EUCLIDEAN RINGS

1. Introduction

The topic of this lecture is *eventually* a general analogue of the unique factorization theorem for the integers:

Theorem 1.1. *Let n be a nonzero integer. Then n factors as*

$$n = \pm p_1^{e_1} \cdots p_r^{e_r}, \quad r \geq 0,\ p_1, \cdots, p_r \in \mathcal{P},\ e_1, \cdots, e_r \in \mathbb{Z}^+,$$

and the factorization is unique.

The proof that a factorization *exists* is easy, at least on the face of it. Consider any positive integer n. If n is irreducible then we are done. Otherwise $n = n_1 n_2$ with $n_1 < n$ and $n_2 < n$, and so we are done by induction. The only worrisome point here is that *irreducible* has appeared as a stand-in synonym for *prime*, suggesting that *prime* might mean something other than *irreducible* to the cognescenti. We will see that indeed the two words mean different things, and that the mathematical use of *prime* is not as we would expect.

By contrast, the proof that the factorization is unique is nuanced. Many books prove unique factorization in $\mathbb{Z}$ by elementary methods, but to me the issues are somehow more naturally (i.e., more clearly, perhaps more easily) discussed in the context of ring theory rather than just in the integers $\mathbb{Z}$. The upshot is that this lecture in some sense proceeds backwards through chapter 1 of Ireland and Rosen. (Nonetheless, you should read the chapter from front to back.)

2. Rings, Integral Domains

Definition 2.1. *A* **commutative ring with identity** *is an algebraic structure*

$$(R, +, \cdot)$$

that satisfies all of the field axioms except (possibly) the existence of multiplicative inverses. That is, for all $r, s, t \in R$ we have

$$\begin{aligned}
&r + s = s + r,\\
&(r + s) + t = r + (s + t),\\
&r \cdot s = s \cdot r,\\
&(r \cdot s) \cdot t = r \cdot (s \cdot t),\\
&r \cdot (s + t) = r \cdot s + r \cdot t.
\end{aligned}$$

and there exist distinct additive and multiplicative identities $0, 1 \in R$ such that for all $r \in R$,

$$\begin{aligned}
&r + 0 = r,\\
&r + s = 0 \quad \textit{for some } s \in R,\\
&r \cdot 1 = r.
\end{aligned}$$

Often we will simply refer to a commutative ring with identity as a **ring**. And we usually omit the "$\cdot$" symbol for multiplication. As in Math 112, for any given $r \in R$, the element $s \in R$ such that $r + s = 0$ is unique, and so it can be unambiguously denoted $-r$.

Definition 2.2. *Given a ring $(R, +, \cdot)$, its* **units group** *is the algebraic structure*

$$(R^\times, \cdot)$$

whose underlying structure is the set of multiplicatively invertible elements of R,

$$R^\times = \{r \in R : rs = 1 \text{ for some } s \in R\},$$

and whose operation is the restriction of the multiplication of R to $R^\times$.

The units group is an abelian group in that the product of two units is a unit (if $rs = 1$ and $r's' = 1$ then $(rr')(ss') = 1$) and that for all $r, s, t \in R^\times$,

$$\begin{aligned} rs &= sr, \\ (rs)t &= r(st), \\ r1 &= r, \end{aligned}$$

and for all $r \in R^\times$,

$$rs = 1 \quad \text{for some } s \in R^\times.$$

The s here is unique, so it can be denoted r^{-1}.

Definition 2.3. *An* **integral domain** *is a ring $(R, +, \cdot)$ satisfying the following property:*

$$\text{For all } r, s \in R, \quad rs = 0 \implies r = 0 \text{ or } s = 0.$$

That is, an integral domain has no *zero-divisors*, i.e., no nonzero elements r, s such that $rs = 0$. (To make sure that the language is clear: *zero-divisor* means *divisor of zero*.) The **cancellation law** holds in any integral domain:

$$\text{If } ab = ac \text{ and } a \neq 0 \text{ then } b = c.$$

Note that we do not prove the cancellation law by multiplying through by a^{-1}—the inverse may not exist. Rather, the argument is that $a(b - c) = 0$ and $a \neq 0$, so that $b - c = 0$.

Some rings to bear in mind, beyond the most obvious example $\mathbb{Z}$ (we usually write R rather than $(R, +, \cdot)$ when the operations are clear) are

- the Gaussian integers $\mathbb{Z}[i]$,
- the *cubic integers* $\mathbb{Z}[\omega]$ where $\omega = \zeta_3 = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$,
- the *polynomial ring* $k[X]$ where k is any field.

