ALGEBRAIC NUMBER THEORY
PART II (EXERCISES)

1. Eisenstein Integers

Exercise 1. Let

$$\omega = \frac{-1+\sqrt{-3}}{2}.$$

Verify that $\omega^2 + \omega + 1 = 0$.

Exercise 2. The set

$$\mathbb{Z}[\omega] = \{a + b\omega \colon a, b \in \mathbb{Z}\}$$

is called the **ring of Eisenstein integers**. Prove that it is a ring. That is, show that for any Eisenstein integers $a + b\omega$, $c + d\omega$ the numbers

$$(a + b\omega) + (c + d\omega), \;\; (a + b\omega) - (c + d\omega), \;\; (a + b\omega)(c + d\omega)$$

are Eisenstein integers as well.

Exercise 3. For any Eisenstein integer $a + b\omega$ define the **norm**

$$N(a + b\omega) = a^2 - ab + b^2.$$

Prove that the norm is multiplicative. That is, for any Eisenstein integers $a + b\omega$, $c + d\omega$ the equality

$$N\left((a + b\omega)(c + d\omega)\right) = N(a + b\omega)N(c + d\omega)$$

holds. Verify that the norm is non-negative: $N(a + b\omega) \geq 0$ for any a, b and $N(a + b\omega) = 0$ if and only if $a = b = 0$.

Exercise 4. We say that γ is an **Eisenstein unit** if $\gamma \mid 1$. Prove that if γ is an Eisenstein unit then its norm is equal to one.

Exercise 5. Find all Eisenstein integers of norm one (there are six of them) and show that all of them are Eisenstein units.

Exercise 6. An Eisenstein integer γ is **prime** if it is not a unit and every factorization $\gamma = \alpha\beta$ with $\alpha, \beta \in \mathbb{Z}[\omega]$ forces one of α or β to be a unit. Find Eisenstein primes among rational primes

$$2, 3, 5, 7, 11, 13.$$

2. Failure of Unique Factorization

Exercise 1. Consider the ring

$$\mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\right\}$$

along with the norm map $N(a + b\sqrt{-5}) = a^2 + 5b^2$, which is known to be multiplicative. Prove that ± 1 are the only units in $\mathbb{Z}[\sqrt{-5}]$.

Exercise 2. Prove that the numbers $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are prime in $\mathbb{Z}[\sqrt{-5}]$.

Exercise 3. Using Exercise 2 prove that the unique factorization fails in $\mathbb{Z}[\sqrt{-5}]$.

3. Rings with Infinitely Many Units

Exercise 1. Find at least one unit different from ± 1 in the rings $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{5}]$. **Hint:** the norm map is $N(a+b\sqrt{d}) = a^2 - db^2$ and it is multiplicative. Convince yourself that $N(a+b\sqrt{d}) = \pm 1$ and then find one solution to the Diophantine equation you obtained.

Exercise 2. Suppose that you have found a unit $a + b\sqrt{d}$. Prove that for any positive integer n the number $(a + b\sqrt{d})^n$ is also a unit. Prove that there are infinitely many units.