are often more powerful than concrete ones, and most opposition has disappeared. Group theory also made it clear that negative results may still be important, and that an insistence on proof can sometimes lead to major discoveries. Suppose that mathematicians had simply assumed without proof that quintics cannot be solved, on the plausible grounds that no one could find a solution. Then no one would have invented group theory to explain *why* they cannot be solved. If mathematicians had taken the easy route, and assumed the solution to be impossible, mathematics and science would have been a pale shadow of what they are today.

That is why mathematicians insist on proofs.

CHAPTER 14

Algebra Comes of Age

Numbers give way to structures

By 1860 the theory of permutation groups was well developed. The theory of invariants – algebraic expressions that do not change when certain changes of variable are performed – had drawn attention to various infinite sets of transformations, such as the *projective group* of all projections of space. In 1868 Camille Jordan had studied groups of motions in three-dimensional space, and the two strands began to merge.

Sophisticated concepts

A new kind of algebra began to appear, in which the objects of study were not unknown numbers, but more sophisticated concepts: permutations, transformations, matrices. Last year's processes had become this year's things. The long-standing rules of algebra often had to be modified to fit the needs of these new structures. Alongside groups, mathematicians started to study structures called rings and fields, and a variety of algebras.

One stimulus to this changing vision of algebras came from partial differential equations, mechanics and geometry: the development of Lie groups and Lie algebras. Another source of inspiration was number theory: here algebraic numbers could be

used to solve Diophantine equations, understand reciprocity laws and even to attack Fermat's Last Theorem. Indeed, the culmination of such efforts was the proof of Fermat's Last Theorem by Andrew Wiles in 1995.

Lie and Klein

In 1869 the Norwegian mathematician Sophus Lie became friendly with the Prussian mathematician Felix Klein. They had a common interest in line geometry, an offshoot of projective geometry introduced by Julius Plücker. Lie conceived a highly original idea: that Galois's theory of algebraic equations should have an analogue for differential equations. An algebraic equation can be solved by radicals only if it has the right kind of symmetries – that is, it has a soluble Galois group. Analogously, Lie suggested, a differential equation can be solved by classical methods only when the equation remains unchanged by a family of continuous transformations. Lie and Klein worked on variations of this idea during 1869–1870; it culminated in 1872 in Klein's characterization of geometry as the invariants of a group, laid down in his Erlangen programme.

This programme grew out of a new way of thinking about Euclidean geometry, in terms of its symmetries. Jordan had already pointed out that the symmetries of the Euclidean plane are rigid motions of several kinds: translations, which slide the plane in some direction; rotations, which turn it about some fixed point; reflections, which flip it over about a fixed line; and, less obviously, glide reflections, which reflect it and then translate it in a direction perpendicular to the mirror line. These transformations form a group, the *Euclidean group*, and they are rigid in the sense that they do not change distances. Therefore they also do not change angles. Now lengths and angles are the basic concepts of Euclid's geometry. So Klein realized that these concepts are the invariants of the Euclidean group, the quantities that do not change when a transformation from the group is applied.

In fact, if you know the Euclidean group, you can deduce its invariants, and from these you get Euclidean geometry.

The same goes for other kinds of geometry. Elliptic geometry is the study of the invariants of the group of rigid motions in a positively curved space, hyperbolic geometry is the study of the invariants of the group of rigid motions in a negatively curved space, and projective geometry is the study of the invariants of the group of projections and so on. Just as coordinates relate algebra to geometry, so invariants relate group theory to geometry. Each geometry defines a corresponding group, the group of all transformations that preserve the relevant geometric concepts. Conversely, every group of transformations defines a corresponding geometry, that of the invariants.

Klein used this correspondence to prove that certain geometries were essentially the same as others, because their groups were identical except for interpretation. The deeper message is that any geometry is defined by its symmetries. There is one exception: Riemann's geometry of surfaces, the curvature of which can change from point to point. It does not quite fit into Klein's programme.

Lie groups

Lie and Klein's joint research led Lie to introduce one of the most important ideas in modern mathematics, that of a continuous transformation group, now known as a *Lie group*. It is a concept that has revolutionized both mathematics and physics, because Lie groups capture many of the most significant symmetries of the physical universe, and symmetry is a powerful organizing principle – both for the underlying philosophy of how we represent nature mathematically, and for technical calculations.

