Spivak, Michael, "Calculus" pag 554 - 566, Publish or Perish Inc. 3rd ed

CHAPTER 28 CONSTRUCTION OF THE REAL NUMBERS

The mass of drudgery which this chapter necessarily contains is relieved by one truly first-rate idea. In order to prove that a complete ordered field exists we will have to explicitly describe one in detail; verifying conditions (1)–(10) for an ordered field will be a straightforward ordeal, but the description of the field itself, of the elements in it, is ingenious indeed.

At our disposal is the set of rational numbers, and from this raw material it is necessary to produce the field which will ultimately be called the real numbers. To the uninitiated this must seem utterly hopeless—if only the rational numbers are known, where are the others to come from? By now we have had enough experience to realize that the situation may not be quite so hopeless as that casual consideration suggests. The strategy to be adopted in our construction has already been used effectively for defining functions and complex numbers. Instead of trying to determine the "real nature" of these concepts, we settled for a definition that described enough about them to determine their mathematical properties completely.

A similar proposal for defining real numbers requires a description of real numbers in terms of rational numbers. The observation, that a real number ought to be determined completely by the set of rational numbers less than it, suggests a strikingly simple and quite attractive possibility: a real number might (and in fact eventually will) be described as a collection of rational numbers. In order to make this proposal effective, however, some means must be found for describing "the set of rational numbers less than a real number" without mentioning real numbers, which are still nothing more than heuristic figments of our mathematical imagination.

If A is to be regarded as the set of rational numbers which are less than the real number α, then A ought to have the following property: If x is in A and y is a rational number satisfying $y < x$, then y is in A. In addition to this property, the set A should have a few others. Since there should be some rational number $x < \alpha$, the set A should not be empty. Likewise, since there should be some rational number $x > \alpha$, the set A should not be all of $\mathbf{Q}$. Finally, if $x < \alpha$, then there should be another rational number y with $x < y < \alpha$, so A should not contain a greatest member.

If we temporarily regard the real numbers as known, then it is not hard to check (Problem 8-17) that a set A with these properties is indeed the set of rational numbers less than some real number α. Since the real numbers are presently in limbo, your proof, if you supply one, must be regarded only as an unofficial comment on these proceedings. It will serve to convince you, however, that we have not failed to notice any crucial property of the set A. There appears to be no reason for hesitating any longer.

DEFINITION

A **real number** is a set α, of rational numbers, with the following four properties:

(1) If x is in α and y is a rational number with $y < x$, then y is also in α.
(2) $\alpha \neq \emptyset$.
(3) $\alpha \neq \mathbf{Q}$.
(4) There is no greatest element in a; in other words, if x is in α, then there is some y in α with $y > x$.

The set of all real numbers is denoted by $\mathbf{R}$.

Just to remind you of the philosophy behind our definition, here is an explicit example of a real number:

$$\alpha = \{x \text{ in } \mathbf{Q}: x < 0 \text{ or } x^2 < 2\}.$$

It should be clear that α is the real number which will eventually be known as $\sqrt{2}$, but it is not an entirely trivial exercise to show that α actually is a real number. The whole point of such an exercise is to prove this using only facts about $\mathbf{Q}$; the hard part will be checking condition (4), but this has already appeared as a problem in a previous chapter (finding out which one is up to you). Notice that condition (4), although quite bothersome here, is really essential in order to avoid ambiguity; without it both

$$\{x \text{ in } \mathbf{Q}: x < 1\}$$

and

$$\{x \text{ in } \mathbf{Q}: x \leq 1\}$$

would be candidates for the "real number 1."

The shift from A to α in our definition indicates both a conceptual and a notational concern. Henceforth, a real number *is*, by definition, a set of rational numbers. This means, in particular, that a rational number (a member of $\mathbf{Q}$) is *not* a real number; instead every rational number x has a natural counterpart which is a real number, namely, $\{y \text{ in } \mathbf{Q}: y < x\}$. After completing the construction of the real numbers, we can mentally throw away the elements of $\mathbf{Q}$ and agree that $\mathbf{Q}$ will henceforth denote these special sets. For the moment, however, it will be necessary to work at the same time with rational numbers, real numbers (sets of rational numbers) and even sets of real numbers (sets of sets of rational numbers). Some confusion is perhaps inevitable, but proper notation should keep this to a minimum. Rational numbers will be denoted by lower case Roman letters (x, y, z, a, b, c) and real numbers by lower case Greek letters (α, β, γ); capital Roman letters (A, B, C) will be used to denote sets of real numbers.

The remainder of this chapter is devoted to the definition of $+$, $\cdot$, and $\mathbf{P}$ for $\mathbf{R}$, and a proof that with these structures $\mathbf{R}$ is indeed a complete ordered field.

We shall actually begin with the definition of **P**, and even here we shall work backwards. We first define $\alpha < \beta$; later, when $+$, $\cdot$, and $\mathbf{0}$ are available, we shall define **P** as the set of all α with $\mathbf{0} < \alpha$, and prove the necessary properties for **P**. The reason for beginning with the definition of $<$ is the simplicity of this concept in our present setup:

Definition. If α and β are real numbers, then $\alpha < \beta$ means that α is contained in β (that is, every element of α is also an element of β), but $\alpha \neq \beta$.

A repetition of the definitions of $\leq$, $>$, $\geq$ would be stultifying, but it is interesting to note that $\leq$ can now be expressed more simply than $<$; if α and β are real numbers, then $\alpha \leq \beta$ if and only if α is contained in β.

If A is a bounded collection of real numbers, it is almost obvious that A should have a least upper bound. Each α in A is a collection of rational numbers; if these rational numbers are all put in one collection β, then β is presumably sup A. In the proof of the following theorem we check all the little details which have not been mentioned, not least of which is the assertion that β *is* a real number. (We will not bother numbering theorems in this chapter, since they all add up to one big Theorem: There is a complete ordered field.)

