tegers, to avoid confusion with the algebraic integers defined in Section 21.3.

The algebraic numbers obviously include $\sqrt{2}$ (a solution of $x^2-2=0$), $\sqrt[3]{2}$ (a solution of $x^3-2=0$), and less obviously $\sqrt{2}+\sqrt{3}$ (see Exercise 21.1.1). The first mathematicians to use algebraic numbers systematically in number theory were Lagrange and Euler around 1770. A spectacular example was given by Euler (1770), when he used the algebraic number $\sqrt{-2}$ to prove the following claim of Fermat: $x=5$ *and* $y=3$ *is the only positive integer solution of* $y^3=x^2+2$. (The equation in fact goes back to Diophantus, who mentioned its integer solution in his Book VI, Problem 17.)

Euler's argument is incomplete but essentially correct, and we complete it later by closer study of the set $\mathbb{Z}[\sqrt{-2}]$ of numbers $a+b\sqrt{-2}$, where $a,b\in\mathbb{Z}$. It goes as follows.

Suppose x and y are integers such that $y^3=x^2+2$. Then

$$y^3=(x+\sqrt{-2})(x-\sqrt{-2}).$$

Assuming numbers of the form $a+b\sqrt{-2}$ "behave like" ordinary integers, we can conclude that $x+\sqrt{-2}$ and $x-\sqrt{-2}$ are *cubes* (since their product is the cube y^3). That is, there are $a,b\in\mathbb{Z}$ such that

$$\begin{aligned}x+\sqrt{-2}&=(a+b\sqrt{-2})^3\\&=a^3+3a^2b\sqrt{-2}+3ab^2(-2)+b^3(-2\sqrt{-2})\\&=a^3-6ab^2+(3a^2b-2b^3)\sqrt{-2}.\end{aligned}$$

Equating real and imaginary parts we get

$$\begin{aligned}x&=a^3-6ab^2\\1&=3a^2b-2b^3=b(3a^2-2b^2)\quad\text{for some } a,b\in\mathbb{Z}.\end{aligned}$$

Now the only integer products equal to 1 are 1×1 and $(-1)\times(-1)$, hence $b=\pm 1$ and therefore $a=\pm 1$, from the second equation. Then the only positive solution for x occurs with $a=-1$, $b=\pm 1$, in which case $x=5$ and hence $y=3$. □

This wonderful flight of fancy, that the numbers $a+b\sqrt{-2}$ "behave like" ordinary integers, can actually be justified. It depends on the theory of divisibility in $\mathbb{Z}[\sqrt{-2}]$, which turns out to be similar to divisibility in $\mathbb{Z}$, already studied in Section 3.3.

EXERCISES

21.1.1 Show that the number $\sqrt{2}+\sqrt{3}$ satisfies the equation $x^4 - 10x^2 + 1 = 0$.

Before starting to investigate divisibility in $\mathbb{Z}[\sqrt{-2}]$, it will be useful to renew our acquaintance with $\mathbb{Z}$, particularly with regard to the behavior of squares, cubes, and their divisors.

21.1.2 Use unique prime factorization to show that a positive integer n is a square if and only if each prime in the prime factorization of n occurs to an even power.

21.1.3 If l and m are positive integers with no common prime divisor, and lm is a square, use Exercise 21.1.2 to show that l and m are both squares.

21.1.4 Show similarly that if l and m are integers with no common prime divisor, and if lm is a cube, then l and m are both cubes.

Thus to prove such results about the numbers $x+\sqrt{-2}$ and $x-\sqrt{-2}$ we need to know, first, that they have no common prime divisor. In the next section we introduce the concept of *norm*, which reduces such divisibility questions to questions about divisibility in the integers.

