

The way of mathematical thought is twofold: the mathematician first proceeds inductively from the particular to the general and then deductively from the general to the particular. Moreover, throughout its development, mathematics has shown two aspects—the conceptual and the computational—the symphonic interleaving of which forms one of the major aspects of the subject’s aesthetic.

Let us therefore begin with the first mathematical structure—numbers. By the Hellenistic times, mathematicians distinguished between two types of numbers: the *rational* numbers, namely those which could be written in the form $\frac{m}{n}$ for some integer m and some positive integer n , and those numbers representing the geometric magnitude of segments of the line, which today we call *real* numbers and which, in decimal notation, are written in the form $m.k_1k_2k_3\ldots$ where m is an integer and the k_i are digits. The fact that the set \mathbb{Q} of rational numbers is not equal to the set \mathbb{R} of real numbers was already noticed by the followers of the early Greek mathematician/mystic Pythagoras. On both sets of numbers we define operations of addition and multiplication which satisfy certain rules of manipulation. Isolating these rules as part of a formal system was a task first taken on in earnest by nineteenth-century British and German mathematicians. From their studies evolved the notion of a field, which will be basic to our considerations. However, since fields are not our primary object of study, we will delve only minimally into this fascinating notion. A serious consideration of field theory must be deferred to an advanced course in abstract algebra.

A nonempty set F together with two functions $F \times F \rightarrow F$, respectively called *addition* (as usual, denoted by $+$) and *multiplication* (as usual, denoted by \cdot or by concatenation), is a *field* if the following conditions are satisfied:

- (1) (*associativity of addition and multiplication*): $a + (b + c) = (a + b) + c$ and $a(bc) = (ab)c$ for all $a, b, c \in F$.
- (2) (*commutativity of addition and multiplication*): $a + b = b + a$ and $ab = ba$ for all $a, b \in F$.
- (3) (*distributivity of multiplication over addition*): $a(b + c) = ab + ac$ for all $a, b, c \in F$.

- (4) (*existence of identity elements for addition and multiplication*): There exist distinct elements of F , which we will denote by 0 and 1 respectively, satisfying $a + 0 = a$ and $a1 = a$ for all $a \in F$.
- (5) (*existence of additive inverses*): For each $a \in F$ there exists an element of F , which we will denote by $-a$, satisfying $a + (-a) = 0$.
- (6) (*existence of multiplicative inverses*): For each $0 \neq a \in F$ there exists an element of F , which we will denote by a^{-1} , satisfying $a^{-1}a = 1$.



With kind permission of the Archives of the Mathematisches Forschungsinstitut Oberwolfach (Weber, Dedekind, Kronecker and Steinitz).

The development of the abstract theory of fields is generally credited to the nineteenth-century German mathematician **Heinrich Weber**, based on earlier work by the German mathematicians **Richard Dedekind** and **Leopold Kronecker**. Another nineteenth-century mathematician, the British **Augustus De Morgan**, was among the first—along with French mathematician François Joseph Servois—to isolate the importance of such properties as associativity, distributivity, and so forth. The final axioms of a field are due to the twentieth-century German mathematician **Ernst Steinitz**.

Note that we did not assume that the elements $-a$ and a^{-1} are unique, though we will soon prove that in fact they are. If a and b are elements of a field F , we will follow the usual conventions by writing $a - b$ instead of $a + (-b)$ and $\frac{a}{b}$ instead of ab^{-1} . Moreover, if $0 \neq a \in F$ and if n is a positive integer, then na denotes the sum $a + \cdots + a$ (n summands) and a^n denotes the product $a \cdots a$ (n factors). If n is a negative integer, then na denotes $(-n)(-a)$ and a^n denotes $(a^{-1})^{-n}$. Finally, if $n = 0$ then na denotes the field element 0 and a^n denotes the field element 1. For $0 = a \in F$, we define $na = 0$ for all integers n and $a^n = 0$ for all positive integers n . The symbol 0^k is not defined for $k \leq 0$.

As an immediate consequence of the associativity and commutativity of addition, we see that the sum of any list a_1, \dots, a_n of elements of a field F is the same, no matter in which order we add them. We can therefore unambiguously write $a_1 + \cdots + a_n$. This sum is also often denoted by $\sum_{i=1}^n a_i$. Similarly, the product of these elements is the same, no matter in which order we multiply them. We can therefore unambiguously write $a_1 \cdots a_n$. This product is also often denoted by $\prod_{i=1}^n a_i$. Also, a simple inductive argument shows that multiplication distributes over arbitrary sums: if $a \in F$ and b_1, \dots, b_n is a list of elements of F then $a(\sum_{i=1}^n b_i) = \sum_{i=1}^n ab_i$.