THEOREM If A is a set of real numbers and $A \neq \emptyset$ and A is bounded above, then A has a least upper bound.

PROOF Let $\beta = \{x\colon x \text{ is in some } \alpha \text{ in } A\}$. Then β is certainly a collection of rational numbers; the proof that β is a real number requires checking four facts.

(1) Suppose that x is in β and $y < x$. The first condition means that x is in α for some α in A. Since α is a real number, the assumption $y < x$ implies that y is in α. Therefore it is certainly true that y is in β.

(2) Since $A \neq \emptyset$, there is some α in A. Since α is a real number, there is some x in α. This means that x is in β, so $\beta \neq \emptyset$.

(3) Since A is bounded above, there is some real number γ such that $\alpha < \gamma$ for every α in A. Since γ is a real number, there is some rational number x which is not in γ. Now $\alpha < \gamma$ means that α is contained in γ, so it is also true that x is not in α for any α in A. This means that x is not in β; so $\beta \neq \mathbf{Q}$.

(4) Suppose that x is in β. Then x is in α for some α in A. Since α does not have a greatest member, there is some rational number y with $x < y$ and y in α. But this means that y is in β; thus β does not have a greatest member.

These four observations prove that β is a real number. The proof that β is the least upper bound of A is easier. If α is in A, then clearly α is contained in β; this means that $\alpha \leq \beta$, so β is an upper bound for A. On the other hand, if γ is an upper bound for A, then $\alpha \leq \gamma$ for every α in A; this means

that α is contained in γ, for every α in A, and this surely implies that β is contained in γ. *This*, in turn, means that $\beta \leq \gamma$; thus β is the least upper bound of A. ∎

The definition of $+$ is both obvious and easy, but it must be complemented with a proof that this "obvious" definition makes any sense at all.

Definition. If α and β are real numbers, then

$$\alpha + \beta = \{x: x = y + z \text{ for some } y \text{ in } \alpha \text{ and some } z \text{ in } \beta\}.$$

THEOREM If α and β are real numbers, then $\alpha + \beta$ is a real number.

PROOF Once again four facts must be verified.

(1) Suppose $w < x$ for some x in $\alpha + \beta$. Then $x = y + z$ for some y in α and some z in β, which means that $w < y + z$, and consequently, $w - y < z$. This shows that $w - y$ is in β (since z is in β, and β is a real number). Since $w = y + (w - y)$, it follows that w is in $\alpha + \beta$.
(2) It is clear that $\alpha + \beta \neq \emptyset$, since $\alpha \neq \emptyset$ and $\beta \neq \emptyset$.
(3) Since $\alpha \neq \mathbf{Q}$ and $\beta \neq \mathbf{Q}$, there are rational numbers a and b with a not in α and b not in β. Any x in α satisfies $x < a$ (for if $a < x$, then condition (1) for a real number would imply that a is in α); similarly any y in β satisfies $y < b$. Thus $x + y < a + b$ for any x in α and y in β. This shows that $a + b$ is not in $\alpha + \beta$, so $\alpha + \beta \neq \mathbf{Q}$.
(4) If x is in $\alpha + \beta$, then $x = y + z$ for y in α and z in β. There are y' in α and z' in β with $y < y'$ and $z < z'$; then $x < y' + z'$ and $y' + z'$ is in $\alpha + \beta$. Thus $\alpha + \beta$ has no greatest member. ∎

By now you can see how tiresome this whole procedure is going to be. Every time we mention a new real number, we must prove that it *is* a real number; this requires checking four conditions, and even when trivial they require concentration. There is really no help for this (except that it will be less boring if you check the four conditions for yourself). Fortunately, however, a few points of interest will arise now and then, and some of our theorems will be easy. In particular, two properties of $+$ present no problems.

THEOREM If α, β, and γ are real numbers, then $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

PROOF Since $(x + y) + z = x + (y + z)$ for all rational numbers x, y, and z, every member of $(\alpha + \beta) + \gamma$ is also a member of $\alpha + (\beta + \gamma)$, and vice versa. ∎

THEOREM If α and β are real numbers, then $\alpha + \beta = \beta + \alpha$.

PROOF Left to you (even easier). ∎

To prove the other properties of $+$ we first define $\mathbf{0}$.

Definition. $\mathbf{0} = \{x \text{ in } \mathbf{Q}\colon x < 0\}$.

It is, thank goodness, obvious that $\mathbf{0}$ is a real number, and the following theorem is also simple.

THEOREM If α is a real number, then $\alpha + \mathbf{0} = \alpha$.

PROOF If x is in α and y is in $\mathbf{0}$, then $y < 0$, so $x + y < x$. This implies that $x + y$ is in α. Thus every member of $\alpha + \mathbf{0}$ is also a member of α.

On the other hand, if x is in α, then there is a rational number y in α such that $y > x$. Since $x = y + (x - y)$, where y is in α, and $x - y < 0$ (so that $x - y$ is in $\mathbf{0}$), this shows that x is in $\alpha + \mathbf{0}$. Thus every member of α is also a member of $\alpha + \mathbf{0}$. ∎

The reasonable candidate for $-\alpha$ would seem to be the set

$$\{x \text{ in } \mathbf{Q}\colon -x \text{ is not in } \alpha\}$$

(since $-x$ not in α means, intuitively, that $-x > \alpha$, so that $x < -\alpha$). But in certain cases this set will not even be a real number. Although a real number α does not have a greatest member, the set

$$\mathbf{Q} - \alpha = \{x \text{ in } \mathbf{Q}\colon x \text{ is not in } \alpha\}$$

may have a *least* element x_0; when α is a real number of this kind, the set $\{x\colon -x \text{ is not in } \alpha\}$ will have a greatest element $-x_0$. It is therefore necessary to introduce a slight modification into the definition of $-\alpha$, which comes equipped with a theorem.

Definition. If α is a real number, then

$-\alpha = \{x \text{ in } \mathbf{Q}\colon -x \text{ is not in } \alpha, \text{ but } -x \text{ is not the least element of } \mathbf{Q} - \alpha\}$.

THEOREM If α is a real number, then $-\alpha$ is a real number.

PROOF

(1) Suppose that x is in $-\alpha$ and $y < x$. Then $-y > -x$. Since $-x$ is not in α, it is also true that $-y$ is not in α. Moreover, it is clear that $-y$ is not the smallest element of $\mathbf{Q} - \alpha$, since $-x$ is a smaller element. This shows that y is in $-\alpha$.

(2) Since $\alpha \neq \mathbf{Q}$, there is some rational number y which is not in α. We can assume that y is not the smallest rational number in $\mathbf{Q} - \alpha$ (since y can always be replaced by any $y' > y$). Then $-y$ is in $-\alpha$. Thus $-\alpha \neq \emptyset$.

(3) Since $\alpha \neq \emptyset$, there is some x in α. Then $-x$ cannot possibly be in $-\alpha$, so $-\alpha \neq \mathbf{Q}$.

(4) If x is in $-\alpha$, then $-x$ is not in α, and there is a rational number $y < -x$ which is also not in α. Let z be a rational number with $y < z < -x$. Then z is also not in α, and z is clearly not the smallest element of $\mathbf{Q} - \alpha$. So $-z$ is in $-\alpha$. Since $-z > x$, this shows that $-\alpha$ does not have a greatest element. ▮

The proof that $\alpha + (-\alpha) = \mathbf{0}$ is not entirely straightforward. The difficulties are not caused, as you might presume, by the finicky details in the definition of $-\alpha$. Rather, at this point we require the Archimedian property of $\mathbf{Q}$ stated on page 550, which does not follow from P1–P12. This property is needed to prove the following lemma, which plays a crucial role in the next theorem.

LEMMA Let α be a real number, and z a positive rational number. Then there are (Figure 1) rational numbers x in α, and y not in α, such that $y - x = z$. Moreover, we may assume that y is not the smallest element of $\mathbf{Q} - \alpha$.

PROOF Suppose first that z is in α. If the numbers

$$z, 2z, 3z, \ldots$$

were *all* in α, then *every* rational number would be in α, since every rational number w satisfies $w < nz$ for some n, by the additional assumption on page 550. This contradicts the fact that α is a real number, so there is some k such that $x = kz$ is in α and $y = (k + 1)z$ is not in α. Clearly $y - x = z$.

Moreover, if y happens to be the smallest element of $\mathbf{Q} - \alpha$, let $x' > x$ be an element of α, and replace x by x', and y by $y + (x' - x)$.

If z is not in α, there is a similar proof, based on the fact that the numbers $(-n)z$ cannot all fail to be in α. ▮

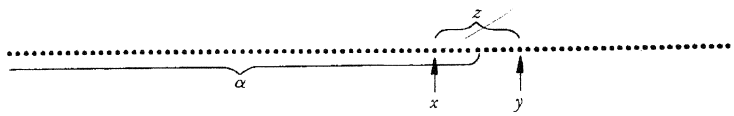

FIGURE 1

THEOREM If α is a real number, then

$$\alpha + (-\alpha) = \mathbf{0}.$$

PROOF Suppose x is in α and y is in $-\alpha$. Then $-y$ is not in α, so $-y > x$. Hence $x + y < 0$, so $x + y$ is in $\mathbf{0}$. Thus every member of $\alpha + (-\alpha)$ is in $\mathbf{0}$.

It is a little more difficult to go in the other direction. If z is in $\mathbf{0}$, then $-z > 0$. According to the lemma, there is some x in α, and some y not in α, with y not the smallest element of $\mathbf{Q} - \alpha$, such that $y - x = -z$. This equation can be written $x + (-y) = z$. Since x is in α, and $-y$ is in $-\alpha$, this proves that z is in $\alpha + (-\alpha)$. ▮

Before proceeding with multiplication, we define the "positive elements" and prove a basic property:

Definition. $\mathbf{P} = \{\alpha \text{ in } \mathbf{R}\colon \alpha > 0\}$.

Notice that $\alpha + \beta$ is clearly in $\mathbf{P}$ if α and β are.

THEOREM If α is a real number, then one and only one of the following conditions holds:

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

PROOF If α contains any positive rational number, then α certainly contains all negative rational numbers, so α contains 0 and $\alpha \neq 0$, i.e., α is in $\mathbf{P}$. If α contains no positive rational numbers, then one of two possibilities must hold:

(1) α contains all negative rational numbers; then $\alpha = 0$.
(2) there is some negative rational number x which is not in α; it can be assumed that x is not the least element of $\mathbf{Q} - \alpha$ (since x could be replaced by $x/2 > x$); then $-\alpha$ contains the positive rational number $-x$, so, as we have just proved, $-\alpha$ is in $\mathbf{P}$.

This shows that *at least one* of (i)–(iii) must hold. If $\alpha = 0$, it is clearly impossible for condition (ii) or (iii) to hold. Moreover, it is impossible that $\alpha > 0$ and $-\alpha > 0$ both hold, since this would imply that $0 = \alpha + (-\alpha) > 0$. ▮

Recall that $\alpha > \beta$ was defined to mean that α contains β, but is unequal to β. This definition was fine for proving completeness, but now we have to show that it is equivalent to the definition which would be made in terms of $\mathbf{P}$. Thus, we must show that $\alpha - \beta > 0$ is equivalent to $\alpha > \beta$. This is clearly a consequence of the next theorem.

THEOREM If α, β, and γ are real numbers and $\alpha > \beta$, then $\alpha + \gamma > \beta + \gamma$.

