MATH 361: NUMBER THEORY — SECOND LECTURE

As a complementary ordering of the ideas in chapter 1 of the Ireland and Rosen text, we discuss unique factorization in a general principal ideal domain, after noting that the rings $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ (where ω is a complex cube root of 1), and $k[X]$ (the ring of formal polynomials over some field) are all PIDs.

Contents

1. Introduction

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

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

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

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 cognoscenti. 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

$$\begin{aligned} &r + s = s + r && (+ \textit{ is commutative}) \\ &(r + s) + t = r + (s + t) && (+ \textit{ is associative}) \\ &r \cdot s = s \cdot r && (\cdot \textit{ is commutative}) \\ &(r \cdot s) \cdot t = r \cdot (s \cdot t) && (\cdot \textit{ is associative}) \\ &r \cdot (s + t) = r \cdot s + r \cdot t && (\textit{the distributive law holds}) \end{aligned}$$

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

$$\begin{aligned} &r + 0 = r && (0 \textit{ is an additive identity}) \\ &r + s = 0 \quad \textit{for some } s \in R && (\textit{additive inverses exist}) \\ &r \cdot 1 = r && (1 \textit{ is a multiplicative identity}). \end{aligned}$$

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* **unit group** *is the algebraic structure*

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

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

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

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

The unit 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:*

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

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:

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

Note that we cannot prove the cancellation law by multiplying through by a^{-1}, because 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 an integral domain. 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:*

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

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

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

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; for example, for irreducibility the condition

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

is equivalent to the condition in the definition, again excluding $r=0$. However, it deserves brief mention that in a general commutative ring with 1, as compared to our more specific environment of an integral domain, the two definitions just given for irreducibility are not equivalent. For example, in the ring $\mathbb{Z}/6\mathbb{Z}$ the factorization $2 = 2 \cdot 4$ shows that 2 does not satisfy the first definition, but 2 does satisfy the second.

4. Generally, Nonzero Prime $\implies$ Irreducible

The cancellation law says that 0 is prime in any integral domain. On the other hand, 0 is not irreducible because the the definition of irreducibility excludes it. The next result says that 0 is exceptional, the only prime that fails to be irreducible.

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

Proof. Let R be an integral domain and let $R^\times$ be its unit group. Consider any nonzero prime r of R. If $r = ss'$ then certainly $r \mid ss'$ and so without loss of generality $r \mid s$. Thus $r = ss' = rts'$ for some t. Because $r \neq 0$ cancellation gives $ts' = 1$, 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. That is, the answer is *yes* for some rings R and *no* for others. For example, consider a subring of the complex number system, and its unit group,

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

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

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

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

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

with $2 \nmid 1 \pm \sqrt{-5}$ because $2(a + b\sqrt{-5}) = 2a + 2b\sqrt{-5} \neq 1 \pm \sqrt{-5}$ for $a, b \in \mathbb{Z}$.

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 $Nn = |n|$ for 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 $z = a+ib \in \mathbb{Z}[i]$. This norm is multiplicative, i.e., $N(zw) = Nz\,Nw$, because $\overline{zw} = \overline{z}\,\overline{w}$ for all $z, w \in \mathbb{C}$ and therefore $N(zw) = zw\overline{zw} = z\overline{z}w\overline{w} = Nz\,Nw$ as claimed.
- 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 $\overline{\omega} = \omega^2$; also $1 + \omega + \omega^2 = 0$, so $\omega^2 = -1 - \omega$.) This norm is multiplicative for the same reason as the previous one.
- For $R = k[X]$, take $Nf = \deg(f)$ for nonzero polynomials $f \in k[X]$. Note that the nonzero constant polynomials have norm 0. This norm is additive rather than multiplicative. Instead we could take $Nf = 2^{\deg(f)}$ to get a multiplicative norm with the nonzero constant polynomials having norm 1, and extend to $N0 = 0$ (apparently the norm of 0 was somehow $-\infty$ a moment ago), or we could take $Nf = a^{\deg(f)}$ for any integer $a > 1$ instead of $a = 2$.