We easily see that \mathbb{Q} and \mathbb{R} , with the usual addition and multiplication, are fields.

A subset G of a field F is a *subfield* if and only if it contains 0 and 1, is closed under addition and multiplication, and contains the additive and multiplicative inverses of all of its nonzero elements. Thus, for example, \mathbb{Q} is a subfield of \mathbb{R} . It is

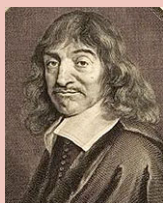
easy to verify¹ that the intersection of a collection of subfields of a field F is again a subfield of F .

We now want to look at several additional important examples of fields.

Example Let $\mathbb{C} = \mathbb{R}^2$ and define operations of addition and multiplication on \mathbb{C} by setting $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$. These operations define the structure of a field on \mathbb{C} , in which the identity element for addition is $(0, 0)$, the identity element for multiplication is $(1, 0)$, the additive inverse of (a, b) is $(-a, -b)$, and

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$$

for all $(0, 0) \neq (a, b)$. This field is called the field of *complex numbers*. The set of all elements of \mathbb{C} of the form $(a, 0)$ forms a subfield of \mathbb{C} , which we normally identify with \mathbb{R} and therefore it is standard to consider \mathbb{R} as a subfield of \mathbb{C} . In particular, we write a instead of $(a, 0)$ for any real number a . The element $(0, 1)$ of \mathbb{C} is denoted by i . This element satisfies the condition that $i^2 = (-1, 0)$ and so it is often written as $\sqrt{-1}$. We also note that any element (a, b) of \mathbb{C} can be written as $(a, 0) + b(0, 1) = a + bi$, and, indeed, that is the way complex numbers are usually written and how we will denote them from now on. If $z = a + bi$, then a is the *real part* of z , which is often denoted by $\operatorname{Re}(z)$, while bi is the *imaginary part* of z , which is often denoted by $\operatorname{Im}(z)$. The field of complex numbers is extremely important in mathematics. From a geometric point of view, if we identify \mathbb{R} with the set of points on the Euclidean line, as one does in analytic geometry, then it is natural to identify \mathbb{C} with the set of points in the Euclidean plane.



With kind permission of the Harvard Arts Museum (Descartes); With kind permission of ETH-Bibliothek Zurich, Image Archive (Euler); With kind permission of Bibliothèque nationale de France (Argand).

The term “imaginary” was coined by the seventeenth-century French philosopher and mathematician **René Descartes**. The use of i to denote $\sqrt{-1}$ was introduced by the eighteenth-century Swiss mathematician **Leonhard Euler**. The geometric representation of the complex numbers was first proposed at the end of the eighteenth century by the Norwegian surveyor Caspar Wessel, and later by the French accountant **Jean-Robert Argand**. It was studied in detail by the nineteenth-century Italian mathematician **Giusto Bellavitis**.

¹When a mathematician says that something is “easy to see” or “trivial”, it means that you are expected to take out a pencil and paper and spend some time—often considerable—checking it out by yourself.

If $z = a + bi \in \mathbb{C}$ then we denote the complex number $a - bi$, called the *complex conjugate* of z , by \bar{z} . It is easy to see that for all $z, z' \in \mathbb{C}$ we have $\overline{z + z'} = \bar{z} + \bar{z}'$, $\overline{-z} = -\bar{z}$, $\overline{zz'} = \bar{z} \cdot \bar{z}'$, $\overline{z^{-1}} = (\bar{z})^{-1}$, and $\overline{\bar{z}} = z$. The number $z\bar{z}$ equals $a^2 + b^2$, which is a nonnegative real number and so has a square root in \mathbb{R} , which we will denote by $|z|$. Note that $|z|$ is nonzero whenever $z \neq 0$. From a geometric point of view, this number is just the distance from the number z , considered as a point in the Euclidean plane, to the origin, just as the usual absolute value $|a|$ of a real number a is the distance between a and 0 on the real line. It is easy to see that if y and z are complex numbers then $|yz| = |y| \cdot |z|$ and $|y + z| \leq |y| + |z|$. Moreover, if $z = a + bi$ then

$$z + \bar{z} = 2a \leq 2|a| = 2\sqrt{a^2} \leq 2\sqrt{a^2 + b^2} = 2|z|.$$

We also note, as a direct consequence of the definition, that $|z| = |\bar{z}|$ for every complex number z and so $z^{-1} = |z|^{-2}\bar{z}$ for all $0 \neq z \in \mathbb{C}$. In particular, if $|z| = 1$ then $z^{-1} = \bar{z}$.