21.2 Gaussian Integers

Beyond $\mathbb{Z}$ itself, the simplest set to "behave like" integers is $\mathbb{Z}[i]$, the set of numbers of the form $a+bi$, where $a, b \in \mathbb{Z}$. These are called the *Gaussian integers*, because Gauss (1832c) was the first to study them and prove their basic properties. $\mathbb{Z}[i]$ is like $\mathbb{Z}$ in being closed under the operations $+$, $-$, and $\times$, but also in having primes and unique prime factorization.

An ordinary prime may be defined as an integer of size >1 that is not the product of integers of smaller size. A *Gaussian prime* may be defined in the same way, provided we make a sensible definition of "size." The ordinary absolute value $|a+bi| = \sqrt{a^2+b^2}$ is a suitable measure, so we say that a Gaussian integer α is a Gaussian prime if $|\alpha| > 1$ but α is not the product of Gaussian integers of smaller absolute value.

It is equivalent to define Gaussian primes in terms of the *square* of the absolute value, known as the *norm* of α, $N(\alpha)$. That is, α is a Gaussian prime if $N(\alpha) > 1$ and α is not the product of Gaussian integers of smaller norm.

The norm has the advantage that $N(a+ib) = a^2+b^2$ is an ordinary positive integer, so we can exploit the known properties of integers. For

example, we can see immediately why *every Gaussian integer has a Gaussian prime factorization.* Namely, if α is not itself a Gaussian prime, then $\alpha = \beta\gamma$, where $N(\beta), N(\gamma) < N(\alpha)$. If β, γ are Gaussian primes, then we have a Gaussian prime factorization of α; if not, at least one of them factorizes into Gaussian integers of smaller norm, and so on. *This process must terminate*, because norms are ordinary integers and hence they cannot decrease in size indefinitely. At termination, we have a Gaussian prime factorization of α.

The *uniqueness* of this prime factorization is a deeper result, for which it is convenient to revert to the absolute value measure of size and interpret $|a + ib|$ as the distance of $a + ib$ from O. This enables us to prove that Gaussian integers have "division with remainder," in a surprisingly geometric manner.

Division property of $\mathbb{Z}[i]$. *For any α and $\beta \neq 0$ in $\mathbb{Z}[i]$, there are μ and ρ in $\mathbb{Z}[i]$ such that*

$$\alpha = \mu\beta + \rho \quad \text{with} \quad |\rho| < |\beta|.$$

Proof. The multiples $\mu\beta$ for $\mu \in \mathbb{Z}[i]$ are sums of terms $\pm\beta$ and $\pm i\beta$. It follows, since the lines from O to β and $i\beta$ are perpendicular, that the numbers $\mu\beta$ lie at the corners of a lattice of squares of side $|\beta|$, as in Figure 21.1.

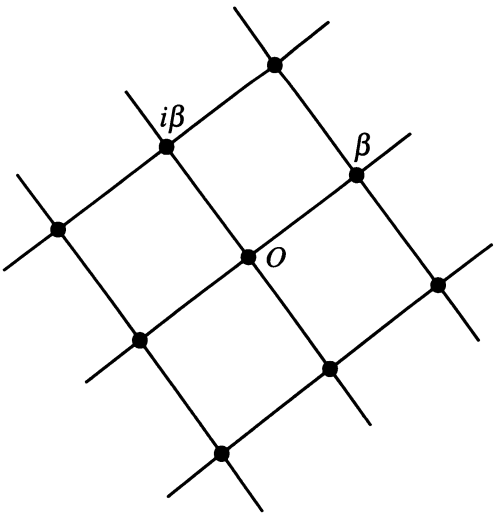

Figure 21.1: Multiples of β in $\mathbb{Z}[i]$

Now α lies in one of these squares, and if we let

$$\rho = \alpha - \text{nearest corner } \mu\beta,$$

it follows that the perpendiculars from α to the nearest sides are of length $\leq |\beta|/2$ (draw a picture). Therefore, since two sides of a triangle have total length greater than the third,

$$|\rho| < \frac{|\beta|}{2} + \frac{|\beta|}{2} = |\beta|,$$

as required. □

The division property of $\mathbb{Z}[i]$ has the following consequences, parallel to those for natural numbers described in Section 3.3.

