13 More Factorization

13.1 Factoring Integer Polynomials

We've seen that $\mathbb{Z}$, $F[x]$, and $\mathbb{Z}[i]$ are unique factorization domains — in fact, we'll later look into a neat application of unique factorization in $\mathbb{Z}[i]$ to a problem in number theory. First we'll discuss factorization in $\mathbb{Z}[x]$. We previously stated the following theorem:

Theorem 13.1
If R is a unique factorization domain, then $R[x]$ is also a unique factorization domain.

We'll prove this for the case $R = \mathbb{Z}$. The proof of the general case is very similar to the proof for $\mathbb{Z}$ — we essentially just have to replace the familiar construction of the gcd over integers with the more abstract notion of gcd in a general UFD, as discussed last time.

Guiding Question
Given a polynomial $P \in \mathbb{Z}[x]$, there's two natural questions we can ask about its factorization:

1. Is it possible to factor P where the factors lie in $\mathbb{Q}[x]$?
2. What about in $\mathbb{Z}[x]$?

There are more tools available for approaching the second question, factoring in $\mathbb{Z}[x]$, which make it possible to reduce the potential factorizations to a finite number of possibilities. One such tool is reducing mod a prime p.

Example 13.2
Consider the polynomial $P(x) = 3x^2 + 2x + 2$. We can show it's impossible to factor P in $\mathbb{Z}[x]$ by reducing mod 2 — we have

$$P(x) \equiv x^3 \pmod{2}.$$

But the only way x^3 factors in $\mathbb{F}_2[x]$ is as $x^3 \cdot 1$ or $x^2 \cdot x$. If P factored as P_1P_2 where P_1 and P_2 had positive degree, then since their leading coefficients must be odd (as these leading coefficients multiply to 3), they must still have positive degree in $\mathbb{F}_2[x]$. So P_1 and P_2 must be congruent to x and x^2 mod 2; in particular, both their free terms are divisible by 2. But the free term of P would then be divisible by 4, which is a contradiction.

This example illustrates one possible trick that can be used to show that a polynomial is irreducible in $\mathbb{Z}[x]$. There are various other tricks as well. For example, the product of the free terms of the factors must equal the free term of the original polynomial; so we can look at all possible factorizations of the free term. On the other hand, factoring polynomials in $\mathbb{Q}[x]$ seems much more difficult, since these tricks no longer work — there's infinitely many ways to factor the free term of the original polynomial as a product of *rationals*, so this argument can't be used to reduce our search to finitely many possibilities.

Fortunately, it turns out that factoring over $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are actually equivalent. To show this, recall the definition of a primitive polynomial from last class, here applied specifically to $\mathbb{Z}[x]$:

Definition 13.3
A polynomial $P \in \mathbb{Z}[x]$ is **primitive** if the gcd of all its coefficients is 1.

Evidently, any nonzero $P \in \mathbb{Z}[x]$ can be written as a product $P = nQ$, where Q is primitive and n is the gcd of the coefficients of P. In fact, any $P \in \mathbb{Q}[x]$ can be scaled to a primitive polynomial, by clearing denominators and factoring out the gcd of its coefficients.

The key point in relating factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ is Gauss's Lemma, which we proved last class:

Lemma 13.4 (Gauss's Lemma)
If P and Q are primitive, then PQ is as well.

Proof Sketch. If PQ is not primitive, then there is some prime p which divides all coefficients of PQ. Now consider P and Q mod p; since both are nonzero mod p, it's clear that their product is nonzero mod p as well — the integers mod p are a field, and for polynomials over a field, it's impossible to multiply two nonzero polynomials and get the zero polynomial. □

Using Gauss's Lemma, we can reduce questions about divisibility in $\mathbb{Z}[x]$ to ones about divisibility in $\mathbb{Q}[x]$, via the following corollary:

Corollary 13.5

If $P, Q \in \mathbb{Z}[x]$ are such that P divides Q in $\mathbb{Q}[x]$ and P is primitive, then P divides Q in $\mathbb{Z}[x]$.