Example The set \mathbb{Q}^2 is a subfield of the field \mathbb{C} defined above. However, it is also possible to define field structures on \mathbb{Q}^2 in other ways. Indeed, let $F = \mathbb{Q}^2$ and let p be a fixed prime integer. Define addition and multiplication on F by setting $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) \cdot (c, d) = (ac + bdp, ad + bc)$.

Again, one can check that F is indeed a field and that, again, the set of all elements of F of the form $(a, 0)$ is a subfield, which we will identify with \mathbb{Q} . Moreover, the additive inverse of $(a, b) \in F$ is $(-a, -b)$ and the multiplicative inverse of $(0, 0) \neq (a, b) \in F$ is

$$\left(\frac{a}{a^2 - pb^2}, \frac{-b}{a^2 - pb^2} \right).$$

(We note that $a^2 - pb^2$ is the product of the nonzero real numbers $a + b\sqrt{p}$ and $a - b\sqrt{p}$ and so is nonzero.) The element $(0, 1)$ of F satisfies $(0, 1)^2 = (p, 0)$ and so one usually denotes it by \sqrt{p} and, as before, any element of F can be written in the form $a + b\sqrt{p}$, where $a, b \in \mathbb{Q}$. The field F is usually denoted by $\mathbb{Q}(\sqrt{p})$. Since there are infinitely-many distinct prime integers, we see that there are infinitely-many ways of defining different field structures on $\mathbb{Q} \times \mathbb{Q}$, all having the same addition.

Example Fields do not have to be infinite. Let p be a positive integer and let $\mathbb{Z}/(p) = \{0, 1, \dots, p-1\}$. For each nonnegative integer n , let us, for the purposes of this example, denote the remainder after dividing n by p as $[n]_p$. Thus we note that $[n]_p \in \mathbb{Z}/(p)$ for each nonnegative integer n and that $[i]_p = i$ for all $i \in \mathbb{Z}/(p)$. We now define operations on $\mathbb{Z}/(p)$ by setting $[n]_p + [k]_p = [n + k]_p$ and $[n]_p \cdot [k]_p = [nk]_p$. It is easy to check that if the integer p is prime then $\mathbb{Z}/(p)$, together with these two operations, is again a field, known as the *Galois field* of order p . This field is usually denoted by $\text{GF}(p)$. While Galois fields were first considered mathematical curiosities, they have since found important applications in coding theory, cryptography, and modeling of computer processes.

These are not the only possible finite fields. Indeed, it is possible to show that for each prime integer p and each positive integer n there exists an (essentially unique) field with p^n elements, usually denoted by $\text{GF}(p^n)$.



With kind permission of Bibliothèque nationale de France (Galois); With kind permission of the American Mathematical Society (Moore).

The nineteenth-century French mathematical genius **Evariste Galois**, who died at the age of 21, was the first to consider such structures. The study of finite and infinite fields was unified in the 1890s by **Eliakim Hastings Moore**, the first American-born mathematician to achieve an international reputation.

Example Some important structures are “very nearly” fields. For example, let $\mathbb{R}_\infty = \mathbb{R} \cup \{\infty\}$, and define operations \boxplus and \boxminus on \mathbb{R}_∞ by setting

$$a \boxplus b = \begin{cases} \min\{a, b\} & \text{if } a, b \in \mathbb{R}, \\ b & \text{if } a = \infty, \\ a & \text{if } b = \infty, \end{cases}$$

and

$$a \boxminus b = \begin{cases} a + b & \text{if } a, b \in \mathbb{R}, \\ \infty & \text{otherwise.} \end{cases}$$

This structure, called the *optimization algebra*, satisfies all of the conditions of a field *except* for the existence of additive inverses (such structures are known as *semi-fields*). As the name suggests, it has important applications in optimization theory and the analysis of discrete-event dynamical systems. There are several other semi-fields which have significant applications and which have been extensively studied.