1. There is a *Euclidean algorithm* for $\mathbb{Z}[i]$, which takes any $\alpha, \beta \in \mathbb{Z}[i]$ and repeatedly divides the larger of the pair by the smaller, keeping the smaller number and the remainder. It ends by finding $\gcd(\alpha, \beta)$, a common divisor of α, β that is greatest in norm.

2. There are $\mu, \nu \in \mathbb{Z}[i]$ such that $\gcd(\alpha, \beta) = \mu\alpha + \nu\beta$.

3. If ϖ is a Gaussian prime that divides $\alpha\beta$, then ϖ divides α or β.

4. The *Gaussian prime factorization of a Gaussian integer is unique*, up to the order of factors and factors of norm 1 (that is, factors ± 1, $\pm i$).

EXERCISES

We know from Section 20.2 that the absolute value is multiplicative, and hence so is the norm: $N(\alpha\beta) = N(\alpha)N(\beta)$. Indeed, this is just a restatement of Diophantus' identity. It follows that *if* α *divides* γ (that is, if $\gamma = \alpha\beta$ for some β), *then* $N(\alpha)$ *divides* $N(\gamma)$ [because $N(\gamma) = N(\alpha)N(\beta)$].

Thus we have a criterion for divisibility in the Gaussian integers based on divisibility in the ordinary integers. Among other things, this enables us to show that certain Gaussian integers are Gaussian primes.

21.2.1 By considering $N(4+i)$, show that $4+i$ is a Gaussian prime.

21.2.2 Show that an ordinary prime of the form $a^2 + b^2$ is *not* a Gaussian prime, and find its Gaussian prime factorization.

Now we modify the above argument for the division property of $\mathbb{Z}[i]$ to show that $\mathbb{Z}[\sqrt{-2}]$ also has it. That is, *if* α *and* $\beta \neq 0$ *are in* $\mathbb{Z}[\sqrt{-2}]$, *then there are* μ *and* ρ *in* $\mathbb{Z}[\sqrt{-2}]$ *such that*

$$\alpha = \mu\beta + \rho \quad \text{with} \quad |\rho| < |\beta|.$$

21.2.3 Show that the multiples $\mu\beta$ of any $\beta \in \mathbb{Z}[\sqrt{-2}]$ lie at the corners of a grid of rectangles, each of which has sides of length $|\beta|$ and $\sqrt{2}|\beta|$.

21.2.4 Deduce from Exercise 21.2.3 and Pythagoras' theorem that any α lies at distance $< |\beta|$ from the nearest multiple $\mu\beta$ of $\beta \neq 0$, and hence that $\mathbb{Z}[\sqrt{-2}]$ has the division property.

As in $\mathbb{Z}[i]$, the division property leads to a Euclidean algorithm for gcd, and eventually to unique prime factorization in $\mathbb{Z}[\sqrt{-2}]$. This enables us to fill in the gaps of Euler's argument in the previous section, as soon as we have checked that $\gcd(x+\sqrt{-2}, x-\sqrt{-2}) = 1$ when $y^3 = x^2 + 2$.

21.2.5 Show that if x and y are ordinary integers with $y^3 = x^2 + 2$, then x is odd.

Finally we invoke the norm in $\mathbb{Z}[\sqrt{-2}]$,

$$N(a + b\sqrt{-2}) = |a + b\sqrt{-2}|^2 = a^2 + 2b^2.$$

21.2.6 Show that $N(x+\sqrt{-2})$ is odd, whereas $N(2\sqrt{-2}) = 2^3$, and hence that

$$1 = \gcd(x+\sqrt{-2}, 2\sqrt{-2}) = \gcd(x+\sqrt{-2}, x-\sqrt{-2}).$$

21.3 Algebraic Integers

The Gaussian integers are an excellent example of algebraic numbers that "behave like" integers, but it is not yet clear what the general concept of "integer" should be. After a period of exploration by Dirichlet, Kummer, Eisenstein, Hermite, and Kronecker in the 1840s and 1850s, the following definition was proposed by Dedekind (1871): an *algebraic integer* is a root of an equation of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0, \quad \text{where } a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}. \quad (*)$$

Thus the definition of algebraic integer results from the definition of algebraic number (Section 21.1) by restricting the polynomials to those with leading coefficient 1, or *monic* polynomials as they are often called.

