1. Units, Associates, and Primes $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$

In Chapter 8, we return to the theme of proving Fermat's Last Theorem. A crucial part of proving FLT for exponent 3 is understanding how factoring works in $\mathbb{Z}[\omega]$, the set of Eisenstein integers. And a fatal mistake in many attempts to prove FLT for higher exponents was to assume that factoring works in more general rings of cyclotomic integers the same way that it does in $\mathbb{Z}$ and $\mathbb{Z}[\omega]$. To be more precise we need to define what it means to be "prime" in $\mathbb{Z}[\omega]$, and to do that we need to introduce some preliminary terminology.

Recall that the Gaussian integers are

$$\mathbb{Z}[i] \;=\; \{a+bi \mid a,b \in \mathbb{Z}\} \;\subset\; \mathbb{C}\,,$$

and the Eisenstein integers are

$$\mathbb{Z}[\omega] \;=\; \{a+b\omega \mid a,b \in \mathbb{Z}\} \;\subset\; \mathbb{C}\,,$$

where $\omega = e^{2i\pi/3} = \frac{1}{2}(-1+i\sqrt{3})$. Both these sets are closed under addition and multiplication and satisfy the first eight of the "fundamental properties" discussed in Section 1.4. (This is essentially what is meant by saying that $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ are "commutative rings.")

The ninth property, existence of multiplicative inverses for nonzero elements, fails (as it does for $\mathbb{Z}$ and $\mathbb{Z}/m$ also). But we may consider the *units* in $\mathbb{Z}[i]$ (or in $\mathbb{Z}[\omega]$) which are the elements for which a multiplicative inverse does exist.

Definition. To say that an element u in $\mathbb{Z}[i]$ is a **unit** in $\mathbb{Z}[i]$ means that there exists an element $v \in \mathbb{Z}[i]$ such that $uv = 1$.

Read Propositions 4.41 and 4.42 (and their proofs) on pages 162-163.

We define units in $\mathbb{Z}[\omega]$ similarly; a unit is an element of $\mathbb{Z}[\omega]$ that has a multiplicative inverse in $\mathbb{Z}[\omega]$.

A related concept to that of a unit is an *associate*.

Definition. To say that an element z of $\mathbb{Z}[i]$ is an **associate** of another element w of $\mathbb{Z}[i]$ means that there is a unit $u \in \mathbb{Z}[i]$ such that $z = uw$.

In fact, if z is an associate of w if and only if w is an associate of z. (This is a small exercise!) So in this case we may say that z and w "are associates."

We define the notion of an associate of an element in $\mathbb{Z}[\omega]$ analogously.

The final preliminary definition we need is that of *divides*.

Definition. To say that an element z of $\mathbb{Z}[i]$ **divides** an element w of $\mathbb{Z}[i]$ (written $z|w$) means that there is an element w' in $\mathbb{Z}[i]$ such that $zw' = w$. In this case, z is called a **divisor** of w, and w is called a **multiple** of z.

We define the term "divides" in $\mathbb{Z}[\omega]$ analogously.

Now we may finally define prime elements of $\mathbb{Z}[i]$.

Definition. To say that an element π of $\mathbb{Z}[i]$ is **prime** (or **irreducible**) means

- $\pi \neq 0$,
- π is not a unit in $\mathbb{Z}[i]$, and
- if $z|\pi$ in $\mathbb{Z}[i]$, then either z is a unit in $\mathbb{Z}[i]$ or z is an associate of π.

We may define primes in $\mathbb{Z}[\omega]$ analogously. See pages 233-234 for the definitions of "divides," "associate," and "irreducible" in a general commutative ring.

2. Polynomial Rings and Finite Fields

Chapter 8 also contains some references to notation and concepts regarding polynomial rings and finite fields.

Given that polynomials with real coefficients may be added and multiplied to obtain more polynomials with real coefficients, it is perhaps not surprising that the set of all polynomials with real coefficients, denoted $\mathbb{R}[x]$, satisfies the first eight of the "fundamental properties" from Section 1.4 and is thus another example of a commutative ring. (Note that in a polynomial ring, polynomials typically do *not* have multiplicative inverses.)

If we wish to consider only polynomials with integer coefficients, we denote this set by $\mathbb{Z}[x]$.