Sophus Lie created the theory of Lie groups in a flurry of activity beginning in the autumn of 1873. The concept of a Lie group has evolved considerably since Lie's early work. In modern terms, a Lie group is a structure having both algebraic and topological

Felix Klein
1849–1925

Klein was born in Düsseldorf to an upper-class family – his father was secretary to the head of the Prussian government. He went to Bonn University, planning to become a physicist, but he became laboratory assistant to Julius Plücker. Plücker was supposed to be working in mathematics and experimental physics, but his interests had focused on geometry, and Klein fell under his influence. Klein's 1868 thesis was on line geometry as applied to mechanics.

By 1870 he was working with Lie on group theory and differential geometry. In 1871 he discovered that non-Euclidean geometry is the geometry of a projective surface with a distinguished conic section. This fact proved, very directly and obviously, that non-Euclidean geometry is logically consistent if Euclidean geometry is. This pretty much ended the controversy over the status of non-Euclidean geometry.

In 1872 Klein became professor at Erlangen, and in his Erlangen programme of 1872 he unified almost all known types of geometry, and clarified links between them, by considering geometry as the invariants of a transformation group. Geometry thereby became a branch of group theory. He wrote this article for his inaugural address, but did not actually present it on that occasion. Finding Erlangen uncongenial, he moved to Munich in 1875. He married Anne Hegel, granddaughter of the famous philosopher. Five years later he went to Leipzig, where he blossomed mathematically.

Klein believed that his best work was in the theory of complex functions, where he made deep studies of functions invariant under various groups of transformations of the complex plane. In particular he developed the theory of the simple group of order 168 in this context. He engaged in rivalry with Poincaré to solve the uniformization problem for complex functions, but his health collapsed, possibly because of the strenuous effort involved.

In 1886 Klein was made professor at the University of Göttingen, and concentrated on administration, building one of the best schools of mathematics in the world. He remained there until retirement in 1913.

properties, the two being related. Specifically, it is a group (a set with an operation of composition that satisfies various algebraic identities, most notably the associative law) and a topological manifold (a space that locally resembles Euclidean space of some fixed dimension but which may be curved or otherwise distorted on the global level), such that the law of composition is continuous (small changes in the elements being composed produce small changes in the result). Lie's concept was more concrete: a group of continuous transformations in many variables. He was led to study such transformation groups while seeking a theory of the solubility or insolubility of differential equations, analogous to that of Évariste Galois for algebraic equations, but today they arise in an enormous variety of mathematical contexts, and Lie's original motivation is not the most important application.

Perhaps the simplest example of a Lie group is the set of all rotations of a circle. Each rotation is uniquely determined by an angle between 0° and 360°. The set is a group because the composition of two rotations is a rotation – through the sum of the corresponding angles. It is a manifold of dimension one, because angles correspond one-to-one with points on a circle, and small arcs of a circle are just slightly bent line segments, a line being Euclidean space of dimension one. Finally, the composition law is continuous because small changes in the angles being added produce small changes in their sum.

A more challenging example is the group of all rotations of three-dimensional space that preserve a chosen origin. Each rotation is determined by an axis – a line through the origin in an arbitrary

direction – and an angle of rotation about that axis. It takes two variables to determine an axis (say the latitude and longitude of the point in which it meets a reference sphere centred on the origin) and a third to determine the angle of rotation; therefore this group has dimension three. Unlike the group of rotations of a circle, it is non-commutative – the result of combining two transformations depends upon the order in which they are performed.

In 1873, after a detour into PDEs, Lie returned to transformation groups, investigating properties of infinitesimal transformations. He showed that infinitesimal transformations derived from a continuous group are not closed under composition, but they *are* closed under a new operation known as the *bracket*, written $[x,y]$. In matrix notation this is the commutator $xy - yx$ of x and y. The resulting algebraic structure is now known as a *Lie algebra*. Until about 1930 the terms Lie group and Lie algebra were not used: instead these concepts were referred to as continuous group and infinitesimal group respectively.

There are strong interconnections between the structure of a Lie group and that of its Lie algebra, which Lie expounded in a three-volume work *Theorie der Transformationsgruppen* (*Theory of Transformation Groups*) written jointly with Friedrich Engel. They discussed in detail four classical families of groups, two of which are the rotation groups in n-dimensional space for odd or even n. The two cases are rather different, which is why they are distinguished. For example, in odd dimensions a rotation always possesses a fixed axis; in even dimensions it does not.

Killing

The next really substantial development was made by Wilhelm Killing. In 1888 Killing laid the foundations of a structure theory for Lie algebras, and in particular he classified all the *simple* Lie algebras, the basic building blocks out of which all other Lie algebras are composed. Killing started from the known structure of the most

straightforward simple Lie algebras, the *special linear* Lie algebras $sl(n)$, for $n \geq 2$. Start with all $n \times n$ matrices with complex entries, and let the Lie bracket of two matrices A and B be $AB - BA$. This Lie algebra is not simple, but the sub-algebra, $sl(n)$, of all matrices whose diagonal terms sum to zero, is simple. It has dimension $n^2 - 1$.

Killing knew the structure of this algebra, and he showed that any simple Lie algebra had a similar kind of structure. It is remarkable that he could prove something so specific, starting only with the knowledge that the Lie algebra is simple. His method was to associate to each simple Lie algebra a geometric structure known as a *root system*. He used methods of linear algebra to study and classify root systems, and then derived the structure of the corresponding Lie algebra from that of the root system. So classifying the possible root system geometries is effectively the same as classifying the simple Lie algebras.

The upshot of Killing's work is remarkable. He proved that the simple Lie algebras fall into four infinite families, now called A_n, B_n, C_n and D_n. Additionally, there were five exceptions: G_2, F_4, E_6, E_7 and E_8. Killing actually thought there were six exceptions, but two of them turned out to be the same algebra in two different guises. The dimensions of the exceptional Lie algebras are 12, 56, 78, 133 and 248. They remain a little mysterious, although we now understand fairly clearly why they exist.

Simple Lie groups

Because of the close connections between a Lie group and its Lie algebra, the classification of simple Lie algebras also led to a classification of the simple Lie groups. In particular the four families A_n, B_n, C_n and D_n are the Lie algebras of the four classical families of transformation groups. These are, respectively, the group of all linear transformations in $(n + 1)$-dimensional space, the rotation group in $(2n + 1)$-dimensional space, the symplectic group in $2n$ dimensions, which is important in classical and quantum mechanics

and optics, and the rotation group in 2n-dimensional space. A few finishing touches to this story were added later; notably the introduction by Harold Scott MacDonald Coxeter and Eugene (Evgenii) Dynkin of a graphical approach to the combinatorial analysis of root systems, now known as *Coxeter* or *Dynkin diagrams*.

Lie groups are important in modern mathematics for many reasons. For example, in mechanics, many systems have symmetries, and those symmetries make it possible to find solutions of the dynamical equations. The symmetries generally form a Lie group. In mathematical physics, the study of elementary particles relies heavily upon the apparatus of Lie groups, again because of certain symmetry principles. Killing's exceptional group E_8 plays an important role in superstring theory, an important current approach to the unification of quantum mechanics and general relativity. Simon Donaldson's epic discovery of 1983 that four-dimensional Euclidean space possesses non-standard differentiable structures rests, fundamentally, on an unusual feature of the Lie group of all rotations in four-dimensional space. The theory of Lie groups is vital to the whole of modern mathematics.

Abstract groups

In Klein's Erlangen programme it is essential that the groups concerned consist of transformations; that is, the elements of the group act on some space. Much of the early work on groups assumed this structure. But further research required one extra piece of abstraction: to retain the group property but throw away the space. A group consisted of mathematical entities that could be combined to yield similar entities, but those entities did not have to be transformations.

Numbers are an example. Two numbers (integer, rational, real, complex) can be added, and the result is a number of the same kind. Numbers form a group under the operation of addition. But numbers are not transformations. So even though the role of groups

as transformations had unified geometry, the assumption of an underlying space had to be thrown away to unify group theory.

Among the first to come close to taking this step was Arthur Cayley, in three papers of 1849 and 1854. Here Cayley said that a group comprises a set of *operators* 1, a, b, c and so on. The compound ab of any two operators must be another operator; the special operator 1 satisfies $1a = a$ and $a1 = a$ for all operators a; finally, the associative law $(ab)c = a(bc)$ must hold. But his operators still operated on something (a set of variables). Additionally, he had omitted a crucial property: that every a must have an inverse a' such that $a'a = aa' = 1$. So Cayley came close, but missed the prize by a whisker.

In 1858 Richard Dedekind allowed the group elements to be arbitrary entities, not just transformations or operators, but he included the commutative law $ab = ba$ in his definition. His idea was fine for its intended purpose, number theory, but it excluded most of the interesting groups in Galois theory, let alone the wider mathematical world. The modern concept of an abstract group was introduced by Walther van Dyck in 1882–3. He included the existence of an inverse, but rejected the need for the commutative law. Fully-fledged axiomatic treatments of groups were provided soon after, by Edward Huntington and Eliakim Moore in 1902, and by Leonard Dickson in 1905.

With the abstract structure of groups now separated from any specific interpretation, the subject developed rapidly. Early research consisted mostly of 'butterfly collecting' – people studied individual examples of groups, or special types, looking for common patterns. The main concepts and techniques appeared relatively quickly, and the subject thrived.

Number theory

Another major source of new algebraic concepts was number theory. Gauss started the process when he introduced what we now call *Gaussian integers*. These are complex numbers $a + bi$, where a and

b are integers. Sums and products of such numbers also have the same form. Gauss discovered that the concept of a prime number generalizes to Gaussian integers. A Gaussian integer is *prime* if it cannot be expressed as a product of other Gaussian integers in a non-trivial way. Prime factorization for Gaussian integers is unique. Some ordinary primes, such as 3 and 7, remain prime when considered as Gaussian integers, but others do not: for example $5 = (2 + i)(2 - i)$. This fact is closely connected with Fermat's theorem about primes and sums of two squares, and Gaussian integers illuminate that theorem and its relatives.

If we divide one Gaussian integer by another, the result need not be a Gaussian integer, but it comes close: it is of the form $a + bi$, where a and b are rational. These are the *Gaussian numbers*. More generally, number theorists discovered that something similar holds if we take any polynomial $p(x)$ with integer coefficients, and then consider all linear combinations $a_1x_1 + \cdots + a_nx_n$ of its solutions $x_1, \ldots, x_n$. Taking $a_1, \ldots, a_n$ to be rational, we obtain a system of complex numbers that is *closed* under addition, subtraction, multiplication and division – meaning that when these operations are applied to such numbers, the result is a number of the same kind. This system constitutes an *algebraic number field*. If instead we require $a_1, \ldots, a_n$, to be integers, the system is closed under addition, subtraction and multiplication, but not division: it is an *algebraic number ring*.

The most ambitious application of these new number systems was Fermat's Last Theorem: the statement that the Fermat equation, $x^n + y^n = z^n$, has no whole number solutions when the power n is three or more. Nobody could reconstruct Fermat's alleged 'remarkable proof' and it seemed increasingly doubtful that he had ever possessed one. However, some progress was made. Fermat found proofs for cubes and fourth powers, Peter Lejeune-Dirichlet dealt with fifth powers in 1828 and Henri Lebesgue found a proof for seventh powers in 1840.

In 1847 Gabriel Lamé claimed a proof for all powers, but Ernst Eduard Kummer pointed out a mistake. Lamé had assumed without proof that uniqueness of prime factorization is valid for algebraic numbers, but this is *false* for some (indeed most) algebraic number fields. Kummer showed that uniqueness fails for the algebraic number field that arises in the study of Fermat's Last Theorem for 23rd powers. But Kummer did not give up easily, and he found a way round this obstacle by inventing some new mathematical gadgetry, the theory of ideal numbers. By 1847 he had disposed of Fermat's Last Theorem for all powers up to 100, except for 37, 59 and 67. By developing extra machinery, Kummer and Dimitri Mirimanoff disposed of those cases too in 1857. By the 1980s similar methods had proved all cases up to the 150,000th power, but the method was running out of steam.

Rings, fields and algebras

Kummer's notion of an ideal number was cumbersome, and Dedekind reformulated it in terms of ideals, special subsystems of algebraic integers. In the hands of Hilbert's school at Göttingen, and in particular Emmy Noether, the entire area was placed on an axiomatic footing. Alongside groups, three other types of algebraic system were defined by suitable lists of axioms: rings, fields and algebras.