Another possibility of generalizing the notion of a field is to consider an algebraic structure which satisfies all of the conditions of a field *except* for the existence of multiplicative inverses, and to replace that condition by the condition that if $a, b \neq 0$ then $ab \neq 0$. Such structures are known as *integral domains*. The set \mathbb{Z} of all integers is the simplest example of an integral domain which is not a field. Algebras of polynomials over a field, which we will consider later, are also integral domains. In a course in abstract algebra, one proves that any integral domain can be embedded in a field.

In the field $\text{GF}(p)$ which we defined above, one can easily see that the sum $1 + \cdots + 1$ (p summands) equals 0. On the other hand, in the field \mathbb{Q} , the sum of any number of copies of 1 is always nonzero. This is an important distinction which we will need to take into account in dealing with structures over fields. We therefore define the *characteristic* of a field F to be equal to the smallest positive integer p such that $1 + \cdots + 1$ (p summands) equals 0—if such an integer p exists—and to be

equal to 0 otherwise. We will not delve deeply into this concept, which is dealt with in courses on field theory, except to note that the characteristic of a field, if nonzero, always turns out to be a prime number, as we shall prove below.

In the definition of a field, we posited the existence of distinct identity elements for addition and multiplication, but did not claim that these elements were unique. It is, however, very easy to prove that fact.

Proposition 2.1 *Let F be a field.*

- (1) *If e is an element of F satisfying $e + a = a$ for all $a \in F$ then $e = 0$;*
- (2) *If u is an element of F satisfying $ua = a$ for all $a \in F$ then $u = 1$.*

Proof By definition, $e = e + 0 = 0$ and $u = u1 = 1$. □

Similarly, we prove that additive and multiplicative inverses, when they exist, are unique. Indeed, we can prove a stronger result.

Proposition 2.2 *If a and b are elements of a field F then:*

- (1) *There exists a unique element c of F satisfying $a + c = b$.*
- (2) *If $a \neq 0$ then there exists a unique element d of F satisfying $ad = b$.*

Proof (1) Choose $c = b - a$. Then

$$\begin{aligned} a + c &= a + (b - a) = a + [b + (-a)] \\ &= a + [(-a) + b] = [a + (-a)] + b = 0 + b = b. \end{aligned}$$

Moreover, if $a + x = b$ then

$$\begin{aligned} x &= 0 + x = [(-a) + a] + x \\ &= (-a) + (a + x) = (-a) + b = b - a, \end{aligned}$$

proving uniqueness.

(2) Choose $d = a^{-1}b$. Then $ad = a(a^{-1}b) = (aa^{-1})b = 1b = b$. Moreover, if $ay = b$ then $y = 1y = (a^{-1}a)y = a^{-1}(ay) = a^{-1}b$, proving uniqueness. □

We now summarize some of the elementary properties of fields, which are all we will need for our discussion.

Proposition 2.3 *If a, b , and c are elements of a field F then:*

- (1) $0a = 0$;
- (2) $(-1)a = -a$;
- (3) $a(-b) = -(ab) = (-a)b$;
- (4) $-(-a) = a$;
- (5) $(-a)(-b) = ab$;
- (6) $-(a + b) = (-a) + (-b)$;
- (7) $a(b - c) = ab - ac$;
- (8) *If $a \neq 0$ then $(a^{-1})^{-1} = a$;*
- (9) *If $a, b \neq 0$ then $(ab)^{-1} = b^{-1}a^{-1}$;*
- (10) *If $a + c = b + c$ then $a = b$;*
- (11) *If $c \neq 0$ and $ac = bc$ then $a = b$;*
- (12) *If $ab = 0$ then $a = b$ or $b = 0$.*

Proof (1) Since $0a + 0a = (0 + 0)a = 0a$, we can add $-(0a)$ to both sides of the equation to obtain $0a = 0$.

(2) Since $(-1)a + a = (-1)a + 1a = [(-1) + 1]a = 0a = 0$ and also $(-a) + a = 0$, we see from Proposition 2.2 that $(-1)a = -a$.

(3) By (2) we have $a(-b) = a[(-1)b] = (-1)ab = -(ab)$ and similarly $(-a)b = -(ab)$.

(4) Since $a + (-a) = 0 = -(-a) + (-a)$, this follows from Proposition 2.2.

(5) From (3) and (4) it follows that $(-a)(-b) = a[-(-b)] = ab$.