In general if k is a set with addition and multiplication that obeys all nine of the "fundamental properties," we say that k is a *field*. Examples of fields include $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. There are finite fields as well; for example, when p is a prime, $\mathbb{Z}/p$ is a field, since every integer not divisible by p has a multiplicative inverse mod p. Because of this, we may denote $\mathbb{Z}/p$ as $\mathbb{F}_p$, to emphasize that it is a field.

As it turns out, if k is any field, then the ring of polynomials whose coefficients are in k, denoted $k[x]$, has a very nice structure; it is known as a *principal ideal domain* (usually abbreviated PID). More on this below.

3. Abstract Structures

References to various abstract structures appear throughout Chapter 8; we do not need to know all the theory, but it may be helpful to have an idea of what the various terms mean.

As mentioned above, a set with two binary operations (addition and multiplication) that obeys the first eight "fundamental properties" in Section 1.4 is known as a **commutative ring** (or sometimes a commutative ring "with one").

Conspicuously absent from the definition of a commutative ring is the existence of multiplicative inverses for nonzero elements (the ninth "fundamental property"). However, some commutative rings (for example, $\mathbb{Z}$) enjoy a multiplicative cancellation law: for all a, b, c in the ring, if $ab = ac$ and $a \neq 0$, then $b = c$. Such commutative rings are called **domains** (or sometimes integral domains).

Notice that if m is composite, then $\mathbb{Z}/m$ does *not* enjoy the multiplicative cancellation law; consider in $\mathbb{Z}/6$

$$\overline{3} \cdot \overline{2} \;=\; \overline{3} \cdot \overline{4} \qquad \text{but} \qquad \overline{2} \neq \overline{4}\,.$$

So $\mathbb{Z}/m$ (for m composite) is an example of a commutative ring that is *not* a domain.

Domains with additional properties include: **unique factorization domains** (UFDs), in which a version of unique prime factorization holds; **principal ideal domains** (PIDs), in which a generalization of Euclid's Lemma holds; and **Euclidean domains**, in which a generalized division algorithm (and thus a generalized Euclidean algorithm) holds. Every Euclidean domain is a PID, and every PID is a UFD.

We know that $\mathbb{Z}$ is a Euclidean domain; in Chapter 8, we will see that $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ are Euclidean domains as well. More general rings of "cyclotomic integers," while they are domains, fail to have unique prime factorization. Many early "proofs" of FLT implicitly assumed that unique prime factorization would hold in these general rings.

4. Constructing Fields as Quotients of Polynomial Rings

Having roughly defined these abstract structures, we may state one important result from Ch 6-7, which plays a crucial role in the proof of FLT for exponent 3. If k is a field, then $k[x]$ is a PID, and if $p(x)$ is irreducible in $k[x]$, then $k[x]$ modulo $p(x)$, denoted $k[x]/(p)$, is a field. (This is analogous to the fact that if p is a prime, then $\mathbb{Z}/p$ is a field.)

For example, $\mathbb{R}$ is a field, so the ring of polynomials with real coefficients, denoted $\mathbb{R}[x]$ is a PID. The polynomial x^2+1 is irreducible in $\mathbb{R}[x]$. So if we look at polynomials with real coefficients "modulo (x^2+1)" we have a field. Here is an example of a computation modulo (x^2+1):

$$(2+x)^2 \;=\; 4+4x+x^2 \;=\; (3+1)+4x+x^2 \;=\; 3+4x+(x^2+1) \;\equiv\; 3+4x \mod (x^2+1)\,.$$

Here we are treating (x^2+1) like zero, since it is the modulus, so to speak. In fact, this means that we can treat x^2 as -1 (since $x^2+1 \equiv 0$.) So, if we are thinking modulo (x^2+1) we could write

$$(2+x)^2 \;=\; 4+4x+x^2 \;\equiv\; 4+4x+(-1) \;\equiv\; 3+4x \mod (x^2+1)\,.$$

Notice that this is essentially the same as:

$$(2+i)^2 \;=\; 4+4i+i^2 \;=\; 4+4i+(-1) \;=\; 3+4i\,.$$

This is no coincidence. Looking at polynomials in $\mathbb{R}[x]$ modulo (x^2+1) gives a field that is the same as the complex numbers!