Chapter 2
The Dedekind–Peano Axioms

Abstract This chapter develops the theory of natural numbers based on Dedekind–Peano Axioms, also known as *Peano Arithmetic*. The basic theory of *ratios* (positive rational numbers) is also developed. It concludes with a section on formal definition by primitive recursion.

2.1 Introduction

With the real numbers and their properties as a starting point, a large part of classical mathematics known as *analysis* can be developed deductively. This includes analytic geometry, calculus, the theory of sequences and series of real and complex numbers and functions, differential equations, and so on.

Mathematicians in the nineteenth century such as Weierstrass, Dedekind, and Cantor produced further analysis and construction of the real numbers which reduced everything down to the notion of natural numbers **N**.

It thus became clear that (with the aid of a certain amount of set theoretic and logical apparatus) the entire body of traditional pure mathematics can be constructed rigorously starting from the theory of natural numbers.[1]

Dedekind, in his profound work [11], and Peano, in his clear and highly modern axiomatic development [59], showed how, in turn, the entire theory of natural numbers could be derived from a few basic axioms and primitive notions. The resulting deductive theory is known today as *Peano Arithmetic*. This chapter develops parts of Peano Arithmetic dealing with properties of natural numbers, fractions, and ratios.

Throughout Part I, we assume that only the primitive Dedekind–Peano notions and axioms are given and that nothing else about any kinds of numbers or their

[1] "God created the natural numbers, all else is work of man," said Kronecker.

A. Dasgupta, *Set Theory: With an Introduction to Real Point Sets*,
DOI 10.1007/978-1-4614-8854-5_2,

properties are known. All familiar notions, like addition, will be formally introduced, and their properties will be derived from the axioms.

2.2 The Dedekind–Peano Axioms

The three primitive Dedekind–Peano notions are: "natural number," "1," and "successor," where the successor of a natural number n is denoted by $S(n)$.

The five axioms involving these primitive notions are the following.

The Dedekind-Peano Axioms. The natural numbers satisfy the axioms:

1. 1 is a natural number.
2. Every natural number n has a unique successor $S(n)$ which also is a natural number.
3. 1 is not the successor of any natural number.
4. No two distinct natural numbers have the same successor (i.e., for all natural numbers m, n, $S(m) = S(n)$ implies $m = n$).
5. Induction: If P is a property of natural numbers such that

   a. 1 has property P, and
   b. whenever a natural number has property P so does its successor,

   then all natural numbers have property P.

Mathematicians found it remarkable that all known properties of natural numbers can be derived from the Dedekind–Peano Axioms.

We define:

$$2 := S(1), \quad 3 := S(2), \quad 4 := S(3), \quad 5 := S(4), \quad 6 := S(5)$$
$$7 := S(6), \quad 8 := S(7), \quad 9 := S(8), \quad 10 := S(9), \quad \text{etc.},$$

adopting the usual decimal notation as a shorthand to replace long formal expressions of the form "$S(\cdots S(S(1))\cdots)$."

Notational convention. Natural numbers will be denoted by lowercase Roman letters such as $a, b, c, m, n, p, x, y, z$, without or with subscripts and/or superscripts. Quantifiers involving these variables will be assumed to range over natural numbers. Thus "for every m there exists n" stands for "for every natural number m there exists a natural number n."

Problem 52. $3 \neq 5$.

Problem 53. *No natural number is its own successor:* $S(n) \neq n$ *for any* n.

Problem 54 (Converse of Axiom 3). *Every natural number other than* 1 *is the successor of some natural number, i.e., if* $n \neq 1$ *then* $n = S(m)$ *for some* m.

At this point, expression such as $1 + 3$ or $(5 + 6) \cdot 7$ or statements like $3 < 5$ cannot be used; such expressions do not even make sense yet, since the operations $+$ and $\cdot$ and the relation $<$ have not been defined.

2.3 Addition, Order, and Multiplication

Addition

Definition 55. The *sum* $m + n$ of two natural numbers m and n is defined "by induction on n" as follows (for any m):

1. $m + 1 := S(m)$, and
2. $m + S(n) := S(m + n)$.

In other words, define $m + 1$ to be $S(m)$ (this is the case $n = 1$), and once $m + n$ is defined, define $m + S(n)$ to be $S(m + n)$. This defines the sum of any two numbers.[2]

Problem 56. $2 + 2 = 4$.

Problem 57. $n + 1 = 1 + n$ *for all* n.

Problem 58. *Addition (as defined above) is associative:*

$$m + (n + p) = (m + n) + p.$$

[Hint: Use induction on p*.]*

Problem 59. *Addition is commutative:* $m + n = n + m$*, for all* m *and* n.

Problem 60. *Cancellation law for addition: If* $m + p = n + p$*, then* $m = n$.

Order

Definition 61. Define $m < n$ if and only if $n = m + p$ for some p. Also, write $m > n$ for $n < m$.

[2]This can be done more rigorously using *the method of definition by primitive recursion* due to Dedekind, covered in the last section of this chapter.

The next few results can be proved without induction.

Problem 62. *$n < S(n)$ for all n.*

Problem 63. *$n \neq n$ for all n; that is, there are no n, p such that $n = n + p$.*

Problem 64. *For all n, either $1 < n$ or $1 = n$. Also, there is no n with $n < 1$.*

Thus 1 is "the least natural number" (less than all other natural numbers).

Problem 65. *$m < n$ if and only if either $S(m) < n$ or $S(m) = n$.*

Problem 66. *$m + k < n + k$ if and only if $m < n$.*

Recall from the previous chapter that a relation on a set is called a *linear order* if it is transitive, irreflexive, and connected on the set.

Theorem 67. *$<$, as defined above, is a linear order on the natural numbers.*

Proof. Transitivity of $<$ is an easy consequence of the associative property of addition: If $m < n$ and $n < p$, then $n = m + r$ and $p = n + s$ for some r, s. Hence $p = n + s = (m + r) + s = m + (r + s) = m + t$, where $t := r + s$, so $m < p$.

Irreflexivity is a direct consequence of Problem 63.

Finally, to show that $<$ is connected, define a property P as follows, writing "$P(k)$" as a shorthand for "k has property P":

$$P(k) \text{ is true if and only if for every } n, \text{ either } k < n, \text{ or } k = n, \text{ or } k > n.$$

We establish $<$ is connected on the set of natural numbers by showing that $P(k)$ is true for all k, which is proved by induction:

First, $P(1)$ is true, as 1 is less than all other natural numbers (Problem 64).

Next, suppose that $P(k)$ is true. Then for every n, either $k < n$ in which case $S(k) < n$ or $S(k) = n$, and so $P(S(k))$ is true; or $k = n$ in which case $S(k) > n$ so $P(S(k))$ is true; or $k > n$ in which case $S(k) > k > n$ by transitivity so again $P(S(k))$ is true. Thus $P(S(k))$ is true if $P(k)$ is true.

Therefore, by induction $P(k)$ is true for every natural number k. □

Theorem 68 (The Well-Ordering Property). *Every nonempty set A of natural numbers has a "least" element $m \in A$ such that for all $k \in A$ either $m < k$ or $m = k$.*

Proof. We prove the equivalent statement that if A has no least element then A must be empty. So suppose that A does not have a least element.

Let P be the property of being less than every member of A, that is, a natural number n has property P if and only if $n < k$ for all $k \in A$.

First, since 1 is less than all other natural numbers and A has no least element, so $1 \notin A$. Hence 1 has property P, again since 1 is less than all other natural numbers.

Next, suppose that n has P. Then $S(n) \notin A$, since otherwise $S(n)$ would be the least element of A: for any $k \in A$ we have $n < k$, so by Problem 65 $S(n) < k$ or

$S(n) = k$. Hence $S(n)$ has P: for any $k \in A$, $n < k$, so $S(n) < k$ or $S(n) = k$ (by Problem 65), but we cannot have $S(n) = k$ since $S(n) \notin A$, so $S(n) < k$. Thus we have shown that if n has P then $S(n)$ has P.

By induction, every natural number has property P, so A is empty. □

Remark. This theorem is actually equivalent to the general induction axiom. It is said to be phrased in the language of *second order arithmetic,* since, unlike most other results of this chapter, it talks about *all* sets of natural numbers.

Problem 69. *If $m > n$ there is a unique k such that $m = n + k$.*

Definition 70 (Subtraction). If $m > n$, define $m - n$ to be the unique k with $m = n + k$.

Multiplication

Definition 71. The *product* $m \cdot n$ of two natural numbers m and n is defined by induction on n as follows (for any m):

1. $m \cdot 1 := m$, and
2. $m \cdot S(n) := (m \cdot n) + m$.

We write mn for $m \cdot n$.

Problem 72. $2 \cdot 3 = 6$.

Problem 73. *Multiplication (as defined above) is distributive over addition:*

$$m(n + p) = mn + mp.$$

[Hint: Use induction on p.]

Problem 74. *Multiplication is associative:*

$$m(np) = (mn)p.$$

[Hint: Use induction on p.]

Problem 75. *Multiplication is commutative: $mn = nm$, for all m and n.*

Problem 76. *Cancellation law for multiplication: If $mp = np$ then $m = n$.*

Problem 77. *$mp < np$ if and only if $m < n$.*

Problem 78. *$m < 2m$.*

Notation. We write n^2 for nn.

Problem 79. *$m^2 < n^2$ if and only if $m < n$.*

Definition 80. Define n to be *even* if and only if $n = 2m$ for some m. Define n to be *odd* if and only if $n = 1$ or $n = S(2m)$ for some m.

Problem 81. *For every n, either n is odd or n is even but not both. Moreover, n is even if and only if $S(n)$ is odd, and n is odd if and only if $S(n)$ is even.*

Problem 82. *n is even if and only if n^2 is even, and n is odd if and only if n^2 is odd.*

Theorem 83. *There do not exist m, n such that $m^2 = 2n^2$.*

Proof. Let $A := \{m \mid m^2 = 2n^2 \text{ for some } n\}$. The result will follow if we show that A is empty, so we assume A is nonempty and derive a contradiction. By the Well-Ordering Property, fix a least member $m \in A$. Then we can fix p such that $m^2 = 2p^2$. Then $p^2 < m^2$ (Problem 78), hence by Problem 79, $p < m$. Also, since m^2 is even, so m is even by the last result. Hence $m = 2q$ for some q. So $2q \cdot 2q = 2p^2$, or $p^2 = 2q^2$. So $p \in A$. But this is impossible since $p < m$ and m is the least member of A. □

Remark. In this proof, we had to avoid number theoretic properties such as reduced fractions, gcds, relatively prime numbers, etc., which are not available to us at this point.

2.4 Fractions and Ratios

Definition 84. A *fraction* is an ordered pair of natural numbers $\langle m, n\rangle$.

Thus $\mathbf{N} \times \mathbf{N}$ is the set of all fractions. For a fraction $\langle m, n\rangle$, m and n are called the *numerator* and *denominator*, respectively.

Definition 85 (Equivalent Fractions). We say that the fractions $\langle m, n\rangle$ and $\langle p, q\rangle$ are *equivalent,* and write $\langle m, n\rangle \sim \langle p, q\rangle$ if and only if $mq = np$.

Problem 86. *$\langle mk, nk\rangle \sim \langle m, n\rangle$. for all m, n, k.*

Problem 87. *$\sim$ is an equivalence relation on the set $\mathbf{N} \times \mathbf{N}$ of all fractions, and so $\mathbf{N} \times \mathbf{N}$ is partitioned into $\sim$-equivalence classes.*

Problem 88. *Find the equivalence classes $[\langle 1, 1\rangle]$, $[\langle 3, 1\rangle]$, and $[\langle 2, 4\rangle]$.*

Definition 89. $\dfrac{m}{n}$ denotes the $\sim$-equivalence class of the fraction $\langle m, n\rangle$:

$$\frac{m}{n} := [\langle m, n\rangle] = \{\langle p, q\rangle \mid \langle p, q\rangle \sim \langle m, n\rangle\}.$$

Such an equivalence class of fractions is called a *ratio* (or *positive rational*):

$$\rho \text{ is a } \textit{ratio} \text{ if and only if } \rho = \frac{m}{n} \text{ for some } m, n.$$

Thus the collection of all ratios is identical to the partition determined by the equivalence relation $\sim$ (equivalence of fractions).

Ratios will be denoted by lowercase Greek letters such as $\rho, \sigma, \tau, \alpha, \beta, \gamma, \xi, \eta$, and ζ, and quantifiers involving these variables will be assumed to range over ratios. Thus "for every ρ there exists σ" really means "for every ratio ρ there exists a ratio σ."

Note. The fraction $\langle m, n\rangle$ should be distinguished from the ratio $\frac{m}{n}$. The fraction $\langle m, n\rangle$ is simply an ordered pair, and therefore is a *member* of $\mathbf{N} \times \mathbf{N}$. The ratio $\frac{m}{n}$ is the set of all fractions equivalent to the fraction $\langle m, n\rangle$, so $\frac{m}{n}$ is an entire set of fractions, and thus is a *subset* of $\mathbf{N} \times \mathbf{N}$.

Problem 90. *Explain what is wrong with the claim:*

$$\frac{n}{1} = n.$$

Problem 91. $\rho = \dfrac{m}{n}$ *if and only if* $\langle m, n\rangle \in \rho$.

Problem 92. $\dfrac{m}{n} = \dfrac{p}{q}$ *if and only if* $\langle m, n\rangle \sim \langle p, q\rangle$.

2.5 Order, Addition, and Multiplication of Fractions and Ratios

Order for Fractions and Ratios

To "compare" two fractions $\langle m, n\rangle$ and $\langle p, q\rangle$, we can (by Problem 86) find corresponding equivalent fractions $\langle mq, nq\rangle \sim \langle m, n\rangle$ and $\langle np, nq\rangle \sim \langle p, q\rangle$ with a "common denominator" nq, and compare just the numerators.

Definition 93. Define $\langle m, n\rangle < \langle p, q\rangle$ if and only if $mq < np$.

Problem 94. *If* $\langle m, n\rangle < \langle p, q\rangle$ *and* $\langle p, q\rangle < \langle r, s\rangle$, *then* $\langle m, n\rangle < \langle r, s\rangle$.

Problem 95. *Given fractions* $\langle m, n\rangle$ *and* $\langle p, q\rangle$, *exactly one of the conditions*

$$\langle m, n\rangle < \langle p, q\rangle, \qquad \langle m, n\rangle \sim \langle p, q\rangle, \qquad \langle m, n\rangle > \langle p, q\rangle,$$

is true.

Problem 96. *If* $\langle m, n\rangle \sim \langle m', n'\rangle$, $\langle p, q\rangle \sim \langle p', q'\rangle$, *and* $\langle m, n\rangle < \langle p, q\rangle$, *then* $\langle m', n'\rangle < \langle p', q'\rangle$.

Thus if a fraction in one class is less than a fraction in another class, then the same is true for all pairs of representatives from the two classes. Hence the following is well defined:

Definition 97. Define $\rho < \sigma$ if and only if there are m, n, p, q with $\rho = \dfrac{m}{n}$, $\sigma = \dfrac{p}{q}$, and $\langle m, n\rangle < \langle p, q\rangle$.

Problem 98. *$<$, as defined in the last definition for ratios, is a linear order on the set of ratios (i.e., transitive, irreflexive, and connected).*

Addition and Multiplication of Fractions and Ratios

To add two fractions $\langle m, n\rangle$ and $\langle p, q\rangle$, we can as before take the corresponding equivalent fractions $\langle mq, nq\rangle \sim \langle m, n\rangle$ and $\langle np, nq\rangle \sim \langle p, q\rangle$ with the common denominator nq, and then add the numerators. For multiplication, the numerators, and separately the denominators, are simply multiplied together.

Definition 99 (Addition of Fractions). The sum of two fractions is defined as

$$\langle m, n\rangle + \langle p, q\rangle \;:=\; \langle mq + np, nq\rangle\,.$$

Problem 100. *If $\langle m, n\rangle \sim \langle m', n'\rangle$ and $\langle p, q\rangle \sim \langle p', q'\rangle$, then*

$$\langle m, n\rangle + \langle p, q\rangle \;\sim\; \langle m', n'\rangle + \langle p', q'\rangle\,.$$

Thus the class of the sum depends only on the classes to which the summands belong, making the following definition for addition of ratios *well defined*:

Definition 101 (Addition of Ratios). The sum of two ratios $\rho = \frac{m}{n}$ and $\sigma = \frac{p}{q}$ is defined as

$$\rho + \sigma = \frac{m}{n} + \frac{p}{q} \;:=\; \frac{mq + np}{nq}.$$

Definition 102 (Multiplication of Fractions). The product of two fractions is defined as

$$\langle m, n\rangle \cdot \langle p, q\rangle \;:=\; \langle mp, nq\rangle\,.$$

Problem 103. *If $\langle m, n\rangle \sim \langle m', n'\rangle$ and $\langle p, q\rangle \sim \langle p', q'\rangle$, then*

$$\langle m, n\rangle \cdot \langle p, q\rangle \;\sim\; \langle m', n'\rangle \cdot \langle p', q'\rangle\,.$$

Thus the class of the product depends only on the classes to which the factors belong. Hence the following is well defined.

Definition 104 (Multiplication of Ratios). The product of two ratios $\rho = \frac{m}{n}$ and $\sigma = \frac{p}{q}$, denoted by $\rho \cdot \sigma$ or $\rho\sigma$, is defined as

$$\rho \cdot \sigma = \frac{m}{n} \cdot \frac{p}{q} := \frac{mp}{nq}.$$

2.6 Properties of Addition and Multiplication of Ratios

Problem 105. $\frac{m}{p} + \frac{n}{p} = \frac{m+n}{p}$, *and* $\frac{m}{p} < \frac{n}{p}$ *if and only if* $m < n$.

Problem 106 (Commutative Laws). $\rho + \sigma = \sigma + \rho$, *and* $\rho\sigma = \sigma\rho$.

Problem 107 (Associative Laws). $(\rho+\sigma)+\tau = \rho+(\sigma+\tau)$, *and* $(\rho\sigma)\tau = \rho(\sigma\tau)$.

Problem 108 (Cancellation Laws). *If* $\rho + \tau = \sigma + \tau$ *or if* $\rho\tau = \sigma\tau$, *then* $\rho = \sigma$.

Problem 109 (Distributive Law). $\rho(\sigma + \tau) = \rho\sigma + \rho\tau$.

Problem 110. $\rho < \rho + \xi$.

Problem 111. *If* $\rho < \sigma$, *then there is a unique* ξ *such that* $\rho + \xi = \sigma$.

Corollary 112. $\rho < \sigma$ *if and only if* $\sigma = \rho + \xi$ *for some (unique)* ξ.

Definition 113 (Subtraction). If $\rho < \sigma$, define $\sigma - \rho$ to be the unique ξ with $\rho + \xi = \sigma$.

Problem 114. $\rho < \sigma$ *if and only if* $\rho + \tau < \sigma + \tau$. *if and only if* $\rho\tau < \sigma\tau$.

Problem 115 (Identity and Reciprocal). $\rho \cdot \frac{1}{1} = \rho$ *and* $\frac{m}{n} \cdot \frac{n}{m} = \frac{1}{1}$.

Problem 116. *For any* ρ, σ *there is a unique* ξ *such that* $\xi \cdot \rho = \sigma$.

Definition 117 (Division). σ/ρ denotes the unique ξ such that $\xi \cdot \rho = \sigma$.

Corollary 118. $(\sigma/\rho)\rho = \sigma$.

Problem 119. *If* $\rho_1 < \sigma_1$ *and* $\rho_2 < \sigma_2$, *then* $\rho_1 + \rho_2 < \sigma_1 + \sigma_2$ *and* $\rho_1\rho_2 < \sigma_1\sigma_2$.

Problem 120 (Difference of Squares). *If* $\alpha < \beta$ *so that* $\beta - \alpha$ *is defined, then* $\beta^2 = \alpha^2 + (\beta - \alpha)(\beta + \alpha)$, *where* σ^2 *stands for* $\sigma \cdot \sigma$.

2.7 Integral Ratios and the Embedding of the Natural Numbers

Definition 121. A ratio ρ is said to be *integral* if $\rho = \frac{m}{1}$ for some m.

Problem 122. ρ *is integral if and only if* $\langle m, 1\rangle \in \rho$ *for some* m.

Problem 123. *$\frac{m}{n}$ is integral if and only if $m = nk$ for some k.*

We will now see that the integral ratios form a subset of the ratios which is structurally identical, or "isomorphic," to the natural numbers in the following sense: There is a one-to-one correspondence between the natural numbers and the integral ratios which preserves the operations of addition and multiplication as well as the order relation (Problem 125). Such a bijection is called an *isomorphism.*

Problem 124. *$\frac{m}{1} = \frac{n}{1}$ if and only if $m = n$. Thus the mapping $n \mapsto \frac{n}{1}$ is a bijection from the set of natural numbers onto the set of integral ratios.*

Problem 125 (Isomorphism of Natural Numbers with Integral Ratios). *For any m, n:*

$$\frac{m}{1} + \frac{n}{1} = \frac{m+n}{1}, \quad \frac{m}{1} \cdot \frac{n}{1} = \frac{m \cdot n}{1}, \quad \text{and} \quad \frac{m}{1} < \frac{n}{1} \text{ if and only if } m < n.$$

Problem 126. *The integral ratios satisfy the five Dedekind–Peano axioms when*

- *1 is interpreted as $\frac{1}{1}$, and*
- *$S\left(\frac{n}{1}\right)$ is interpreted as $\frac{S(n)}{1}$.*

At this point, the natural numbers and the integral ratios become interchangeable since all the properties of the natural numbers listed in the initial sections are possessed by the integral ratios.

Therefore, we throw away the natural numbers[3] and use the corresponding integral ratios in their place. The old natural numbers are not used directly anymore, and so we now deal with only one type of numbers, namely the ratios, which include the "new natural numbers" (really the integral ratios) as a subset.

This process is known as *embedding the natural numbers into the ratios.*

Definition 127 (New Meaning for the Natural Number Symbols). With the old natural numbers thrown out, the integral ratio $\frac{n}{1}$ will now be denoted simply by the letter n and called *the natural number n* (similarly for other lowercase Roman letters). Not only lowercase Roman letters now denote the new natural numbers (integral ratios) by default, but also any other symbol previously used for a natural number will now denote the corresponding new natural number.

For example, the symbol 1 now stands for the integral ratio $\frac{1}{1}$, the symbol 2 for the integral ratio $\frac{2}{1}$, etc. The resulting notational ambiguity is not a real problem, as the intended interpretation can be determined from context.

[3] Phrase of Edmund Landau [47].

This allows us to mix symbols that were previously assigned to different types, and "$n + \rho$" and "$n \cdot \rho$" now become valid terms. But we remind the reader again that *lowercase Roman letters will denote the new natural numbers (really the integral ratios), and lowercase Greek letters will continue to denote arbitrary ratios.* Fractions will no longer be used.

Problem 128. $\dfrac{m}{n} = m/n$. *Also, since* $\sigma \cdot 1 = \sigma = 1 \cdot \sigma$, *so* $\sigma/1 = \sigma$ *and* $\sigma/\sigma = 1$. *Finally,* $\sigma(1/\sigma) = 1$.

2.8 The Archimedean and Fineness Properties

Problem 129 (The Archimedean Property for Ratios). *For any* ρ, σ *there is* n *such that* $n\rho > \sigma$.

Problem 130. *For any* ρ, *there exists* $\sigma > \rho$, *and also there exists* $\tau < \rho$.

Problem 131 (Density). *If* $\rho < \sigma$, *then there is* τ *such that:*

$$\rho < \tau < \sigma.$$

The last two results express the fact that *the ratios form a dense linear order without end points.*

Definition 132. We say that the pair L, U is a *Dedekind partition* of the ratios if L and U are nonempty sets forming a partition of the ratios such that every ratio in L is smaller than every ratio in U, that is, $\rho < \sigma$ for all $\rho \in L$ and $\sigma \in U$.

For example, if $L := \{\rho \mid \rho < 1\}$ and $U := \{\rho \mid \rho \geq 1\}$, then L, U forms a Dedekind partition of the ratios.

Problem 133. *If* L, U *is a Dedekind partition of the ratios, then* L *is "downward closed under* $<$*" meaning that if* $\rho \in L$ *and* $\rho' < \rho$ *then* $\rho' \in L$, *and similarly* U *is upward closed under* $>$.

The following property, which we call the *Fineness Property* for ratios, is closely related to the Archimedean property.[4] It will be used in the next section and in the next chapter when we study Dedekind partitions in detail.

Theorem 134 (Fineness Property for Ratios). *If* L, U *is a Dedekind partition of the ratios, then for any* ϵ *there are* $\rho \in L$ *and* $\sigma \in U$ *such that* $\sigma - \rho < \epsilon$, *that is,* $\sigma < \rho + \epsilon$.

[4]The notion can be defined for (the positive elements of) any ordered field, where it will hold if and only if the field is Archimedean. A Dedekind partition L, U satisfying the condition of Theorem 134 is sometimes called a *Scott cut.*

Remark. Like Theorem 68, this is a result of *second order arithmetic*, since, unlike most other results of this chapter, it quantifies over *sets* of ratios.

Proof. Let ϵ be given. Fix $\alpha \in L$ and $\beta \in U$. By the Archimedean property fix a natural number n with $n > 1/\alpha$ and also $n > 1/\epsilon$. Then $1/n < \alpha$, and so $1/n \in L$. Also $1/n < \epsilon$. There is k such that $k/n > \beta$ (by the Archimedean property again), and so there is k with $k/n \in U$, hence by the Well-Ordering property we can fix the least natural number m such that $m/n \in U$. Then $m \neq 1$ since $1/n \notin U$. Hence $m = p + 1$ for some p. Put $\rho = p/n$ and $\sigma = m/n$. Then $\sigma \in U$ and since m is the least natural number for which $m/n \in U$, so $\rho = p/n \in L$. Finally, $\sigma = \rho + 1/n < \rho + \epsilon$. □

2.9 Irrationality of $\sqrt{2}$ and Density of Square Ratios

Definition 135. We write ρ^2 for $\rho\rho$. A ratio σ is said to be a *square ratio* if $\sigma = \rho^2$ for some ρ. A ratio σ is said to be a *nonsquare ratio* if it is not a square ratio, i.e., if there is no ρ such that $\sigma = \rho^2$.

For example, 1 is a square ratio since $1 = 1^2$, but 2 is a nonsquare ratio by Theorem 83:

Problem 136. *There is no ρ such that $\rho^2 = 2$.*

Problem 137. *$\rho < \sigma$ if and only if $\rho^2 < \sigma^2$.*

The following says that the square ratios are "dense" in the set of all ratios:

Theorem 138 (Density of Square Ratios). *Given $\rho < \sigma$, there is β such that $\rho < \beta^2 < \sigma$.*

Proof. Let $\rho < \sigma$, and put $L := \{\gamma \mid \gamma^2 \leq \rho\}$ and $U := \{\gamma \mid \gamma^2 > \rho\}$. Then L, U is a Dedekind partition by Problem 137, so by the fineness property we can fix $\alpha \in L$ and $\beta \in U$ with $\beta - \alpha < (\sigma - \rho)/(2(\sigma + 1))$. We can assume $\beta < \sigma + 1$ (since otherwise we could have replaced β by $\sigma + 1/2$), and so $\beta + \alpha < 2\beta < 2(\sigma + 1)$. Hence by Problem 120:

$$\rho < \beta^2 = \alpha^2 + (\beta - \alpha)(\beta + \alpha) < \rho + (\beta - \alpha)(2(\sigma + 1)) < \rho + (\sigma - \rho) = \sigma.$$

□

Corollary 139. *If $\rho^2 < 2$, then there is $\sigma > \rho$ with $\rho^2 < \sigma^2 < 2$. Similarly, if $\rho^2 > 2$, then there is $\sigma < \rho$ with $\rho^2 > \sigma^2 > 2$.*

Corollary 140. *$L := \{\rho \mid \rho^2 < 2\}$ and $U := \{\rho \mid \rho^2 > 2\}$ form a Dedekind partition of the ratios with L having no largest element and U having no smallest element.*

In the last corollaries, we could obviously replace 2 by any nonsquare ratio.

Like the square ratios, the nonsquare ratios are also dense in the set of all ratios:

Corollary 141. *Given $\rho < \sigma$, there is some nonsquare ratio τ such that $\rho < \tau < \sigma$.*

Proof. Let $\rho < \sigma$. Then $\rho/2 < \sigma/2$, so $\rho/2 < \beta^2 < \sigma/2$, or $\rho < 2\beta^2 < \sigma$ for some β. But $2\beta^2$ is a nonsquare ratio, as otherwise $(2\beta^2)/\beta^2 = 2$ would be a square ratio. □

Remark. Although $\sqrt{2}$ does not exist (as a ratio), we do have arbitrarily close approximations to it both from below and from above: Given any ϵ, we can apply the fineness property to the Dedekind partition $L := \{\rho \mid \rho^2 < 2\}$ and $U := \{\rho \mid \rho^2 > 2\}$ to get $\rho \in L$ and $\sigma \in U$ with $\sigma - \rho < \epsilon$. Since we expect $\sqrt{2}$ (whatever it may be) to lie between ρ and σ, we can regard ρ and σ as approximations differing from the target $\sqrt{2}$ by an amount less than ϵ.

Problems Using Concepts from Abstract Algebra

The following problems are meant for students with prior exposure to abstract algebra.

Problem 142. *The ratios form an abelian group under multiplication.*

Problem 143. *Generalize the fineness property for the positive elements of an ordered field. Then show that the positive elements of an ordered field has the fineness property if and only if the field is Archimedean.*

Our method of going from the natural numbers to the ratios is a basic method in algebra in which one embeds a given commutative cancellative semigroup A into a group constructed from a pairs of elements of A and forming a quotient. The semigroup we started with was $\mathbf{N}$ with the operation of multiplication, but addition could have been incorporated as well.

Problem 144. *Construct the integral domain $\mathbf{Z}$ of signed integers from $\mathbf{N}\times\mathbf{N}$, where $\langle m, n\rangle$ is identified with $\langle p, q\rangle$ if and only if $m + q = n + p$, by defining addition and multiplication appropriately.*

The following result of Dedekind shows that the Dedekind–Peano axioms characterize the natural numbers with the successor function up to isomorphism:

Problem 145 (Dedekind). *If $\overline{S}\colon \overline{N} \to \overline{N}$ with $\overline{1} \in \overline{N}$, $\underline{S}\colon \underline{N} \to \underline{N}$ with $\underline{1} \in \underline{N}$, and if both structures satisfy the Dedekind–Peano axioms, then there is a unique bijection h from $\overline{N}$ onto $\underline{N}$ which preserves 1 and the successor functions, that is such that $h(\overline{1}) = \underline{1}$ and $h(\overline{S}(n)) = \underline{S}(h(n))$ for all $n \in \overline{N}$.*

2.10 Recursive Definitions*

Recall that we had "defined" addition of natural numbers by the following *recursion equations*:

$$m + 1 := S(m), \qquad \text{and} \qquad m + S(n) := S(m + n).$$

But this is not an explicit definition! We took it for granted (as was done in the work of Peano) that a two-place function $+$ (the mapping $(m, n) \mapsto m + n$) satisfying the above equations exists, without giving any rigorous justification for its existence. Similarly, multiplication of natural numbers was "defined" by recursion equations without proper justification.

Dedekind introduced a general method, known as *primitive recursion*, which provides such justification. It assures the *existence and uniqueness* of functions which are defined implicitly using recursion equations having forms similar to the ones for addition and multiplication.

We will formulate and prove a general version of Dedekind's principle of recursive definition, from which the existence and uniqueness for the addition and multiplication functions can be immediately derived.

Principles of Recursive Definition

The following *Basic Principle of Recursive Definition* is perhaps the simplest yet very useful result for defining functions recursively.

Theorem 146 (Basic Principle of Recursive Definition). *If Y is a set, $a \in Y$, and $h: Y \to Y$, then there is a unique $f: \mathbf{N} \to Y$ such that*

$$f(1) = a, \qquad \textit{and} \qquad f(n + 1) = h(f(n)) \ \textit{for all } n \in \mathbf{N}.$$

Informally, this says that given $a \in Y$ and $h: Y \to Y$, we can form the infinite sequence $\langle a, h(a), h(h(a)), \dots \rangle$.

Proof. First note that the uniqueness of the function f can be established by an easy and routine induction, so let us prove existence.

Let $I_n := \{1, 2, \dots, n\} = \{k \in \mathbf{N} \mid 1 \leq k \leq n\}$ denote the set of first n natural numbers. The proof uses *functions $u: I_n \to Y$ having domain I_n,* i.e., finite sequences from Y of length n (with varying n).

Let us say that a function *u is partially h-recursive with domain I_n* if $u: I_n \to Y$, $u(1) = a$, and $u(k + 1) = h(u(k))$ for all k with $1 \leq k < n$.

We first prove by induction that for every $n \in \mathbf{N}$ there is a unique partially h-recursive u with domain I_n.

Basis step ($n = 1$): Let $v: \{1\} \to Y$ be defined by setting $v(1) = a$. Then v is partially h-recursive with domain I_1. Moreover, if $u, u': I_1 \to Y$ are partially h-recursive functions with domain I_1, then $u(1) = a = u'(1)$, so $u = u'$ since 1 is the only element in their domain $I_1 = \{1\}$. So there is a unique partially h-recursive v with domain I_1, establishing the basis step.

Induction step: Suppose that $n \in \mathbf{N}$ is such that there is a unique partially h-recursive v with domain I_n (induction hypothesis). We fix this v for the rest of this step, and define $w: I_{n+1} \to Y$ by setting $w(k) := v(k)$ for $k \leq n$ and $w(k) := h(v(n))$ if $k = n + 1$. Then w is easily seen to be partially h-recursive with domain I_{n+1}. Moreover, if $u, u': I_{n+1} \to Y$ are partially h-recursive with domain I_{n+1}, then the restrictions $u \restriction_{I_n}$ and $u' \restriction_{I_n}$ are partially h-recursive with domain I_n, so they must be identical by induction hypothesis, i.e., $u(k) = u'(k)$ for $1 \leq k \leq n$. In particular, $u(n) = u'(n)$, so $u(n + 1) = h(u(n)) = h(u'(n)) = u'(n + 1)$, which gives $u = u'$. Thus there is a unique partially h-recursive w with domain I_{n+1}, which finishes the induction step.

Thus for each n there is a unique partially h-recursive function with domain I_n; let us denote this function by u_n.

Now define $f: \mathbf{N} \to Y$ by setting:

$$f(n) := u_n(n).$$

First, $f(1) = a$ since $u_1(1) = a$. Next, the restriction of u_{n+1} to I_n equals u_n (by uniqueness, since the restriction is partially h-recursive), so $u_{n+1}(n) = u_n(n)$. Hence $f(n + 1) = u_{n+1}(n + 1) = h(u_{n+1}(n)) = h(u_n(n)) = h(f(n))$. Thus f satisfies the recursion equations of the theorem. □

To handle functions of multiple variables, the following theorem is used.

Theorem 147 (General Principle of Recursive Definition). *For any $g: X \to Y$ and $h: X \times \mathbf{N} \times Y \to Y$, there is a unique function $f: X \times \mathbf{N} \to Y$ such that for all $x \in X$ and $n \in \mathbf{N}$:*

$$f(x, 1) = g(x) \quad \text{and} \quad f(x, n + 1) = h(x, n, f(x, n)).$$

Here f is being defined by recursion on the second variable n, that is, n is the *variable of recursion* ranging over $\mathbf{N}$, while x is a *parameter* ranging over the set X. This is the most general form of recursive definition, where both the parameters (in X) and the values (in Y) come from arbitrary sets.

Proof. The proof is essentially the same as that of Theorem 146, since the additional parameter does not play any significant role in the recursion. The details are left as an exercise for the reader. □

Theorem 148 (Course of Values Recursion). *Let Y be a nonempty set and Y^* denote the set of all finite sequences (strings) of elements from Y. Given any $G: Y^* \to Y$ there is a unique $f: \mathbf{N} \to Y$ such that*

$$f(n) = G(\langle f(k) \mid k < n\rangle) \text{ for all } n \in \mathbf{N}.$$

Denoting the empty string by ε, this means that $f(1) = G(\varepsilon)$, $f(2) = G(\langle f(1)\rangle)$, $f(3) = G(\langle f(1), f(2)\rangle)$, etc.

Proof. Let $h_G: Y^* \to Y^*$ be the function defined by

$$h_G(u) := u^\frown G(u), \quad \text{i.e.} \quad h_G(\langle u_1, \ldots, u_n\rangle) := \langle u_1, \ldots, u_n, G(u)\rangle\,.$$

Here $u^\frown y = u * \langle y\rangle$ denotes the string obtained from the string u by appending the element $y \in Y$, so that $\text{len}(u^\frown y) = \text{len}(u) + 1$. The Basic Principle of Recursive Definition (Theorem 146) gives a unique function $\phi: \mathbf{N} \to Y^*$ with

$$\phi(1) = h_G(\varepsilon), \qquad \text{and} \qquad \phi(n+1) = h_G(\phi(n)) \quad \text{for all } n \in \mathbf{N}.$$

Now note that $\phi(n)$ is a finite sequence of length n for every n, and put $f(n) := \phi(n)(n) =$ the last coordinate of the finite sequence $\phi(n)$. □

The form of recursion in the above theorem generalizes to transfinite ordinals, where it is called *transfinite recursion* (see Theorem 622 and Theorem 650).

Primitive Recursion

We start with a special case, which is an immediate corollary of Theorem 147.

Theorem 149 (Primitive Recursion for Two-Place Functions). *Given a one-variable function $g: \mathbf{N} \to \mathbf{N}$ and a three-variable function $h: \mathbf{N}^3 \to \mathbf{N}$, there is a unique two variable function $f: \mathbf{N} \to \mathbf{N}$ such that for all $m, n \in \mathbf{N}$:*

$$f(m, 1) = g(m), \quad \text{and} \quad f(m, S(n)) = h(m, n, f(m, n)).$$

The result of this theorem is often expressed by saying that *the function f is obtained from the function g and h by primitive recursion*.

Proof. This is simply Theorem 147 with $X = Y = \mathbf{N}$. □

We can now give a full justification for our original recursive definition of addition, by showing that the two-place function $+$ can be obtained from the successor function by primitive recursion as follows:

Let $g = S$ be the successor function, and let h be the function defined by $h(m, n, p) = S(p)$. Applying the last theorem with these g and h gives a two-place function f satisfying

$$f(m, 1) = S(m), \qquad \text{and} \qquad f(m, S(n)) = S(f(m, n)).$$

But these are the same as our original recursion equations for defining addition, as is easily verified by writing $m + n$ for $f(m, n)$:

$$m + 1 = S(m), \qquad \text{and} \qquad m + S(n) = S(m + n).$$

Once we have justified the addition function, we can use it to obtain the multiplication function ($\langle m, n\rangle \mapsto mn$) by primitive recursion.

Problem 150. *Prove that the multiplication function can be obtained from the identity function and the addition function using primitive recursion, verifying that it gives our original recursion equations for defining multiplication.*

The most general version of the primitive recursion principle, which is again an immediate corollary of Theorem 147, is formulated as follows:

Theorem 151 (The General Principle of Primitive Recursion). *Given a $(k-1)$-place function g and a $(k+1)$-place function h on $\mathbf{N}$, there is a unique k-place function f on $\mathbf{N}$ such that for all $x_1, x_2, \ldots, x_k \in \mathbf{N}$:*

$$f(x_1, \ldots, x_{k-1}, 1) = g(x_1, \ldots, x_{k-1}), \quad \textit{and}$$
$$f(x_1, \ldots, x_{k-1}, S(x_k)) = h(x_1, \ldots, x_k, f(x_1, \ldots, x_k)).$$

Proof. This is Theorem 147 with $X = \mathbf{N}^{k-1}$ and $Y = \mathbf{N}$. □

As before, the function f in the above theorem is said to be *defined by primitive recursion from g and h*.

After obtaining the addition and multiplication functions, one can keep applying primitive recursion repeatedly to define more and more functions on $\mathbf{N}$. Essentially all commonly used functions, such as exponentiation, the factorial function, the gcd function, and so on, can be obtained via primitive recursion.

Problem 152. *Define the factorial function (one-place) as well as the exponentiation function (two-place) from the multiplication function using primitive recursion.*

Problem 153. *What familiar single-variable function is defined using the following primitive recursion equations?*

$$f(1) = 1 \quad \textit{and} \quad f(S(m)) = h(m, f(m)), \qquad \textit{where } h(m, n) := nS(m).$$

Remark. Principles of primitive recursion, such as Theorem 151, are results of *second order arithmetic* which involve quantification over *functions* of natural numbers: Functions are defined *implicitly* by assertions of the form "there is a unique function satisfying such and such recursion equations." This is unavoidable in the Dedekind–Peano system $\langle \mathbf{N}, 1, S\rangle$. However, if $+$ and $\cdot$ are also added as primitives to obtain the extended system $\langle \mathbf{N}, 1, S, +, \cdot\rangle$, then primitive recursion is no longer necessary and functions such as exponentiation can be explicitly defined.

The reason for this is that $+$ and $\cdot$ have sufficient power to express the notion of *finite sequences* (represented in a coded form as natural numbers), and so one can essentially replicate the process given in the proof of Theorem 146 to produce explicit definitions.

http://www.springer.com/978-1-4614-8853-8

Set Theory
With an Introduction to Real Point Sets
Dasgupta, A.
2014, XV, 444 p. 17 illus., Hardcover
ISBN: 978-1-4614-8853-8
A product of Birkhäuser Basel