In a *ring*, operations of addition, subtraction and multiplication are defined, and they satisfy all the usual laws of algebra except for the commutative law of multiplication. If this law also holds, we have a *commutative ring*.

In a *field*, operations of addition, subtraction, multiplication and division are defined, and they satisfy all the usual laws of algebra including the commutative law of multiplication. If this law fails, we have a *division ring*.

An *algebra* is like a ring, but its elements can also be multiplied by various constants, the real numbers, complex numbers or – in the most general setting – by a field. The laws of addition are the usual

Emmy Amalie Noether
1882–1935

Emmy Noether was the daughter of the mathematician Max Noether and Ida Kaufmann, both of Jewish origin. In 1900 she qualified to teach languages but instead decided her future lay in mathematics. At that time German universities allowed women to study courses unofficially if the professor gave permission, and she did this from 1900 to 1902. Then she went to Göttingen, attending lectures by Hilbert, Klein and Minkowski in 1903 and 1904.

She gained a doctorate in 1907, under the invariant theorist Paul Gordan. Her thesis calculated a very complicated system of invariants. For men, the next step would be Habilitation, but this was not permitted for women. She stayed home in Erlangen, helping her disabled father, but she continued her research and her reputation quickly grew.

In 1915 she was invited back to Göttingen by Klein and Hilbert, who struggled to get the rules changed to allow her on to the faculty. They finally succeeded in 1919. Soon after her arrival she proved a fundamental theorem, often called Noether's Theorem, relating the symmetries of a physical system to conservation laws. Some of her work was used by Einstein to formulate parts of general relativity. In 1921 she wrote a paper on ring theory and ideals, taking an abstract axiomatic view. Her work formed a significant part of Bartel Leendert van der Waerden's classic text *Moderne Algebra*.

When Germany fell under Nazi rule she was dismissed because she was Jewish, and she left Germany to take up a position in the USA. Van der Waerden said that for her, 'relationships among numbers, functions and operations became transparent, amenable to generalization and productive only after they have been ... reduced to general conceptual relationships.'

ones, but the multiplication may satisfy a variety of different axioms. If it is associative, we have an associative algebra. If it satisfies some laws related to the commutator $xy - yx$, it is a Lie algebra.

There are dozens, maybe hundreds of different types of algebraic structure, each with its own list of axioms. Some have been invented just to explore the consequences of interesting axioms, but most arose because they were needed in some specific problem.

Finite simple groups

The high point of 20th century research on finite groups was the successful classification of all finite simple groups. This achieved for finite groups what Killing had achieved for Lie groups and their Lie algebras. Namely, it led to a complete description of all possible basic building blocks for finite groups, the *simple* groups. If groups are molecules, the simple groups are their constituent atoms.

Killing's classification of simple Lie groups proved that these must belong to one of four infinite families A_n, B_n, C_n and D_n, with exactly five exceptions, G_2, F_4, E_6, E_7 and E_8. The eventual classification of all finite simple groups was achieved by too many mathematicians to mention individually, but the overall programme for solving this problem was due to Daniel Gorenstein. The answer, published in 1888–90, is strangely similar: a list of infinite families, and a list of exceptions. But now there are many more families, and the exceptions number 26.

The families comprise the alternating groups (known to Galois) and a host of groups of Lie type which are like the simple Lie groups but over various finite fields rather than the complex numbers. There are some curious variations on this theme, too. The exceptions are 26 individuals, with hints of some common patterns, but no unified structure. The first proof that the classification is complete came from the combined work of hundreds of mathematicians, and its total length was around 10,000 pages. Moreover, some crucial parts of the proof were not published. Recent work by those remaining in this area of research has involved reworking the classification in a more streamlined manner, an approach made possible by already knowing the answer. The results are appearing as a series of textbooks, totalling around 2000 pages.

