. We know that for any $a \in I$, we can write $a = bq + r$, with $r = 0$ or $\sigma(r) < \sigma(b)$. The second case is impossible — we have $r \in I$, but we chose b to have minimal size of the nonzero elements in I — so we must have $r = 0$. So b divides all elements of I, which means $I = (b)$. □

However, this isn't *very* general — there are many rings which it *doesn't* cover.

Example 12.10
The ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, and therefore not a PID or Euclidean domain.

Proof. We have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

It's possible to show that all of the elements 2, 3, and $1 \pm \sqrt{-5}$ are irreducible, so R does not have unique factorization.

Note that it *is* still possible to bound $\sigma(r)$ in terms of $\sigma(b)$ by the same geometric argument as before; but this bound will not be strong enough to imply $\sigma(r) < \sigma(b)$. □

Student Question. *The size functions in our examples have nice properties — the size functions on $\mathbb{Z}$ and $\mathbb{Z}[i]$ are multiplicative, and the size function in $F[x]$ satisfies $\sigma(PQ) = \sigma(P) + \sigma(Q)$. Does something like this have to hold in general?*

Answer. *No — the ones that we've seen in our examples* do *satisfy additional properties, but we didn't need those nice properties for the argument to work. The definition itself also doesn't guarantee any other nice properties. For example, in a field, the size function can be* anything *— every element is divisible by every nonzero element, so we can perform division even without remainder (meaning that $r = 0$).*

12.3 Polynomial Rings

Every PID is a UFD, but the converse is not true! There are cases where unique factorization is true, but there are non-principal ideals. For example, we'll see that $\mathbb{Z}[x]$ and $\mathbb{C}[x_1, \ldots, x_n]$ are UFDs. But the ideal $(2, x) \subset \mathbb{Z}[x]$ and the ideal $(x, y) \subset \mathbb{C}[x, y]$ are not principal.

The theorem that will imply both of these examples is the following.

Theorem 12.11
If R is a UFD, then $R[x]$ is also a UFD.

Corollary 12.12
The rings $\mathbb{Z}[x]$ and $\mathbb{C}[x_1, \ldots, x_n]$ are UFDs.

Proof of Corollary. For $\mathbb{Z}[x]$, this follows directly from the theorem (since we know $\mathbb{Z}$ is a PID). Meanwhile, for $\mathbb{C}[x_1, \ldots, x_n]$, we can use induction: we have

$$\mathbb{C}[x_1, \ldots, x_n] = \mathbb{C}[x_1, \ldots, x_{n-1}][x_n]$$

by thinking of n-variable polynomials as polynomials in the last variable x_n, whose coefficients are polynomials in the other $n - 1$ variables — for example,

$$x + xy + y^2x^2 + xy^2 = (x) + (x)y + (x + x^2)y^2$$

is a polynomial in y whose coefficients are in $\mathbb{C}[x]$. So using induction, this follows immediately from the theorem as well. □

12.3.1 Greatest Common Divisors

To prove Theorem 12.11, we'll need the concept of a gcd in R.

Definition 12.13
In a domain R, a **greatest common divisor** of two elements $a, b \in R$, denoted $\gcd(a, b)$, is an element d such that d divides both a and b, and any other element δ that divides both a and b must also divide d.

A gcd may or may not exist. But if $\gcd(a, b)$ exists, it is unique up to association, i.e., up to multiplying by a unit — if d and d' are both gcd's of a and b, then we must have $d \mid d'$ and $d' \mid d$. This implies we have $d = ud'$ and $d' = zd$ for some elements u and z. Then $d = uzd$, and since R is a domain, we have $uz = 1$, so u and z are both units.

Example 12.14
In $\mathbb{Z}[\sqrt{-5}]$, there is no gcd of $2 + 2\sqrt{-5}$ and 6.

Proof. Note that 2 is a common divisor of $2 + 2\sqrt{-5}$ and 6, and it's maximal in the sense that if multiplied by any non-unit element, the result is no longer a common divisor. So if the gcd existed, it would have to be 2 (up to association). But $1 + \sqrt{-5}$ has the same property — in particular, $1 = \sqrt{-5}$ is a common divisor but does not divide 2. So there cannot exist a gcd. □

Proposition 12.15
In a UFD, the gcd of any two elements always exists.

Proof. The usual way of calculating the gcd using prime factorization (for example, in the case of integers) works in any PID. More explicitly, to find $\gcd(a, b)$ we can write down the factorizations of a and b, and take the smaller power of each irreducible element. □

Note 12.16
In a PID, if $\gcd(a, b) = d$, then we have $(a, b) = (d)$, which means d can be written in the form $ap + bq$. But this is not true in general — for example, in $\mathbb{C}[x, y]$, we have $\gcd(x, y) = 1$, but $1 \notin (x, y)$.

12.3.2 Gauss's Lemma

Our goal is to analyze factorization in $R[x]$. We know how factorization works in R, and we *also* know how factorization works in a closely related ring — if $F = \mathrm{Frac}(R)$, then since F is a field, $F[x]$ is a PID. To relate factorization in $R[x]$ to factorization in these two better-understood rings, we use Gauss's Lemma.

Definition 12.17
A polynomial $P \in R[x]$ is **primitive** if the gcd of all its coefficients is a unit.

Lemma 12.18 (Gauss's Lemma)
If $P, Q \in R[x]$ are primitive, then so is PQ.

Proof. It's enough to show that for any irreducible $p \in R$, we can find a coefficient of PQ not divisible by p (as then by unique factorization, no element other than units can divide the gcd of its coefficients).

Let $P = \sum a_i x^i$ and $Q = \sum b_j x_j$, and let m be the maximal integer with $m \nmid a_m$ and n the maximal integer with $n \nmid b_n$. Then in PQ, the coefficient of x^{m+n} comes from $a_m b_n$, and other terms $a_i b_j$ where at least one of a_i and b_j is divisible by p; so this coefficient cannot be divisible by p. □

Using this, we can get a good sense of which polynomials are irreducible in R — as we'll see later, these are the irreducible elements of R, and primitive polynomials in $R[x]$ which are irreducible in $F[x]$, where $F = \mathrm{Frac}(R)$. So we can use unique factorization in R and in $F[x]$ to prove unique factorization in $R[x]$.

Resource: Algebra II Student Notes

Spring 2022

Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng