In Kummer's time it was thought that $\mathbb{Z}[\zeta_n]$ was the key to Fermat's last theorem, because if $a,b,c \in \mathbb{Z}$ are such that $a^n + b^n = c^n$, then the nth power $a^n + b^n$ factorizes into n linear factors in $\mathbb{Z}[\zeta_n]$. In fact, this was the basis of a mistaken "proof " by Lamé (1847). However, Kummer noticed that such arguments break down, precisely because *unique prime factorization fails in* $\mathbb{Z}[\zeta_n]$. Kummer showed that this happens for $n \geq 23$, and he created the theory of ideal numbers in an attempt to repair the damage. In this respect, ideal numbers were only partially successful (not that it matters, now that we have Wiles' proof of Fermat's last theorem), but they proved their worth elsewhere. Dedekind's revision of Kummer's idea gave us the concept of ideal, which is indispensable in algebra today.

For a treatment of primes of the form $x^2 + 5y^2$ using ideals, see Artin (1991), and for more on the history of $x^2 + ny^2$, see the introduction to Dedekind (1877), and Cox (1989). The latter picks up another remarkable thread in the story of algebraic numbers—the modular function. As mentioned in the exercises to Section 16.5, the modular function is a function of lattice shapes, and for this reason it has something to say about ideals of imaginary quadratic integers. To find out what, see Cox's book, or McKean and Moll (1997).

Exercises

There is an "easy direction" of Fermat's theorems about x^2+y^2, x^2+2y^2, and x^2+3y^2 that can be proved with the help of congruences. This direction shows that primes are *not* representable in the given forms if they have the wrong remainders on division by 4, 8, and 3, respectively. (Compare with Exercises 1.5.2 and 3.2.1.)

21.6.1 Show that

1. An odd prime $x^2+y^2 \not\equiv 3 \pmod 4$.
2. An odd prime $x^2+2y^2 \not\equiv 5$ or $7 \pmod 8$.
3. An odd prime $x^2+3y^2 \not\equiv 2 \pmod 3$.

The "hard direction" of Fermat's theorems, finding the x^2 and y^2 to represent primes with the right remainders, involves more than we can cover completely here. However, for x^2+y^2 and x^2+2y^2 it involves unique prime factorization in $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$, both of which were discussed earlier in this chapter.

For x^2+3y^2, the proof involves not so much $\mathbb{Z}[\sqrt{-3}]$ as the larger ring

$$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \left\{m + \frac{1+\sqrt{-3}}{2}n : m,n \in \mathbb{Z}\right\}.$$

21.6.2 Show that $(1+\sqrt{-3})/2$ is an algebraic integer and that $\mathbb{Z}[(1+\sqrt{-3})/2]$ contains $\mathbb{Z}[\sqrt{-3}]$.

21.6.3 Show that 2, $1+\sqrt{-3}$, and $1-\sqrt{-3}$ are primes of $\mathbb{Z}[\sqrt{-3}]$, and deduce that 4 has two distinct prime factorizations in $\mathbb{Z}[\sqrt{-3}]$.

21.6.4 By a geometric argument like those used for $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$, show that $\mathbb{Z}[(1+\sqrt{-3})/2]$ has unique prime factorization.

21.7 Rings and Fields

Kronecker is famous for saying "God made the natural numbers, the rest is the work of man." [This is reported, for example, in his obituary by Weber (1892)]. Algebraic number theory was very much what he had in mind, because Kronecker, like Dedekind, saw number theory as the source of the most interesting problems, and the inspiration for all mathematical concepts. We can at least agree that number theory was the inspiration for two of the most important *algebraic* concepts: rings and fields.

Perhaps the first step toward abstract algebra was the introduction of negative numbers, creating the ring $\mathbb{Z}$ of integers from the natural numbers. This seems to have been a very difficult step, because mathematicians for many centuries (say, from the time of Diophantus to Descartes) lived in a halfway house where negative numbers were only partially accepted—sometimes being admitted in intermediate calculations, but not allowed as answers. Likewise, it was a long time before the "ratios" of the Greeks became the *field* $\mathbb{Q}$ of rational numbers.

Thus the first level of abstraction, the creation of inverses for addition and multiplication, took place unconsciously over thousands of years. The next level, identifying *axioms* for rings and fields, took place in the nineteenth century, mainly under the influence of algebraic number theory. The ring axioms are essentially the result of writing down the properties of + and × that algebraic integers share with the ordinary integers, and the field axioms are the properties that algebraic numbers share with rational numbers.

The concept of field was implicit in the work of Abel and Galois in the theory of equations, but it became explicit when Dedekind introduced *number fields of finite degree* as the setting for algebraic number theory. He saw that the ring of all algebraic integers is not a convenient ring, because it has no "primes." This is because $\sqrt{\alpha}$ is an algebraic integer if α is, hence there is always a nontrivial factorization $\alpha = \sqrt{\alpha}\sqrt{\alpha}$ in the ring of all algebraic integers. On the other hand, the algebraic integers in a field generated from a single algebraic number α of degree n,

$$\mathbb{Q}(\alpha)=\{a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}:a_0,a_1,\ldots,a_{n-1}\in\mathbb{Q}\},$$

have better behavior. The algebraic integers β in $\mathbb{Q}(\alpha)$ have a norm $N(\beta)$ that is an ordinary integer, and this guarantees the existence of primes, as we have seen in special cases like $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$, which are the algebraic integers in the fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-2})$ of degree 2.

By drawing attention to the field $\mathbb{Q}(\alpha)$ of degree n, Dedekind also brought to light some *vector space* structure: the *basis* $1,\alpha,\alpha^2,\ldots,\alpha^{n-1}$ of $\mathbb{Q}[\alpha]$, the *linear independence* of these basis elements over $\mathbb{Q}$, and the *dimension* (equal to the degree) of $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$. Despite the long history of linear algebra, dating back 2000 years in China at least, again it was the greater generality afforded by algebraic number theory that finally brought its fundamental concepts to light.

The next level of abstraction was reached in the twentieth century and was, in fact, the work of a woman, Emmy Noether. In the 1920s she developed concepts for discussing common properties of different algebraic structures, such as groups and rings. One of the things groups and rings have in common is *homomorphisms*, or structure-preserving maps. A map $\varphi: G\to G'$ is a *homomorphism of groups* if $\varphi(gh)=\varphi(g)\varphi(h)$ for any $g,h\in G$. Similarly, a map $\varphi: R\to R'$ is a homomorphism of rings if $\varphi(r+s)=\varphi(r)+\varphi(s)$ and $\varphi(rs)=\varphi(r)\varphi(s)$ for any $r,s\in R$. From this higher vantage point, normal subgroups (Section 19.2) and ideals can be seen as instances of the same concept. Each is the *kernel* of a homomorphism φ: the set of elements mapped by φ to the identity element (1 for a group, 0 for a ring).

Exercises

It is not clear that $\mathbb{Q}(\alpha)$ (as defined above) is a field for any algebraic number α. The hardest part is to prove that the quotient of any two of its elements is also an element. Some inkling of the difficulty may be grasped by working out the special case of $\mathbb{Q}(i)$.

21.7.1 Show that, if $a_1,b_1,a_2,b_2\in\mathbb{Q}$, then $\frac{a_1+ib_1}{a_2+ib_2}$ is of the form $a+ib$, where $a,b\in\mathbb{Q}$.

It is also not obvious that the kernel of a group homomorphism is a normal subgroup, partly because the definition of normal subgroup in Section 19.2 is not the most convenient for this purpose. It is easier to prove that the kernel of a ring homomorphism is an ideal, using the definition of an ideal given in Section 21.4.

21.7.2 Suppose that R is a ring and φ maps R into another ring in such a way that $\varphi(r+s)=\varphi(r)+\varphi(s)$ and $\varphi(rs)=\varphi(s)\varphi(s)$ for any $r,s\in R$. Show that the set

$$\{r:\varphi(r)=0\}$$

has the two defining properties of an ideal.

The equivalence of kernels and ideals may be illustrated in $\mathbb{Z}$ by the ideal (3) of multiples of 3.

21.7.3 Find a homomorphism of $\mathbb{Z}$ whose kernel is (3).

21.8 Biographical Notes: Dedekind, Hilbert, and Noether

Richard Dedekind (Figure 21.3) was born in 1831 in Brunswick, the home town of Gauss, into an academic family. His father, Julius, was professor of law at the Collegium Carolinum, and his mother, Caroline Emperius, was the daughter of another professor there. Richard was the youngest of four children in a close-knit family. They remained in Brunswick for most of their lives, and Richard lived with his sister Julie (both of them being unmarried) until 1914. Sounds dull, but this seemingly eventless life was the background to revolutionary activity in mathematics, in its way as provocative as the work of Galois.

Dedekind became interested in mathematics in high school, after coming to the conclusion that chemistry and physics were not sufficiently logical. He attended the Collegium Carolinum, the scientific academy that Gauss also attended, before entering Göttingen University in 1850. There he became friends with Riemann and made rapid academic progress, completing a thesis under Gauss's supervision in 1852. After the death of Gauss in 1855, Dirichlet was appointed to Gauss's chair, and he became the third major influence on Dedekind's career. After a brief period at the Polytechnikum in Zürich (now known as the ETH), a position that he won in competition with Riemann, Dedekind returned to the Polytechnikum in Brunswick, where he remained for the rest of his life. It was not a prestigious position, but the home comforts enabled him to concentrate on mathematics.

Dedekind was the last student of Gauss, and Gauss's number theory was the inspiration for much of Dedekind's work, as it was for many of the great German mathematicians of the nineteenth century. When Dedekind

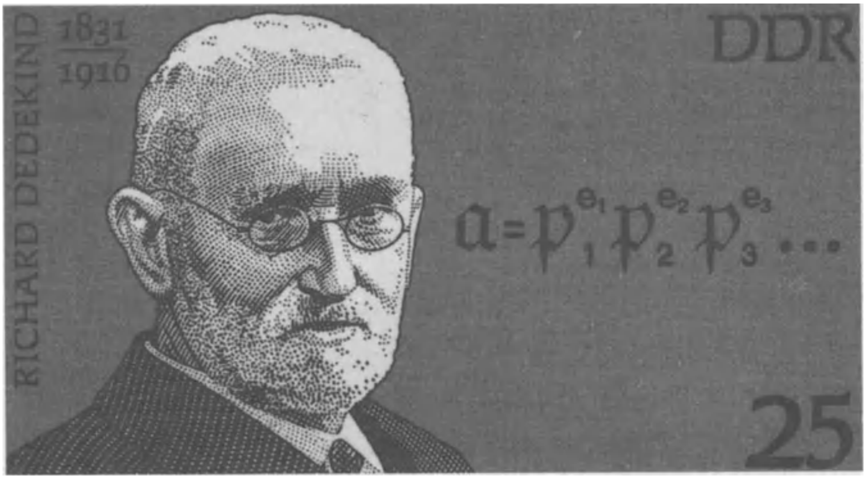

Figure 21.3: Richard Dedekind

started, the new generation of Eisenstein, Dirichlet, and Kronecker was finally beginning to understand Gauss's ideas, and making further progress. Dirichlet in particular made Gauss more approachable with his elegant and readable *Vorlesungen über Zahlentheorie* [Lectures on Number Theory, Dirichlet (1863)], which simplified much of Gauss's difficult theory of quadratic forms and added stunning new results and proofs of his own. The climax of Dirichlet's lectures is a *class number formula*, giving a uniform description of the number of inequivalent quadratic forms with given discriminant. The lectures were edited by Dedekind and first published in 1863, four years after Dirichlet's death. Dedekind took this project very seriously and made it virtually his life's work, bringing out further editions in 1871, 1879, and 1894, each time adding supplementary material, until the supplements amounted to more than Dirichlet's book itself. The theory of ideals made its first appearance in the 1871 edition, and was expanded and deepened in 1879 and 1894, eventually including a lot of Galois theory as well.

However, Dedekind was disappointed in the low enthusiasm for ideals shown by other mathematicians, and in 1877 he attempted a more popular approach. Dedekind (1877) is nearly perfect for the modern reader—clear, concise, and well motivated—but apparently it was still too abstract for his contemporaries. The theory of ideals did not really catch on until it was given a new exposition by Hilbert (1897), as we shall see below.

In the meantime, Dedekind had made several other great contributions to mathematics that were slowly taking root:

- the theory of real numbers as "Dedekind cuts,"
- the theory of Riemann surfaces as algebraic function fields,
- the characterization of natural numbers as an "inductive set."

What these contributions had in common, and what made them hard for Dedekind's contemporaries to grasp, was the idea of treating *infinite sets* as mathematical objects. Dedekind actually started doing this in 1857, when he treated congruence modulo n as the arithmetic of residue classes

$$\begin{aligned} 0 \bmod n &= \{0, \pm n, \pm 2n, \ldots\}, \\ 1 \bmod n &= \{1, 1 \pm n, 1 \pm 2n, \ldots\}, \\ &\vdots \\ n-1 \bmod n &= \{n-1, n-1 \pm n, n-1 \pm 2n, \ldots\}, \end{aligned}$$

which are added and multiplied according to the rules

$$\begin{aligned} (i \bmod n) + (j \bmod n) &= (i+j) \bmod n, \\ (i \bmod n)(j \bmod n) &= (i \cdot j) \bmod n. \end{aligned}$$

[We mentioned multiplication of residue classes in Section 19.1.] The idea of adding or multiplying sets by adding or multiplying *representatives* transfers directly to Dedekind cuts and, with some modification, to ideals and Riemann surfaces. Dedekind hoped that this cornucopia of applications would convince his colleagues of the value of the idea that "mathematical objects are sets," but it was a hard idea to sell. At first he was joined only by Cantor, who took up the theory of infinite sets as enthusiastically as Dedekind took up the applications (see Chapter 23).

Dedekind had to wait decades before his ideas entered the mainstream (and in some cases after they had been rediscovered by others—for example, his theory of natural numbers became the "Peano axioms"), but fortunately he lived long enough. He died in 1916 at the age of 84.

David Hilbert (Figure 21.4) was born in 1862 in Königsberg and died in Göttingen in 1943. His father, Otto, was a judge, and David may have inherited his mathematical ability from his mother, about whom we know little except that her maiden name was Erdtmann. Königsberg was in the remote eastern part of Prussia (it is now Kaliningrad, a small, disconnected piece of Russia), but with a strong mathematical tradition dating back to Jacobi. When Hilbert attended university there in the 1880s he became friends with Hermann Minkowski, a former child mathematical prodigy two years his junior, and Adolf Hurwitz, who was three years older and a professor in Königsberg from 1884. The three used to discuss mathematics on long walks, and Hilbert seems to have picked up his basic mathematical education in this way. In later life he made "mathematical walks" an important part of the education of his own students.

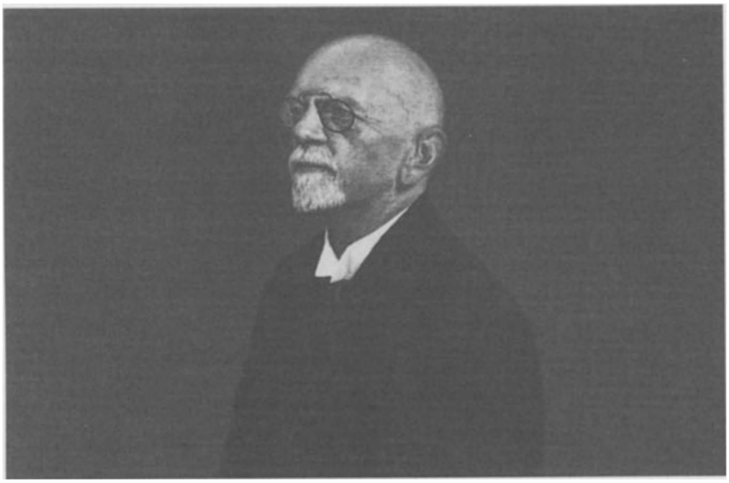

Figure 21.4: David Hilbert

Hilbert's first research interest was in the theory of invariants, an algebraic topic then held in high esteem. An elementary example of an invariant is the discriminant $b^2 - 4ac$ of a quadratic form, which Lagrange (1773b) noticed was invariant when the form was transformed into an equivalent form (Section 21.6). By Hilbert's time, invariant theory had become a jungle, with success depending mainly on the ability to hack through formidable calculations. The "king of invariant theory," Paul Gordan of Erlangen, was notorious for papers consisting almost entirely of equations—in fact, the story goes that he had assistants fill in any words that were necessary. In 1888 Hilbert swept all this away by solving the main problem of invariant theory, in a simple and purely conceptual man-