Note that $k[X]$ is a ring of functions rather than a ring of numbers.

3. Prime and Irreducible Elements

Definition 3.1. *Let R be a ring. An element r of R* **divides** *an element s of R if $s = rr'$ for some $r' \in R$. The symbolic notation for r* divides *s is*

$$r \mid s.$$

A nonunit r of R is **prime** *if:*

$$\text{For all } s, s' \in R, \quad r \mid ss' \implies r \mid s \text{ or } r \mid s'.$$

Let $R^\times$ be the unit group of R. A nonunit r of R is **irreducible** *if:*

$$\text{For all } s, s' \in R, \quad ss' = r \implies s \in R^\times \text{ or } s' \in R^\times.$$

Thus primality is a criterion about how a given ring element fits into products, while irreducibility is a criterion about how products fit into a given element. There are ways to rewrite the definitions of *prime* and *irreducible* to further emphasize their symmetry (e.g., for irreducibility, the condition

$$\text{for all } s, s' \in R, \quad ss' = r \implies r \mid s \text{ or } r \mid s'$$

is equivalent to the condition in the definition), but our phrasings of the definitions are fairly standard.

4. Generally Prime $\implies$ Irreducible

The cancellation law says that 0 is prime in any integral domain. On the other hand, 0 is not irreducible since $0 \cdot 0 = 0$ but neither factor 0 of 0 is a unit. The next result says that 0 is exceptional in being a prime that is not irreducible.

Proposition 4.1. *In any integral domain, nonzero primes are irreducible.*

Proof. Let R be an integral domain and let $R^\times$ be its units group. Consider any nonzero prime r of R. If $r = ss'$ then $s \mid r$ and (without loss of generality) $r \mid s$. Thus $r = ss' = rus'$. Since $r \neq 0$ we have $us' = 1$ by cancellation, and consequently $s' \in R^\times$. □

The converse question is

Are the irreducible elements of an integral domain prime?

This question does not have a general answer. For example, consider a subring of the complex number system and its unit group,

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}, \qquad R^\times = \{\pm 1\}.$$

Then R is an integral domain. The element 2 of R is irreducible because for all $s, s' \in R$,

$$ss' = 2 \implies s\overline{s}s'\overline{s'} = 4 \implies s\overline{s} = 2 \text{ or } s \text{ is a unit or } s' \text{ is a unit},$$

but the condition $s\overline{s} = 2$ is impossible in R since $s\overline{s} = a^2 + 5b^2$ for some $a, b \in \mathbb{Z}$. On the other hand 2 is not prime because

$$2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \quad \text{but} \quad 2 \nmid (1 + \sqrt{-5}) \text{ and } 2 \nmid (1 - \sqrt{-5}).$$

(For instance, if $2 \mid 1 + \sqrt{-5}$ then also $2 = \overline{2} \mid \overline{1 + \sqrt{-5}} = 1 - \sqrt{-5}$, and consequently $4 = 2 \cdot 2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$, which is false.)

5. Euclidean Domains

Definition 5.1. *The integral domain R is* **Euclidean** *if it comes equipped with a* **norm** *function*

$$N : R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

such that the following condition holds: For all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that

$$a = qb + r, \quad r = 0 \text{ or } Nr < Nb.$$

Here q is the **quotient** *obtained on dividing a by b, and r is the* **remainder**.

All of our example rings from earlier are Euclidean.

- For $R = \mathbb{Z}$, take $Nn = |n|$ all nonzero $n \in \mathbb{Z}$.
- For $R = \mathbb{Z}[i]$, take $Nz = z\overline{z} = |z|^2 = a^2+b^2$ for all nonzero $z = a+ib \in \mathbb{Z}[i]$.
- For $R = \mathbb{Z}[\omega]$, take $Nz = z\overline{z} = |z|^2 = a^2 - ab + b^2$ for all nonzero $z = a + \omega b \in \mathbb{Z}[\omega]$. (Note that $\overline{\omega} = \omega^2$.)
- For $R = k[X]$, take $Nf = \deg(f)$ for nonzero polynomials $f \in k[X]$. Note that nonzero constant polynomials have norm 0.

In each case we need to verify that the specified norm makes the integral domain Euclidean.

