1

What is a Galois field?

A *Galois field* is a field that has a finite number of elements. Such fields belong to the small quantity of the most fundamental mathematical objects that serve to describe all other mathematical structures and models.

Another example of such fundamental objects is the well-known prime numbers:

$$p = 2, 3, 5, 7, 11, 13, 17, 19, 23, \dots, 997, 1009, \dots;$$

these are the positive integers that each have only two integer divisors (namely 1 and the number itself). By convention we do not take the number 1 to be prime.

An immediate natural question, to which this notion leads, is already rather difficult: *is the set of all the primes finite*? In other words, can the above sequence of primes be continued indefinitely?

The answer to this question was discovered in antiquity: *the sequence of prime numbers is infinite*, i.e. there is no maximal prime number.

To prove it, assume the opposite, i.e. that there is a maximal prime p, and consider the number

$$(2 \times 3 \times 5 \times \cdots \times p) + 1 \,.$$

This has remainder (residue) 1 when we divide it by any prime number $2, 3, \dots, p$. This number (which is greater than p and so, by assumption, is not prime) is not, therefore, divisible by any of them. Hence, it has a prime divisor which is greater than p – a contradiction. Therefore, *there is no maximal prime number* p.

This remarkable mathematical result avoids the question that interests us, as scientists, most: *how often* are primes encountered in the sequence of all the natural numbers $\{1, 2, 3, 4, 5, 6, \dots\}$? Do the intervals between consecutive

prime numbers grow as the numbers we consider become large? What is the millionth prime expressed as a decimal number?

The first scientist to study this problem was Adrien Marie Legendre (1752–1833), who had considered (in the eighteenth century) tables of primes up to 10^6 and who had discovered empirically the following *law of the decline in density of the primes*: the average distance between consecutive prime numbers of order of n, grows with n like $\ln n$ (here, ln is the natural logarithm, which is the logarithm to the base $e \approx 2.71828\ldots$, where the 'Euler number' e is

$$e = \lim_{k\to\infty}\left(1+\frac{1}{k}\right)^k = \sum_{m=0}^{\infty}\frac{1}{m!}\,.$$

Thus, for example, $\ln 10 \approx 2.3$, and the average distance between consecutive primes close to 10 is slightly greater than 2, since

$$7-5=2\,,\ 11-7=4\,,\ 13-11=2\,.$$

The primes in the region of $n = 100$ are 89, 97, 101, 103, so their average separation is $4\frac{2}{3}$. This distance should be compared with $\ln 100 = 2\ln 10 \simeq 4.6$ from Legendre's law, and it is thus confirmed satisfactorily even for $n = 100$.

Of course, the existence of pairs of *twins* (that is, of prime pairs whose difference is 2, such as 5 and 7, 17 and 19, 29 and 31) contradicts the expected increasing separation of consecutive prime numbers, provided that the number of such twins is infinite, which is conjecturally true. (This conjecture is one of the most celebrated unproved statements of modern number theory.)

Unfortunately, Legendre's empirical observations were not appreciated by the mathematical community of the time, since 'he had proved nothing, but only considered some millions of examples'. It is true that he succeeded in 'deducing' his law from empirical statistical observations, but he was unable to provide a strict mathematical proof that in the asymptotic limit, as $n \to \infty$, the average distance between primes coincides with his proposed value of $\ln n$.

Kolmogorov said to me several times, concerning his studies on hydrodynamical turbulence: 'do not try to find in my works any theorem that proves the statements I make: I am unable to deduce them from the basic (Navier–Stokes) equations of hydrodynamics. My results on the solutions of these equations are not *proved*, but they are *true*, which is more important than all proofs.'

The first person who appreciated Legendre's discoveries was the Russian mathematician Tchebyshev. He first proved that even if the average distance between consecutive primes in the neighbourhood of a large number n does not behave asymptotically as $\ln n$, its relation to this Legendre value remains

bounded, i.e. the average distance lies between $c_1 \ln n$ and $c_2 \ln n$ (where $c_1 < c_2$ were explicitly calculated).

Later, he proved more: provided that any oscillations between the above limits would die out as n grows, implying that the average distance to the asymptotic value would be $c \ln n$ for some constant c, then *the constant* c *cannot be different from* 1.

This is not yet sufficient to *prove* the Legendre asymptotic formula, since there remains the possibility of non-vanishing oscillations between $c_1 \ln n$ and $c_2 \ln n$, therefore, never leading to the $c \ln n$ behaviour.

However, about 100 years after Legendre's discovery, two celebrated mathematicians, Hadamard (from France) and de la Vallée Poussin (from Belgium), proved that the oscillations do indeed die out for $n \to \infty$, yielding the $c \ln n$ asymptotic behaviour of the average distance between the consecutive primes in the neighbourhood of n.

