CHAPTER 28 FIELDS

Throughout this book a conscientious attempt has been made to define all important concepts, even terms like "function," for which an intuitive definition is often considered sufficient. But **Q** and **R**, the two main protagonists of this story, have only been named, never defined. What has never been defined can never be analyzed thoroughly, and "properties" P1–P13 must be considered assumptions, not theorems, about numbers. Nevertheless, the term "axiom" has been purposely avoided, and in this chapter the logical status of P1–P13 will be scrutinized more carefully.

Like **Q** and **R**, the sets **N** and **Z** have also remained undefined. True, some talk about all four was inserted in Chapter 2, but those rough descriptions are far from a definition. To say, for example, that **N** consists of 1, 2, 3, etc., merely names some elements of **N** without identifying them (and the "etc." is useless). The natural numbers *can* be defined, but the procedure is involved and not quite pertinent to the rest of the book. The Suggested Reading list contains references to this problem, as well as to the other steps that are required if one wishes to develop calculus from its basic logical starting point. The further development of this program would proceed with the definition of **Z**, in terms of **N**, and the definition of **Q** in terms of **Z**. This program results in a certain well-defined set **Q**, certain explicitly defined operations $+$ and $\cdot$, and properties P1–P12 as *theorems*. The final step in this program is the construction of **R**, in terms of **Q**. It is this last construction which concerns us. Assuming that **Q** has been defined, and that P1–P12 have been proved for **Q**, we shall ultimately *define* **R** and *prove* all of P1–P13 for **R**.

Our intention of proving P1–P13 means that we must define not only real numbers, but also addition and multiplication of real numbers. Indeed, the real numbers are of interest only as a set together with these operations: how the real numbers behave with respect to addition and multiplication is crucial; what the real numbers may actually be is quite irrelevant. This assertion can be expressed in a meaningful mathematical way, by using the concept of a "field," which includes as special cases the three important number systems of this book. This extraordinarily important abstraction of modern mathematics incorporates the properties P1–P9 common to **Q**, **R**, and **C**. A **field** is a set F (of objects of any sort whatsoever), together with two "binary operations" $\boldsymbol{+}$ and $\bullet$ defined on F (that is, two rules which associate to elements a and b in F, other elements $a \boldsymbol{+} b$ and $a \bullet b$ in F) for which the following conditions are satisfied:

(1) $(a \boldsymbol{+} b) \boldsymbol{+} c = a \boldsymbol{+} (b \boldsymbol{+} c)$ for all a, b, and c in F.

(2) There is some element $\mathbf{0}$ in F such that

- (i) $a \boldsymbol{+} \mathbf{0} = a$ for all a in F,
- (ii) for every a in F, there is some element b in F such that $a \boldsymbol{+} b = \mathbf{0}$.

(3) $a \boldsymbol{+} b = b \boldsymbol{+} a$ for all a and b in F.
(4) $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ for all a, b, and c in F.
(5) There is some element $\mathbf{1}$ in F such that $\mathbf{1} \neq \mathbf{0}$ and

  (i) $a \bullet \mathbf{1} = a$ for all a in F,
  (ii) For every a in F with $a \neq \mathbf{0}$, there is some element b in F such that $a \bullet b = \mathbf{1}$.

(6) $a \bullet b = b \bullet a$ for all a and b in F.
(7) $a \bullet (b \boldsymbol{+} c) = a \bullet b \boldsymbol{+} a \bullet c$ for all a, b, and c in F.

The familiar examples of fields are, as already indicated, **Q**, **R**, and **C**, with $\boldsymbol{+}$ and $\bullet$ being the familiar operations of $+$ and $\cdot$. It is probably unnecessary to explain why these are fields, but the explanation is, at any rate, quite brief. When $\boldsymbol{+}$ and $\bullet$ are understood to mean the ordinary $+$ and $\cdot$, the rules (1), (3), (4), (6), (7) are simply restatements of P1, P4, P5, P8, P9; the elements which play the role of $\mathbf{0}$ and $\mathbf{1}$ are the numbers 0 and 1 (which accounts for the choice of the symbols $\mathbf{0}$, $\mathbf{1}$); and the number b in (2) or (5) is $-a$ or a^{-1}, respectively. (For this reason, in an arbitrary field F we denote by $\boldsymbol{-a}$ the element such that $a \boldsymbol{+} (\boldsymbol{-a}) = \mathbf{0}$, and by $a^{\mathbf{-1}}$ the element such that $a \bullet a^{\mathbf{-1}} = \mathbf{1}$, for $a \neq \mathbf{0}$.)