Proof. We have $Q = P \cdot S$ for some $S \in \mathbb{Q}[x]$. Now write $S = aT/b$ where $T \in ZZ[x]$ is primitive, and a and b are integers with $b \neq 0$. Then the equation can be rewritten as

$$bQ = aPT.$$

By Gauss's Lemma, PT is primitive, so the gcd of all coefficients of aPT is exactly a. Meanwhile, b certainly divides all coefficients of bQ, so it divides all coefficients of aPT as well, which means $b \mid a$. As a result, $a/b \in \mathbb{Z}$, so $S \in \mathbb{Z}[x]$ and P divides Q in $\mathbb{Z}[x]$ as well. □

Note 13.6

There's a different way to phrase this proof — for polynomials $P \in \mathbb{Z}[x]$, we can define the **content** of P, denoted $c(P)$, as the gcd of the coefficients of P. It's possible to extend this to polynomials in $\mathbb{Q}[x]$ as well, such that for any $T \in \mathbb{Q}[x]$ and $a \in \mathbb{Q}$, we have $c(aT) = a \cdot c(T)$. Then Gauss's Lemma states that $c(PQ) = c(P)c(Q)$ for any $P, Q \in \mathbb{Z}[x]$, and therefore for any $P, Q \in \mathbb{Q}[x]$ as well. Now in this proof we have $Q = PS$, which means $c(Q) = c(P)c(S)$. But $c(Q)$ is an integer and $c(P) = 1$, so $c(S)$ must be an integer as well; therefore S has integer coefficients.

As a result, factoring in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are in fact equivalent.

Example 13.7

The polynomial $3x^2 + 2x + 2$ is irreducible in $\mathbb{Z}[x]$, so it cannot be factored in $\mathbb{Q}[x]$ either.

Corollary 13.8

The irreducible elements in $\mathbb{Z}[x]$ fall into two categories: $\pm p$ for prime integers p, and primitive polynomials which are irreducible in $\mathbb{Q}[x]$.

It's not necessarily easy to tell whether a polynomial is irreducible; but this does mean that answering the question of whether a polynomial is irreducible in $\mathbb{Q}[x]$ is as easy as answering it in $\mathbb{Z}[x]$.

Proof. It's clear that both categories of elements are irreducible — the primes are clearly irreducible in $\mathbb{Z}[x]$, since the only way to factor a constant polynomial is as a product of constants. Meanwhile, if a polynomial is irreducible in $\mathbb{Q}[x]$, then the only way it can be factored is by pulling out constant factors; but this is impossible for a primitive polynomial, so all such polynomials must be irreducible in $\mathbb{Z}[x]$ as well.

On the other hand, if P is not of either form, then we'll show that P can be factored and therefore is not irreducible. First, if $\deg(P) = 0$ (meaning P is an integer), then it's clear that it must be prime in order to be irreducible.

Now assume that $\deg(P) \geq 1$. If P is not primitive, then we can pull out the greatest common divisor of its coefficients. Meanwhile, if P is primitive but factors in $\mathbb{Q}[x]$, then $P = Q_1Q_2$. We can rescale Q_1 by taking integers a and b such that aQ_1/b is in $\mathbb{Z}[x]$ and primitive. Then by Lemma 13.5, aQ_1/b must divide P in $\mathbb{Z}[x]$ as well, giving a nontrivial factorization of P. □

Theorem 13.1 for $\mathbb{Z}$ follows as a corollary.

Corollary 13.9
The polynomials with integer coefficients, $\mathbb{Z}[x]$, form a unique factorization domain.

Proof. As usual, we need to prove that a factorization *exists* and is *unique*.