- Verifying that the $\mathbb{Z}$-norm makes $\mathbb{Z}$ Euclidean is easy: Given $a, b \in \mathbb{Z}$ with $b \neq 0$, let
$$S = \{a - qb : q \in \mathbb{Z}\}.$$
Note that S contains nonnegative elements (those arising from $q \leq a/b$ if $b > 0$, those arising from $q \geq a/b$ if $b < 0$), and let r be the least nonnegative element of S. Then indeed $a = qb + r$, and $Nr = r$ must be less than b because otherwise S has a smaller nonnegative element $r - b$.
- To verify that the $\mathbb{Z}[i]$-norm makes $\mathbb{Z}[i]$ Euclidean, consider any $a, b \in \mathbb{Z}[i]$ with $b \neq 0$. Note that $a/b = r + is$ where $r, s \in \mathbb{Q}$. Then $a/b = r + is$ sits in the unit box about some point $q = m + in \in \mathbb{Z}[i]$. Consequently $a/b - q$ sits in the unit box about 0. It follows that $N(a/b - q) \leq 1/2 < 1$, and so since the norm (extended to $\mathbb{Q}[i]$) is multiplicative, $N(a - qb) < Nb$.
- The verification that $\mathbb{Z}[\omega]$ is Euclidean is very similar. This time the parallelogram about 0 is the points $s + \omega t$ where $-1/2 \leq s < 1/2$ and $-1/2 \leq t < 1/2$. Any point in the parallelogram has norm at most $3/4$, hence norm strictly less than 1.
- The verification that the $k[X]$-norm makes $k[X]$ Euclidean is a matter of polynomial long division. Specifically, given $a, b \in k[X]$ with $b \neq 0$, proceed as follows.
  - (*Initialize*)
    Set $q = 0$ and $r = f$. Let $g = b_m x^m + \cdots$. (So $f = qg + r$.)
  - (*Iterate*)
    While $\deg r \geq \deg g$,
    let $r = r_n x^n + \cdots$ and set $\delta = (r_n/b_m)x^{n-m}$
    replace q by $q + \delta$
    replace r by $r - \delta g$. (Still $f = qg + r$, and $\deg r$ has decreased.)
  - (*Terminate*)
    Return q and r. (Now $f = qg + r$, and $\deg r < \deg g$.)

6. Ideals, Principal Ideals

Definition 6.1. *Let R be a ring. A subset I of R is called an* **ideal** *if*

(1) *I is closed under addition: for all $i, j \in I$, also $i + j \in I$.*
(2) *I is strongly closed under multiplication: for all $r \in R$ and $i \in I$, also $ri \in I$.*

The definition of ideal may seem unmotivated. The point is that ideals are the correct subrings for the creation of quotient rings, just as normal subgroups are the correct subgroups for the creation of quotient groups. But we do not discuss quotient structures here.

For example, let R be a ring, pick any element $r_0 \in R$ and let (r_0) denote the set of all multiples of r_0,

$$(r_0) = \{rr_0 : r \in R\}.$$

For instance, $(2) = \{0, \pm 2, \pm 4, \cdots\}$ in $\mathbb{Z}$. Similarly, pick any two elements $r_0, s_0 \in R$ and let (r_0, s_0) denote the set of all R-linear combinations of r_0 and s_0,

$$(r_0, s_0) = \{rr_0 + ss_0 : r, s \in R\}.$$

For instance, $(2, 3) = \{-1 \cdot 2 + 1 \cdot 3, \cdots\} = \{1, \cdots\} = \mathbb{Z}$ in $\mathbb{Z}$, while $(2, 4) = (2)$ and $(4, 6) = (2)$ as well.

Definition 6.2. *The ideal I is* **principal** *if it takes the form $I = (r)$ for some $r \in R$.*

So far, all of the ideals that we have seen are principal. (**NOT** "principle.") For an example of a nonprincipal ideal, let $R = \mathbb{Z}[\sqrt{-5}]$ and let

$$I = (2, 1 + \sqrt{-5}).$$

Recalling that $N(a + b\sqrt{-5}) = a^2 + 5b^2$, note that $N2 = 4$ and $N(1 + \sqrt{-5}) = 6$. Suppose that I is principal, i.e., $I = (r)$ for some $r \in \mathbb{Z}[\sqrt{-5}]$. Then

$$2 = rs \text{ for some } s, \text{ so } Nr \mid N2 = 4,$$

and

$$1 + \sqrt{-5} = rs' \text{ for some } s', \text{ so } Nr \mid N(1 + \sqrt{-5} = 6.$$

Thus $Nr \mid 2$. But the condition $Nr = 2$ is impossible. And the condition $Nr = 1$ forces $I = \mathbb{Z}[\sqrt{-5}]$, which is false. (Any element of I is $r = 2s + (1 + \sqrt{-5})t$ where $s, t \in \mathbb{Z}[\sqrt{-5}]$, and a little algebra shows that $r = a + b\sqrt{-5}$ where a and b have the same parity. Thus $r \neq 1$, i.e., $1 \notin I$, and so the ideal is not the full ring.) In conclusion, I can not be a principal ideal.