(6) Since $(a + b) + [(-a) + (-b)] = a + b + (-a) + (-b) = 0$ and $(a + b) + [-(a + b)] = 0$, the result follows from Proposition 2.2.

(7) By (3) we have $a(b - c) = ab + a(-c) = ab + [-(ac)] = ab - ac$.

(8) Since $(a^{-1})^{-1}a^{-1} = 1 = aa^{-1}$, this follows from Proposition 2.2.

(9) Since $(a^{-1}b^{-1})(ba) = a^{-1}ab^{-1}b = 1 = (ab)^{-1}(ba)$, the result follows from Proposition 2.2.

(10) This is an immediate consequence of adding $-c$ to both sides of the equation.

(11) This is an immediate consequence of multiplying both sides of the equation by c^{-1} .

(12) If $b = 0$ we are done. If $b \neq 0$ then by (1) it follows that multiplying both sides of the equation by b^{-1} will yield $a = 0$. \square

The following two propositions are immediate consequences of Proposition 2.3.

Proposition 2.4 *Let a be a nonzero element of a finite field F having q elements. Then $a^{-1} = a^{q-2}$.*

Proof If $q = 2$ then $F = \text{GF}(2)$ and $a = 1$, so the result is immediate. Hence we can assume $q > 2$. Let $B = \{a_1, \dots, a_{q-1}\}$ be the nonzero elements of F , written in some arbitrary order. Then $aa_i \neq aa_h$ for $i \neq h$ since, were they equal,

we would have $a_i = a^{-1}(aa_i) = a^{-1}(aa_h) = a_h$. Therefore $B = \{aa_1, \dots, aa_{q-1}\}$ and so $\prod_{i=1}^{q-1} a_i = \prod_{i=1}^{q-1} (aa_i) = a^{q-1} [\prod_{i=1}^{q-1} a_i]$. Moreover, this is a product of nonzero elements of F and so, by Proposition 2.3(12), is also nonzero. Therefore, by Proposition 2.3(11), $1 = a^{q-1}$, and so $aa^{-1} = 1 = a^{q-1} = a(a^{q-2})$, implying that $a^{-1} = a^{q-2}$. \square

Proposition 2.5 *If F is a field having characteristic $p > 0$, then p is prime.*

Proof Assume that p is not prime. Then $p = hk$, where $0 < h, k < p$. Therefore, $a = h1_F$ and $b = k1_F$ are nonzero elements of F . But $ab = (hk)1_F = p1_F = 0$, contradicting Proposition 2.3(12). \square

Of course, one can use Proposition 2.3 to prove many other identities among elements of a field. A typical example is the following

Proposition 2.6 (Hua's identity) *If a and b are nonzero elements of a field F satisfying $a \neq b^{-1}$ then*

$$a - aba = (a^{-1} + [b^{-1} - a]^{-1})^{-1}.$$

Proof We note that

$$\begin{aligned} a^{-1} + (b^{-1} - a)^{-1} &= a^{-1}[(b^{-1} - a) + a](b^{-1} - a)^{-1} \\ &= a^{-1}b^{-1}(b^{-1} - a)^{-1}, \end{aligned}$$

so $(a^{-1} + [b^{-1} - a]^{-1})^{-1} = (b^{-1} - a)ba = a - aba$. \square



Loo-Keng Hua was a major twentieth-century Chinese mathematician.

Exercises

Exercise 1

Let F be a field and let $G = F \times F$. Define operations of addition and multiplication on G by setting $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) \cdot (c, d) = (ac, bd)$. Do these operations define the structure of a field on G ?

Exercise 2

Let K be the set of the following four-tuples of elements of $\text{GF}(3)$:

$$(0, 0, 0, 0), (1, 2, 1, 1), (2, 1, 2, 2), (1, 0, 0, 1), (2, 2, 1, 2), \\ (2, 0, 0, 2), (0, 1, 2, 0), (0, 2, 1, 0), (1, 1, 2, 1).$$

Define operations of addition and multiplication on K so that it becomes a field.

Exercise 3

Let $r \in \mathbb{R}$ and let $0 \neq s \in \mathbb{R}$. Define operations \boxplus and \boxtimes on $\mathbb{R} \times \mathbb{R}$ by $(a, b) \boxplus (c, d) = (a + c, b + d)$ and $(a, b) \boxtimes (c, d) = (ac - bd(r^2 + s^2), ad + bc + 2rbd)$. Do these operations, considered as addition and multiplication, respectively, define the structure of a field on $\mathbb{R} \times \mathbb{R}$?