In addition to **Q**, **R**, and **C**, there are several other fields which can be described easily. One example is the collection F_1 of all numbers $a + b\sqrt{2}$ for a, b in **Q**. The operations $\boldsymbol{+}$ and $\bullet$ will, once again, be the usual $+$ and $\cdot$ for real numbers. It is necessary to point out that these operations really do produce new elements of F_1:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}, \quad \text{which is in } F_1;$$
$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2}, \quad \text{which is in } F_1.$$

Conditions (1), (3), (4), (6), (7) for a field are obvious for F_1: since these hold for all real numbers, they certainly hold for all real numbers of the form $a + b\sqrt{2}$. Condition (2) holds because the number $0 = 0 + 0\sqrt{2}$ is in F_1 and, for $\alpha = a + b\sqrt{2}$ in F_1 the number $\beta = (-a) + (-b)\sqrt{2}$ in F_1 satisfies $\alpha + \beta = 0$. Similarly, $1 = 1 + 0\sqrt{2}$ is in F_1, so (5i) is satisfied. The verification of (5ii) is the only slightly difficult point. If $a + b\sqrt{2} \neq 0$, then

$$a + b\sqrt{2} \cdot \frac{1}{a + b\sqrt{2}} = 1;$$

it is therefore necessary to show that $1/(a + b\sqrt{2})$ is in F_1. This is true because

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a - b\sqrt{2})(a + b\sqrt{2})} = \frac{a}{a^2 - 2b^2} + \frac{(-b)}{a^2 - 2b^2}\sqrt{2}.$$

(The division by $a - b\sqrt{2}$ is valid because the relation $a - b\sqrt{2} = 0$ could be true only if $a = b = 0$ (since $\sqrt{2}$ is irrational) which is ruled out by the hypothesis $a + b\sqrt{2} \neq 0$.)

The next example of a field, F_2, is considerably simpler in one respect: it contains only two elements, which we might as well denote by $\mathbf{0}$ and $\mathbf{1}$. The operations an ordered field: let **P** be the set of all $a + b\sqrt{2}$ which are positive real numbers (in the ordinary sense). The field F_3 can also be made into an ordered field; the description of **P** is left to you.

It is natural to introduce notation for an arbitrary ordered field which corresponds to that used for **Q** and **R**: we define

$$\begin{array}{lll} a > b & \text{if} & a - b \text{ is in } \mathbf{P}, \\ a < b & \text{if} & b > a, \\ a \leq b & \text{if} & a < b \text{ or } a = b, \\ a \geq b & \text{if} & a > b \text{ or } a = b. \end{array}$$

Using these definitions we can reproduce, for an arbitrary ordered field F, the definitions of Chapter 7:

> A set A of elements of F is **bounded above** if there is some x in F such that $x \geq a$ for all a in A. Any such x is called an **upper bound** for A. An element x of F is a **least upper bound** for A if x is an upper bound for A and $x \leq y$ for every y in F which is an upper bound for A.

Finally, it is possible to state an analogue of property P13 for **R**; this leads to the last abstraction of this chapter:

> A **complete ordered field** is an ordered field in which every nonempty set which is bounded above has a least upper bound.

The consideration of fields may seem to have taken us far from the goal of constructing the real numbers. However, we are now provided with an intelligible means of formulating this goal. There are two questions which will be answered in the remaining two chapters:

1. Is there a complete ordered field?
2. Is there only one complete ordered field?

Our starting point for these considerations will be **Q**, assumed to be an ordered field, containing **N** and **Z** as certain subsets. At one crucial point it will be necessary to assume another fact about **Q**:

> Let x be an element of **Q** with $x > 0$. Then for any y in **Q** there is some n in **N** such that $nx > y$.

This assumption, which asserts that the rational numbers have the Archimedean property of the real numbers, does not follow from the other properties of an ordered field (for the example that demonstrates this conclusively see reference [14] of the Suggested Reading). The important point for us is that when **Q** is explicitly constructed, properties P1–P12 appear as theorems, and so does this additional

$\mathbf{+}$ and $\boldsymbol{\cdot}$ are described by the following tables.

$\mathbf{+}$	**0**	**1**
0	**0**	**1**
1	**1**	**0**

$\boldsymbol{\cdot}$	**0**	**1**
0	**0**	**0**
1	**0**	**1**

The verification of conditions (1)–(7) are straightforward, case-by-case checks. For example, condition (1) may be proved by checking the 8 equations obtained by setting $a, b, c = \mathbf{0}$ or $\mathbf{1}$. Notice that in this field $\mathbf{1} \mathbf{+} \mathbf{1} = \mathbf{0}$; this equation may also be written $\mathbf{1} = \mathbf{-1}$.