The mathematical community claims, therefore, that Hadamard and de la Vallée Poussin made a great discovery concerning the distribution of large prime numbers.

It seems to me that this claim is rather unfair. These great mathematicians simply proved the *existence* of the distribution law.

Both 'scientific' facts, namely the asymptotic proportionality, to $\ln n$, of the average separation, and that the constant of proportionality equals 1, were discovered by Legendre and Tchebyshev, to whom one should attribute the great discovery of the law of distribution of primes described above.

In this book, therefore, I shall follow Legendre rather than Hadamard: I shall discuss empirical numerical observations that suggest some new (and astonishing) natural laws whose transformation to mathematical theorems might have to wait some hundred years (as happened in the case of the law of distribution of primes), despite the fact that the discovery of these new laws is quite within the reach of high-school students, even without the use of computers, although using computers might accelerate numerical experiments[†].

In addition to the prime numbers, another example of a fundamental mathematical object is provided by *regular polyhedra* (also called 'Platonic solids', even though Plato did not discover them). There are five such bodies: the tetrahedron (with 4 faces), the octahedron (with 8 faces), the cube (with 6 faces), the icosahedron (from the Greek 'icos' for its 20 faces) and the dodecahedron (from the Greek 'dodeca' for its 12 faces) – see Figure 1.1.

[†] I used no computers in the experiments that led me personally to the results below: my students, who verified that machines gave the same answers as I did, discovered that my calculations contained many fewer mistakes than those done by using computers.

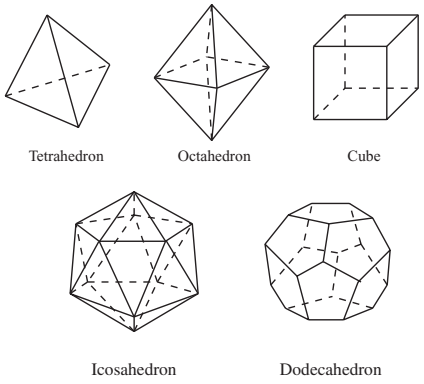

Figure 1.1 Regular polyhedra

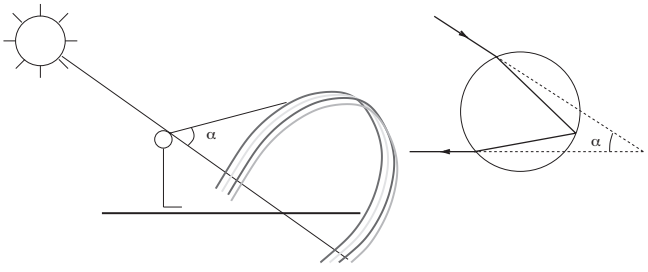

Figure 1.2 The origin of rainbows

The dodecahedron was used by Kepler to describe the orbital radius law of planets in the solar system.

The regular polyhedra are related in a strange way to a domain of physics which seems to be quite different – namely the theory of *optical caustics*, which provides, for instance, an explanation of the phenomenon that the angular radius of a rainbow is $\alpha = 42^\circ$, and describes how galaxies are concentrated at large scales in the universe.

Kolmogorov explained that the special beauty of mathematical theories is due to the way they reveal *unexpected relations between quite different natural phenomena* (say, between the theories of the electric and magnetic fields as described by Maxwell's equations).

In distinction to the fundamental objects in the examples above, the applications of Galois fields to the natural sciences are yet to be discovered. I hope that they will appear rather soon, and I would like to shorten the time till then by giving a geometric presentation of Galois field theory. My description is

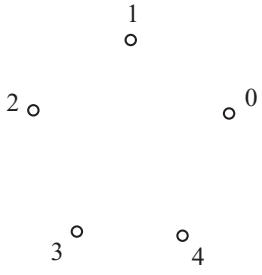

Figure 1.3 A finite circle: the Galois field $\mathbb{Z}_5$

closer to the scientific approach than to the axiomatic–algebraic superabstract style that dominates current presentations of this algebraic theory.

The simplest example of a Galois field is the field of residues modulo a prime number p (Figure 1.3).

Thus, for $p = 2$ we get the field consisting of two elements:

$$\mathbb{Z}_2 = \{0, 1\} ,$$

with its usual arithmetic

$$0 + 0 = 0 , \quad 0 + 1 = 1 + 0 = 1 , \quad 1 + 1 = 0 ,$$
$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0 , \quad 1 \cdot 1 = 1 .$$

This 'binary' arithmetic is the basis for calculating with computers, which use the binary system. Thus, the simplest Galois field is extremely useful:

$$(\text{the field } \mathbb{Z}_2) \implies (\text{computers}) .$$

The general notion of a field is very similar to this simple example: there are two operations (called 'addition' and 'multiplication'), having the usual properties of commutativity and associativity and satisfying the ordinary distributive law; and one can divide the elements of the field by any element of the field different from 0.