PROOF The hypothesis $\alpha > \beta$ implies that β is contained in α; it follows immediately from the definition of $+$ that $\beta + \gamma$ is contained in $\alpha + \gamma$. This shows that $\alpha + \gamma \geq \beta + \gamma$. We can easily rule out the possibility of equality, for if

$$\alpha + \gamma = \beta + \gamma,$$

then

$$\alpha = (\alpha + \gamma) + (-\gamma) = (\beta + \gamma) + (-\gamma) = \beta,$$

which is false. Thus $\alpha + \gamma > \beta + \gamma$. ▮

Multiplication presents difficulties of its own. If $\alpha, \beta > 0$, then $\alpha \cdot \beta$ can be defined as follows.

Definition. If α and β are real numbers and $\alpha, \beta > \mathbf{0}$, then

$$\alpha \cdot \beta = \{z\colon z \leq 0 \text{ or } z = x \cdot y \text{ for some } x \text{ in } \alpha \text{ and } y \text{ in } \beta \text{ with } x, y > 0\}.$$

THEOREM If α and β are real numbers with $\alpha, \beta > \mathbf{0}$, then $\alpha \cdot \beta$ is a real number.

PROOF As usual, we much check four conditions.

(1) Suppose $w < z$, where z is in $\alpha \cdot \beta$. If $w \leq 0$, then w is automatically in $\alpha \cdot \beta$. Suppose that $w > 0$. Then $z > 0$, so $z = x \cdot y$ for some positive x in α and positive y in β. Now

$$w = \frac{wz}{z} = \frac{wxy}{z} = \left(\frac{w}{z} \cdot x\right) \cdot y.$$

Since $0 < w < z$, we have $w/z < 1$, so $(w/z) \cdot x$ is in α. Thus w is in $\alpha \cdot \beta$.

(2) Clearly $\alpha \cdot \beta \neq \emptyset$.

(3) If x is not in α, and y is not in β, then $x > x'$ for all x' in α, and $y > y'$ for all y' in β. Hence $xy > x'y'$ for all such positive x' and y'. So xy is not in $\alpha \cdot \beta$; thus $\alpha \cdot \beta \neq \mathbf{Q}$.

(4) Suppose w is in $\alpha \cdot \beta$, and $w \leq 0$. There is some x in α with $x > 0$ and some y in β with $y > 0$. Then $z = xy$ is in $\alpha \cdot \beta$ and $z > w$. Now suppose $w > 0$. Then $w = xy$ for some positive x in α and some positive y in β. Moreover, α contains some $x' > x$; if $z = x'y$, then $z > xy = w$, and z is in $\alpha \cdot \beta$. Thus $\alpha \cdot \beta$ does not have a greatest element. ∎

Notice that $\alpha \cdot \beta$ is clearly in $\mathbf{P}$ if α and β are. This completes the verification of all properties of $\mathbf{P}$. To complete the definition of $\cdot$ we first define $|\alpha|$.

Definition. If α is a real number, then

$$|\alpha| = \begin{cases} \alpha, & \text{if } \alpha \geq \mathbf{0} \\ -\alpha, & \text{if } \alpha \leq \mathbf{0}. \end{cases}$$

Definition. If α and β are real numbers, then

$$\alpha \cdot \beta = \begin{cases} \mathbf{0}, & \text{if } \alpha = \mathbf{0} \text{ or } \beta = \mathbf{0} \\ |\alpha| \cdot |\beta|, & \text{if } \alpha > \mathbf{0}, \beta > \mathbf{0} \text{ or } \alpha < \mathbf{0}, \beta < \mathbf{0} \\ -(|\alpha| \cdot |\beta|), & \text{if } \alpha > \mathbf{0}, \beta < \mathbf{0} \text{ or } \alpha < \mathbf{0}, \beta > \mathbf{0}. \end{cases}$$

As one might suspect, the proofs of the properties of multiplication usually involve reduction to the case of positive numbers.

THEOREM If α, β, and γ are real numbers, then $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$.

PROOF This is clear if $\alpha, \beta, \gamma > \mathbf{0}$. The proof for the general case requires considering separate cases (and is simplified slightly if one uses the following theorem). ∎

THEOREM If α and β are real numbers, then $\alpha \cdot \beta = \beta \cdot \alpha$.

PROOF This is clear if $\alpha, \beta > \mathbf{0}$, and the other cases are easily checked. ∎

Definition. $\mathbf{1} = \{x \text{ in } \mathbf{Q}\colon x < 1\}$.
(It is clear that $\mathbf{1}$ is a real number.)

THEOREM If α is a real number, then $\alpha \cdot \mathbf{1} = \alpha$.

PROOF Let $\alpha > \mathbf{0}$. It is easy to see that every member of $\alpha \cdot \mathbf{1}$ is also a member of α. On the other hand, suppose x is in α. If $x \leq 0$, then x is automatically in $\alpha \cdot \mathbf{1}$. If $x > 0$, then there is some rational number y in α such that $x < y$. Then $x = y \cdot (x/y)$, and x/y is in $\mathbf{1}$, so x is in $\alpha \cdot \mathbf{1}$. This proves that $\alpha \cdot \mathbf{1} = \alpha$ if $\alpha > \mathbf{0}$.

If $\alpha < \mathbf{0}$, then, applying the result just proved, we have

$$\alpha \cdot \mathbf{1} = -(|\alpha| \cdot |\mathbf{1}|) = -(|\alpha|) = \alpha.$$

Finally, the theorem is obvious when $\alpha = \mathbf{0}$. ∎

Definition. If α is a real number and $\alpha > \mathbf{0}$, then

$\alpha^{-1} = \{x \text{ in } \mathbf{Q}\colon x \leq 0$, or $x > 0$ and $1/x$ is not in α, but $1/x$ is not the smallest member of $\mathbf{Q} - \alpha\}$;

if $\alpha < \mathbf{0}$, then $\alpha^{-1} = -(|\alpha|^{-1})$.

THEOREM If α is a real number unequal to $\mathbf{0}$, then α^{-1} is a real number.

PROOF Clearly it suffices to consider only $\alpha > \mathbf{0}$. Four conditions must be checked.

(1) Suppose $y < x$, and x is in α^{-1}. If $y \leq 0$, then y is in α^{-1}. If $y > 0$, then $x > 0$, so $1/x$ is not in α. Since $1/y > 1/x$, it follows that $1/y$ is not in α, and $1/y$ is clearly not the smallest element of $\mathbf{Q} - \alpha$, so y is in α^{-1}.
(2) Clearly $\alpha^{-1} \neq \emptyset$.
(3) Since $\alpha > \mathbf{0}$, there is some positive rational number x in α. Then $1/x$ is not in α^{-1}, so $\alpha^{-1} \neq \mathbf{Q}$.
(4) Suppose x is in α^{-1}. If $x \leq 0$, there is clearly some y in α^{-1} with $y > x$ because α^{-1} contains some positive rationals. If $x > 0$, then $1/x$ is not in α. Since $1/x$ is not the smallest member of $\mathbf{Q} - \alpha$, there is a rational number y not in α, with $y < 1/x$. Choose a rational number z with $y < z < 1/x$. Then $1/z$ is in α, and $1/z > x$. Thus α^{-1} does not contain a largest member. ∎

In order to prove that α^{-1} is really the multiplicative inverse of α, it helps to have another lemma, which is the multiplicative analogue of our first lemma.

LEMMA Let α be a real number with $\alpha > \mathbf{0}$, and z a rational number with $z > 1$. Then there are rational numbers x in α, and y not in α, such that $y/x = z$. Moreover, we can assume that y is not the least element of $\mathbf{Q} - \alpha$.

PROOF Suppose first that z is in α. Since $z - 1 > 0$ and

$$z^n = (1 + (z - 1))^n \geq 1 + n(z - 1),$$

it follows that the numbers

$$z, z^2, z^3, \ldots$$

cannot all be in α. So there is some k such that $x = z^k$ is in α, and $y = z^{k+1}$ is not in α. Clearly $y/x = z$. Moreover, if y happens to be the least element of $\mathbf{Q} - \alpha$, let $x' > x$ be an element of α, and replace x by x' and y by yx'/x.

If z is not in α, there is a similar proof, based on the fact that the numbers $1/z^k$ cannot all fail to be in α. ▮

THEOREM If α is a real number and $\alpha \neq \mathbf{0}$, then $\alpha \cdot \alpha^{-1} = \mathbf{1}$.

PROOF It obviously suffices to consider only $\alpha > \mathbf{0}$, in which case $\alpha^{-1} > \mathbf{0}$. Suppose that x is a positive rational number in α, and y is a positive rational number in α^{-1}. Then $1/y$ is not in α, so $1/y > x$; consequently $xy < 1$, which means that xy is in $\mathbf{1}$. Since all rational numbers $x \leq 0$ are also in $\mathbf{1}$, this shows that every member of $\alpha \cdot \alpha^{-1}$ is in $\mathbf{1}$.

To prove the converse assertion, let z be in $\mathbf{1}$. If $z \leq 0$, then clearly z is in $\alpha \cdot \alpha^{-1}$. Suppose $0 < z < 1$. According to the lemma, there are positive rational numbers x in α, and y not in α, such that $y/x = 1/z$; and we can assume that y is not the smallest element of $\mathbf{Q} - \alpha$. But this means that $z = x \cdot (1/y)$, where x is in α, and $1/y$ is in α^{-1}. Consequently, z is in $\alpha \cdot \alpha^{-1}$. ▮

We are almost done! Only the proof of the distributive law remains. Once again we must consider many cases, but do not despair. The case when all numbers are positive contains an interesting point, and the other cases can all be taken care of very neatly.

THEOREM If α, β, and γ are real numbers, then $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

PROOF Assume first that $\alpha, \beta, \gamma > \mathbf{0}$. Then both numbers in the equation contain all rational numbers ≤ 0. A positive rational number in $\alpha \cdot (\beta + \gamma)$ is of the form $x \cdot (y + z)$ for positive x in α, y in β, and z in γ. Since $x \cdot (y + z) = x \cdot y + x \cdot z$, where $x \cdot y$ is a positive element of $\alpha \cdot \beta$, and $x \cdot z$ is a positive element of $\alpha \cdot \gamma$, this number is also in $\alpha \cdot \beta + \alpha \cdot \gamma$. Thus, every element of $\alpha \cdot (\beta + \gamma)$ is also in $\alpha \cdot \beta + \alpha \cdot \gamma$.

On the other hand, a positive rational number in $\alpha \cdot \beta + \alpha \cdot \gamma$ is of the form $x_1 \cdot y + x_2 \cdot z$ for positive x_1, x_2 in α, y in β, and z in γ. If $x_1 \leq x_2$, then $(x_1/x_2) \cdot y \leq y$, so $(x_1/x_2) \cdot y$ is in β. Thus

$$x_1 \cdot y + x_2 \cdot z = x_2[(x_1/x_2)y + z]$$

is in $\alpha \cdot (\beta + \gamma)$. Of course, the same trick works if $x_2 \leq x_1$.

To complete the proof it is necessary to consider the cases when α, β, and γ are not all > 0. If any one of the three equals 0, the proof is easy and the cases involving $\alpha < 0$ can be derived immediately once all the possibilities for β and γ have been accounted for. Thus we assume $\alpha > 0$ and consider three cases: β, $\gamma < 0$, and $\beta < 0$, $\gamma > 0$, and $\beta > 0$, $\gamma < 0$. The first follows immediately from the case already proved, and the third follows from the second by interchanging β and γ. Therefore we concentrate on the case $\beta < 0$, $\gamma > 0$. There are then two possibilities:

(1) $\beta + \gamma \geq 0$. Then

$$\alpha \cdot \gamma = \alpha \cdot ([\beta + \gamma] + |\beta|) = \alpha \cdot (\beta + \gamma) + \alpha \cdot |\beta|,$$

so

$$\begin{aligned} \alpha \cdot (\beta + \gamma) &= -(\alpha \cdot |\beta|) + \alpha \cdot \gamma \\ &= \alpha \cdot \beta + \alpha \cdot \gamma. \end{aligned}$$

(2) $\beta + \gamma \leq 0$. Then

$$\alpha \cdot |\beta| = \alpha \cdot (|\beta + \gamma| + \gamma) = \alpha \cdot |\beta + \gamma| + \alpha \cdot \gamma,$$

so

$$\alpha \cdot (\beta + \gamma) = -(\alpha \cdot |\beta + \gamma|) = -(\alpha \cdot |\beta|) + \alpha \cdot \gamma = \alpha \cdot \beta + \alpha \cdot \gamma. \blacksquare$$

This proof completes the work of the chapter. Although long and frequently tedious, this chapter contains results sufficiently important to be read in detail at least once (and preferably not more than once!). For the first time we know that we have not been operating in a vacuum—there is indeed a complete ordered field, the theorems of this book are not based on assumptions which can never be realized. One interesting and horrid possibility remains: there may be several complete ordered fields. If this is true, then the theorems of calculus are unexpectedly rich in content, but the properties P1–P13 are disappointingly incomplete. The last chapter disposes of this possibility; properties P1–P13 completely characterize the real numbers—anything that can be proved about real numbers can be proved on the basis of these properties alone.

PROBLEMS

There are only two problems in this set, but each asks for an entirely different construction of the real numbers! The detailed examination of another construction is recommended only for masochists, but the main idea behind these other constructions is worth knowing. The real numbers constructed in this

chapter might be called "the algebraist's real numbers," since they were purposely defined so as to guarantee the least upper bound property, which involves the ordering $<$, an algebraic notion. The real number system constructed in the next problem might be called "the analyst's real numbers," since they are devised so that Cauchy sequences will always converge.

1. Since every real number ought to be the limit of some Cauchy sequence of rational numbers, we might try to *define* a real number to be a Cauchy sequence of rational numbers. Since two Cauchy sequences might converge to the same real number, however, this proposal requires some modifications.

(a) Define two Cauchy sequences of rational numbers $\{a_n\}$ and $\{b_n\}$ to be *equivalent* (denoted by $\{a_n\} \sim \{b_n\}$) if $\lim_{n\to\infty} (a_n - b_n) = 0$. Prove that $\{a_n\} \sim \{a_n\}$, that $\{a_n\} \sim \{b_n\}$ if $\{b_n\} \sim \{a_n\}$, and that $\{a_n\} \sim \{c_n\}$ if $\{a_n\} \sim \{b_n\}$ and $\{b_n\} \sim \{c_n\}$.

(b) Suppose that α is the set of all sequences equivalent to $\{a_n\}$, and β is the set of all sequences equivalent to $\{b_n\}$. Prove that either $\alpha \cap \beta = \emptyset$ or $\alpha = \beta$. (If $\alpha \cap \beta \neq \emptyset$, then there is some $\{c_n\}$ in both α and β. Show that in this case α and β both consist precisely of those sequences equivalent to $\{c_n\}$.)

Part (b) shows that the collection of all Cauchy sequences can be split up into disjoint sets, each set consisting of all sequences equivalent to some fixed sequence. We define a real number to be such a collection, and denote the set of all real numbers by $\mathbf{R}$.

(c) If α and β are real numbers, let $\{a_n\}$ be a sequence in α, and $\{b_n\}$ a sequence in β. Define $\alpha + \beta$ to be the collection of all sequences equivalent to the sequence $\{a_n + b_n\}$. Show that $\{a_n + b_n\}$ is a Cauchy sequence and also show that this definition does not depend on the particular sequences $\{a_n\}$ and $\{b_n\}$ chosen for α and β. Check also that the analogous definition of multiplication is well defined.

(d) Show that $\mathbf{R}$ is a field with these operations; existence of a multiplicative inverse is the only interesting point to check.

(e) Define the positive real numbers P so that $\mathbf{R}$ will be an ordered field.

(f) Prove that every Cauchy sequence of real numbers converges. Remember that if $\{\alpha_n\}$ is a sequence of real numbers, then each α_n is itself a collection of Cauchy sequences of rational numbers.

2. This problem outlines a construction of "the high-school student's real numbers." We define a real number to be a pair $(a, \{b_n\})$, where a is an integer and $\{b_n\}$ is a sequence of natural numbers from 0 to 9, with the proviso that the sequence is not eventually 9; intuitively, this pair represents $a + \sum_{n=1}^{\infty} b_n 10^{-n}$. With this definition, a real number is a very concrete object, but the difficulties involved in defining addition and multi-

plication are formidable (how do you add infinite decimals without worrying about carrying digits infinitely far out?). A reasonable approach is outlined below; the trick is to use least upper bounds right from the start.

(a) Define $(a, \{b_n\}) < (c, \{d_n\})$ if $a < c$, or if $a = c$ and for some n we have $b_n < d_n$ but $b_j = d_j$ for $1 \leq j < n$. Using this definition, prove the least upper bound property.

(b) Given $\alpha = (a, \{b_n\})$, define $\alpha_k = a + \sum_{n=1}^{k} b_n 10^{-n}$; intuitively, α_k is the rational number obtained by changing all decimal places after the kth to 0. Conversely, given a rational number r of the form $a + \sum_{n=1}^{k} b_n 10^{-n}$, let r' denote the real number $(a, \{b_n'\})$, where $b_n' = b_n$ for $1 \leq n \leq k$ and $b_n' = 0$ for $n > k$. Now for $\alpha = (a, \{b_n\})$ and $\beta = (c, \{d_n\})$ define

$$\alpha + \beta = \sup \{(\alpha_k + \beta_k)' : k \text{ a natural number}\}$$

(the least upper bound exists by part (a)). If multiplication is defined similarly, then the verification of all conditions for a field is a straightforward task, not highly recommended. Once more, however, existence of multiplicative inverses will be the hardest.

CHAPTER 29 UNIQUENESS OF THE REAL NUMBERS

We shall now revert to the usual notation for real numbers, reserving boldface symbols for other fields which may turn up. Moreover, we will regard integers and rational numbers as special kinds of real numbers, and forget about the specific way in which real numbers were defined. In this chapter we are interested in only one question: are there any complete ordered fields other than **R**? The answer to this question, if taken literally, is "yes." For example, the field F_3 introduced in Chapter 25 is a complete ordered field, and it is certainly not **R**. This field is a "silly" example because the pair (a, a) can be regarded as just another name for the real number a; the operations

$$(a, a) + (b, b) = (a + b, a + b),$$
$$(a, a) \cdot (b, b) = (a \cdot b, a \cdot b),$$

are consistent with this renaming. This sort of example shows that any intelligent consideration of the question requires some mathematical means of discussing such renaming procedures.

If the elements of a field F are going to be used to rename elements of **R**, then for each a in **R** there should correspond a "name" $f(a)$ in F. The notation $f(a)$ suggests that renaming can be formulated in terms of functions. In order to do this we will need a concept of function much more general than any which has occurred until now; in fact, we will require the most general notion of "function" used in mathematics. A function, in this general sense, is simply a rule which assigns to some things, other things. To be formal, a **function** is a collection of ordered pairs (of objects of any sort) which does not contain two distinct pairs with the same first element. The **domain** of a function f is the set A of all objects a such that (a, b) is in f for some b; this (unique) b is denoted by $f(a)$. If $f(a)$ is in the set B for all a in A, then f is called a function **from** A **to** B. For example,

if $f(x) = \sin x$ for all x in **R** (and f is defined only for x in **R**), then f is a function from **R** to **R**; it is also a function from **R** to $[-1, 1]$;

if $f(z) = \sin z$ for all z in **C**, then f is a function from **C** to **C**;

if $f(z) = e^z$ for all z in **C**, then f is a function from **C** to **C**; it is also a function from **C** to $\{z \text{ in } \mathbf{C}: z \neq 0\}$;

θ is a function from $\{z \text{ in } \mathbf{C}: z \neq 0\}$ to $\{x \text{ in } \mathbf{R}: 0 \leq x < 2\pi\}$;

if f is the collection of all pairs $(a, (a, a))$ for a in **R**, then f is a function from **R** to F_3.

Suppose that F_1 and F_2 are two fields; we will denote the operations in F_1 by $\oplus$, $\odot$, etc. and the operations in F_2 by $+$, $\cdot$, etc. If F_2 is going to be considered as a collection of new names for elements of F_1, then there should be a function from F_1 to F_2 with the following properties:

(1) The function f should be one-one, that is, if $x \neq y$, then we should have $f(x) \neq f(y)$; this means that no two elements of F_1 have the same name.
(2) The function f should be "onto," that is, for every element z in F_2 there should be some x in F_1 such that $z = f(x)$; this means that every element of F_2 is used to name some element of F_1.
(3) For all x and y in F_1 we should have

$$f(x \oplus y) = f(x) + f(y),$$
$$f(x \odot y) = f(x) \cdot f(y);$$

this means that the renaming procedure is consistent with the operations of the field.

If we are also considering F_1 and F_2 as ordered fields, we add one more requirement:

(4) If $x \lessdot y$, then $f(x) < f(y)$.

A function with these properties is called an *isomorphism* from F_1 to F_2. This definition is so important that we restate it formally.

DEFINITION

If F_1 and F_2 are two fields, an **isomorphism** from F_1 to F_2 is a function f from F_1 to F_2 with the following properties:

(1) If $x \neq y$, then $f(x) \neq f(y)$.
(2) If z is in F_2, then $z = f(x)$ for some x in F_1.
(3) If x and y are in F_1, then

$$f(x \oplus y) = f(x) + f(y),$$
$$f(x \odot y) = f(x) \cdot f(y).$$

If F_1 and F_2 are ordered fields we also require:

(4) If $x \lessdot y$, then $f(x) < f(y)$.

The fields F_1 and F_2 are called **isomorphic** if there is an isomorphism between them. Isomorphic fields may be regarded as essentially the same—any important property of one will automatically hold for the other. Therefore, we can, and should, reformulate the question asked at the beginning of the chapter; if F is a complete ordered field it is silly to expect F to equal $\mathbf{R}$—rather, we would like to know if F is isomorphic to $\mathbf{R}$. In the following theorem, F will be a field, with operations $+$ and $\cdot$, and "positive elements" $\mathbf{P}$; we write $a < b$ to mean that $b - a$ is in $\mathbf{P}$, and so forth.

THEOREM If F is a complete ordered field, then F is isomorphic to $\mathbf{R}$.