Our final example of a field is rather silly: F_3 consists of all pairs (a, a) for a in $\mathbf{R}$, and $\mathbf{+}$ and $\boldsymbol{\cdot}$ are defined by

$$(a, a) \mathbf{+} (b, b) = (a + b, a + b),$$
$$(a, a) \boldsymbol{\cdot} (b, b) = (a \cdot b, a \cdot b).$$

(The $+$ and $\cdot$ appearing on the right side are ordinary addition and multiplication for $\mathbf{R}$.) The verification that F_3 is a field is left to you as a simple exercise.

A detailed investigation of the properties of fields is a study in itself, but for our purposes, fields provide an ideal framework in which to discuss the properties of numbers in the most economical way. For example, the consequences of P1–P9 which were derived for "numbers" in Chapter 1 actually hold for any field; in particular, they are true for the fields $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$.

Notice that certain common properties of $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ do not hold for all fields. For example, it is possible for the equation $\mathbf{1} \mathbf{+} \mathbf{1} = \mathbf{0}$ to hold in some fields, and consequently $a \mathbf{-} b = b \mathbf{-} a$ does not necessarily imply that $a = b$. For the field $\mathbf{C}$ the assertion $1 + 1 \neq 0$ was derived from the explicit description of $\mathbf{C}$; for the fields $\mathbf{Q}$ and $\mathbf{R}$, however, this assertion was derived from further properties which do not have analogues in the conditions for a field. There is a related concept which does use these properties. An **ordered field** is a field F (with operations $\mathbf{+}$ and $\boldsymbol{\cdot}$) together with a certain subset $\mathbf{P}$ of F (the "positive" elements) with the following properties:

(8) For all a in F, one and only one of the following is true:

(i) $a = \mathbf{0}$,
(ii) a is in $\mathbf{P}$,
(iii) $\mathbf{-}a$ is in $\mathbf{P}$.

(9) If a and b are in $\mathbf{P}$, then $a \mathbf{+} b$ is in $\mathbf{P}$.
(10) If a and b are in $\mathbf{P}$, then $a \boldsymbol{\cdot} b$ is in $\mathbf{P}$.

We have already seen that the field $\mathbf{C}$ cannot be made into an ordered field. The field F_2, with only two elements, likewise cannot be made into an ordered field: in fact, condition (8), applied to $\mathbf{1} = \mathbf{-1}$, shows that $\mathbf{1}$ must be in $\mathbf{P}$; then (9) implies that $\mathbf{1} \mathbf{+} \mathbf{1} = \mathbf{0}$ is in $\mathbf{P}$, contradicting (8). On the other hand, the field F_1, consisting of all numbers $a + b\sqrt{2}$ with a, b in $\mathbf{Q}$, certainly can be made into assumption; if we really began from the beginning, no assumptions about $\mathbf{Q}$ would be necessary.

PROBLEMS

1. Let F be the set $\{0, 1, 2\}$ and define operations $\boldsymbol{+}$ and $\boldsymbol{\cdot}$ on F by the following tables. (The rule for constructing these tables is as follows: add or multiply in the usual way, and then subtract the highest possible multiple of 3; thus $2 \cdot 2 = 4 = 3 + 1$, so $2 \cdot 2 = 1$.)

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Show that F is a field, and prove that it cannot be made into an ordered field.

2. Suppose now that we try to construct a field F having elements 0, 1, 2, 3 with operations $\boldsymbol{+}$ and $\boldsymbol{\cdot}$ defined as in the previous example, by adding or multiplying in the usual way, and then subtracting the highest possible multiple of 4. Show that F will *not* be a field.

3. Let $F = \{0, 1, \alpha, \beta\}$ and define operations $\boldsymbol{+}$ and $\boldsymbol{\cdot}$ on F by the following tables.

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Show that F is a field.

4. (a) Let F be a field in which $\mathbf{1} \boldsymbol{+} \mathbf{1} = \mathbf{0}$. Show that $a \boldsymbol{+} a = \mathbf{0}$ for all a (this can also be written $a = \boldsymbol{-}a$).

(b) Suppose that $a \boldsymbol{+} a = \mathbf{0}$ for some $a \neq \mathbf{0}$. Show that $\mathbf{1} \boldsymbol{+} \mathbf{1} = \mathbf{0}$ (and consequently $b \boldsymbol{+} b = \mathbf{0}$ for all b).