(Warning: Ireland and Rosen are a little casual on pages 12–13. They extend the norms here to $\mathbb{Q}[i]$ and $\mathbb{Q}[\omega]$ in sections 1.4.1 and 1.4.2. In 1.4.1 they have $\lambda \in \mathbb{Q}[i]$ but then $\alpha, \gamma \in \mathbb{Z}[i]$. In 1.4.2 they define $\lambda \in \mathbb{Z}[\omega]$ but then use it in $\mathbb{Q}[\omega]$.)

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 $Nb = |b|$ 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 $r, s \in \mathbb{Q}$. (Here we are tacitly using the fact that $\mathbb{Z}(i) = \mathbb{Q}(i) = \mathbb{Q}[i]$.) 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. (See figure 1.) It follows that $N(a/b - q) \leq 1/2 < 1$, and so because the norm (extended to $\mathbb{Q}[i]$) is multiplicative, $N(a - qb) < Nb$. Alternatively, to work only in $\mathbb{Z}[i]$, one can argue that given $a, b \in \mathbb{Z}[i]$ with $b \neq 0$, some translate $r = a - qb$ lies in the square having side-midpoints $\pm b/2$ and $\pm ib/2$. (See figure 2.) The points of the square having maximal norm are the corners, of norm $Nb/2$.
- The verification that $\mathbb{Z}[\omega]$ is Euclidean is very similar. This time we have a hexagon about 0 (see figure 3), and any point in the hexagon has norm at most $1/3$, hence strictly less than 1. Again if we want to work only in $\mathbb{Z}[\omega]$ rather than carry out any division, the hexagonal lattice and the gray hexagon are scaled by b. (See figure 4.)
- The verification that the $k[X]$-norm makes $k[X]$ Euclidean is a matter of polynomial long division. Specifically, given $f, g \in k[X]$ with $g \neq 0$, proceed as follows.

```
○ (Initialize)
  Set $q = 0$ and $r = f$. (So $f = qg + r$.) Let $g = b_m x^m + \cdots$.
○ (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 $\deg r < \deg g$.)
```

Similarly to $\mathbb{Z}[i]$ one can show that $\mathbb{Z}[i\sqrt{2}]$ is Euclidean, using a box that is no longer a square, and similarly to $\mathbb{Z}[\omega]$ one can show that $\mathbb{Z}[(-1 + i\sqrt{7})/2]$ and $\mathbb{Z}[(-1 + i\sqrt{11})/2]$ are Euclidean, using hexagons that are no longer regular.

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. One explanation is that a ring is sort of like a vector space over itself in that pairs of elements can be added and any element can be multiplied by the ring elements; from this point of view an ideal is analogous to a subspace. A second explanation 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; that said, we do not discuss quotient structures here. A third explanation is that the next example shows that some

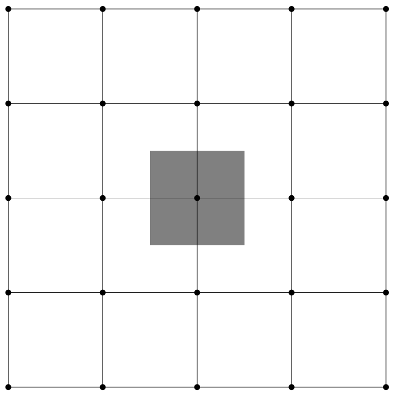

FIGURE 1. $a/b - q$ lies in the gray for some $q \in \mathbb{Z}[i]$; the lattice is $\mathbb{Z}[i]$