PROOF Since two fields are defined to be isomorphic if there is an isomorphism between them, we must actually construct a function f from $\mathbf{R}$ to F which is an isomorphism. We begin by defining f on the integers as follows:

$$f(0) = \mathbf{0},$$
$$f(n) = \underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{n \text{ times}} \quad \text{for } n > 0,$$
$$f(n) = -\underbrace{(\mathbf{1} + \cdots + \mathbf{1})}_{|n| \text{ times}} \quad \text{for } n < 0.$$

It is easy to check that

$$f(m + n) = f(m) + f(n),$$
$$f(m \cdot n) = f(m) \cdot f(n),$$

for all integers m and n, and it is convenient to denote $f(n)$ by $\boldsymbol{n}$. We then define f on the rational numbers by

$$f(m/n) = \boldsymbol{m/n} = \boldsymbol{m \cdot n^{-1}}$$

(notice that $\mathbf{1} + \cdots + \mathbf{1} \neq \mathbf{0}$ if $n > 0$, since F is an ordered field). This definition makes sense because if $m/n = k/l$, then $ml = nk$, so $\boldsymbol{m \cdot l = k \cdot n}$, so $\boldsymbol{m \cdot n^{-1} = k \cdot l^{-1}}$. It is easy to check that

$$f(r_1 + r_2) = f(r_1) + f(r_2),$$
$$f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2),$$

for all rational numbers r_1 and r_2, and that $f(r_1) < f(r_2)$ if $r_1 < r_2$.

The definition of $f(x)$ for arbitrary x is based on the now familiar idea that any real number is determined by the rational numbers less than it. For any x in $\mathbf{R}$, let A_x be the subset of F consisting of all $f(r)$, for all rational numbers $r < x$. The set A_x is certainly not empty, and it is also bounded above, for if r_0 is a rational number with $r_0 > x$, then $f(r_0) > f(r)$ for all $f(r)$ in A_x. Since F is a complete ordered field, the set A_x has a least upper bound; we define $f(x)$ as sup A_x.

We now have $f(x)$ defined in two different ways, first for rational x, and then for any x. Before proceeding further, it is necessary to show that these two definitions agree for rational x. In other words, if x is a rational number, we want to show that

$$\sup A_x = f(x),$$

where $f(x)$ here denotes $\boldsymbol{m/n}$, for $x = m/n$. This is not automatic, but depends on the completeness of F; a slight digression is thus required.

Since F is complete, the elements

$$\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{n \text{ times}} \quad \text{for natural numbers } n$$

form a set which is not bounded above; the proof is exactly the same as the proof for **R** (Theorem 8-2). The consequences of this fact for **R** have exact analogues in F: in particular, if a and b are elements of F with $a < b$, then there is a rational number r such that

$$a < f(r) < b.$$

Having made this observation, we return to the proof that the two definitions of $f(x)$ agree for rational x. If y is a rational number with $y < x$, then we have already seen that $f(y) < f(x)$. Thus every element of A_x is $< f(x)$. Consequently,

$$\sup A_x \leq f(x).$$

On the other hand, suppose that we had

$$\sup A_x < f(x).$$

Then there would be a rational number r such that

$$\sup A_x < f(r) < f(x).$$

But the condition $f(r) < f(x)$ means that $r < x$, which means that $f(r)$ is in the set A_x; this clearly contradicts the condition $\sup A_x < f(r)$. This shows that the original assumption is false, so

$$\sup A_x = f(x).$$

We thus have a certain well-defined function f from **R** to F. In order to show that f is an isomorphism we must verify conditions (1)–(4) of the definition. We will begin with (4).

If x and y are real numbers with $x < y$, then clearly A_x is contained in A_y. Thus

$$f(x) = \sup A_x \leq \sup A_y = f(y).$$

To rule out the possibility of equality, notice that there are rational numbers r and s with

$$x < r < s < y.$$

We know that $f(r) < f(s)$. It follows that

$$f(x) \leq f(r) < f(s) \leq f(y).$$

This proves (4).

Condition (1) follows immediately from (4): If $x \neq y$, then either $x < y$ or $y < x$; in the first case $f(x) < f(y)$, and in the second case $f(y) < f(x)$; in either case $f(x) \neq f(y)$.

To prove (2), let a be an element of F, and let B be the set of all rational numbers r with $f(r) < a$. The set B is not empty, and it is also bounded above, because there is a rational number s with $f(s) > a$, so that $f(s) > f(r)$ for r in B, which implies that $s > r$. Let x be the least upper bound of B; we claim

that $f(x) = a$. In order to prove this it suffices to eliminate the alternatives

$$f(x) < a,$$
$$a < f(x).$$

In the first case there would be a rational number r with

$$f(x) < f(r) < a.$$

But this means that $x < r$ and that r is in B, which contradicts the fact that $x = \sup B$. In the second case there would be a rational number r with

$$a < f(r) < f(x).$$

This implies that $r < x$. Since $x = \sup B$, this means that $r < s$ for some s in B. Hence

$$f(r) < f(s) < a,$$

again a contradiction. Thus $f(x) = a$, proving (2).

To check (3), let x and y be real numbers and suppose that $f(x + y) \neq f(x) + f(y)$. Then either

$$f(x + y) < f(x) + f(y) \quad \text{or} \quad f(x) + f(y) < f(x + y).$$

In the first case there would be a rational number r such that

$$f(x + y) < f(r) < f(x) + f(y).$$

But this would mean that

$$x + y < r.$$

Therefore r could be written as the sum of two rational numbers

$$r = r_1 + r_2, \quad \text{where } x < r_1 \text{ and } y < r_2.$$

Then, using the facts checked about f for *rational* numbers, it would follow that

$$f(r) = f(r_1 + r_2) = f(r_1) + f(r_2) > f(x) + f(y),$$

a contradiction. The other case is handled similarly.

Finally, if x and y are positive real numbers, the same sort of reasoning shows that

$$f(x \cdot y) = f(x) \cdot f(y);$$

the general case is then a simple consequence. ∎

This theorem brings to an end our investigation of the real numbers, and resolves any doubts about them: There *is* a complete ordered field and, up to isomorphism, only one complete ordered field. It is an important part of a mathematical education to follow a construction of the real numbers in detail, but it is not necessary to refer ever again to this particular construction. It is utterly irrelevant that a real number happens to be a collection of rational numbers, and such a fact should never enter the proof of any important