Exercise 4

Define a new operation \dagger on \mathbb{R} by setting $a \dagger b = a^3b$. Show that \mathbb{R} , on which we have the usual addition and this new operation as multiplication, satisfies all of the axioms of a field with the exception of one.

Exercise 5

Let $1 < t \in \mathbb{R}$ and let $F = \{a \in \mathbb{R} \mid a < 1\}$. Define operations \oplus and \odot on F as follows:

- (1) $a \oplus b = a + b - ab$ for all $a, b \in F$;
- (2) $a \odot b = 1 - t^{\log_t(1-a)\log_t(1-b)}$ for all $a, b \in F$.

For which values of t does F , together with these operations, form a field?

Exercise 6

Show that the set of all real numbers of the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, where $a, b, c, d \in \mathbb{Q}$, forms a subfield of \mathbb{R} .

Exercise 7

Is $\{a + b\sqrt{15} \mid a, b \in \mathbb{Q}\}$ a subfield of \mathbb{R} ?

Exercise 8

Show that the field \mathbb{R} has infinitely-many distinct subfields.

Exercise 9

Let F be a field and define a new operation $*$ on F by setting $a * b = a + b + ab$. When is $(F, +, *)$ a field?

Exercise 10

Let F be a field and let G_n be the subset of F consisting of all elements which can be written as a sum of n squares of elements of F .

- (1) Is the product of two elements of G_2 again an element of G_2 ?
- (2) Is the product of two elements of G_4 again an element of G_4 ?

Exercise 11

Let $t = \sqrt[3]{2} \in \mathbb{R}$ and let S be the set of all real numbers of the form $a + bt + ct^2$, where $a, b, c \in \mathbb{Q}$. Is S a subfield of \mathbb{R} ?

Exercise 12

Let F be a field. Show that the function $a \mapsto a^{-1}$ is a permutation of $F \setminus \{0_F\}$.

Exercise 13

Show that every $z \in \mathbb{C}$ satisfies

$$z^4 + 4 = (z - 1 - i)(z - i + i)(z + 1 + i)(z + 1 - i).$$

Exercise 14

In each of the following, find the set of all complex numbers $z = a + bi$ satisfying the given relation. Note that this set may be empty or may be all of \mathbb{C} . Justify your result in each case.

- (a) $z^2 = \frac{1}{2}(1 + i\sqrt{3})$;
- (b) $(\sqrt{2})|z| \geq |a| + |b|$;
- (c) $|z| + z = 2 + i$;
- (d) $z^4 = 2 - (\sqrt{12})i$;
- (e) $z^4 = -4$.

Exercise 15

Let y be a complex number satisfying $|y| < 1$. Find the set of all complex numbers z satisfying $|z - y| \leq |1 - \bar{y}z|$.

Exercise 16

Let z_1, z_2 , and z_3 be complex numbers satisfying the condition that $|z_i| = 1$ for $i = 1, 2, 3$. Show that $|z_1z_2 + z_1z_3 + z_2z_3| = |z_1 + z_2 + z_3|$.

Exercise 17

For any $z_1, z_2 \in \mathbb{C}$, show that $|z_1|^2 + |z_2|^2 - z_1\bar{z}_2 - \bar{z}_1z_2 = |z_1 - z_2|^2$.

Exercise 18

Show that $|z + 1| \leq |z + 1|^2 + |z|$ for all $z \in \mathbb{C}$.

Exercise 19

If $z \in \mathbb{C}$, find $w \in \mathbb{C}$ satisfying $w^2 = z$.

Exercise 20

Define new operations \circ and \diamond on \mathbb{C} by setting $y \circ z = |y|z$ and

$$y \diamond z = \begin{cases} 0 & \text{if } y = 0, \\ \frac{1}{|y|}yz & \text{otherwise} \end{cases}$$

for all $y, z \in \mathbb{C}$. Is it true that $w \diamond (y \circ z) = (w \diamond y) \circ (w \diamond z)$ and $w \circ (y \diamond z) = (w \circ y) \diamond (w \circ z)$ for all $w, y, z \in \mathbb{C}$?

Exercise 21

Let $0 \neq z \in \mathbb{C}$. Show that there are infinitely-many complex numbers y satisfying the condition $y\bar{y} = z\bar{z}$.

Exercise 22

(Abel's inequality) Let z_1, \dots, z_n be a list of complex numbers and, for each $1 \leq k \leq n$, let $s_k = \sum_{i=1}^k z_i$. For real numbers a_1, \dots, a_n satisfying $a_1 \geq a_2 \geq \dots \geq a_n \geq 0$, show that $|\sum_{i=1}^n a_i z_i| \leq a_1(\max_{1 \leq k \leq n} |s_k|)$.



With kind permission of the Archives of the Mathematisches Forschungsinstitut Oberwolfach.

The nineteenth-century Norwegian mathematical genius **Niels Henrik Abel** died tragically at the age of 26.

Exercise 23

Let $0 \neq z_0 \in \mathbb{C}$ satisfy the condition $|z_0| < 2$. Show that there are precisely two complex numbers, z_1 and z_2 , satisfying $|z_1| + |z_2| = 1$ and $z_1 + z_2 = z_0$.

Exercise 24

If p is a prime positive integer, find all subfields of $\text{GF}(p)$.

Exercise 25

Find 10^{-1} in $\text{GF}(33)$.

Exercise 26

Find elements $c, d \neq \pm 1$ in the field $\mathbb{Q}(\sqrt{5})$ satisfying $cd = 19$.

Exercise 27

Let F be the set of all real numbers of the form

$$a + b(\sqrt[3]{5}) + c(\sqrt[3]{5})^2,$$

where $a, b, c \in \mathbb{Q}$. Is F a subfield of \mathbb{R} ?

Exercise 28

Let p be a prime positive integer and let $a \in \text{GF}(p)$. Does there necessarily exist an element b of $\text{GF}(p)$ satisfying $b^2 = a$?

Exercise 29

Let $F = \text{GF}(11)$ and let $G = F \times F$. Define operations of addition and multiplication on G by setting $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) \cdot (c, d) = (ac + 7bd, ad + bc)$. Do these operations define the structure of a field on G ?

Exercise 30

Let F be a field and let G be a finite subset of $F \setminus \{0\}$ containing 1 and satisfying the condition that if $a, b \in F$ then $ab^{-1} \in G$. Show that there exists an element $c \in G$ such that $G = \{c^i \mid i \geq 0\}$.

Exercise 31

Let F be a field satisfying the condition that the function $a \mapsto a^2$ is a permutation of F . What is the characteristic of F ?

Exercise 32

Is $\mathbb{Z}/(6)$ an integral domain?

Exercise 33

Let $F = \{a + b\sqrt{5} \in \mathbb{Q}(\sqrt{5}) \mid a, b \in \mathbb{Z}\}$. Is F an integral domain?

Exercise 34

Let F be an integral domain and let $a \in F$ satisfy $a^2 = a$. Show that $a = 0$ or $a = 1$.

Exercise 35

Let a be a nonzero element in an integral domain F . If $b \neq c$ are distinct elements of F , show that $ab \neq ac$.

Exercise 36

Let F be an integral domain and let G be a nonempty subset of F containing 0 and 1 and closed under the operations of addition and multiplication in F . Is G necessarily an integral domain?

Exercise 37

Let U be the set of all positive integers and let F be the set of all functions from U to \mathbb{C} . Define operations of addition and multiplication on F by setting

$f + g : k \mapsto f(k) + g(k)$ and $fg : k \mapsto \sum_{i,j=k} f(i)g(j)$ for all $k \in U$. Is F , together with these operations, an integral domain? Is it a field?

Exercise 38

Let F be the set of all functions f from \mathbb{R} to itself of the form $f : t \mapsto \sum_{k=1}^n [a_k \cos(kt) + b_k \sin(kt)]$, where the a_k and b_k are real numbers and n is some positive integer. Define addition and multiplication on F by setting $f + g : t \mapsto f(t) + g(t)$ and $fg : t \mapsto f(t)g(t)$ for all $t \in \mathbb{R}$. Is F , together with these operations, an integral domain? Is it a field?

Exercise 39

Show that every integral domain having only finitely-many elements is a field.

Exercise 40

Let F be a field of characteristic other than 2 in which there exist elements a_1, \dots, a_n satisfying $\sum_{i=1}^n a_i^2 = -1$. (This happens, for example, in the case $F = \mathbb{C}$.) Show that for any $c \in F$ there exist elements b_1, \dots, b_k of F satisfying $c = \sum_{i=1}^k b_i^2$.