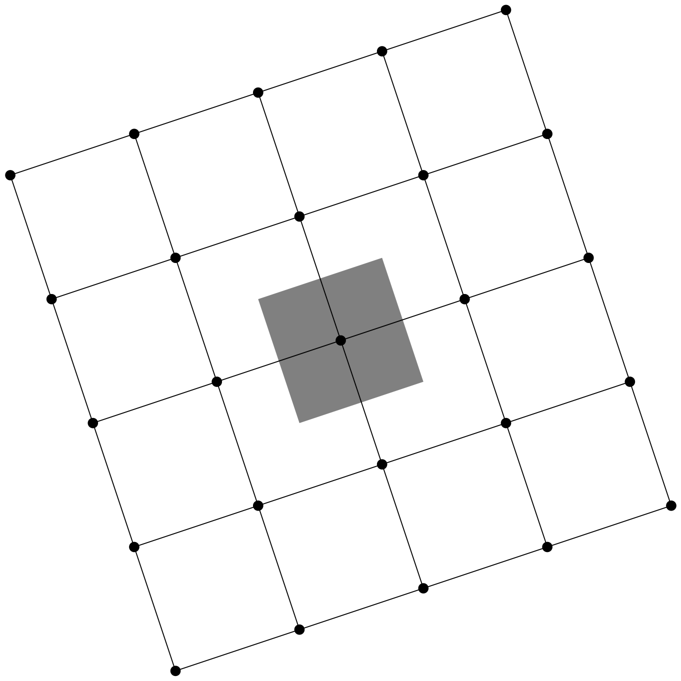

FIGURE 2. $a - qb$ lies in the gray for some $q \in \mathbb{Z}[i]$; the lattice is $b\mathbb{Z}[i]$

ideals can be viewed as essentially being elements but other ideals are needed as well. Indeed, ideals are so named because they were conceived as *ideal numbers*, numbers that we wish were present even when they aren't.

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,

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

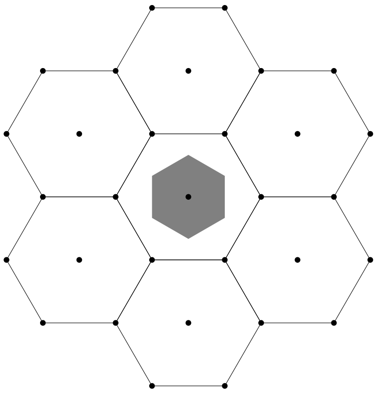

FIGURE 3. $a/b - q$ lies in the gray for some $q \in \mathbb{Z}[\omega]$; the lattice is $\mathbb{Z}[\omega]$

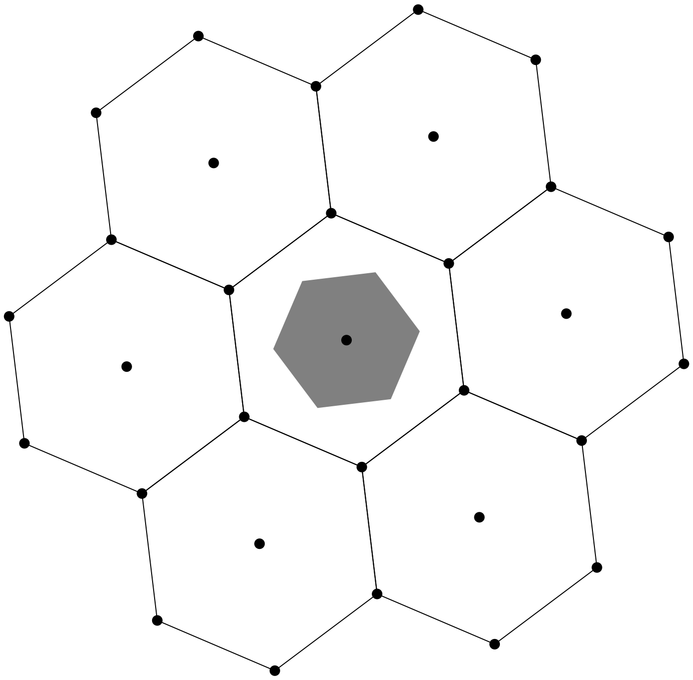

FIGURE 4. $a - qb$ lies in the gray for some $q \in \mathbb{Z}[\omega]$; the lattice is $b\mathbb{Z}[\omega]$