The most mysterious of the exceptional simple groups, and the largest, is the *monster*. Its order is

$$2^{46}\times3^{20}\times5^{9}\times7^{6}\times11^{2}\times13^{3}\times17\times19\times23\times29\times31\times41\times47\times59\times71$$

which equals

808017424794512875886459904961710757005754368000000000

and is roughly 8×10^{53}. Its existence was conjectured in 1973 by Bernd Fischer and Robert Griess. In 1980 Griess proved that it existed, and gave an algebraic construction as the symmetry group of a 196,884-dimensional algebra. The monster seems to have some unexpected links with number theory and complex analysis, stated by John Conway as the Monstrous Moonshine conjecture. This conjecture was proved by Richard Borcherds in 1992, and he was awarded a Fields Medal – the most prestigious award in mathematics – for it.

Fermat's Last Theorem

The application of algebraic number fields to number theory developed apace in the second half of the 20th century, and made contact with many other areas of mathematics, including Galois theory and algebraic topology. The culmination of this work was a proof of Fermat's Last Theorem, some 350 years after it was first stated.

The really decisive idea came from a beautiful area that lies at the heart of modern work on Diophantine equations: the theory of elliptic curves. These are equations in which a perfect square is equal to a cubic polynomial, and they represent the one area of Diophantine equations that mathematicians understand pretty well. However, the subject has its own big unsolved problems. The biggest of all is the Taniyama–Weil conjecture, named after Yutaka Taniyama and André Weil. This says that every elliptic curve can be represented in terms of modular functions – generalizations of trigonometric functions studied in particular by Klein.

What abstract algebra did for them

In his 1854 book *The Laws of Thought*, George Boole showed that algebra can be applied to logic, inventing what is now known as Boolean algebra.

Here we can do no more than convey a flavour of Boole's ideas. The most important logical operators are *not*, *and* and *or*. If a statement S is true, then not-S is false, and vice versa. S and T is true if, and only if, both S and T are true. S or T is true provided at least one of S, T is true – possibly both. Boole noticed that if we rewrite T as 1 and S as 0, then the algebra of these logical operations is very similar to ordinary algebra, provided we think of 0 and 1 as integers modulo 2, so that $1 + 1 = 0$ and –S is the same as S. So not-S is 1+S, S and T is ST, and S or T is S+T+ST. The sum S+T corresponds to *exclusive* or (written *xor* by computer scientists). S *xor* T is true provided T is true or S is true, but not both. Boole discovered that his curious algebra of logic is entirely self-consistent if you bear its slightly weird rules in mind and use them systematically. This was one of the first steps towards a formal theory of mathematical logic.

Early in the 1980s Gerhard Frey found a link between Fermat's Last Theorem and elliptic curves. Suppose that a solution to Fermat's equation exists; then you can construct an elliptic curve with very unusual properties – so unusual that the curve's existence seems highly improbable. In 1986 Kenneth Ribet made this idea precise by proving that if the Taniyama–Weil conjecture is true, then Frey's curve cannot exist. Therefore the presumed solution of Fermat's equation cannot exist either, which would prove Fermat's Last Theorem. The approach depended on the Taniyama–Weil conjecture, but it showed that Fermat's Last Theorem is not just an isolated historical curiosity. Instead, it lies at the heart of modern number theory.

Andrew Wiles

1953 –

Andrew Wiles was born in 1953 in Cambridge, England. At the age of 10 he read about Fermat's Last Theorem and resolved to become a mathematician and prove it. By the time of his PhD he had pretty much abandoned this idea, because the theorem seemed so intractable, so he worked on the number theory of 'elliptic curves', an apparently different area. He moved to the USA and became a Professor at Princeton.

By the 1980s it was becoming clear that there might be an unexpected link between Fermat's Last Theorem and a deep and difficult question about elliptic curves. Gerhard Frey made this link explicit, by means of the so-called Taniyama–Shimura conjecture. When Wiles heard of Frey's idea he stopped all of his other work to concentrate on Fermat's Last Theorem, and after seven years of solitary research he convinced himself that he had found a proof, based on a special case of the Taniyama–Shimura Conjecture. This proof turned out to have a gap, but Wiles and Richard Taylor repaired the gap and a complete proof was published in 1995.

Other mathematicians soon extended the ideas to prove the full Taniyama–Shimura Conjecture, pushing the new methods further. Wiles received many honours for his proof, including the Wolf Prize. In 1998, being just too old for a Fields Medal, traditionally limited to people under 40, he was awarded a special silver plaque by the International Mathematical Union. He was made a Knight Commander of the Order of the British Empire in 2000.