The residues after division by 3 form the field $\mathbb{Z}_3$, consisting of three elements $\{0, 1, 2\}$ (where $1/2 = 2$, since $2 \cdot 2 = 1$ for the residues modulo 3: $(3a + 2)(3b + 2) = 9ab + 6a + 6b + 4 = 3c + 1$).

On the other hand, the four residues after division of the integers by 4 do not form a field, since the element 2 cannot be inverted (the residue $2x$ is sometimes 0, sometimes 2, but it is different from 1, whatever the remainder x).

However, there does exist a field of four elements, though the operations are different from the above example. To find these operations is a useful exercise, one that is neither too difficult, nor too easy for a beginner.

The finite fields are called *Galois fields*, since Galois discovered the following two remarkable properties of them:

1. *The number of elements of a finite field is an integer of the form p^n, where p is a prime; and for any prime p and any natural number n there exists a finite field having just p^n elements.*

Thus, there exist fields with

$$2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27$$

elements, but there is no field with

$$6, 10, 12, 14, 15, 18, 20, 21, 22, 24, 26$$

elements.

2. *The field of p^n elements is defined unambiguously by the number of its elements (up to isomorphism).*

Thus, a computer using the field $\mathbb{Z}_2$ at Moscow, and another computer, working in Paris, might each use a different copy of this field. The Parisian might denote the elements of the field by α and β (instead of 0 and 1), and define the operations according to the table:

$$\alpha + \alpha = \beta + \beta = \beta\,, \quad \alpha + \beta = \beta + \alpha = \alpha\,,$$
$$\alpha \cdot \alpha = \alpha\,, \quad \alpha \cdot \beta = \beta \cdot \alpha = \beta \cdot \beta = \beta\,.$$

But this field is isomorphic to the Moscow field of residues $\mathbb{Z}_2$, differing only in the notation $\alpha \sim 1$ and $\beta \sim 0$. The fact that phenomena are independent of notation is a deep notion, one that is also at the foundation of relativity theory and so the whole of relativistic physics.

I shall not give here proofs of the above-formulated existence and uniqueness theorems for the field of p^n elements. *I shall instead describe, by explicit tabulation, the operations in this field*. Strangely, I have not seen in published form the science-oriented description of finite fields that I present below.

Every field contains the 0 element (zero), which has the property of not changing any element to which it is added. All the other elements of the field form *the multiplicative group of the field* (i.e. a group under multiplication) since each non-zero element can be inverted.

This group is always cyclic: there exists an element A of the field such that every non-zero element of the field has the form A^k, where $1 \le k \le p^n - 1$ for the field of p^n elements.

I shall not prove the cyclic property (though its proof is not too difficult), since this result adds to the theory only the following statement, loved

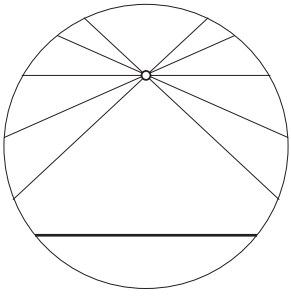

Figure 1.4 Lobachevsky plane

by axiomatisers: *the only finite fields are those with a cyclic multiplicative subgroup*.

In other words, we can consider the theory, explained below, as describing finite fields with an additional axiom: namely, the multiplicative group of the field is cyclic, or in other words a *primitive element* exists whose powers provide all the non-zero elements of the field.

The *absence of any different finite field* is a nice addition to this theory, but the theory itself does not depend on this additional property of our axioms.

It is worthwhile to observe that the exaggerated attention to the difficult study of the independence of axioms makes the algebraic and abstract theories of mathematicians unnecessarily hard and intimidating for scientists.

Thus, the *Lobachevsky plane* is simply the interior disc of the unit circle, whose interior points are called 'Lobachevsky points', and whose 'Lobachevsky lines' are chords of the unit circle. The boundary circle (which does not belong to the Lobachevsky plane) is called 'absolute'.

It is very easy to see that these objects (forming the so-called *Klein model* of the Lobachevsky plane – although, of course, they had been invented by A. Cayley) – satisfy all but one of the axioms of Euclidean geometry ('there exists one, and only one, line connecting two given points', etc.). The exception is the 'parallel axiom': *there exist an infinity of Lobachevsky lines going through a given Lobachevsky point and having no common Lobachevsky points with a given Lobachevsky line that does not contain the given Lobachevsky point* (that is, an infinity of chords, see Figure 1.4).

This list of obvious scientific facts can be completed by a (difficult) formal theorem: *there exists no Lobachevsky plane other than the Klein model described above*. Of course, this is true up to isomorphisms: the theorem states that the axioms for the Lobachevsky plane imply that this plane is isomorphic to the Klein model.