For instance, $(2) = \{0, \pm 2, \pm 4, \dots\}$ 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, $(2, 3) = \{-1 \cdot 2 + 1 \cdot 3, \dots\} = \{1, \dots\} = \mathbb{Z}$ 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 $r \in R$.*

(Note: princi**PAL**. An easy mistake is to misspell it "principle ideal.") So far, all of the ideals that we have seen are principal. For an example of a nonprincipal ideal, let $R = \mathbb{Z}[\sqrt{-5}]$ and let

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

Using the norm function $N(a+b\sqrt{-5}) = a^2+5b^2$ (which takes products to products but which we do not claim has the Euclidean property), 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 $\Longrightarrow$ 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 $b \neq 0$. Because R is Euclidean, we have for any $a \in I$ some $q, r \in R$ such that

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

Because 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,

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

Better than backtracking this way, we can maintain a little more information through the forward Euclidean algorithm in order to have the linear combination coefficients at hand as well when it terminates. The method to do so is laid out in the first problem set for this course. The Euclidean algorithm 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 algorithm. 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 $\Longrightarrow$ (Irreducible $\Longrightarrow$ 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 $r \mid s'$. Because 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. □

9. PID $\Longrightarrow$ 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). Because R is a PID, in fact $I = (r)$ for some $r \in R$. Because $r \in I$, 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. $\big((\text{Irreducible} \implies \text{Prime}) \text{ and Noetherian}\big) \implies \text{UFD}$

Definition 10.1. *An integral domain in which every nonzero element factors as a product of finitely many irreducible elements, with the irreducible elements determined uniquely up to units, 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, because otherwise we could create a a nonstabilizing chain of ideals,

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

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

$$r = p_1 \cdots p_s = v q_1 \cdots q_t$$

where v is a unit, and all p_i and q_j are irreducible, and without loss of generality $s \leq t$, then

$$p_s \mid q_1 \cdots q_t,$$

so that because p_s is prime we have (after reindexing if necessary)

$$p_s \mid q_t$$

and thus, because q_t is irreducible, in fact $p_s = q_t$ after multiplying q_t by a unit if necessary. Cancel the common irreducible from both sides to get

$$p_1 \cdots p_{s-1} = v q_1 \cdots q_{t-1}.$$

By induction on s, these factorizations agree—the base case is that $1 = v q_1 \cdots q_t$ forces $t = 0$ and then $v = 1$—and we are done. □

11. Summary

We have shown that for integral domains,

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

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

This all may seem pointlessly Byzantine, but the issues here are already live in 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 while this isn't hard to show for our revised notion of *prime*, showing that the answer is what we would phrase *For irreducible n* raises the issue of whether *prime* and *irreducible* mean the same thing. For any $n \in \mathbb{Z}^+$ it is easy to show that

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

But to show that if n is irreducible then $\mathbb{Z}/n\mathbb{Z}$ is a field requires the nontrivial fact that irreducibles are prime in $\mathbb{Z}$.

- Similarly, a standard argument that there is no square root of 2 in $\mathbb{Q}$ tacitly makes at least partial use of unique factorization. The argument is some version of:

  > *Let $r \in \mathbb{Q}$ satisfy $r^2 = 2$. Because r is a nonzero rational number, it takes the form $r = 2^e r'$ where $e \in \mathbb{Z}$ and $r' \in \mathbb{Q}$ is nonzero with 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.*

  This argument assumes that the power of 2 dividing a nonzero integer is unique. This uniqueness is easier to show than full blown unique factorization, but it does need to be shown to make the argument valid.