One reason that this definition suggested itself was a result proved by Eisenstein (1850) that the numbers satisfying such equations are closed under $+$, $-$, and $\times$. It follows, since algebraic numbers inherit the properties

of $+$, $-$, and $\times$ from $\mathbb{C}$, that algebraic integers form a *commutative ring with unit*, as defined in Section 20.3.

Another reason for the restriction to monic polynomials is that the *rational* algebraic integers are precisely the ordinary integers. This property of monic polynomials was pointed out by Gauss (1801), article 11, and it is quite easy to prove. We suppose that the equation (*) has a rational solution that is not an ordinary integer. Then we may assume that the solution is of the form $x = r/pq$, where p, q, r are ordinary integers and p is a prime not dividing r. Substituting this value for x in (*), and multiplying through by $(pq)^n$, we get

$$r^n = -a_{n-1}r^{n-1}(pq) - \cdots - a_1 r(pq)^{n-1} - a_0(pq)^n.$$

However, this is impossible, because p divides the right-hand side but not the left.

In practice, it is difficult to work in the ring of all algebraic integers, and we prefer to work in smaller rings such as $\mathbb{Z}[i]$ or $\mathbb{Z}[\sqrt{-2}]$. The exercises in the previous section show that $\mathbb{Z}[\sqrt{-2}]$ is the perfect setting for Euler's proof that $y^3 = x^2 + 2$ has only one positive solution in $\mathbb{Z}$.

The advantage of rings such as $\mathbb{Z}[i]$ or $\mathbb{Z}[\sqrt{-2}]$ is that they have the concept of norm, which allows us to define the concept of prime and to show that each element of the ring has a prime factorization. However, the *uniqueness* of prime factorization is not guaranteed, and in a sense we were lucky to find it in $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$.

A more typical ring of algebraic integers is

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

In this ring $|a + b\sqrt{-5}| = \sqrt{a^2 + 5b^2}$, and hence the norm is

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

As before, we define a *prime* to be a number of norm >1 that is not the product of numbers of smaller norm, and it follows as in $\mathbb{Z}[i]$ that every member of $\mathbb{Z}[\sqrt{-5}]$ factorizes into primes of $\mathbb{Z}[\sqrt{-5}]$.

It is likewise true that if β divides α in $\mathbb{Z}[\sqrt{-5}]$, then $N(\beta)$ divides $N(\alpha)$ in $\mathbb{Z}$. Hence α is a prime of $\mathbb{Z}[\sqrt{-5}]$ if $N(\alpha)$ is not divisible by any smaller norm $\neq 1$, that is, by any smaller integer of the form $a^2 + 5b^2 \neq 1$.

Examples of primes in $\mathbb{Z}[\sqrt{-5}]$ are

$$\begin{aligned} 2, &\quad \text{because } N(2) = 4, \\ 3, &\quad \text{because } N(3) = 9, \\ 1+\sqrt{-5}, &\quad \text{because } N(1+\sqrt{-5}) = 6, \\ 1-\sqrt{-5}, &\quad \text{because } N(1-\sqrt{-5}) = 6. \end{aligned}$$

Hence it follows that 6 has *two different prime factorizations* in $\mathbb{Z}[\sqrt{-5}]$:

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

In the 1840s Kummer noticed examples of the failure of unique prime factorization, and he realized that it is a serious problem. He wrote:

> It is greatly to be lamented that this virtue of the real numbers [that is, of the ordinary integers] to be decomposable into prime factors, always the same ones for a given number, does not also belong to the complex numbers [that is, the algebraic integers]; were this the case, the whole theory, which is still laboring under such difficulties, could easily be brought to a conclusion. For this reason, the complex numbers we have been considering seem imperfect, and one may well ask whether one ought not to look for another kind which would preserve the analogy with the real numbers with respect to such a fundamental property.
>
> [Translation by Weil (1975) from Kummer (1844).]

Kummer found "another kind of number" that preserved the property of unique prime factorization, and he called them *ideal numbers*. Today we know them under the name of *ideals*.

EXERCISES

Although ordinary fractions, such as 1/2, are not algebraic integers, some "algebraic fractions" are.

21.3.1 Show that the golden ratio $(1+\sqrt{5})/2$ is an algebraic integer.

21.3.2 Find the three algebraic integers that satisfy the equation $x^3 - 1 = 0$.

Eisenstein's theorem that the algebraic integers are closed under $+$, $-$, and $\times$ was given a new proof by Dedekind (1871) using linear algebra.

21.3.3 Suppose that α and β are algebraic integers satisfying the equations

$$\alpha^a + p_{a-1}\alpha^{a-1} + \cdots + p_1\alpha + p_0 = 0,$$
$$\beta^b + q_{b-1}\beta^{b-1} + \cdots + q_1\beta + q_0 = 0.$$

Deduce from these that any power $\alpha^{a'}$ may be written as a linear combination of $1, \alpha, \alpha^2, \ldots, \alpha^{a-1}$ with ordinary integer coefficients, and any power $\beta^{b'}$ as a linear combination of $1, \beta, \beta^2, \ldots, \beta^{b-1}$ with ordinary integer coefficients.

21.3.4 Now let $\omega_1, \omega_2, \ldots, \omega_n$ denote the $n = ab$ products of the form $\alpha^{a'}\beta^{b'}$, where $a' < a$ and $b' < b$. Show that, if ω denotes any one of $\alpha + \beta$, $\alpha - \beta$, or $\alpha\beta$, then we have n equations with ordinary integer coefficients $k_j^{(i)}$:

$$\omega\omega_1 = k_1'\omega_1 + k_2'\omega_2 + \cdots + k_n'\omega_n,$$
$$\omega\omega_2 = k_1''\omega_1 + k_2''\omega_2 + \cdots + k_n''\omega_n,$$
$$\vdots$$
$$\omega\omega_n = k_1^{(n)}\omega_1 + k_2^{(n)}\omega_2 + \cdots + k_n^{(n)}\omega_n.$$

21.3.5 Explain why the equations in Exercise 21.3.4 have a nonzero solution for $\omega_1, \omega_2, \ldots, \omega_n$, and hence that

$$\begin{vmatrix} k_1' - \omega & k_2' & \ldots & k_n' \\ k_1'' & k_2'' - \omega & \ldots & k_n'' \\ \ldots & \ldots & \ldots & \ldots \\ k_1^{(n)} & k_2^{(n)} & \ldots & k_n^{(n)} - \omega \end{vmatrix} = 0.$$

Also explain why this is a monic equation, with ordinary integer coefficients, for $\omega = \alpha + \beta, \alpha - \beta$, or $\alpha\beta$.

21.4 Ideals

Kummer did not explicitly define his "ideal numbers." Rather, he observed that prime algebraic integers sometimes behave *as if* they are nontrivial products, and from their behavior he inferred the behavior of their "ideal factors." Dedekind (1871) showed that "ideal factors" could be realized by sets of actual numbers, and he called these sets *ideals*. In his (1877) work he used the numbers in $\mathbb{Z}[\sqrt{-5}]$ to illustrate his method, showing that 2 and 3 behave as if they are products of primes—$2 = \alpha^2$ and $3 = \beta_1\beta_2$—and then showing how α, β_1, and β_2 may be realized as ideals.