We review the algebraic structure and the geometry of complex numbers and introduce two notable subrings: the Gaussian integers and the Eisenstein integers. See Chapter 3, especially Section 3.2 and the following parts of Section 3.4: from the subsection, "Norms," pages 116-117 (up to and including Proposition 3.35), from the subsection "Gaussian Integers, Pythagorean Triples Revisited," page 119 (up to and including Proposition 3.37), and from the subsection "Eisenstein Integers," pages 120-121 (up to and including Proposition 3.38).

1. The Algebraic Structure of the Complex Numbers

Informally, the complex numbers may be presented as the set of all "numbers" of the form $x + iy$, where x and y are real numbers and i is an "imaginary" number with the property that $i^2 = -1$. (Since $0^2 = 0$ and every negative or positive real number has a positive square, it is clear that this "number," i, if it exists, cannot be a real number.)

Taking the existence of this "number" i for granted, and proceeding optimistically (namely, assuming that the rules of arithmetic for real numbers also apply to complex numbers), we may derive rules for the addition and multiplication of complex numbers:

$$(x_1 + iy_1) \ + \ (x_2 + iy_2) \ = \ (x_1 + x_2) \ + \ i(y_1 + y_2) \, ,$$

$$[(x_1 + iy_1) \ \cdot \ (x_2 + iy_2) \ = \ x_1x_2 + iy_1x_2 + ix_1y_2 + (-1)y_1y_2 \ = \ (x_1x_2 - y_1y_2) \ + \ i(x_1y_2 + y_1x_2) \, .$$

A more formal development of the complex numbers defines the set of complex numbers, $\mathbb{C}$, as the set of ordered pairs of real numbers:

$$\mathbb{C} \ = \ \{(x, y) \mid x, y \in \mathbb{R}\} \ = \ \mathbb{R}^2 \, .$$

Addition is defined component-wise (as for 2-dimensional vectors over $\mathbb{R}$), and multiplication is defined in order to match the formula above, suggested by intuition:

$$(x_1, y_1) \cdot (x_2, y_2) \ = \ (x_1x_2 - y_1y_2, \ x_1y_2 + y_1x_2) \, .$$

If we define i to be the complex number $(0, 1)$, then we can prove that $i^2 = -1$, and we can use the more intuitive notation $x + iy$ instead of (x, y). Given these definitions, it is not difficult (though somewhat tedious) to prove that $\mathbb{C}$ is a real vector space and a commutative ring. See Propositions 3.8 and 3.9 pages 93-95.

It takes a little more work to prove the field axiom: the existence of multiplicative inverses for nonzero elements. The simplest route is via the complex conjugate: for $z = x + iy \in \mathbb{C}$, we define its complex conjugate $\overline{z}$ by:

$$\overline{z} \ = \ x - iy \, .$$

See Proposition 3.10, page 96, for several useful properties of the complex conjugate. Given a nonzero complex number z, we prove that its multiplicative inverse is:

$$z^{-1} \ = \ \frac{\overline{z}}{z\overline{z}} \, .$$

Notice that the denominator is a real scalar, which is the square of the magnitude of z. See Proposition 3.11, page 96.

Thus $\mathbb{C}$ is a real vector space and a field.

2. The Geometry of the Complex Numbers

We visualize the complex numbers in a coordinate plane, where the horizontal axis is the "real axis" and the vertical axis is the "imaginary axis." A complex number $x + iy$ is located at the point (x, y). Since addition of complex numbers is defined componentwise, the same way that addition of 2-dimensional vectors over $\mathbb{R}$ is defined, we may add of complex numbers geometrically using the parallelogram law (or the head-to-tail rule); see Figure 3.2 in page 93.

The geometry of multiplication is most simply understood once the complex numbers are put in polar form. The modulus of a complex number $z = x + iy$ is its magnitude as a vector:

$$|z| \;=\; \sqrt{z\overline{z}} \;=\; \sqrt{x^2 + y^2}\,.$$

The argument of a complex number is an angle, measured counter-clockwise from the positive real axis to the ray from the origin to z. Letting r be the modulus of z and θ the argument. Then we may write z in polar form as follows:

$$z \;=\; r(\cos\theta + i\sin\theta)\,.$$

A more concise notation is exponential polar form:

$$z \;=\; re^{i\theta}\,.$$

Given two complex numbers $z_1 = r_1 e^{i\theta_1}$ and $z_2 = r_2 e^{i\theta_2}$, their product is

$$z_1 z_2 \;=\; (r_1 r_2)e^{i(\theta_1+\theta_2)}\,.$$

In words, to multiply complex numbers we **multiply moduli** and **add arguments**. (See Theorem 3.18.)

For example, if z_1 is a distance of 3 from the origin and z_2 is a distance of 4 from the origin, then $z_1 z_2$ is a distance of 12 from the origin. And if z_1 is on a ray 30° counterclockwise from the positive real axis and z_2 is on a ray 45° counterclockwise from the positive real axis, then $z_1 z_2$ is on a ray 75° counterclockwise from the positive real axis.

In particular, if a complex number u lies on the unit circle (i.e. $|u| = 1$) and if z is any nonzero complex number, then uz is obtained from z by a rotation by an angle equal to the argument of u.

3. The Norm, the Gaussian Integers and the Eisenstein Integers

The norm of a complex number z is simply the square of its modulus:

$$N(z) \;=\; |z|^2 \;=\; z\overline{z}\,.$$

The norm has several nice properties; see Proposition 3.35, page 117.

The Gaussian integers, denoted $\mathbb{Z}[i]$, are complex numbers whose real and imaginary parts are integers:

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

Geometrically, they form a square lattice in the complex plane.

It is not difficult to check that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

The Eisenstein integers, denoted in this text by $\mathbb{Z}[\omega]$, are:

$$\mathbb{Z}[\omega] \;=\; \{a + b\omega \mid a, b \in \mathbb{Z}\}\,, \quad \text{where } \omega \;=\; \tfrac{1}{2}(-1 + \sqrt{3}\,i)\,.$$

The complex number ω is called a cube root of unity, since $\omega^3 = 1$, as can be verified directly. Note that this means ω is a root of the polynomial $x^3 - 1$, which factors as $(x-1)(x^2 + x + 1)$. The two complex roots are ω and $\overline{\omega}$, as can be verified using the quadratic formula. It is not difficult to check that:

$$\overline{\omega} \;=\; \tfrac{1}{2}(-1 - \sqrt{3}\,i) \;=\; \omega^{-1} \;=\; \omega^2 \;=\; -1 - \omega\,.$$

Geometrically, the Eisenstein integers form a triangular lattice in the complex plane.