Definition 6.3. *An integral domain in which every ideal is principal is called a* **principal ideal domain**.

Principal ideal domain is usually abbreviated to *PID*.

7. Euclidean $\implies$ PID

Proposition 7.1. *Every Euclidean domain is a PID.*

Proof. Let R be a Euclidean domain. Let I be a nonzero ideal in R. Let $b \in I$ be an element of least norm. Note that $b \neq 0$. Since R is Euclidean, we have for any $a \in I$ some $q, r \in R$ such that

$$a = qb + r, \quad r = 0 \text{ or } Nr < Nb.$$

Since I is an ideal and $a, b \in I$, also $r \in I$, making the condition $Nr < Nb$ impossible. Thus $r = 0$, and so $a = qb$. That is, every element of I is a multiple of b and hence $I = (b)$. □

As an application of the proposition, consider a PID R. For any $x, y \in R$ the ideal (x, y) takes the form $(x, y) = (z)$ for some $z \in R$. The ideal-generator z is a common divisor of x and y. Also, z is a linear combination of x and y,

$$z = ax + by \quad \text{for some } a, b \in R.$$

The display shows that any common divisor w of x and y divides z. Thus z is the *greatest* common divisor of x and y. That is, the greatest common divisor of x and y is a linear combination of x and y that generates the ideal (x, y). In symbols, $(x, y) = (\gcd(x, y))$. For this reason, the greatest common divisor $\gcd(x, y)$ is usually written (x, y) without the *gcd*; the collision of (x, y) as gcd-notation and as ideal-notation is a nonissue because the gcd and the ideal are essentially the same thing. We saw this earlier with our calculations that $(2, 3) = (1)$, $(2, 4) = (2)$, and $(4, 6) = (2)$ in $\mathbb{Z}$.

Continuing with the ideas of the previous paragraph, we compute a gcd by finding an ideal-generator,

$$\begin{aligned}(826, 1890) &= (826, 1890 - 2 \cdot 826)\\ &= (238, 826) = (238, 826 - 3 \cdot 238)\\ &= (112, 238) = (112, 238 - 2 \cdot 112)\\ &= (14, 112) = (14, 112 - 8 \cdot 14)\\ &= (0, 14) = (14).\end{aligned}$$

Thus $\gcd(826, 1890) = 14$. (The process just demonstrated is the venerable *Euclidean algorithm*). And furthermore, we can backtrack to express the gcd as a linear combination of the two given numbers,

$$\begin{aligned}14 &= 238 - 2 \cdot 112\\ &= 238 - 2 \cdot (826 - 3 \cdot 238)\\ &= 7 \cdot 238 - 2 \cdot 826\\ &= 7 \cdot (1890 - 2 \cdot 826) - 2 \cdot 826\\ &= -16 \cdot 826 + 7 \cdot 1890.\end{aligned}$$

This process shows that we know how to solve any equation of the form

$$ax + by = c,$$

where $a, b, c \in \mathbb{Z}$ are the given coefficients and we seek integer solutions (x, y). Solutions exist if and only if $\gcd(a, b) \mid c$, in which case we can find one particular solution via the Euclidean algorithm, as above. All other solutions differ from the particular solution by solutions to the homogenized equation $ax + by = 0$, which is easy to solve: after dividing a and b by their gcd we get $a'x + b'y = 0$ where $\gcd(a', b') = 1$, and so the solutions are $(x, y) = n(b', -a')$ for all $n \in \mathbb{Z}$.

8. PID $\implies$ (Irreducible $\implies$ Prime)

Proposition 8.1. *Let R be a PID. Then every irreducible element of R is prime.*

Proof. Let $r \in R$ be irreducible. Suppose that $r \mid ss'$ and $r \nmid s$. We need to show that $r \mid s'$.

Since r is irreducible and $r \nmid s$, in fact $(r, s) = (1)$. Thus there exist $a, b \in R$ such that $ar + bs = 1$.