Exercise 41

Let p be a prime integer. Show that for each $a \in \text{GF}(p)$ there exist elements b and c of $\text{GF}(p)$, not necessarily distinct, satisfying $a = b^2 + c^2$.

Exercise 42

Let F be a field in which we have elements a, b , and c (not necessarily distinct) satisfying $a^2 + b^2 + c^2 = -1$. Show that there exist (not necessarily distinct) elements d and e of F , satisfying $d^2 + e^2 = -1$.

Exercise 43

Is every nonzero element of the field $\text{GF}(5)$ in the form 2^i for some positive integer i ? What happens in the case of the field $\text{GF}(7)$?

Exercise 44

Find the set of all fields F in which there exists an element a satisfying the condition that $a + b = a$ for all $b \in F \setminus \{a\}$.

Exercise 45

(Binomial formula) If a and b are elements of a field F , and if n is a positive integer, show that $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$.

Exercise 46

Let F be a field of characteristic $p > 0$. Show that the function $\gamma : F \rightarrow F$ defined by $\gamma : a \mapsto a^p$ is monic.

Exercise 47

Let a and b be nonzero elements of a finite field F , and let m and n be positive integers satisfying $a^m = b^n = 1$. Show that there exists a nonzero element c of F satisfying $c^k = 1$, where k is the least common multiple of m and n .

Exercise 48

If a is a nonzero element of a field F , show that $(-a)^{-1} = -(a^{-1})$.

Exercise 49

Let $F = \text{GF}(7)$ and let $K = F \times F$. Define addition and multiplication on K by setting $(a, b) + (c, d) = (a + b, c + d)$ and $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$. Do these operations turn K into a field? What happens if $F = \text{GF}(5)$?

Exercise 50

A field F is *orderable* if and only if there exists a subset P closed under addition and multiplication such that for each $a \in F$ precisely one of the following conditions holds: (i) $a = 0$; (ii) $a \in P$; (iii) $-a \in P$. Show that $\text{GF}(5)$ is not orderable.

Exercise 51

Let F be a field and let K be the set of all functions $f \in F^{\mathbb{Z}}$ satisfying the condition that there exists an integer (perhaps negative) n_f such that $f(i) = 0$ for all $i < n_f$. Define operations of addition and multiplication on K by setting $f + g : i \mapsto f(i) + g(i)$ and $fg : i \mapsto \sum_{j+h=i} f(j)g(h)$. Show that K is a field, called the *field of formal Laurent series* over F .²

Exercise 52

Let F be a field. Find $A = \{(x, y) \in F^2 \mid x^2 + y^2 = 1\}$.

Exercise 53

Let F be a field having characteristic $p > 0$ and let $c \in F$. Show that there is at most one element b of F satisfying $b^p = c$.

Exercise 54

A *ternary ring* is a set R containing distinguished elements 0 and 1, together with a function $\theta : R^3 \rightarrow R$ satisfying the following conditions:

- (1) $\theta(1, a, 0) = \theta(a, 1, 0) = a$ for all $a \in R$;
- (2) $\theta(a, 0, c) = \theta(0, a, c) = c$ for all $c \in R$;
- (3) If $a, b, c \in R$ then there is a unique element y of R satisfying $\theta(a, b, y) = c$;
- (4) If $a, a', b, b' \in R$ with $a \neq a'$ then there is a unique element x of R satisfying $\theta(x, a, b) = \theta(x, a', b')$;
- (5) If $a, a', b, b' \in R$ with $a \neq a'$ then there are unique elements x and y of R satisfying $\theta(a, x, y) = b$ and $\theta(a', x, y) = b'$.

²These series were first studied by the nineteenth-century French engineer and mathematician, **Pierre Alphonse Laurent**.

Such structures have applications in projective geometry. If F is a field, show that we can define a function $\theta : F^3 \rightarrow F$ in such a way that F becomes a tertiary ring (with 0 and 1 being the neutral elements of the field).

Exercise 55

For $h = 1, 2, 3$, let $z_h = a_h + b_h i$ be a complex number satisfying $|z_h| = 1$. Assume, moreover, that $\sum_{i=1}^3 z_i = 0$. Show that the points (a_h, b_h) are the vertices of an equilateral triangle in the Euclidean plane.

The Linear Algebra a Beginning Graduate Student
Ought to Know

Golan, J.S.

2012, XI, 497 p. 199 illus., Softcover

ISBN: 978-94-007-2635-2