It is interesting that Lobachevsky was unable to prove his main and quite remarkable statement: *the parallelism axiom of Euclidean geometry is independent of the other axioms*; that is, it cannot be deduced from them.

The model described above (and invented many years after Lobachevsky worked) proved just this independence result.

Indeed, *if one could use the failure of the Euclidean parallels axiom to deduce a contradiction* (which contradiction would indeed prove the axiom), *then the model would also be false providing therefore a contradiction within the usual Euclidean geometry* (concerning the ordinary geometry of the chords of a circle).

The proofs of fundamental mathematical facts are, in many cases, much simpler than the formal details that make mathematics textbooks so difficult.

2

The organisation and tabulation of Galois fields

Multiplication in a Galois field that consists of n elements, 0 and $\{A^k\}$, $1 \le k \le n-1$, is simply the addition of the 'logarithms' k of the elements (where we consider these logarithms as the residues of the numbers k modulo $n-1$):

$$0 \cdot A^k = 0\,, \quad A^k \cdot A^\ell = A^{k+\ell};$$

if $k + \ell > n - 1$, one replaces the sum by $k + \ell - (n-1)$ to reduce the sum to a value smaller than n.

It remains to define the addition operation. Denoting the element A^k of the field by the sign k, we arrive at the following *tropical operation* $*$ over these logarithms:

$$A^k + A^\ell = A^{k*\ell}\,.$$

The modern term 'tropical', taken by me to mean 'exotic', is used when one lowers the level of the algebraic operations, transforming multiplication to addition, and replacing addition by the lower-level 'tropical addition' operation, with respect to which the normal addition is distributive, as is normal multiplication with respect to normal addition:

$$x(y+z) = xy + xz \quad \text{is replaced by} \quad x + (y * z) = (x+y) * (x+z)\,.$$

An example of such tropical addition is the operation $x * y = \max(x, y)$ for the real numbers. One can obtain this tropical operation from normal addition by using logarithms accompanied by the short wave asymptotic expansion of quantum mechanics, when the wave length h approaches 0. The relation

$$\frac{x *_h y}{h} = \ln(e^{x/h} + e^{y/h})$$

defines the tropical addition operation $*_h$, tending to $\max(x, y)$ as $h \to 0$.

While all these things are obvious, they imply a non-obvious 'tropical' conclusion: replacing multiplication and addition operations with their tropical versions (i.e. addition and maximum), one can transform many formulas and theorems of calculus (such as Fourier series theory) into their (non-evident) 'tropical' versions, providing interesting results in convex analysis and linear programming.

Consider for simplicity the case of the field F of $z = p^2$ elements. It contains the 'scalar' elements $1, 2 = 1 + 1, \dots$. Since this field is finite, one of the sums must coincide with the other. Hence, for some m, the sum of m 1s (equal to the difference of the coincident sums) equals 0 i.e. $m = 1 + \cdots + 1 = 0$. We shall suppose the number m to be the minimal value for which this statement is true.

We shall now prove that $m = p$. We will say that each element x is equivalent to any element of the form $x + 1 + \cdots + 1$, where the number of 1s is at most m. Each equivalence class consists of m elements, and these classes are disjoint. Therefore the number m of scalar elements is a divisor of the number p^2 of elements of the field. Thus, m is either p or p^2.

The second case is impossible. Consider the scalar element $x = 1 + \cdots + 1$ (p times). This element of the field of p^2 elements has no inverse element, since no integer of the form pq leaves the residue 1 when divided by p^2. Therefore, $x = 0$ and the number of scalars is thus $m = p$.

Consider the element 1 together with a primitive element A of our field. Adding each of them fewer than p times, we create the p^2 sums $uA + v1$. All these elements are different (otherwise we would obtain $A = (-v/u) \cdot 1$, and therefore all the elements of the field would be scalars, which is impossible, since the number of scalars is p, which is smaller than p^2).

Thus, the field of p^2 elements consists exactly of linear combinations $F = \{uA + v1\}$ with coefficients $u \in \mathbb{Z}_p$, $v \in \mathbb{Z}_p$.

In this sense we have distributed all the elements of the field in the form of a $p \times p$ square (or rather of the 'finite torus' $\mathbb{Z}_p^2$ of Figure 2.1, this being the 2-plane over the field $\mathbb{Z}_p$).

So we have filled the $z = p^2$ cells of this finite torus with the p^2 'logarithmic symbols' $\{\infty; 1, \dots, z - 1\}$, where the symbol k, which is a residue modulo $z - 1$, denotes the element A^k of the field F, the symbol ∞ representing[†] the zero element of the field.

This filling process provides a simple interpretation of the tropical operation $*$; namely, the sum of the elements of the field that correspond to the symbols

[†] During my lecture, the students suggested denoting $\ln 0$ by $-\infty$, but I kept the symbol ∞ since I do not know whether $A > 1$ in F.