We'll first prove existence. First, by factoring out constants we can write $P = p_1 \cdots p_\ell P_1$ such that P_1 is primitive and the p_i are primes. If P_1 is irreducible in $\mathbb{Q}[x]$, we are done, as it is also irreducible in $\mathbb{Z}[x]$. Otherwise, P_1 factors in $\mathbb{Q}[x]$, and we can rescale both factors so that they are primitive elements of $ZZ[x]$, so then P_1 factors in $\mathbb{Z}[x]$. We can continue to attempt to factor the two resulting factors of P_1. As we keep on factoring, the degrees of our polynomials decrease at every step, so the factorization process must terminate — which means that eventually, all our polynomials become irreducible.

Now we'll prove uniqueness. As in all the other cases where we proved uniqueness, it is enough to show that if an irreducible polynomial $P \in \mathbb{Z}[x]$ divides Q_1Q_2, then P divides either Q_1 or Q_2. (Then similarly to in the proof that every PID is a UFD, given two factorizations $P_1 \cdots P_n$ and $Q_1 \cdots Q_m$, we can show that P_1 must appear in the second factorization as well, cancel it out from both, and repeat with the remaining factorizations until we've matched up all the factors.)

In order to show this result, we have two cases. First, if P is an integer prime $p \in \mathbb{Z}$, then this follows directly from the fact that the product of two nonzero polynomials in $(\mathbb{Z}/p\mathbb{Z})[x]$ is nonzero, as $\mathbb{Z}/p\mathbb{Z}$ is a field.

Otherwise, P is primitive and irreducible in $\mathbb{Q}[x]$. We have that if $P \mid Q_1Q_2$, then $P \mid Q_1$ or $P \mid Q_2$ in $\mathbb{Q}[x]$ (since $\mathbb{Q}$ is a field, so $\mathbb{Q}[x]$ is a PID and therefore a UFD). By Lemma 13.5, since P is primitive, then P must divide Q_1 or Q_2 in $\mathbb{Z}[x]$.

So this shows that for any irreducible $P \in \mathbb{Z}[x]$, if $P \mid Q_1Q_2$ then $P \mid Q_1$ or $P \mid Q_2$, as desired. □

As mentioned earlier, the same proof used to show that $\mathbb{Z}[x]$ is a UFD would work if we replaced $\mathbb{Z}$ with *any* UFD R. For example, we can even take R to be $\mathbb{Z}[x]$, now that we know it's a UFD; this shows that $\mathbb{Z}[x, y]$ is also a UFD.

13.2 Gaussian Primes

Unique factorization in $\mathbb{Z}[i]$ has an interesting application — it can be used to solve a problem in number theory.

Guiding Question
Which integers can be written as $n = a^2 + b^2$ for integers a and b?

Example 13.10
We can write $5 = 2^2 + 1^2$, while 6 and 21 cannot be written as a sum of squares.

On the way to proving the answer, we'll classify irreducible elements in $\mathbb{Z}[i]$. (Since $\mathbb{Z}[i]$ is a UFD, the irreducible elements are exactly the primes, so we will use "prime" and "irreducible" interchangeably here.) This is an example of how the abstract property of unique factorization can lead to concrete results.

First, note that $n = a^2 + b^2$ can be rewritten as $n = (a + bi)(a - bi)$. This makes it clear that if n and m can be written in the form $a^2 + b^2$, then so can mn — if $n = \alpha\overline{\alpha}$ and $m = \beta\overline{\beta}$, then $(\alpha\beta)(\overline{\alpha\beta})$. So the property is multiplicative, which motivates considering the special case where n is prime.

Lemma 13.11
Let $p \in \mathbb{Z}$ be a prime number. Then $p = a^2 + b^2$ if and only if p is *not* a prime in $\mathbb{Z}[i]$.

We refer to primes in $\mathbb{Z}[i]$ as **Gaussian primes**.

Proof. First, if p were a Gaussian prime and we could write p as a sum of squares, then we would have

$$p = (a + bi)(a - bi),$$

which would mean p must divide either $a + bi$ or $a - bi$. In either case, p would need to divide both a and b, which is impossible.