5. (a) Show that in any field we have

$$\underbrace{(\mathbf{1}+\cdots+\mathbf{1})}_{m\text{ times}}\cdot\underbrace{(\mathbf{1}+\cdots+\mathbf{1})}_{n\text{ times}}=\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{mn\text{ times}}$$

for all natural numbers m and n.

(b) Suppose that in the field F we have

$$\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{m\text{ times}}=0$$

for some natural number m. Show that the smallest m with this property must be a prime number (this prime number is called the **characteristic** of F).

6. Let F be any field with only finitely many elements.

(a) Show that there must be distinct natural numbers m and n with

$$\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{m\text{ times}}=\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{n\text{ times}}.$$

(b) Conclude that there is some natural number k with

$$\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{k\text{ times}}=\mathbf{0}.$$

7. Let a, b, c, and d be elements of a field F with $a\cdot d-b\cdot c\neq\mathbf{0}$. Show that for any α and β in F the equations

$$\begin{aligned}a\cdot x+b\cdot y&=\alpha,\\ c\cdot x+d\cdot y&=\beta,\end{aligned}$$

can be solved for x and y in F.

8. Let a be an element of a field F. A "square root" of a is an element b of F with $b^2=b\cdot b=a$.

(a) How many square roots does $\mathbf{0}$ have?

(b) Suppose $a\neq\mathbf{0}$. Show that if a has a square root, then it has two square roots, unless $\mathbf{1}+\mathbf{1}=\mathbf{0}$, in which case a has only one.

9. (a) Consider an equation $x^2+b\cdot x+c=\mathbf{0}$, where b and c are elements of a field F. Suppose that $b^2-\mathbf{4}\cdot c$ has a square root r in F. Show that $(-b+r)/\mathbf{2}$ is a solution of this equation. (Here $\mathbf{2}=\mathbf{1}+\mathbf{1}$ and $\mathbf{4}=\mathbf{2}+\mathbf{2}$.)

(b) In the field F_2 of the text, both elements clearly have a square root. On the other hand, it is easy to check that neither element satisfies the equation $x^2+x+\mathbf{1}=\mathbf{0}$. Thus some detail in part (a) must be incorrect. What is it?

10. Let F be a field and a an element of F which does *not* have a square root. This problem shows how to construct a bigger field F', containing F, in which a does have a square root. (This construction has already been carried through in a special case, namely, $F = \mathbf{R}$ and $a = -1$; this special case should guide you through this example.)

Let F' consist of all pairs (x, y) with x and y in F. If the operations on F are $\boldsymbol{+}$ and $\cdot$, define operations $\oplus$ and $\odot$ on F' as follows:

$$(x, y) \oplus (z, w) = (x \boldsymbol{+} z, y \boldsymbol{+} w),$$
$$(x, y) \odot (z, w) = (x \cdot z \boldsymbol{+} a \cdot y \cdot w, y \cdot z \boldsymbol{+} x \cdot w).$$

(a) Prove that F', with the operations $\oplus$ and $\odot$, is a field.

(b) Prove that

$$(x, \mathbf{0}) \oplus (y, \mathbf{0}) = (x \boldsymbol{+} y, \mathbf{0}),$$
$$(x, \mathbf{0}) \odot (y, \mathbf{0}) = (x \cdot y, \mathbf{0}),$$

so that we may agree to abbreviate $(x, \mathbf{0})$ by x.

(c) Find a square root of $a = (a, \mathbf{0})$ in F'.

11. Let F be the set of all four-tuples (w, x, y, z) of real numbers. Define $\boldsymbol{+}$ and $\cdot$ by

$$(s, t, u, v) \boldsymbol{+} (w, x, y, z) = (s + w, t + x, u + y, v + z),$$
$$(s, t, u, v) \cdot (w, x, y, z) = (sw - tx - uy - vz, sx + tw + uz - vy,$$
$$sy + uw + vx - tz, sz + vw + ty - ux).$$

(a) Show that F satisfies all conditions for a field, except (6). At times the algebra will become quite ornate, but the existence of multiplicative inverses is the only point requiring any thought.

(b) It is customary to denote

$$(0, 1, 0, 0) \text{ by } i,$$
$$(0, 0, 1, 0) \text{ by } j,$$
$$(0, 0, 0, 1) \text{ by } k.$$

Find all 9 products of pairs i, j, and k. The results will show in particular that condition (6) is definitely false. This "skew field" F is known as the **quaternions**.