Andrew Wiles, as a child, had dreamed of proving Fermat's Last Theorem, but when he became a professional he decided that it was just an isolated problem – unsolved, but not really important.

Ribet's work changed his mind. In 1993 he announced a proof of the Taniyama–Weil conjecture for a special class of elliptic curves, general enough to prove Fermat's Last Theorem. But when the paper was submitted for publication, a serious gap emerged. Wiles had almost given up when 'suddenly, totally unexpectedly, I had this incredible revelation ... it was so indescribably beautiful, it was so simple and so elegant, and I just stared in disbelief.' With the aid of Richard Taylor, he revised the proof and repaired the gap. His paper was published in 1995.

We can be sure that whatever ideas Fermat had in mind when he claimed to possess a proof of his Last Theorem, they must have been very different from the methods used by Wiles. Did Fermat really have a simple, clever proof, or was he deluding himself? It is a puzzle that, unlike his Last Theorem, may never be resolved.

Abstract mathematics

The move towards a more abstract view of mathematics was a natural consequence of the growing variety of its subject matter. When mathematics was mostly about numbers, the symbols of algebra were simply placeholders for numbers. But as mathematics grew, the symbols themselves started to take on a life of their own. The meaning of the symbols became less significant than the rules by which those symbols could be manipulated. Even the rules were not sacred: the traditional laws of arithmetic, such as the commutative law, were not always appropriate in new contexts.

It was not only algebra that became abstract. Analysis and geometry also focused on more general issues, for similar reasons. The main change in viewpoint occurred from the middle of the 19th century to the middle of the 20th. After that, a period of consolidation set in, as mathematicians tried to balance the conflicting needs of abstract formalism and applications to science. Abstraction and generality go hand in hand, but abstraction can also

What abstract algebra does for us

Galois fields form the basis of a coding system that is widely used in a variety of commercial applications, especially CDs and DVDs. Every time you play music, or watch a video, you are using abstract algebra.

These methods are known as *Reed–Solomon* codes, after Irving Reed and Gustave Solomon who introduced them in 1960. They are error-correcting codes based on a polynomial, with coefficients in a finite field, constructed from the data being encoded, such as the music or video signals. It is known that a polynomial of degree n is uniquely determined by its values at n distinct points. The idea is to calculate the polynomial at more than n points. If there are no errors, any subset of n data points will reconstruct the same polynomial. If not, then provided the number of errors is not too large, it is still possible to deduce the polynomial.

In practice the data are represented as encoded blocks, with $2^m - 1$ m-bit symbols per block, where a bit is a binary digit, 0 or 1. A popular choice is $m = 8$, because many of the older computers work in bytes – sequences of eight bits. Here the number of symbols in a block is 255. One common Reed–Solomon code puts 223 bytes of encoded data in each 255 byte block, using the remaining 32 bytes for parity symbols which state whether certain combinations of digits in the data should be odd or even. This code can correct up to 16 errors per block.

obscure the meaning of mathematics. But the issue is no longer whether abstraction is useful or necessary: abstract methods have proved their worth by making it possible to solve numerous long-standing problems, such as Fermat's Last Theorem. And what seemed little more than formal game-playing yesterday may turn out to be a vital scientific or commercial tool tomorrow.

CHAPTER 15

Rubber Sheet Geometry

Qualitative beats quantitative

The main ingredients of Euclid's geometry – lines, angles, circles, squares and so on – are all related to *measurement*. Line segments have lengths, angles are a definite size with 90° differing in important ways from 91° or 89°, circles are defined in terms of their radii, squares have sides of a given length. The hidden ingredient that makes all of Euclid's geometry work is length, a metric quantity, one which is unchanged by rigid motions and defines Euclid's equivalent concept to motion, congruence.

Topology

When mathematicians first stumbled across other types of geometry, these too were metric. In non-Euclidean geometry, lengths and angles are defined; they just have different properties from lengths and angles in the Euclidean plane. The arrival of projective geometry changed this: projective transformations can change lengths, and they can change angles. Euclidean geometry and the two main kinds of non-Euclidean geometry are rigid. Projective geometry is more