Consequently $ars' + bss' = s'$. But $r \mid ars' + bss'$, and hence $r \mid s'$ as desired. $\square$

9. PID $\implies$ Noetherian

Definition 9.1. *A ring R is* **Noetherian** *if any ascending chain of ideals in R,*

$$I_1 \subset I_2 \subset I_3 \subset \cdots,$$

eventually stabilizes, meaning that the I_n are equal for all n after some starting index N.

Proposition 9.2. *Let R be a PID. Then R is Noetherian.*

Proof. Given an ascending chain of ideals in R,

$$I_1 \subset I_2 \subset I_3 \subset \cdots,$$

let

$$I = \bigcup_{n=1}^{\infty} I_n.$$

Then I is an ideal of R (exercise). Since R is a PID, in fact $I = (r)$ for some $r \in R$. Since $r \in I$, in fact $r \in I_N$ for some N. Thus $I = (r) \subset I_N \subset I$, so that $I_N = I$. Consequently $I_n = I$ for all $n \geq N$. □

10. (Noetherian and (Irreducible $\implies$ Prime)) $\implies$ UFD

Definition 10.1. *An integral domain in which unique factorization holds is called a* **unique factorization domain***, or* **UFD***.*

Proposition 10.2. *Let R be a Noetherian integral domain in which all irreducible elements are prime. Then R is a UFD.*

Proof. Let r be a nonzero element of R. The Noetherian property of R gives a factorization of r into finitely many irreducibles, since otherwise we could create a a nonstabilizing chain of ideals,

$$(r) \subset (r/r_1) \subset (r/(r_1 r_2)) \subset (r/(r_1 r_2 r_3)) \subset \cdots.$$

The fact that irreducibles are prime makes the factorization unique, since if

$$r = u p_1^{e_1} \cdots p_s^{e_s} = v q_1^{f_1} \cdots q_t^{f_t}$$

where u, v are units, and all p_i and q_j are irreducible, then

$$p_1 \mid q_1^{f_1} \cdots q_s^{f_s}$$

so that since p_1 is prime we have (after reindexing if necessary)

$$p_1 \mid q_1$$

and thus, after multiplying q_1 by a unit if necessary, $p_1 = q_1$. Repeat the argument from here starting from

$$r/p_1 = u p_1^{e_1 - 1} \cdots p_s^{e_s} = v q_1^{f_1 - 1} \cdots q_t^{f_t}.$$

By induction on $\sum e_i$ we have $s \leq t$ and $e_i \leq f_i$ for $i = 1, \cdots, s$. But by symmetry we also have $t \leq s$ and $f_i \leq e_i$ for $i = 1, \cdots, t$. Thus the factorization is unique. □

11. Summary

We have shown that

$$\boxed{\text{Euclidean} \implies \text{PID} \implies \left\{\begin{array}{l}\text{irreducible} \implies \text{prime}\\ \text{Noetherian}\end{array}\right\} \implies \text{UFD.}}$$

And our rings $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$, and $k[X]$ are all Euclidean, so they are UFDs.

This all may seem pointlessly Byzantine, but the issues here are already live in utterly elementary contexts. For example:

- Math 112 exercises have to dance around the question

  For what positive integers n is $\mathbb{Z}/n\mathbb{Z}$ a field?

  Everybody knows morally that the answer is *For prime n*. However, the problem is that for any $n \in \mathbb{Z}^+$ it is easy to show that

  $$n \text{ is prime} \implies \mathbb{Z}/n\mathbb{Z} \text{ is a field} \implies n \text{ is irreducible.}$$

  But to show that $\mathbb{Z}/n\mathbb{Z}$ is a field only if n is prime requires the subtle fact that irreducibles are prime in $\mathbb{Z}$.
- Similarly, any argument that there is no square root of 2 in $\mathbb{Q}$ tacitly makes use of unique factorization. Ultimately the argument boils down to

  Let $r \in \mathbb{Q}$ satisfy $r^2 = 2$. Then $r = 2^e r'$ where $e \in \mathbb{Z}$ and $r' \in \mathbb{Q}$ has no 2's in its numerator or its denominator. Thus $2 = r^2 = 2^{2e}(r')^2$. But this is impossible because there are no 2's in $(r')^2$ and so the left side has one power of 2 while the right side has an even number of 2's.

  The problem with the argument is that without unique factorization, a number with one power of 2 conceivably could equal a number with an even number of 2's.