Meanwhile, if p is not a Gaussian prime, since it's real and doesn't factor in $\mathbb{Z}$, it must factor as $p = \alpha\overline{\alpha}$ for some $\alpha \in \mathbb{Z}[i]$ which is not in $\mathbb{Z}$. So then $\alpha = a + bi$ for some integers a and b, which means $p = a^2 + b^2$. □

So answering our initial question for primes is equivalent to figuring out which integer primes are also Gaussian primes.

Lemma 13.12

Let $p \in \mathbb{Z}$ be a prime number. Then p is *not* prime in $\mathbb{Z}[i]$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

Proof. First, 2 factors as $2 = (1 + i)(1 - i)$. Now suppose $p > 2$.

Claim. *p is not a prime in $\mathbb{Z}[i]$ if and only if there exists $\alpha \in \mathbb{Z}[i]$ such that $p \nmid \alpha$, but $p \mid \alpha\overline{\alpha}$.*

Proof. By definition, p is not a prime in $\mathbb{Z}[i]$ if and only if there exist α and β such that p divides $\alpha\beta$, but not α or β. It immediately follows that if there exists an $\alpha \in \mathbb{Z}[i]$ with the described properties, then p is not prime. On the other hand, if p is not prime, then take α and β such that neither is divisible by p but $\alpha\beta$ is; then

$$p \mid \alpha\beta\overline{\alpha\beta} = (\alpha\overline{\alpha})(\beta\overline{\beta}).$$

Since p is an integer prime, and both $\alpha\overline{\alpha}$ and $\beta\overline{\beta}$ are integers, then p must divide one of them, and either α or β has the described properties. □

This turns the question into one over $\mathbb{F}_p$ — then p is not a prime in $\mathbb{Z}[i]$ if and only if there exist $a, b \in \mathbb{F}_p$, which are not both 0, such that

$$a^2 + b^2 = 0.$$

Since $\mathbb{F}_p$ is a field, we can divide by b^2 and rewrite the equation as $-1 = (ab^{-1})^2$, so this is true if and only if -1 is a square in $\mathbb{F}_p$.

Now consider the abelian group $\mathbb{F}_p^\times$ (the multiplicative group of $\mathbb{F}_p$) which has order $p - 1$. The only element of order 2 is -1, since

$$x^2 - 1 = (x - 1)(x + 1)$$

has no roots other than ± 1, and 1 has order 1. This gives a homomorphism $\varphi : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ sending $\alpha \to \alpha^2$. Then $\ker(\varphi) = \{\pm 1\}$, so by the homomorphism theorem, $\operatorname{im}(\varphi)$ has $(p - 1)/2$ elements.

But -1 is a square in $\mathbb{F}_p$ if and only if it is in the image of φ. Since $\operatorname{im}(\varphi)$ is a subgroup of $\mathbb{F}_p^\times$, this occurs if and only if $\operatorname{im}(\varphi)$ contains an element of order 2 (since the only possible element of order 2 is -1).

But $\operatorname{im}(\varphi)$ contains an element of order 2 if and only if $|\operatorname{im}(\varphi)| = (p - 1)/2$ is divisible by 2 — one direction follows from the fact that the order of every element divides the order of the group, and the other follows from the Sylow Theorems. So -1 is a square if and only if $(p - 1)/2$ is even, or equivalently $p \equiv 1 \pmod 4$.

So an odd integer prime p is *not* a Gaussian prime if and only if $p \equiv 1 \pmod 4$. □

This proof can be used to classify the Gaussian primes up to association (multiplying by units, here ± 1 and $\pm i$).

Theorem 13.13

The full list of primes in $\mathbb{Z}[i]$, up to association, can be constructed as follows: consider all integer primes p.

- If $p \equiv 3 \pmod 4$, then p itself is a Gaussian prime.
- If $p \equiv 1 \pmod 4$, then it factors as $(a - bi)(a + bi)$, and both factors $a \pm bi$ are Gaussian primes.
- If $p = 2$, then it factors as $(1 + i)(1 - i)$, and since $1 + i$ and $1 - i$ are associate, they correspond to the same Gaussian prime.

Resource: Algebra II Student Notes
Spring 2022
Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng